International Journal for Rapid Research in Engineering Technology & Applied Science
Vol IX Issue VI June 2023
ISSN Online:- (2455-4723)

A Review on Cloud Computing Security and Privacy

Poonam Singh rajput ,M.Tech. Scholar
Deepak Mishra ,Assistant Prof.
Department - Computer Science Engineering
VNS Faculty of Engineering Bhopal
vnsit.amit@gmail.com

Abstract: this paper discussed about how data is kept safe in cloud computing. It is a study of data stored in the cloud and the security issues that come with it. The paper will go into depth about the methods and approaches to data security that is used all over the world to protect data as much as possible by reducing risks and threats. cloud computing has become increasingly popular in recent years as it offers many advantages such as scalability, cost efficiency, and accessibility from anywhere. However, storing data in the cloud also poses significant security risks that must be addressed to ensure the safety of data. One of the main security concerns when it comes to cloud computing is data privacy. When data is stored in the cloud, it is important to ensure that only authorized users have access to it. Encryption techniques can be used to protect data from unauthorized access by encrypting the data before it is stored in the cloud. Access controls and identity management systems can also be implemented to ensure that only authorized users can access the data. Another security concern is data integrity, which refers to the accuracy and completeness of data. Data can be corrupted, altered or deleted accidentally or maliciously, so it is essential to have measures in place to prevent such incidents. Data integrity can be ensured through data backups, checksums, and version controls. this paper literature about various cloud based techniques for privacy and security.

Keywords: Author Guide, Article, Camera-Ready Format, Paper Specifications, Paper Submission

I INTRODUCTION

The text must be in English. Authors whose English Cloud computing links together a lot of computing, storage, and software resources to make a huge pool of shared virtual resources from which users can buy services like electricity. As cloud computing apps have become more and more popular, they have spread into many different fields, such as scientific study, production, education, shopping, entertainment, etc.

What you need to know about cloud computing The technology of virtualization in cloud computing gives end users access to useful resources. Cloud computing has features like being easy to control, scalable, and available. Cloud computing also has the benefits of being cheap, easy to use, global, having multiple tenants, being flexible, and being stable. Cloud computing mainly offers three service delivery models and four development patterns (http://www.cloudsecurityalliance.org/): infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), public cloud, private cloud, hybrid cloud, community cloud, and virtual private cloud (Fig. 1).

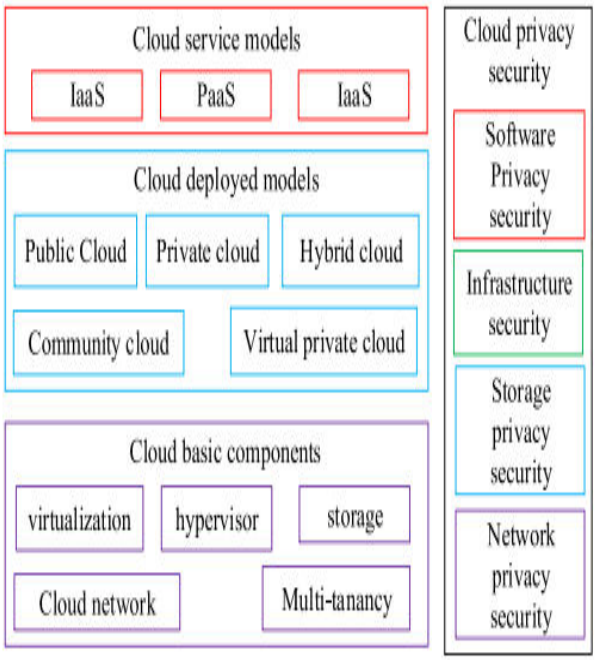

Fig. 1. Cloud computing framework.

