e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:04/Issue:01/January-2022 Impact Factor- 6.752 www.irjmets.com

# RESOLVING SECURITY AND DATA CONCERNS IN CLOUD COMPUTING BY UTILIZING A DECENTRALIZED CLOUD COMPUTING OPTION

**Mr. Gopala Krishna Sriram**[*1]

[*1]Software Architect, Edgesoft Corp, Mckinney, TX USA.

## ABSTRACT

There are a variety of security concerns around cloud computing infrastructure technology. Some of these include infrastructure security against threats, data privacy, integrity, and infrastructure stability. In modern cloud computing, there are two models that cloud computing infrastructures follow: centralized cloud computing and decentralized cloud computing. Centralized cloud computing is susceptible to outages, data breaches, and other security threats. Decentralized cloud computing is more resilient to outages due to geo-redundancy technology, and data is better protected by encryption through Reid Solomon erasure coding.

**Keywords:** Security Practices; Cybersecurity; Data Integrity; Cloud Computing; Decentralized Cloud Computing; Blockchain; Geo-Redundancy; Reed Solomon Erasure Coding, Etc.

## I. INTRODUCTION

Cloud computing refers to a computing infrastructure solution where resources such as data storage are delivered as a service that is reference able from anywhere in the world.[1] The most commonly referenced and accepted definition of cloud computing comes from The National Institute of Standards and Technology's (NIST), which defines cloud computing 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".[2] The idea of cloud computing has revolutionized the way that computing infrastructures are developed, deployed, and utilized by users, enterprises, and developers. Cloud computing has evolved and gained popularity due to its desirable attributes such as scalability and elasticity in both infrastructure itself and the cost, with many providers offering pay-as-you-go methods instead of all-encompassing prices, and the increased security and data integrity that comes with cloud infrastructures.

Cloud computing allows services and resources to be consumed using an on-demand method. Resources such as storage or virtualization resources can be accessed from anywhere in the world at a moment's notice. This is different from traditional resource accessibility, where one would have to install hardware to a local workstation or server before beginning to utilize it, and the hardware was limited in its capacity. Cloud resources can be added easily and seamlessly without any manual intervention on local hardware.

By storing data or utilizing resources that are part of cloud infrastructure, resources and data are physically stored in either one geographical location such as a data center, or they are stored in a variety of geographically diverse locations, such as a variety of data centers. Cloud computing infrastructures that have the entirety of data and resources stored in one geographical location are referred to as centralized cloud computing infrastructures, whereas cloud computing infrastructures that have data and resources stored in a variety of different geographical locations are referred to as decentralized cloud computing infrastructures.[3] Figure 1 depicts a visual representation of a centralized cloud computing infrastructure versus a decentralized cloud computing infrastructure.

A blockchain network is a technology infrastructure that is distributed and uses digital ledger technology to encrypt, track, and secure all transactions on the network. Blockchain networks are immutable, meaning every transaction and record that is transmitted over a blockchain network is unable to be changed or edited.[3] This is a layer of security that decentralized cloud computing infrastructures utilize since most decentralized cloud providers build their infrastructures off of blockchain networks. Some of the most common of these networks are the IPFS, Sia, or Storj networks.

Blockchain networks are inherently more secure than traditional networks, which are what most centralized cloud computing infrastructures utilize.

Though cloud computing infrastructures can be used for resources to run virtual machines, containerized

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:04/Issue:01/January-2022 Impact Factor- 6.752 www.irjmets.com

systems, or other virtual systems, this research paper will cover the aspect of storing data within a cloud computing infrastructure and the security concerns relating to data storage.

Since data stored in cloud computing infrastructures can be accessed from anywhere in the world, there are several security concerns and problems associated with using cloud computing, despite the numerous benefits associated with it. The main points of concern regarding cloud computing security include data security, with the first and foremost being user data privacy and protection, data integrity when stored in data center locations, (as opposed to users or enterprises storing their data locally in their workstation environment), cloud computing infrastructure stability, and cloud computing infrastructure administration.[4]

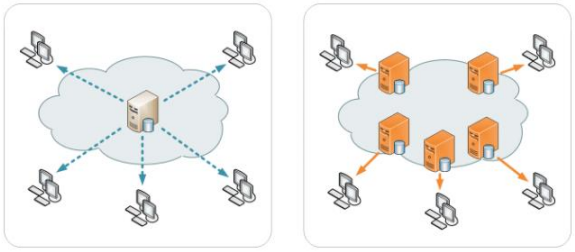

**Figure 1**: Centralized cloud computing infrastructure (left), decentralized cloud computing infrastructure (right).

## II. SECURITY

Regardless of the type of cloud computing infrastructure, users and enterprises alike are heavily concerned with a variety of security concerns, both regarding cybersecurity attacks, data privacy and integrity, and cloud computing infrastructure stability.

