IJARST

International Journal For Advanced Research In Science & Technology

A peer reviewed international journal www.ijarst.in

ISSN: 2457-0362

ANALYSIS ON PRIVACY-PRESERVING ENHANCEMENT ON CLOUD DATA STORAGE MANAGEMENT

[1]VANGALA KALYANI

Facaulty, at JNTUH Univercity

Email Id: echo.kalyani@gmail.com

ABSTRACT

Nowadays, more and more data are being created and analysed. Users were able to save their data in the cloud and access it whenever they needed to owe to Cloud Storage Service (CSS). Due to the possibility that sensitive data will be shared with unauthorised parties, outsourcing to the cloud raises serious privacy concerns. That's why encryption is a must before sending data off-site. Traditional key search-oriented encryption methods, on the other hand, can't handle basic activities or direct searches on encrypted data. As a result, there is a pressing need for a more robust and safe method of storing data on the cloud, from which it can be quickly retrieved as needed. The study's goal was to develop security for retrieving data from the cloud. To address this pressing issue, we have provided a comprehensive overview of the most up-to-date methods and strategies in use today. We divide the methods of protecting privacy into four groups: those that rely on cryptography, those that rely on probability, those that rely on anonymization, and those that rely on rankings. In addition, a taxonomy of methods for protecting sensitive administrative information has been developed by our team. In addition, we provided a thorough evaluation of the privacy-protecting methods from the perspective of meeting privacy-protecting standards. Therefore, it is extremely desirable to provide methods for deploying effective auditing and accountability procedures that monitor the usage of data records in an anonymous fashion while also tracking the provenance to protect the data's privacy.

Key words: Cloud computing, Data storage, Privacy, Data analysis.

1. INTRODUCTION

As the number of people using the cloud increases at an exponential rate, so do their requirements and their need for new and innovative cloud computing techniques. This is where cloud computing's emphasis on shared resources comes in handy; it's an essential component of any Internet of Things setup. When it comes to data and resources, the cloud is agnostic in terms of location, allowing users to access them from anywhere in the world using an internet-connected device. Devices connected via the Internet of Things have the same global access to information and resources. IoT infrastructure requires standard cloud services such as scalability, availability, portability, and the ability to pool resources on-demand. In addition to improving service reliability through resource pooling, the elastic and on-demand features also allow for greater service efficiency and adaptability. All of these arguments suggest that the Internet of Things and Cloud computing standards should be integrated.

If you're concerned about the safety of your data on the cloud, you should look at cloud data security, a crucial subfield of cloud computing. In this respect, firewalls and VPNs play an important role in protecting cloud users' anonymity and data. The highly private information is accessible to the external cloud because resource pooling is a need in the cloud.

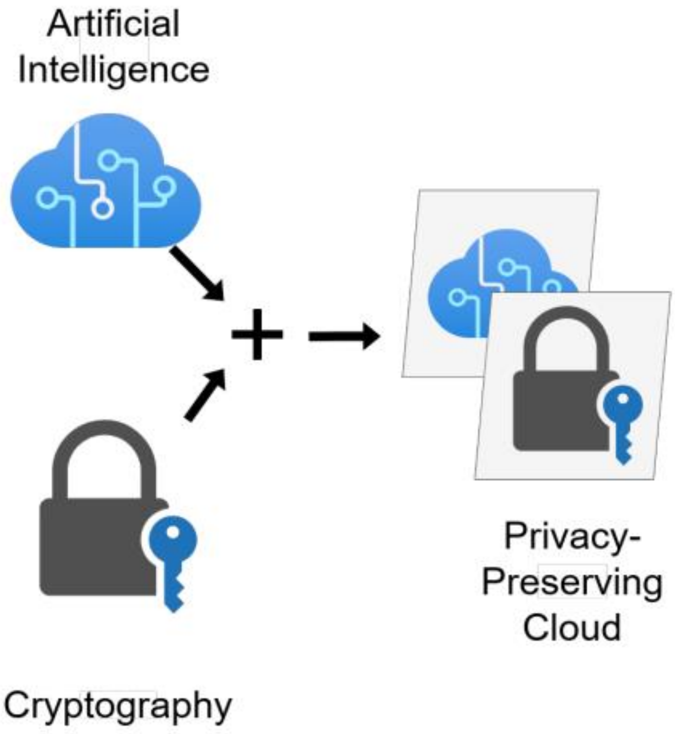

Fig. 1. Designing for Privacy in Cloud Computing Environments.

