Academic Writing

for Beginners

Final Exam

学　号 (Student ID No.): 199076003

姓　名 (Name): Arafat Hosen

专　业 (Program): Software Engineering

研究方向 (Research Field): Cloud Computing

导师姓名 (Supervisor Name): SHANG Laping

安徽工业大学国际教育学院

School of International Education, Anhui University of Technology

2022 年(year) 12 月(month)

Research Proposal

By bachelor candidates
At
Anhui University of Technology

Research Proposal

1.论文题目 Thesis Title	Resolve security and data for the cloud computing by decentralized option.

2.摘要 Abstract:

Cloud computing has been established as a technology for furnishing requirements- acquainted and use-dependent IT coffers, which now are being used more constantly for business information systems. Particularly in terms of integration of decentralized information systems, cloud systems are furnishing a stable result approach. Still, data security is one of the biggest challenges when using cloud systems and a main reason why numerous companies avoid using cloud services. The question we're facing is how cloud systems for integration of decentralized information systems have to be designed, in terms of technology and association, so that sequestration laws of the cloud stoner can be guaranteed. This donation summarizes the results of a system comparison of decentralized cloud systems in social networks, a conditions analysis grounded on a literature analysis, and a model for organizational situations of cloud systems, deduced from the conditions analysis. There are a variety of security enterprises around cloud computing structure technology. Some of these include structure security against pitfalls, data sequestration, integrity, and structure stability. In ultramodern cloud computing, there are two models that cloud calculating architectures follow centralized cloud computing and decentralized cloud computing. Centralized cloud computing is susceptible to outages, data breaches, and other security pitfalls. Decentralized cloud computing is more flexible to outages due to geo redundancy technology, and data is better defended by encryption through Reid Solomon erasure coding.

3.摘要 Key words:

Cybersecurity, Data Integrity, Cloud Computing, Decentralized Cloud Computing, Blockchain.

4. 引言 Introduction:

Cloud computing allows services and coffers to be consumed using an on- demand system, coffers similar to storehouse or virtualization coffers can be penetrated from anywhere in the world at a moment’s notice. This is different from traditional resource availability, where one would have to install a tackle to an original workstation or garçon before beginning to use it, and the tackle was limited in its capacity. Cloud Coffers can be added fluently and seamlessly without any homemade intervention on original tackle. By storing data or exercising coffers that are part of cloud structure, coffers and data are physically stored in either one geographical position similar to a data center, or they're stored in a variety of geographically different locales, similar to a variety of data centers. Cloud computing architectures that have the wholeness of data and coffers stored in one geographical position are pertained to as centralized cloud calculating architectures, whereas cloud computing architectures that have data and coffers stored in a variety of different geographical locales are pertained to as decentralized cloud calculating architectures. There depicts a visual representation of a centralized pall calculating structure versus a decentralized Cloud Calculating structure. A blockchain network is a technology structure that's distributed and uses digital tally technology to encrypt, track, and secure all deals on the network. Blockchain networks are inflexible, meaning every sale and record that's transmitted over a blockchain network is unfit to be changed or edited. This is a subcaste of security that decentralized cloud computing architectures use since utmost decentralized cloud providers make their architectures off of blockchain networks. Some of the most common of these networks are the IPFS, Sia, or Storj networks. Blockchain networks are innately more secure than traditional networks, which are what utmost centralized cloud computing architectures use.

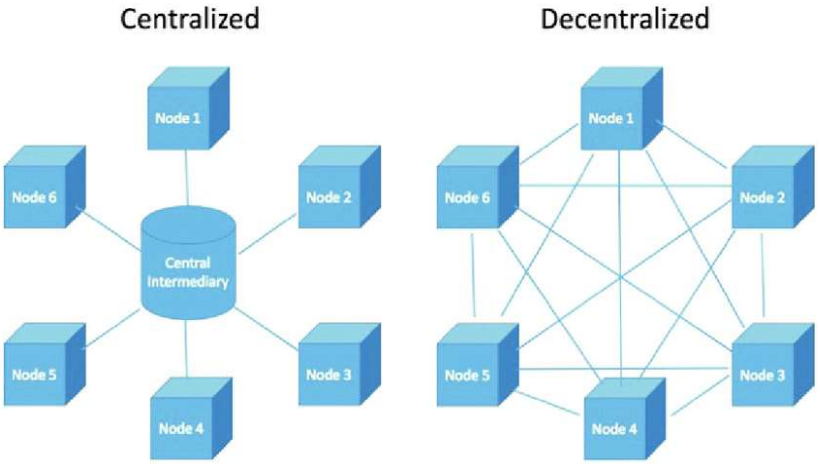

Figure 1: Centralized cloud computing infrastructure (left), decentralized cloud computing infrastructure (right).