IaaS uses computer hardware (network storage, virtual server/computer, data centre, processor, and memory) as a service. It offers infrastructure scalability and provisioning without needing a lot of money or time. IaaS also works on security issues like firewalls, intrusion detection, tracking of virtual machines, and other areas. PaaS is part of the software of the service model. It offers services in the form of development tools, frameworks, designs, programmes, and integrated development environments.PaaS has to deal with a lot of problems, such as how to work with third parties, how to build software over its entire lifecycle, and how to keep the core infrastructure secure. SaaS is a group of remote computing services that let third-party providers install applications from a distance. On the cloud platform, a customer can use the Internet to run apps from cloud service companies.[1-4]

II LITERATURE REVIEW

Ashish Joshi et.al. (2022) Millions of people around the world use the cloud setting to handle and share data because of its benefits. A cloud system must always offer protection and privacy for info. When users use and share information widely, security holes are made. The goal of this study is to talk about the cloud environment, its pros and cons, and the research trends that will shape the future of safe data processing and sharing. The common problem is caused by the fact that more and more businesses are using cloud computing. So, using any device to load and receive data from the cloud providers' facilities raises a number of security and privacy risks, such as data change, data loss, and theft. Insiders getting in without permission are one of the biggest problems that could happen. Even though there are ways to stop cloud managers from getting unauthorised access, those ways haven't worked to keep them from getting to client data in the cloud. Information security is judged by how well a system protects the CIA triad, which is made up of the information security traits of confidentiality, integrity, and availability. In this study, we looked at these kinds of situations. This study's research showed risks to cloud data security, attacks on the cloud, and weaknesses in a number of factors that affect cloud computing.[5]

Fengling Wang et.al. (2021) Concerns about data protection have become a big deal in the big data cloud computing world. This paper gives an outline of how big data cloud computing is thought of, what it looks like, and what kinds of advanced technologies are used. Details are given about data access, data isolation, data consistency, data destruction, data transfer, and data sharing in terms of data quality and privacy control. In the end, virtualization design and related strategies are suggested to protect against threats and improve data security in a big data cloud setting.[6]

Suganya M et.al. (2022) Concerns about data protection have become a big deal in the big data cloud computing world. This paper gives an outline of how big data cloud computing is thought of, what it looks like, and what kinds of advanced technologies are used. Details are given about data access, data isolation, data consistency, data destruction, data transfer, and data sharing in terms of data quality and privacy control. In the end, virtualization design and related strategies are suggested to protect against threats and improve data security in a big data cloud setting.[7]

Shilpi Mishra et.al. (2022) Amazon has a wide range of IT services that businesses can use to build their own private virtual clouds and keep full control over their systems. Amazon Web Services can be used for both business projects and IT projects. The cloud is attractive to security workers because it saves money and works well, but it also has a lot of security and safety problems. Amazon Web Services (AWS) has created EC2 instances, which they say will make cloud computing safe for highly regulated businesses. This is part of their work to help businesses with cloud computing security and compliance problems. Cloud computing has some problems, but these problems also give us a chance to learn about many things connected to cloud computing. A big worry is the security and privacy of data that is kept and handled on the computers of cloud service providers. In this study, the security and privacy of cloud computing are looked at from a number of different angles. In this piece, we've learned more about the security problems of cloud computing and looked at the methods and solutions that the cloud service industry has used to deal with them. The goal of this study is to put light on the rapidly growing cloud services market and the different challenges, such as network problems, that are coming up.[8]

Jia Yu et.al. (2021) People think that Provable Data Possession is an important way to make sure that the data saved on faraway computers is correct. Recently, a new provable data possession method was suggested. The writers said that this plan could ensure that the storage would be fixed. In this study, we show that this method can't meet this basic security requirement. In particular, we show that a bad cloud can make a proof that can be checked by a third-party reviewer even if it doesn't store the whole user file.[9]

M Janani Priya et.al. (2022) as cloud computing technology gets better, more and more businesses are using cloud tools for their business needs. Data about

business deals, communications, business model design, and a lot of other things are gathered and kept in the cloud platform, which is often accessed by business partners in Dubai. From a security point of view, data saved in the cloud needs to be very well protected and can only be viewed after logging in. The suggested system is focused on analyzing a cloud integrity auditing model in which the security and privacy-protecting system is inspected and privacy is chosen by a machine learning algorithm. The suggested model is made with a hybrid CatBoost algorithm (HCBA), and the input data is saved in the cloud platform using Bring your own encryption key (BYOEK). The security of the BYOEK model is tested and confirmed by comparing the amount of time it takes to run the programme to the amount of time it takes to send data.[10]