Data saved in the cloud is only accessible by those who have been allowed access, which is why privacy is so crucial in this context. The confidentiality of information kept in the cloud cannot be ensured without adequate data privacy protections. It is shown in Figure 1 how a Privacy Preserving Cloud system incorporates AI and Cryptography principles to ensure user confidentiality at every level of the system.

Numerous variations on the cloud concept are realised through various service providers' offerings. Numerous cloud computing systems can be accessed from cloud service providers including Google, Microsoft, and Amazon. Google Apps Engine, Microsoft Azure, and the Amazon Cloud are three of the most well-known examples. Additionally, ACME corporation has integrated VMware based v-Cloud to allow for many organisations to share computing resources. The cloud can be broken down into public clouds, private clouds, and hybrid clouds, each with their own set of advantages and disadvantages. Hybrid clouds combine characteristics of both public and private clouds, while public clouds belong to and are used by the public and private clouds belong to and are used only by a single organisation. Massive cloud service providers like Google, Amazon, and IBM provide the vast majority of the market's current cloud services. Unlike public clouds, in which anyone can utilise the provider's services, private clouds limit access to only those who have been granted permission. The hybrid cloud incorporates both the public and private cloud models into a single solution, making it the ideal solution for businesses with a need for both types of clouds.

2. LITERATURE REVIEW

Cloud service providers have a responsibility to address user concerns about data security and privacy [1]. A look back at some prior research and results is shown here. The absence of security and secrecy is a major drawback to Mobile Cloud Computing (MCC), but it does help us meet our needs for plentiful resources in portable devices. Therefore, the security concerns and difficulties of mobile cloud computing have been examined in [2].

Data integrity (DI), data confidentiality (DC), and availability are all very important features of cloud storage that are investigated in [3]. Also, among the many useful tools that Cloud Computing has made accessible to companies and consumers alike, Storage as a Service is among the most well-known and widely-used (StaaS).

The authors of [4] warn about the security risks posed by cloud service platforms in the medical area and offer some potential remedies. In [4], a technique for denying unauthorised users access while protecting user privacy and data security was outlined.

This section reviews the available surveys about Cloud Computing's infrastructure and the idea of security. In addition, in the first subsection of this section, we have explored the privacy and security of data, storage, and communication [5], and in the subsequent subsections, we have investigated the fundamental security concept in Cloud Computing. Security hazards associated with Secure Data Sharing, as well as other topics like cryptography and steganography, have also been discussed in recent polls. Authentication and security audits are then discussed, along with data provenance, difficulties, risks, threats, and attacks.

The authors of [6] and [7] have introduced a solution to overcome security issues relating to confidentiality, integriy, and availability in cloud systems, while the authors of [8] have analysed the solution of different categories of risks in cloud systems, including infrastructure threats, host threats, and service providers' threats. Consultants are an integral component of the service providers working with the implementation, and in [9] the authors have taken this into account by viewing data privacy and security through the lens of proper training.

Cloud computing security is discussed in [11], and the effects of extended clouds like Mobile Edge Computing (MEC) and fog on the cloud computing network diagram are explored in [10]. To mitigate the damage caused by cloudbursting with DoS attacks or distributed DoS attacks, the authors of [12] created a unique technique they call Cloud Bursting Brokerage and Aggregation (CBBA) and analysed the secure sharing mechanism.

The authors of [14] explain the model, control, and management of rechargeable batteries like Li-ion batteries used in IoT, while [13] discusses the importance of securing Smart Grids on cloud-based software platforms. Even more so, [15] revealed the weaknesses and hazards in the live migration of Virtual Machine, claiming that there is no acceptable method to offer security.

In [16], Sun and Aida have shown how they achieve the security of user applications with a method for running applications that require enormous resources on both local computing resources and Infrastructure-as-a-Service Cloud (IaaS) by employing machine learning, much like [17], where the authors show how they overcame several fundamental issues and improved CPU frequency in Virtual Machine with Workflow Scheduling. Three methods covering data confidentiality and integrity, authentication, and permission of operations are introduced in [18], which also analyses the security of live migration in virtualization.

