A DECENTRALIZED CLOUD COMPUTING OPTION FOR RESOLVING SECURITY AND DATA CONCERNS

Mr. Pramod Kumar Thota[1]., Mr. Bhanu Chander Pachimadla[2]
1,2 Assistant Professor, Department Of CSE.,
(✉pramodkumarathota88@gmail.Com, ✉bhanuchander121@mrcew.ac.in)
1,2 Malla Reddy College Of Engineering For Women., Maisammaguda., Medchal., Ts, India

ABSTRACT

Security threats are widespread in the cloud computing architecture. Threats to infrastructure, data privacy, data integrity, and stable infrastructure are all examples. These days, cloud infrastructures may be either centralized or decentralized, depending on the desired level of centralization and degree of independence from other nodes. Unfortunately, there are a number of security risks associated with relying on a centralized cloud service. Due to geo-redundancy technology and Reid Solomon erasure coding, decentralized cloud computing is more robust to outages, and data is better safeguarded.

I. INTRODUCTION

The term "cloud computing" is used to describe a kind of IT infrastructure service model in which resources like data storage are made available over the Internet and may be accessed from any location. [1] Cloud computing is defined by the NIST as "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" (NIST, 2013). [2] When it comes to building, deploying, and using IT systems, the concept of cloud computing has completely changed the manner in which customers, businesses, and programmers do business. Increased security and data integrity, as well as the flexibility and scalability of cloud infrastructures, have contributed to cloud computing rise in popularity. Many cloud service providers now offer pay-as-you-go models rather than fixed rates.

Cloud computing enables on-demand access to services and resources. Whether it is storage or virtualized resources, they may be accessible instantly from any location in the globe. In the past, accessing resources included installing hardware on a local workstation or server before using them, and such hardware often had restricted capabilities. The addition of cloud resources requires no special configuration or installation on user-operated devices. Data and resources that are part of a cloud infrastructure can be stored in a centralized location, like a data centre, or they can be distributed across a number of different locations, creating a distributed cloud infrastructure. [3] In Figure 1, we see a comparison between two types of cloud computing architectures: one that is centralized and one that is distributed. A block chain network is a decentralized database that employs digital ledger technology to record and

Verify all exchanges that take place inside it. Because of the nature of block chain networks, no changes can be made to any data that has been transferred over one. [3] Since most decentralized cloud providers construct their infrastructures on block chain networks; this adds an extra degree of protection to the data stored in the cloud. IPFS, Sea, and Story are three of the most well-known examples of such networks. Most centralized cloud computing infrastructures use insecure conventional networks, whereas block chain networks have intrinsic security advantages.

However, although virtual machines (VMs) may be hosted on cloud computing infrastructures, containerized applications have the advantage of being more portable and requiring less infrastructure systems, or other virtual systems, this study will discuss the storage of data inside a cloud computing infrastructure and the security problems related to such storage. Although there are many advantages to adopting cloud computing, there are also many security issues and challenges due to the fact that data stored in cloud computing infrastructures may be accessed from anywhere in the world. User data privacy and protection, data integrity when stored in data centre locations (as opposed to users or enterprises storing their data locally on their workstation environment), cloud computing infrastructure stability, and cloud computing infrastructure administration are the primary points of concern when it comes to cloud computing security. [4]

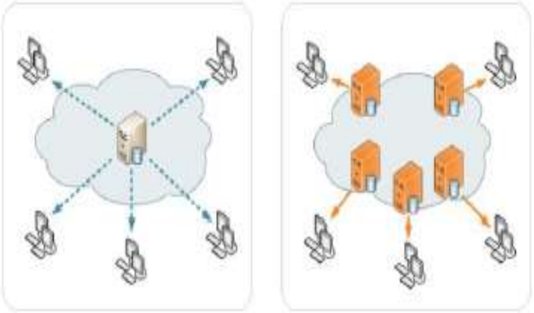


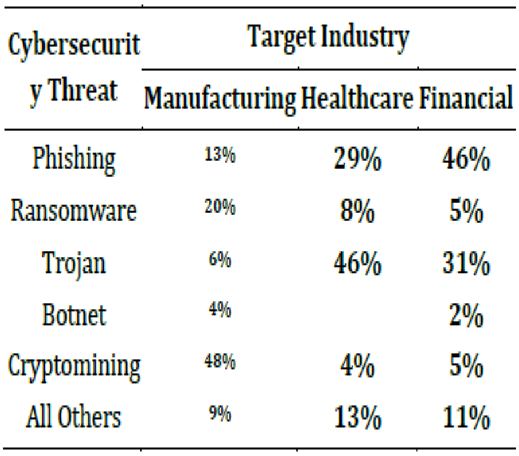
Figure 1: Centralized cloud computing infrastructure (left), decentralized cloud computing infrastructure (right).