L. Megalan Leo et.al. (2022) Because of cloud storage, more and more people want to send their info to someone else. To protect privacy, private data should be locked down before outsourcing. There are many readable encryption systems that make sure the data they protect is visible. As cloud computing grows, more and more people want to store their info on servers in the cloud. The main goal of this system is to make a cloud server with strong encryption and decryption data logics and to keep registration sites and different data owners and users from having to enter the same information more than once. New security problems need to be fixed so that more customers can use the public cloud to process their data. Since the cloud as a whole has problems with maintaining room, the proposed system must include a new way to offer data services without duplicating them. Using a third-party registration centre to store data on a computer far away is a big security risk in cloud computing. This system uses an unbreakable 256-bit encryption method to process data using a Message Digest Algorithm (MD5) and an Intelligent Data Hashing Algorithm (DHA). This gives the best level of security.[11]

Henry Chima Ukwuoma et.al. (2021) since the beginning of cloud computing, data security in the cloud has been a major concern. Many models have been offered and put into place, but data breaches still happen. Since encryption is the most common way to keep data safe in the cloud, the arrival of quantum computing means that we need to come up with a better system that will keep data safe for both the cloud and quantum computing. Quantum computing, on the other hand, will make some cryptosystems weak and useless, while others will be able to stand up to it. This paper suggests an efficient system for cloud data security using the McEliece and NTRU cryptosystems to protect data in cloud computing and quantum computing. A version of McEliece will be used to protect user passwords, and a version of NTRU will be used to protect user data.[12]

Randolph Loh et.al. (2021) Data splitting protects privacy by breaking up data into pieces that can be saved and shared distantly. Most data tasks can be done with it because data can be kept in plain text instead of using cryptography. But most of the current methods for splitting data don't take into account data that is already in the multi-cloud. This wastes resources because it means the material has to be broken up again. This work suggests a method for splitting data that makes use of data already in the multi-cloud. It improves the way data is split by lowering the amount of splitting processes and fragments that come out of them. So, reducing the number of storage places a data owner has to keep track of. Broadcast queries find third-party data pieces so that expensive actions don't have to be done when data is split. This work looks at things to think about when using fragments from third parties and how they can be used with current data splitting methods. The suggested framework was also used to add to the powers of a data-splitting mechanism that was already in place.[13]

Yash Gupta et.al. (2023) Cloud data protection is the process of keeping information safe that a company stores, sends, or processes in the cloud, whether the information is in the company's hands or in the hands of a third party. More and more businesses are no longer building and running their own data centres. Instead, they are putting their apps and data in the cloud. This study looked into cloud computing and how data saved on clouds is kept safe. This study also came to the conclusion that in the coming years, many more companies and users will be attracted to the cloud for sharing data together, and that the security of these data will be of the utmost importance to cloud providers around the world. The goal of the poll is to find out which cloud service people of different ages prefer and what problems they face. It also asks if they think the current laws are enough to protect their data privacy and, most importantly, if their data is safe when it's kept in the cloud.[14]

III PRIVACY SECURITY OF CLOUD COMPUTING

The way cloud computing is built is what causes most security problems. First, the parts of tech are different and spread out, so they aren't always easy to keep track of. Second, when sharing, editing, and saving data, the cloud service provider (CSP) could give away private information. Because cloud computing is based on technology, the security flaws of existing technologies will be carried over to a cloud computing platform, making the

security risks even worse. A threat to privacy and safety from information security to network security to cloud computing security, there is always a need to protect the safety and privacy of information.

Privacy data security: Due to the way services are outsourced, the security risks of cloud privacy, such as data disclosure, privacy disclosure, access rights management, and problems with deleting data, stand out.

Access control and identity authentication: Cloud computing uses a lot of resources, and the handling of access control and identity verification gets a lot more complicated. (3) Security for virtualization: Even though service providers have planned and put in place ways to keep virtual machines separate, attacks between virtual machines can't be stopped fully. When virtual machines are moved, the security domain will also change.

- **Multi-tenant and cross-domain sharing:** Security for multiple users and multiple tenants must be provided. Cross-domain makes service permission and access control harder, and trust transfer between two cloud computing groups needs to be looked at again.
- **Advanced Persistent Threat (APT):** APT is a planned attack on a cloud computing system that has set up some hidden interest groups.
- **System security vulnerabilit**y: Due to the complexity of cloud computing, many service companies have different management and service levels. This means that security holes will make the cloud more dangerous.
- **Insider threat:** When spies at a service provider leak information, either by accident or on purpose, the security policy is often no longer true. This has become an important problem in cloud computing security.
- **Wrong application of cloud service:** When cloud computing is used wrong, it can cause problems for users, service providers, or third parties. Using cloud services illegally will also have serious effects.
- **Service availability:** Many security issues cause cloud computing services to be unavailable, and denial of service threats have become an important security goal for cloud service companies.