**Types of Cybersecurity Threats**

There are new types of cybersecurity threats emerging every day as new technology develops and evolves. Cloud computing is not immune to traditional cybersecurity threats, and in fact, is more susceptible to certain types of threats.

**Phishing:** Phishing refers to the practice of sending fraudulent information or messages that appear to be from genuine, trusted sources in an attempt to elicit sensitive information from the target.

**Ransomware:** Ransomware refers to malicious computer programs or software that prevent the user from using the computer or workstation until a sum of money or another demand is relinquished.

**Trojan**: In Cybersecurity, Trojan refers to a malicious computer program or software that is packaged to appear as if it is a useful, legitimate piece of software but in the background runs malicious processes meant to record sensitive information and relay it back to the distributor of the Trojan software.

**Botnet:** A botnet refers to a private network of computers that have all been infected with a harmful or malicious piece of software and controlled in unison for unwanted activity such as mass distribution of spam messages.

**Distributed Denial of Service**: A distributed denial of service attack refers to a malicious attack meant to disturb a network service or resource by flooding the resource with inbound requests to overload its resources and make it unavailable to legitimate requests.

**Adware:** Adware refers to malicious programs that display advertisements with the intent to sell products or services.

**Crypto-mining:** Crypto-mining refers to the practice of using computers for the mining of cryptocurrency without the user's knowledge. This results in a monetary gain for the party who deployed the crypto mining malicious software.

According to the CISCO 2021 Cyber Security Threat Trends report, the top cybersecurity threat of 2021 was crypto-mining attacks.[5] Table 1 displays the results of the CISCO Cyber Security Threat Trends report, showing the different types of cybersecurity threats and the percentage that each threat type has gone up since 2020, with different percentages based on industry. This table uses the financial, healthcare, and manufacturing industries for comparison.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:04/Issue:01/January-2022 Impact Factor- 6.752 www.irjmets.com

**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% |

Industries that store their data on cloud computing infrastructure are included in this data, though they are not represented individually. Through the data, the threat that had the largest increase overall (all industry percentages together) was the cybersecurity threat of phishing, which was up 88% total from 2020.

Phishing can take many forms and cloud computing is especially susceptible to phishing attacks. Many cloud computing infrastructures include file-sharing options, often in the form of an email link sent to the individual the file is being shared with. This email can be replicated and made fraudulent, leading to successful phishing attacks in which the target believes a colleague has sent them a file through the cloud computing infrastructure file share, only to be led to a false document that records private information.

Data stored in traditional centralized cloud computing infrastructures are susceptible to all of the previously listed cybersecurity threats. The traditional cloud computing infrastructure model does not take into account methods to counteract these threats, and each cloud provider has its own methods for securing its cloud against as many of these threats as possible. The decentralized cloud computing infrastructure model, however, has many innate security measures, with most being measures that are inherited from the blockchain networks that decentralized cloud computing infrastructures are built on top of.

**Data Privacy**

Since cloud computing resources can be accessed from around the world, data privacy is often the foremost concern of users and enterprises. Data privacy concerns include data security in regards to cybersecurity threats as mentioned above, but also data privacy from 'bad actors' or individuals who act independently to access and exploit personal data.

Data privacy can be increased through data encryption methods. When storing data in cloud infrastructure, data is not always encrypted by default. In many cases, when storing data to a centralized cloud, the user or enterprise uploading the data must first encrypt it before uploading it for maximum security. When storing data on a decentralized cloud, however, data is encrypted both in transit and while at rest. Since data is stored in a variety of geographical locations, each piece of a data file is encrypted separately. One piece of a data file is referred to as a shard of data. Each shard is unable to be decrypted or accessed without first being compiled with the other shards. This encryption method is known as Ried Solomon erasure coding. [3] Figure 2 shows a visual example of how data is stored through erasure coding on different storage resources referred to as nodes in this figure. The grid that the data is spread across can be a small network of nodes, but in modern decentralized cloud computing, this grid often refers to a blockchain network. Data stored across a variety of nodes has increased security against cybersecurity threats, as it must be compiled before it can be accessed, and it can only be accessed by the user who uploaded the data to the blockchain network. This technology eliminates malicious attacks that seek to steal and retain data content since data content is inaccessible to anyone but the data owner.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:04/Issue:01/January-2022 Impact Factor- 6.752 www.irjmets.com