Table 1 Comparative study of different security based solutions

References	Year	Objective	Technique used	Dataset	Evaluation Metrics
Lahmar and Mezni [19]	2021	Achieve security in multicloud systems	Fuzzy FCA, RS	-	-
Pachala et al.[20]	2021	To achieve security and privacy in cloud data	Hybrid technique	-	Memory consumption, encryption/decryption time, total authentication on time
Torkura et al. [21]	2021	To distinguish malicious activity and illegal change	CSBAuditor		Detection rate, response time, latency
Zhu et al.[22]	2021	Design a scheduling scheme to optimize makespan and total cost	MCS, HCPS, MABC		Make span, cost and resource utilization
Megouache et al. [23]	2020	To achieve data confidentiality and integrity in mutlicloud	VPN, RSA	Public data and confidential data of insured person	Download time, Processor usage
Viswanath and Krishna [24]	2020	Secure model to restrict the insiderattacks	Hybrid encryption technique	Real time health data from web site	Throughput, running time, encryption and decryption time

Cao et al.[25]	2019	Design tri-storage failure recovery system	Tri-SFRS	Medical IoTdata	Latency, overheadtime

Using the STRE method, a cloud user can search and spread its encrypted data across many autonomous clouds administered by separate CSPs, ensuring its safety even if some or all of those CSPs should fail. STRE's advantage is a somewhat concealed search pattern, in addition to its dependability. Table 1 provides a quick overview of the reviewed devices' main features.

3. PRIVACY ISSUES IN CLOUD COMPUTING

- **Malicious behavior of the cloud provider:** It is possible that the cloud service provider will access, use, or mine the user's data in an unsavoury or simply inquisitive manner. As a matter of fact, an unreliable service provider can decrypt a user's data by evaluating or analysing it repeatedly while remaining unaware of the encryption. There are a number of potential dangers that could jeopardise the privacy of data that has been outsourced to cloud servers, including the frequency analysis assault, which involves the repetitive examination of user searches, and the surface analysis attack. Later on, this survey will discuss a few methods that can be used to prevent the server from gaining access to the user's information.

Lack of user control: There is an absence of visibility and management over user data and applications when they are handled in the cloud. To be sure, customers are no longer the legal owners of the underlying infrastructure. As a result, they lack authority over the underlying cloud infrastructure but do have some influence over it thanks to the management interfaces provided by the service provider. The service model also determines the extent to which the customer is given control.

- **Malicious outsiders:** The cloud's shared nature and the fact that multiple users can access the same resources at once pose a security risk. As a matter of fact, due to the virtualized and pooled nature of resources in multi-tenant public cloud environments, free trial offers, and unlimited access of network and resources at a lower price, malicious cloud service subscribers can target the data of legal users who share the same resources and violate their protections, and then spread to other victims.

- **Achieving regulatory compliance:** Issues may arise legally when moving data from one cloud provider in one region to another in another due to the difficulty in assuring regulatory compliance across international borders.

- **Data proliferation:** Most cloud service companies have many redundant data centres in case of disaster. More importantly, data owners have no say over how their data moves throughout the cloud or even across clouds. Accordingly, it is conceivable for a third-party server to violate data.

- **Information disclosure:** Numerous challenges arise when attempting to encrypt data using homomorphic encryption while working in the cloud. In actuality, there are a number of limitations connected with existing encryption solutions, including the intricacy of procedures, the infeasibility of solutions, the poor quality of encryption keys, and the requirement that particular activities be performed on decrypted data stored in cloud servers. Therefore, users' data privacy may be jeopardised if sensitive information is made public.

- **Dynamic provision:** The nature of cloud computing makes it difficult to determine who is accountable for maintaining data privacy. Additionally, due to the dynamic provisioning of cloud subcontractors participating in user data processing, some services may come from a malicious source. So now the user has less faith in the sub-providers and less confidence that his data will be handled securely.

- **Unauthorized secondary usage:** Data saved or processed on the cloud is vulnerable to theft or other misuse. The cloud service provider, for instance, may sell customers' sensitive information to their rivals.

4. RSERACH METHODOLOGY

4.1 Data privacy

The term "privacy" refers to a person's or a group's capacity to conceal or reveal certain aspects of themselves or their activities. The following are elements of private space.

i. When: A person may be more worried about the information that is being revealed right now or in the near future than they are about anything that happened in the past.
ii. How: A user may feel at ease if friends may make special requests for his or her information, but he or she may not like regular and automatic alerts.
iii. Extent: It's possible that a user might like to have their data reported as a fuzzy cluster rather than a single point.

Customers' personal information and context must be kept private and handled responsibly in commercial transactions. Laws, protocols, standards, and practises are all part of ensuring an appropriate level of privacy for individuals' private information within an organisation.

