RESOLVING SECURITY AND DATA CONCERNS IN CLOUD COMPUTING BYUTILIZING A DECENTRALIZED CLOUD COMPUTING OPTION

V.Chiranjeevi [1], P.Ashwini [2], S.Nagamani [3]

[1]Assistant Professor, Swarna Bharathi Institute of Science & Technology, India, E-mail: chiru508@gmail.com.
[2]Assistant Professor, Swarna Bharathi Institute of Science & Technology, India, E-mail: ashwini.podila@gmail.com.
[3]Assistant Professor, Swarna Bharathi Institute of Science & Technology, India, E-mail: nagamanikunchipudi@gmail.com.

ABSTRACT

The technology that supports cloud computing is fraught with security risks. Data privacy and integrity, infrastructure stability, and protection against attacks are a few of them. Centralized and decentralized cloud computing are the two main concepts used by today's cloud computing infrastructures. Data leaks, outages, and other security dangers are all too real with centralized cloud computing. Data is better safeguarded by encryption using Reid Solomon erasure coding, and decentralized cloud computing is more robust to failures thanks to geo-redundancy technology.
Computing in the Cloud; Decentralized Cloud Computing; Blockchain; Geo-Redundancy;Security Practices; Cybersecurity; Data Integrity; etc.

INTRODUCTION

Cloud computing is a method of establishing a computer network in which data storage and other resources are made available as a service and may be accessed remotely. [1] According to the National Institute of Standards and Technology's (NIST) definition, "A template for providing the suitable and when needed access to the internet, to a collective pool of programmable grids, storage, servers, software, and amenities that can be rapidly emancipated, with little communication and supervision from the provider," cloud computing is most often used and agreed upon. [2] The concept of cloud computing has completely altered the development, deployment, and use of computer infrastructures for customers,organizations, and developers alike. In recent years, cloud computing has grown in popularity thanks to its many appealing features, such as its scalability and cost-elasticity (many providers now offer pay-as-you-go instead of flat rates), and the enhanced security and data integrity that accompanies cloud infrastructures. The ability to access resources and services on demand is a key feature of cloud computing. Storage and virtualization resources, for example, are instantly accessible from any location in the globe. This is in contrast to the old-fashioned method of accessing resources, which included installing hardware on a local workstation or server before using it, and that technology had its limitations. Without touching any local hardware, adding cloud resources is a breeze. If you use resources or store data in the cloud, they are either physically kept in one place, like a data center, or in several places, spread out around the globe, like a network of interconnected computers. A centralized cloud computing infrastructure stores all of its data and resources in a single physical location, while a decentralized cloud computing infrastructure stores data and resources in multiple physical locations from different providers. [3] The difference between a decentralized and a centralized cloud computing architecture is shown graphically in Figure 1. All transactions on a blockchain network are encrypted, tracked, and secured by means of digital ledger technology. The network is dispersed and operates on this principle. Every record and transaction sent via a blockchain network is permanent and cannot be altered in any way since blockchain networks are immutable. [3] Most decentralized cloud providers base their infrastructures on blockchainnetworks, therefore this is an additional layer of security that decentralized cloud computing infrastructures use. The IPFS, Sia, and Storj networks are among the most popular examples of such systems. Most centralized cloud computing infrastructures use conventional networks, which are fundamentally less secure than blockchain networks. While virtual machine resources are available in cloud computing infrastructures, containerized.This research paper will discuss the topic of data storage in the cloud and the security issues that come with it, as it pertains to virtual systems. Despite the many advantages, there are a number of security risks and issues related to

cloud computing due to the global accessibility of data housed in these infrastructures. Concerns about cloud computing security primarily revolve around data security, specifically the privacy and protection of user data, the integrity of data stored in data centers (as opposed to on-premises workstations), the stability of the cloud computing infrastructure, and the administration of the cloud computing infrastructure.

SECURITY

Cybersecurity threats, data privacy and integrity, and the reliability of cloud computing infrastructure are among the many security concerns that consumers and companies have about cloud computing. Different Forms of Cybersecurity Risks New cybersecurity dangers emerge daily as a result of the rapid development and evolution of technology. Even while it may be more vulnerable to certain forms of conventional cybersecurity risks, cloud computing is not completely safe. Sending deceptive information or communications that seem to be from legitimate, trustworthy sources in order to get sensitive information from the target is known as phishing.Malicious software or programs known as ransomware encrypt data and make the user pay a ransom or comply with additional demands before restoring access to their machine. In the field of cybersecurity, a Trojan horse is a piece of software that masquerades as a useful and legitimate application while actually running malicious processes designed to steal sensitive data and send it back to the software's creator. Botnet: A botnet is a private network of computers that have all been infected with malicious software and are controlled together to do undesired tasks, including sending out spam messages in bulk. An assault known as a distributed denial of service (DDoS) aims to disrupt a service or resource on a network by overwhelming it with requests from outside sources, making it inaccessible to those who really need it. Malicious software that displays advertising with the purpose of selling goods or services is known as adware. Crypto-mining: Using a computer to mine cryptocurrency invisibly is known as crypto-mining. The perpetrator of the crypto mining malware benefits monetarily from this. The CISCO 2021 Cyber Security Threat Trends research ranked crypto-mining attacks as the most significant cybersecurity concern for the year 2021. [5] According to the CISCO Cyber Security Threat Trends study, which is shown in Table 1, several forms of cybersecurity risks have increased by different percentages since 2020, with variable percentages depending on industry. For the purpose of this table, comparisons are made between the manufacturing, healthcare, and finance sectors.