II. SECURITY

Users and businesses alike worry about cyber security assaults, data privacy and integrity, and the reliability of cloud computing infrastructure. Various Cyber security Dangers As new technologies emerge, there is a constant emergence of new sorts of cyber security risks. The use of cloud computing is not safe from the same sorts of cyber security risks as on-premises systems, and in some cases is even more vulnerable. The term "phishing" is used to describe an online scam in which the perpetrator poses as a trustworthy entity in order to trick the victim into giving over personal information. The term "ransom ware" is used to describe malicious software or programs that encrypt data or otherwise hold the user's computer or workstation hostage until a ransom is paid or some other demand is met.

In the context of cyber security, a Trojan is a malicious computer program or software that is disguised to look like a legitimate and helpful piece of software, but which, in reality, secretly runs malicious processes designed to record sensitive information and relay it back to the distributor of the Trojan software. Bitnet is short for "bionetwork," which describes a group of computers infected with malicious software and coordinated to do undesired tasks, such as sending out large amounts of spam. One kind of cyber attack is known as a distributed denial of service attack, and its goal is to disrupt a service or resource on a network by overwhelming it with so many requests that it can no longer serve genuine ones. Adware, short for "advertising-supported software," describes harmful applications that purposefully show commercials to generate revenue. Without the knowledge of the user, computers may be used for cryptographic money mining, a process known as crypto-mining. Whoever has installed the crypto mining malware will reap financial benefits as a consequence. The CISCO 2021 Cyber Security Threat Trends study identified crypto-mining assaults as the year's most pressing cyber security concern. The CISCO Cyber Security Threat Trends report's findings are shown in Table 1 below, and they indicate how various industries face varying degrees of vulnerability to various forms of cyber attack since 2020. The financial sector, the healthcare sector, and the manufacturing sector are all compared in the table below.

Table 1 shows the year-over-year growth rates (in percentage terms) of several cyber security threats in 2021. (Amounts split down by the kind of businesses that are the focus of attacks).



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%

The data includes but does not specifically reflect industries that use cloud computing infrastructure to store their data. According to the statistics, phishing is the most prominent cyber security threat, increasing by 88% between 2020 and now. This growth is the result of a combination of increases in individual industries.

Cloud computing is particularly vulnerable to phishing assaults, which may take numerous forms. File-sharing functions are often available in cloud computing environments, and typically take the form of an email link forwarded to the intended recipient. The recipient may think a co-worker has given them a file over the cloud computing infrastructure file sharing, but in reality they are being sent to a spoof document that logs sensitive information. This email may be reproduced and rendered fake. All the aforementioned cyber security risks may affect data stored in classic centralized cloud computing environments. Each cloud provider has its own ways for protecting its cloud against as many of these hazards as possible, and these strategies are not accounted for in the typical cloud computing architecture model. Nonetheless, the paradigm of decentralized cloud computing infrastructures contains numerous inherent security safeguards, most of which are inherited from the block chain networks upon which they are based.

Data Privacy

Users and businesses alike are understandably concerned about maintaining the security of their data while using cloud computing services, given that these services may be accessed from anywhere in the globe. Concerns about data privacy include not just data security in the face of cyber security risks, as described above, but also data privacy in the face of "bad actors," or persons acting independently to obtain and abuse personal data. Encryption techniques may protect sensitive information and keep it private. Data is not always encrypted by default when stored on cloud infrastructure. It is common practice for users and businesses to encrypt data before keeping it in a centralized cloud. Data stored in a decentralized cloud, on the other hand, is encrypted both in transit and at rest. With data spread across several places, it is necessary to encrypt the data independently at each stop along its journey. A shard of data is a single chunk of information from a larger file. Each shard requires the other shards in order to be encrypted and accessed. RiedSolomon erasure coding is the name given to this particular kind of encryption. [3] Erasure coding is shown graphically in Figure 2 as data is stored on several nodes representing various storage resources. While in the past this "grid" might have been a relatively limited network of nodes, in today's decentralized cloud environment, it most often refers to a block chain. Data stored across several nodes is more secure against cyber attacks since it must be compiled before access, and only the person who first submitted the data to the block chain network has access to the data. Since this technology makes data unavailable to anybody accept the data owner, it prevents harmful attempts that aim to steal and keep the content.

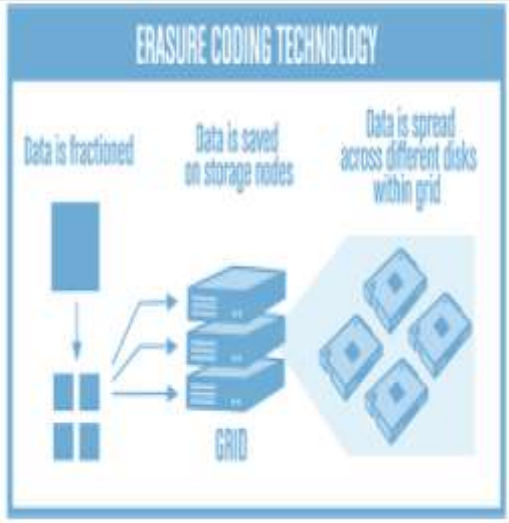

ERASURE CODING TECHNOLOGY
Data is fractioned
Data is saved on storage nodes
Data is spread across different disks within grid
GRID

Figure 2: Visual representation of erasure coding technology.