In a cloud environment where user data is protected, prying eyes won't be able to infer anything about a user's habits based on the frequency or duration of their visits (not direct data leakage). Research into Oblivious RAM (ORAM) has been extensive. ORAM technology makes use of several data copies to conceal users' genuine data-visiting intentions. ORAM has already been implemented to protect the privacy of cloud users and other sensitive data, so it's no secret that it's a promising solution. ORAM method is the state-of-the-art implementation of this problem.

There are four distinct types of privacy concerns that arise in the cloud, and they are as follows:

i. how to protect users' data from being misused, stolen, or sold without their knowledge or consent while yet allowing them to access and modify their data in the cloud.
ii. how to ensure data replications are lawful and consistent when storing user data in numerous convenient

locations. and stay away from data theft, disclosure, and tampering.

iii. whose duty it is to ensure compliance with privacy laws regarding individual data?

iv. to what extent it is possible to identify, check, and verify the involvement of cloud subcontractors in processing.

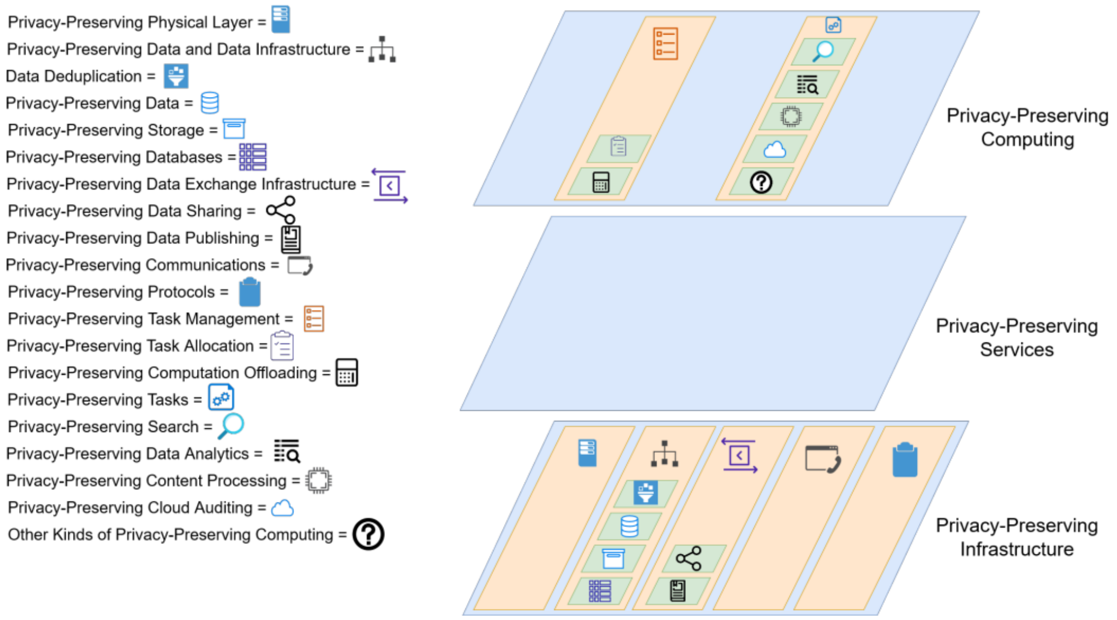
Privacy-Preserving Physical Layer =
Privacy-Preserving Data and Data Infrastructure =
Data Deduplication =
Privacy-Preserving Data =
Privacy-Preserving Storage =
Privacy-Preserving Databases =
Privacy-Preserving Data Exchange Infrastructure =
Privacy-Preserving Data Sharing =
Privacy-Preserving Data Publishing =
Privacy-Preserving Communications =
Privacy-Preserving Protocols =
Privacy-Preserving Task Management =
Privacy-Preserving Task Allocation =
Privacy-Preserving Computation Offloading =
Privacy-Preserving Tasks =
Privacy-Preserving Search =
Privacy-Preserving Data Analytics =
Privacy-Preserving Content Processing =
Privacy-Preserving Cloud Auditing =
Other Kinds of Privacy-Preserving Computing =
Privacy-Preserving Computing
Privacy-Preserving Services
Privacy-Preserving Infrastructure

Fig. 2. The Layered Architecture of Privacy-Preserving Cloud.

The three primary layers of the Layered Architecture are depicted as three huge blue parallelograms in Figure 2. The orange parallelograms depict the sublayers found within these larger layers. The green parallelograms depict the subsublayers, which are located within the sublayers. A legend explaining what each of the symbols represents can be found to the left of the main image.