IV CHALLENGES OF A SECURED CLOUD SYSTEM

The development of a secure and reliable cloud system faces three important challenges. They are,

Outsourcing-Outsourcing can reduce the cost of capital and operating costs for cloud customers. The problem without control has become one of main reasons of cloud uncertainty. To address the issue of outsourcing security, cloud providers need to maintain credibility by providing credible computing or data storing; second, outsourcing data and computing need to be verified to customers in relations of security services. Since sensitive data is not under the control of the owner, outsourcing can violate privacy.

Multi-tenancy-Multi-tenancy is defined as cloud platform communal or used by multiple customers. In addition, in a virtualized situation, certain resource allocation strategies can be used to place data going to dissimilar customers on same physical computer. Opponents who may also be true cloud customers can take advantage of coexistence problem (Parashar et al., 2013) and detect a number of security threats, such as Data leaks, computer violations, flood attacks, etc. (Parashar et al., 2013). . Although multi-lease is an unavoidable choice for cloud providers due to its economic efficiency, it poses new threats to cloud platforms. Without Varying multi-tenant paradigm will no doubt design new security mechanisms to deal with high risks.

Mass data and intensive computing- Cloud computing can handle massive data storage and highly qualified computer tasks. Thus, old-style security mechanisms may not be sufficient due to insurmountable calculation or statement costs. For example, to check the veracity of rarely stored data, it is unworkable to cut out perfect data set. For this reason, new strategies and agreements are predictable. As long as the current World Wide Web architecture and standards can promote the development of cloud computing, it can be considered a true solution for all aspects of computing value. The elusive reason is that it brings a lot of convenience to users and system owners. Their feasibility, ease of use, cost, etc. Depending on the user and the provider, it can also lead to many inconveniences and problems. Therefore, many organizations and companies want to deploy distributed solutions to their own substructure. There are many attributes and variables in the cloud system. These attributes and variables define the whole system and affect the mentioned benefits and problems. One of the buildings is very important (Bhuvaneshvaran et al., 2012).This cloud computing model provides dissimilar kinds of security services in different forms. It covers the basic service events for companies or other comparable systems, such as identity verification, accounting, authorization, identity management, etc. Integrity and confidentiality are the main concerns for file security systems. Confidentiality confirms

that only the intended recipient can access the data, or integrity ensures that the data remains intact when the recipient needs to retrieve the data. These two basic attributes and other attributes can be solved using encryption technology.

V LIMITATIONS OF CLOUD COMPUTING:

There are also some limitations of cloud computing:

Performance and Latency: Cloud computing services rely on the internet to connect users to computing resources, which can result in performance and latency issues. The distance between the user and the cloud data center, as well as network congestion, can impact the speed and responsiveness of applications running in the cloud.

Reliability: Cloud computing services are dependent on the reliability and availability of internet connectivity and cloud infrastructure. Outages or disruptions in either of these areas can cause downtime or data loss.

Compatibility: Applications or systems that were designed to run on-premises may not be compatible with cloud computing infrastructure, which can make it challenging to migrate to the cloud. This can result in additional costs and time required to modify or rewrite applications.

Security and Privacy: Cloud computing services require data to be stored and processed outside of an organization's on-premises infrastructure, which can raise security and privacy concerns. Organizations may be hesitant to entrust sensitive data to a third-party provider.

Integration: Integration between cloud services and on-premises infrastructure can be complex, requiring specialized skills and expertise. The more complex the integration, the greater the risk of errors, downtime, or data loss.

Limited Control: Cloud computing services are often provided on a shared infrastructure, which means that organizations may have limited control over the underlying hardware and software. This can make it difficult to address issues such as hardware failure or software vulnerabilities.