Data Integrity

One other thing to think about when it comes to cloud computing is the security of your data. [6] Due to the distributed nature of cloud computing, data integrity may be compromised by events like power outages, device failure, and natural disasters. If data is simply saved on the cloud, without any other backup or storage place, data loss is possible due to any of these circumstances. Because of this, many individuals and businesses use what is known as a multi-cloud solution, in which data is stored and backed up by many cloud service providers. Data saved in a centralized cloud computing infrastructure is the only thing to worry about; in a decentralized cloud computing architecture, data is stored utilizing geo-redundancy. The term "geo-redundancy" refers to the strategy of storing data in many geographically dispersed places, such that even if some of the information is lost in one of those sites, the rest of it may still be retrieved. [3]

Guaranteeing that information has not been altered, either maliciously or inadvertently, by any other users is yet another aspect of data integrity. All save the original uploaded have read/write access to data in a decentralized cloud computing architecture. This ensures the content, rather than the physical, integrity of the data. [3] Since every transaction on a block chain-based decentralized cloud infrastructure is documented in great detail, users are able to verify that no unauthorized parties have altered or accessed their data by seeing when it was last edited and by whom.

Centralized Cloud Computing Infrastructure Stability

Cloud outages may be caused by natural catastrophes or power outages in certain areas, which might take down the whole cloud service for an extended period of time. Many businesses and sectors lost money in December of 2021 when the Amazon Web Services US East 1 region went down. Businesses such as Netflix, Disney, and many more were impacted by the outage. [7] Due to this incident, many people started to doubt the reliability of the cloud computing infrastructure and began exploring other methods of data storage and resource hosting.

Decentralized Cloud Computing Infrastructure Stability

When compared to the centralized cloud model, the stability problems associated with decentralized cloud architecture are much reduced. Geo-redundant resources are used in decentralized cloud computing infrastructures so that if one resource or area goes down, traffic may be redirected to another zone where data and resources are still available. [3] This is because, in a decentralized cloud environment, resources and data are automatically replicated across several locations, so that downtime is eliminated unless a sufficient number of locations are also suffering downtime. Sometimes, each branch is situated in a whole distinct area, rather than just a different structure, from the others. Since no one part of the decentralized cloud computing infrastructure is responsible for keeping the whole thing running smoothly, this kind of cloud computing is more reliable than the more conventional centralized models.

Cloud Computing Infrastructure Administration

Administration is always a worry with any service or resource. Hundreds of thousands of pet bytes of data are often stored on the cloud by a single firm, including crucial financial, customer, and tax records. Since the management of the cloud provider has the ability to access or edit sensitive data, the business must have faith in the cloud provider in order to store this information there. Administrators of cloud infrastructure wouldn't intentionally conduct anything bad, but if their accounts were hacked due to lax security measures or a cyber attack (such as phishing), they may be used to commit crimes. While this is a valid worry, many cloud providers have implemented stringent security measures and give extensive security training for their admits to mitigate the risk. However, a distributed cloud computing architecture eliminates this worry. There is no central authority or manager over a block chain network, and no user has greater privileges than any other. Along with the aforementioned data security methods, such as erasure coding and data encryption, this gives piece of mind and better data protection.

III. CONCLUSION

Scalability, user-friendliness, pay-as-you-go pricing, and accessibility are just a few of the advantages of today's cloud computing models. In the realm of cloud computing, there are two distinct sorts of networks: the older, more established network, and the newer, less popular network. The former refers to systems where data is stored and processed by a single entity, while the latter refers to systems where data is stored and processed by several entities. The increasingly popular centralized cloud computing infrastructure architecture provides a single point of data failure, which may lead to security issues, privacy and integrity problems. Due to the use of a block chain network, better data integrity and privacy via encryption and erasure coding, and the elimination of a single point of failure by means of geo-redundancy, the paradigm of decentralized cloud computing infrastructure is inherently secure. By eliminating the central server, all of the problems and security risks of the original centralized cloud architecture are eliminated in the decentralized approach. Although businesses and consumers are using centralized clouds more often at the moment, this is expected to change as more people learn about the advantages of the decentralized cloud and its capacity to keep data safe.

IV. REFERENCES

[1] Foster, I., Zhao, Y., Raicu, I., Lu, S.. Cloud computing and grid computing 360-degree compared. In: Grid Computing 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 Block chain-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, Yinchuan & 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/