5. DATA AVAILABILITY

Data availability refers to the degree to which a user's data may be utilised or recovered in the face of calamities like hard disc damage, IDC fire, and network outages, and the methods by which a user checks their data rather than depending entirely on the credit guarantee of the cloud service provider.

Since cloud service providers must adhere to local legislation, customers worry that their data may be illegally stored on servers in another country. The data's privacy and integrity are additional concerns that must be reassured by the cloud service provider. The cloud service provider's responsibility is to be transparent with the client about these kinds of issues and to earn the client's trust. The cloud service provider must reassure customers that their data is secure and clarify the applicability of local legislation. Data storage location, relocation, cost, availability, and security are the primary topics of this study.

User confidence in the cloud can be boosted by making data easier to find. Cloud storage reduces the complexity of the cloud by providing users with a transparent storage solution, but at the expense of users' capacity to exert agency over their own data. Benson et al. [26] looked at geographical replication proofs and managed to track down Amazon cloud data.

5.1. Reliable Storage Agreement

Untrusted storage typically exhibits aberrant behaviour, such as cloud service providers deleting customer data during updates, which is difficult to monitor using merely simple data encryption. Another feature of a solid storage agreement is the ability to make edits alongside other users in real time.

As stated by Mahajan et al. [27], Depot guarantees both Fork-Join-Causal-Consistency and eventual consistency. It's resistant to discarding attacks and adaptable enough to accommodate the addition of additional safeguards in a secure cloud storage ecosystem (such as Amazon S3).

SPORC [28] by Feldman et al. offers secure and dependable real-time contact and collaboration amongst several users with the assistance of a trusted cloud environment; insecure cloud servers have access to only the encrypted data.

While the reliable storage protocol facilitates certain kinds of operations, this support is quite restricted, and most calculations must be performed locally on the client device.

4.2. Reliability of Hard-Drive

The cloud mostly uses hard drives as a storage medium at the moment. Storage in the cloud is based on the dependability of hard drives. The error rate of hard drives was investigated by Pinheiro et al. [29] using data from the past. It was shown that hard disc error rates tend to cluster in predictable ways, but are unrelated to operating conditions like temperature and frequency of use. As it stands, the SMART approach is not reliable enough to predict hard drives' error rates. Tsai et al. [30] studied the correlation between these two types of faults and found that soft faults have a low probability of foretelling hard mistakes on hard discs.

CONCLUSION

The advent of cloud computing is one of the most fascinating moments in the history of computer technology. There are major roadblocks to mainstream adoption of cloud computing, the biggest of which being worries about data security and privacy. Reducing the expenses of storing and processing data is essential for each company, despite the fact that data analysis is always one of the most important duties. Not one company will feel safe transferring their data and information to the cloud unless there is trust between cloud service providers and their clients. Researchers have come up with a plethora of strategies for protecting cloud-based data and giving it the highest level of security feasible. However, because to the broad adoption of Cloud Computing across numerous industries and technologies, a considerable number of private data may be at risk. People are starting to pay attention to the developing privacy concerns in Cloud Computing. Technology and methods for Privacy-Preserving Cloud Computing have arisen as a result of research into this problem, with the aim of ensuring users' anonymity and confidentiality in the cloud.

REFERENCES

1. A. Yazdinejad, R. M. Parizi, A. Bohlooli, A. Dehghantanha, and K.-K. R. Choo, "A high-performance framework for a network programmable packet processor using p4 and fpga," Journal of Network and Computer Applications, vol. 156, p. 102564, 2020.
2. S. A. . M. A. S. Elameer, "A review in security issues and challenges on mobile cloud computing (mcc)," in Proceedings of 1st Annual International Conference on Information and Sciences (AiCIS), Fallujah, Iraq, November 2018.
3. A. K. B. S. M, "A review on challenges of security for secure data storage in cloud," in Proceedings of International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, November 2019.
4. K. L. C. C. J. G. Q. L. Y. Guo, "A review of research on security of cloud service platform in medical environment," in Proceedings of IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), Yilan, Taiwan, May 2019.
5. A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "An efficient packet parser architecture for software-defined 5g networks," Physical Communication, vol. 53, p. 101677, 2022.
6. X. N. H. Suo, "Security in the cloud computing: A review," in Proceedings of 2012 2nd International Conference on Computer Science and Network Technology, Changchun, China, December 2012.
7. N. P. E. D. N. V. C. Lambrinoudakis, "It's all in the cloud: Reviewing cloud security," in Proceedings of IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, Vietri sul Mare, Italy, December 2013.
8. G. S. V. A. G. Suganya, "A comprehensive review on cloud computing security," in Proceedings of International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, March 2017.
9. V. B. P. K. K. B. P. Lohani, "A review of security of the cloud computing over business with implementation," in Proceedings of International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Greater Noida, India, February 2016.
10. S. N. S. A. G. A. F. D. Hutchison, "The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective," IEEE

Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2586–2595, 2017.