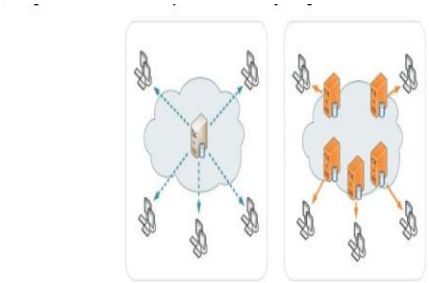

Figure 1: Centralized cloud computing infrastructure (left), decentralized cloud computing infrastructure (right).

Table 1: 2021 Percentage of Increase for Different Cybersecurity Threats Since 2020. (Percentages broken down by threats targeted to different industries).

Cybersecurity Threat	Target Industry		
	Manufacturing	Healthcare	Financial
Phishing	13%	29%	46%
Ransomware	20%	8%	5%
Trojan	6%	46%	31%
Botnet	4%		2%
Cryptomining	48%	4%	5%
All Others	9%	13%	11%

This data includes industries that use cloud computing infrastructure to store their data, however it does not include stood alone. According to the statistics, the danger that had the greatest rise across the board (in every sector) the cybersecurity risk of phishing, which increased by a total of 88% from 2020.There are many different kinds of phishing assaults, and cloud computing is one of the most vulnerable. A great deal of cloud One feature of many computer systems is the ability to share files with other users. This feature is often communicated via email. Someone is receiving the file. It is possible to successfully conduct phishing attacks by duplicating and altering this email assaults in which the victim thinks a coworker has delivered them a file over the internet share a file, you can end up on a phony document that steals sensitive data. Information kept in conventional, centralised cloud storage systems is vulnerable to all of the aforementioned identified cybersecurity risks.Cloud computing as it has always been conceptualized fails to account for approaches to mitigate these risks; furthermore, every cloud service provider has its

own strategy for protecting its customers' data from a large number of these dangers. But the paradigm of decentralized cloud computing has several built-in security protocols, the majority of which are derived from blockchain networks can serve as the foundation for decentralized cloud computing systems.Security of Personal Information Data privacy is often the top concern when using cloud computing resources since they are accessible from anywhere in the globe. problem for businesses and their customers. Data security in the context of cybersecurity is one example of a data privacy problem concerns, as previously stated, as well as the protection of personal information from so-called "bad actors" or those who engage in illicit activities on their own get and use private information. Data encryption technologies may enhance data privacy. When putting information in the cloud, Unfortunately, not all data is encrypted by default. Data storage in a centralized cloud often requires either the user or For utmost security, the organization submitting the data must encrypt it prior to uploading. Regarding data storage Data encryption is implemented on a decentralized cloud platform for both transit and at-rest scenarios. Because information is kept in a many different places, data files are encrypted individually. A data file's each chunk is called a fragment of information. It is necessary to compile each shard before decrypting or accessing it. among the remaining fragments. The term for this kind of encryption is Ried Solomon erasure coding. Figure 2 displays an graphical representation of the process of storing data on various storage resources called nodes using erasure coding shown here. The data grid could consist of a simple network of nodes, however in today's blockchain network is a common example of decentralized cloud computing. Information collected from many sources nodes is more secure against cyberattacks because it is computable before being accessible. and no one other than the original data uploader may see it on the blockchain. This technological advancement renders data unavailable, therefore preventing hostile attempts that aim to steal and store data content. whomever is not the data owner.

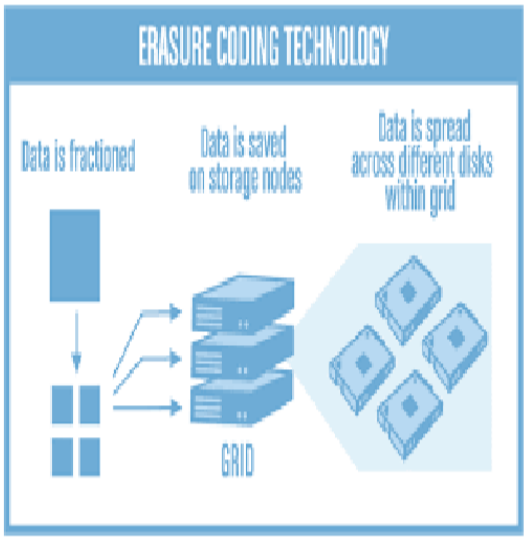

Figure 2: Visual representation of erasure coding technology.