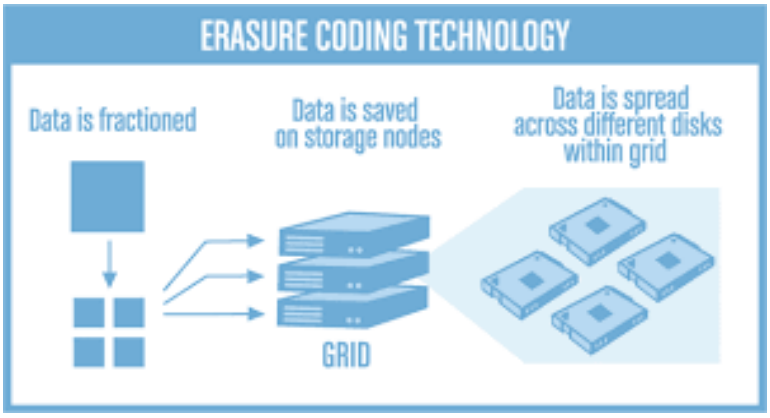


**Figure 2:** Visual representation of erasure coding technology.

**Data Integrity**

Another concern around cloud computing and data stored on it is the integrity of that data.[6] Cloud computing resources are stored in a variety of locations, which may be susceptible to common events that affect data integrity such as power outages, hardware failure, or natural disaster. Any of these factors could affect data integrity, and if data is only stored in the cloud without any secondary backup or storage location, data can be lost. For this reason, many users and enterprises utilize what is known as a multi-cloud solution, where data is replicated across a variety of cloud computing providers for redundancy. This concern only applies to data stored in a centralized cloud computing infrastructure, since decentralized cloud computing infrastructures store data using geo-redundancy. Geo-redundancy is the practice of storing data across a variety of locations, so if one location is susceptible to data loss, the remaining data can still be accessed.[3]

Another attribute to data integrity is assuring that data cannot be changed or edited by other users, intentionally in a malicious way or by mistake. In a decentralized cloud computing infrastructure, data is not mutable by anyone except the user that uploaded the data. This assures that data holds its integrity as far as content, rather than physical integrity.[3] Since every transaction on a decentralized cloud infrastructure that is built on a blockchain network is recorded extensively, users can see exactly when data was modified by themselves and track changes and edits, assuring that no one else has changed or accessed their data.

**Centralized Cloud Computing Infrastructure Stability**

Centralized cloud computing infrastructures are easily affected by geographical outages or disasters, resulting in the cloud infrastructure being offline for a period of time. In December of 2021, many industries and enterprises suffered losses due to an outage of the Amazon Web Services US East 1 region. This outage affected companies such as Netflix, Disney, and thousands of others.[7] This outage caused many to question the stability of the cloud computing infrastructure and look into other options for their data storage and resource hosting.

**Decentralized Cloud Computing Infrastructure Stability**

A decentralized cloud computing infrastructure does not provoke the same stability concerns that the centralized cloud computing model does. Decentralized cloud computing infrastructures use geo-redundant resources, which means that if one resource or region goes down, traffic is routed to another region where data and resources are still accessible and available.[3] This is because decentralized cloud computing replicates resources and data across different locations automatically, eliminating outages unless a significant amount of the locations are experiencing outages. Each location is often located in drastically different places than the other locations, such as in entirely different locations rather than just different buildings. This means there is no single point of failure for a decentralized cloud computing infrastructure, giving decentralized cloud computing high stability in comparison to traditional centralized cloud computing infrastructures.

**Cloud Computing Infrastructure Administration**

With any resource or service, the administration of the service or resource is always an area for concern. Cloud computing is often utilized for storing hundreds of thousands of petabytes of data per enterprise, which often includes vital business records such as revenue, customer data, and tax data. Storing this kind of data on a cloud computing infrastructure requires that the enterprise trusts the administration of the cloud provider since they

have the means to access or modify that data. Cloud infrastructure administrators would not in good conscience do something of that nature, but if their accounts were to be compromised due to poor security practices or cybersecurity attacks such as phishing, their accounts could be used for malicious activity. For this reason, many cloud providers have heavy security and security training for their administrators to avoid this scenario, though it remains a concern of users and enterprises alike.

This concern, however, is not applicable to a decentralized cloud computing infrastructure. Blockchain networks are not centrally administrated or managed, and no individual user has access to more permissions than another on a blockchain network. This provides peace of mind and increased data security, along with the aforementioned data security measures such as erasure coding and data encryption.

## III. CONCLUSION

Modern cloud computing has numerous benefits, such as scalability, ease of use, cost-saving pay-as-you-go methods, and universal accessibility. There are two types of cloud computing infrastructures, one that is known as the traditional and most widely used and accepted infrastructure, and another more recently developed and less used infrastructure. These are the centralized cloud computing infrastructure and the decentralized cloud computing infrastructure respectively. The centralized cloud computing infrastructure model is more widely used, but has several security risks, data privacy and integrity concerns, and has a single point of data failure. The decentralized cloud computing infrastructure model has innate security due to its blockchain network utilization, increased data integrity and privacy through encryption and erasure coding, and no single point of failure through geo-redundancy. The decentralized cloud computing model solves all the flaws and concerns associated with the traditional centralized cloud computing model. Though right now the decentralized cloud is less utilized by consumers and enterprises alike, that is likely to change given the number of benefits that come with the decentralized cloud and its ability to protect and secure data.

## 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 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/