11. M. M. A. K. D. G. A. K. N. S. P. A. Z. K. M. A. P. Mahmud, "Applications and evaluations of bio-inspired approaches in cloud security: A review," IEEE Access, vol. 8, pp. 180 799–180 814, 2020.
12. P. J. D. R. S. Patidar, "A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment," in Proceedings of World Congress on Information and Communication Technologies, Mumbai, India, December 2011.
13. B. G. A. B. P. Haller, "A survey on cloud-based software platforms to implement secure smart grids," in Proceedings of 49th International Universities Power Engineering Conference (UPEC), ClujNapoca, Romania, September 2014.
14. F. H. K. S. Y. F. X. Y. X. Yi, "Online soc estimation for li-ion batteries: A survey explore the distributed secure cloud management to battery packs," in Proceedings of 12th IEEE Conference on Industrial Electronics and Applications (ICIEA), Siem Reap, Cambodia, June 2017.
15. N. A. A. K. M. A. Shibli, "Survey on secure live virtual machine (vm) migration in cloud," in Proceedings of 2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan, December 2013.
16. H. S. K. Aida, "A hybrid and secure mechanism to execute parameter survey applications on local and public cloud resources," in Proceedings of IEEE Second International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, November-December 2010.
17. S. I. C. on Advanced Cloud and B. D. (CBD), "Exploration of secured workflow scheduling models in cloud environment: A survey," in Proceedings of Akindipe Olusegun Francis Bugingo Emmanuel Defu Zhang Wei Zheng Yingsheng Qin Dongzhan Zhang, Lanzhou, China, August 2018.
18. A. U. P. Lakkadwala, "Secure live migration of vm's in cloud computing: A survey," in Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization, Noida, India, October 2014.
19. Lahmar, F. and Mezni, H., 2021. Security-aware multi-cloud service composition by exploiting rough sets and fuzzy FCA. Soft Computing, 25(7), pp.5173-5197.
20. Pachala, S., Rupa, C. and Sumalatha, L., 2021. An improved security and privacy management system for data in multi-cloud environments using a hybrid approach. Evolutionary Intelligence, pp.1-17.
21. Torkura, K.A., Sukmana, M.I., Cheng, F. and Meinel, C., 2021. Continuous auditing and threat detection in multi-cloud infrastructure. Computers & Security, 102, p.102124.

22. Zhu, Q.H., Tang, H., Huang, J.J. and Hou, Y., 2021. Task Scheduling for Multi-Cloud Computing Subject to Security and Reliability Constraints. IEEE/CAA Journal of AutomaticaSinica, 8(4), pp.848-865.
23. Megouache, L., Zitouni, A. and Djoudi, M., 2020. Ensuring user authentication and data integrity in multi-cloud environment. Human- centric Computing and Information Sciences, 10, pp.1-20.
24. Viswanath, G. and Krishna, P.V., 2020. Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, pp.1-8.
25. Cao, R., Tang, Z., Liu, C. and Veeravalli, B., 2019. A scalable multicloud storage architecture for cloud-supported medical internet of things. IEEE Internet of Things Journal, 7(3), pp.1641-1654.
26. K. Benson, R. Dowsley, and H. Shacham, “Do you know where your cloud files are?” in Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pp. 73–82, ACM, October 2011.
27. P. Mahajan, S. Setty, S. Lee et al., “Depot: cloud storage with minimal trust,”ACM Transactions on Computer Systems, vol. 29, no. 4, article 12, 2011.
28. A. J. Feldman, W. P. Zeller, M. J. Freedman, and E. W. Felten, “SPORC: group collaboration using untrusted cloud resources,” in Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI ’10), vol. 10, pp. 337– 350, 2010.
29. E. Pinheiro, W.-D. Weber, and L. A. Barroso, “Failure trends in a large disk drive population,” in Proceedings of the 5th USENIX conference on File and Storage Technologies (FAST '07), vol. 7, pp. 17–23.
30. T. Tsai, N. Theera-Ampornpunt, and S. Bagchi, “A study of soft error consequences in hard disk drives,” in Proceeding of the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '12), pp. 1–8, Boston, Mass,USA, June 2012.