Ensuring the Authenticity of Data Data integrity is another issue with cloud computing and stored data. [6] Power outages, device failure, and natural disasters are regular occurrences that might compromise data integrity, and they could happen wherever that cloud computing resources are kept. Data loss is possible if there is no alternative backup or storage site other than the cloud, as any of these things might compromise data integrity. Data replication across many cloud providers provides consumers and companies with redundancy, which is why multi-cloud solutions are so popular. Data saved in a decentralized cloud computing infrastructure uses geo-redundancy, therefore this is only an issue with centralized cloud computing infrastructures. When data is stored across many places, it increases the likelihood that it will be accessible even if one of those sites has a data loss. This technique is known as geo-redundancy. Data integrity also includes making sure that other users can't alter or alter data, either maliciously or accidentally. The only person who can make changes to data in a decentralized cloud system is the original uploader. The content integrity, not the physical integrity, of data is guaranteed by this. [3] By meticulously documenting each and every transaction on a blockchain-based decentralized cloud architecture, users can verify that no one else has tampered with their data by seeing when they personally made modifications and by tracking who else made updates. Dependability of a Centralized Cloud Computing System. It doesn't take much for natural catastrophes or widespread power outages to knock centralized cloud computing systems down for a while. The Amazon Web Services US East 1 region went down in December of 2021, causing losses for numerous sectors and businesses. Many businesses were impacted by this outage, including Disney, Netflix, and many more. [7] Many people started to doubt the reliability of the cloud computing system after this

outage and sought for alternatives to hosting their data and resources. Predictability of a Decentralized Cloud Computing Architecture In contrast to the centralized cloud computing architecture, which has stability problems, a decentralized cloud computing infrastructure does not. The use of geo-redundant resources in decentralized cloud computing infrastructures ensures that data and resources may still be accessed in the event of a resource or area outage. [3] Because data and resources are automatically replicated across several sites in decentralized cloud computing, disruptions are eliminated until a large number of locations are down. The locations of the many sites are sometimes quite different from one another, sometimes even in the same building. In contrast to more conventional, centralized cloud computing models, decentralized cloud computing is very stable since it does not rely on any one central location. Infrastructure Management for Cloud Computing There is always room for improvement in the management of any service or resource. Storage of hundreds of thousands of petabytes of data, including revenue, customer, and tax records, is commonplace in cloud computing for most enterprises. The organization must have faith in the cloud provider's management to store this kind of data on their infrastructure, as theypossess the ability to access or alter that data. Cloud infrastructure managers would never knowingly conduct something like that, but if their accounts were hijacked by phishing or other cybersecurity assaults, their passwords may be exploited for malevolent purposes. Even though this is still a worry for businesses and individuals alike, many cloud providers take security seriously and give extensive training to their admins. But in a decentralized cloud system, this won't be an issue at all. There is no central authority or manager in charge of a blockchain network, and all users have equal access to the network's rights. This, in addition to the previously stated data security measures like erasure coding and data encryption, gives you piece of mind and increases data security.

CONCLUSION

Scalability, user-friendliness, cost-effective pay-as-you-go pricing, and universal accessibility are just a few of the many advantages of modern cloud computing. Two distinct cloud computing architectures exist: the more established and well-known "traditional" architecture, and the newer, less popular "modern" architecture. Both the centralized and decentralized cloud computing infrastructures are in use today. Although more people use it, the centralized cloud computing infrastructure model isn't without its security flaws, privacy issues, and potential for data corruption due to a single point of failure. With the use of blockchain technology, geo-redundancy ensures that there is no single point of failure, encryption and erasure coding boost data integrity and privacy, and the decentralized cloud computing infrastructure architecture offers inherent security. When compared to the old, centralized cloud computing architecture, the new, decentralized approach eliminates all of the problems and worries. There are a lot of advantages to using a decentralized cloud, like the capacity to safeguard data, so even if consumers and businesses aren't using it much just now, that will probably change.

I. REFERENCES

[1] Foster, I., Zhao, Y., Raicu, I., Lu, S.. Cloud computing and grid computing 360-degree compared. In: GridComputing Environments Workshop, 2008. GCE ’08. 2008, p. 1–10. doi:10.1109/GCE.2008.4738445.

[2] Mell P, Grance T. Version 15 The NIST definition of cloud computing October 7. National Institute of Standards and Technology; 2009 http://csrc.nist.gov/ groups/SNS/cloud-computing

[3] S. Wang, Y. Zhang and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," in IEEE Access, vol. 6, pp. 38437-38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[4] W. Liu, "Research on cloud computing security problem and strategy," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 1216-1219, doi: 10.1109/CECNet.2012.6202020.

[5] Cisco affiliates, 2021 Cyber security threat trends- phishing, crypto top the list, 2021. https://learn- umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

[6] Sun, Yunchuan& Zhang 张均胜, Junsheng&Xiong, Yongping& Zhu, Guangyu. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks. 2014. 1-9. 10.1155/2014/190903.

[7] Renato Losio, AWS US-EAST-1 Outage: Postmortem and Lessons Learned, 2021. https://www.infoq.com/news/2021/12/aws-outage-postmortem/