VI CONCLUSION

The movement towards better ways to store data in the cloud is getting stronger as more people use cloud computing to store data. Data that is stored in the cloud can be at risk if it is not protected properly. This paper gave a review of three types of security issues and talked about the risks and security threats to data in the cloud. Virtualization is looked at to see what dangers the host poses. Threats from Public cloud and multitenancy have also been talked about. One of the main points of this paper was the security of data in the cloud and how it can be threatened and how to fix that. We've talked about data in different states and the best ways to secure data in the cloud. The study gave an outline of block cypher, stream cypher, and hash function, which are used to encrypt data in the cloud while it is at rest or in motion.

References

1. problem. arXiv preprint arXiv: (2016). 1609.01107.
2. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A.,& Zaharia, M. A view of cloud computing. Communications of the ACM, (2010). 53(4), 50-58.
3. Mell, P., & Grance, T. The NIST definition of cloud computing. National Institute of Standards and Technology, (2011). 53(6), 50.
4. Aljawarneh, S. A., & Alkhateeb, F. Cloud computing in healthcare: A comprehensive review. Journal of Medical Systems, (2021). 45(2), 1-23.
5. Ashish Joshi;Aditya Raturi;Santosh Kumar;Ankur Dumka;Devesh Pratap Singh Improved Security and Privacy in Cloud Data Security and Privacy: Measures and Attacks 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP) Year: 2022 |
6. Fengling Wang;Han Wang;Liang Xue Research on Data Security in Big Data Cloud Computing Environment 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) Year: 2021 |
7. Suganya M;T. Sasipraba Security and Privacy-Efficient Encryption Algorithm for Cloud Data Using Genetic Prime Crossover Technique 2022 1st International Conference on Computational Science and Technology (ICCST) Year: 2022 |
8. Shilpi Mishra;Manish Kumar;Niharika Singh;Stuti Dwivedi A Survey on AWS Cloud Computing Security Challenges & Solutions 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) Year: 2022 |

9. Jia Yu;Rong Hao Comments on "SEPDP: Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage" IEEE Transactions on Services Computing Year: 2021 |
10. M Janani Priya;G Yamuna Privacy preserving Data security model for Cloud Computing Technology 2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN) Year: 2022 |
11. L. Megalan Leo;S. Yogalakshmi;A. Veeramuthu;V. Kalist;A. Anne Frank Joe Experimental Analysis of Data Storage and Integrity Management over Cloud Environment using Integrated Data Security Strategy2022 International Conference on Electronics and Renewable Systems (ICEARS)Year: 2022 |
12. Henry Chima Ukwuoma;Arome Gabriel Junior;Aderonke Thompson;Boniface Kayode Alese Optimised Privacy Model for Cloud Data2021 16th International Conference on Computer Science & Education (ICCSE)Year: 2021
13. Randolph Loh;Vrizlynn L. L. Thing Data Privacy in Multi-Cloud: An Enhanced Data Fragmentation Framework 2021 18th International Conference on Privacy, Security and Trust (PST) Year: 2021
14. Yash Gupta;Neetu Narayan Data Security in Cloud Computation 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence) Year: 2023
15. Christian Banse; Immanuel Kunz; Angelika Schneider; Konrad Weiss Cloud Property Graph: Connecting Cloud Security Assessments with Static Code Analysis 2021 IEEE 14th International Conference on Cloud Computing (CLOUD) Year: 2021
16. Amit Kumar Singh Sanger; Rahul Johari Survey of Security Issues in Cloud 2022 International Mobile and Embedded Technology Conference (MECON) Year: 2022 |
17. Shuai Li; Fangfang Dang; Ying Yang; Han Liu; Yifan Song Research on Computer Network Security Protection System Based on Level Protection in Cloud Computing Environment 2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA) Year: 2021
18. Bahrami, S., Sanaei, M. H., & Abolfazli, S. (2019). Cloud computing in education: A review. Journal of Educational Technology Development and Exchange, 12(1), 1-22.
19. Wang, Y., Jin, H., & Li, C. (2020). The potential of cloud computing in healthcare: A systematic review. Journal of Medical Systems, 44(6), 1-11.
20. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A.,& Zaharia, M. A view of cloud computing. Communications of the ACM, (2010). 53(4), 50-58.
21. Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A., & Ullah Khan, S. The rise of "big data" on cloud computing: Review and open research issues. Information Systems, 2015, 47, 98-115.
22. Mell, P., & Grance, T. The NIST definition of cloud computing. National Institute of Standards and Technology, 2011, 53(6), 50.