5. 文献综述 Review of literature:

Security:

Regardless of the type of cloud computing infrastructure, there are different information security issues of great concern to users and businesses that relate to cyber security attacks, data protection and integrity, as well as the stability of cloud computing infrastructure. Types of Cyber Security Threats As new technology develops and evolves, new types of cyber security threats emerge every day. Cloud computing is not immune to traditional cyber security threats and is actually more susceptible to certain threats. Phishing: Phishing is the act of sending fraudulent information or messages that appear to be from genuine and reliable sources with the intention of obtaining sensitive information from the target. Ransomware: Ransomware refers to malicious computer programs or software that prevent a user from using a computer or workstation until a sum of money or other demand is transferred. Trojan: In cybersecurity, a Trojan refers to a malicious computer program or software packaged with code that appears to be useful, legitimate software, but runs malicious processes in the background to store sensitive information and transmit it to the distributor. trojan Botnet: A botnet refers to a private network of computers infected with malicious or malicious software and controlled together to engage in unwanted activity such as mass distribution of spam. Distributed Denial of Service Attack: A distributed denial of service attack refers to a malicious attack designed to disrupt a network service or resource by flooding the resource with incoming requests to overload its resources and prevent legitimate requests from being accepted. Adware: Adware refers to malware that displays advertisements with the intention of selling products or services. Cryptomining: Cryptomining is the use of computers to mine cryptocurrency without the user's knowledge. This results in financial gain for the party deploying the crypto mining malware. According to the CISCO 2021 Cybersecurity Threat Trends Report, the top cybersecurity threat in 2021 was cryptomining attacks.[5] Table 1 shows the results of the CISCO Cybersecurity Threat Trends Report and the different security threats. The percentage of each threat type has increased since 2020, , by different percentages across industries. This table uses financial, healthcare and manufacturing industries for comparison. Industries that store their data in a cloud computing infrastructure are included in this data, although they are not represented separately. According to the data, the cybersecurity threat of phishing has grown the most (all economic sectors combined by , percent), which has grown by a total of 88% since 2020. Phishing can take many forms and cloud computing is particularly vulnerable to phishing attacks. Many cloud computing infrastructures include file sharing options, often in the form of an email link sent to the person to whom the file is shared. This email can be copied and forged, leading to successful phishing attacks where the target believes a colleague has sent them a file via cloud computing infrastructure file sharing, resulting in a fake document that stores private information. Data stored in traditional centralized cloud computing infrastructures is vulnerable to all the cyber security threats listed previously. The traditional cloud computing infrastructure model does not consider methods to combat these threats, and each cloud provider has its own methods to protect the cloud from as many of these threats as possible. However, the distributed cloud computing infrastructure model includes many proprietary security measures, most of which are inherited from the blockchain networks on which distributed cloud computing infrastructures are built.

Table: 2022 Percentage of Increase for Different Cybersecurity Threats Since 2021. (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%	0%	2%
Cryptomining	48%	4%	5%
All Others	9%	13%	11%

6. 研究方法 Research Methods:

Data privacy: Since cloud computing coffers can be penetrated from around the world, data sequestration is frequently the foremost concern of druggies and enterprises. Data sequestration enterprises include data security in regards to cybersecurity pitfalls as mentioned over, but also data sequestration from ‘ bad actors ’ or individualities who act singly to access and exploit particular data. Data sequestration can be increased through data encryption styles. When storing data in cloud structure, data isn't always translated by dereliction. In numerous cases, when storing data to a centralized cloud, the stoner or enterprise uploading the data must first cipher it before uploading it for maximum security. When storing data on a decentralized cloud, still, data is translated both in conveyance and while at rest. Since data is stored in a variety of geographical locales, each piece of a data train is translated independently. One piece of a data train is pertained to as a shard of data. Each shard is unfit to be deciphered or penetrated without first being collected with the other shards. This encryption system is known as Reed Solomon erasure coding. [3] Figure 2 shows a visual Illustration of how data is stored through erasure rendering on different storehouse coffers pertained to as bumps in this figure. The grid that the data is spread across can be a small network of bumps, but in ultramodern decentralized cloud computing, this grid frequently refers to a blockchain network. Data stored across a variety of bumps has increased security against cybersecurity pitfalls, as it must be collected before it can be penetrated, and it can only be penetrated by the stoner who uploaded the data to the blockchain network. This technology eliminates vicious attacks that seek to steal and retain data content since data content is unapproachable to anyone but the data proprietor. Data Integrity Another concern around cloud computing and data stored on it's the integrity of that data. [6] cloud computing coffers are stored in a variety of locales, which may be susceptible to common events that affect data integrity similar as power outages, tackle 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 storehouse position, data can be lost. For this reason, numerous druggies and enterprises use what's known as a multi-cloud result, where data is replicated across a variety of cloud computing providers for redundancy. This concern only applies to data stored in a centralized cloud calculating structure, since decentralized cloud computing architectures store data using geo- redundancy. Geo-redundancy is the practice of storing data across a variety of locales, so Still, the remaining data can still be penetrated, if one position is susceptible to data loss. [3] Another trait to data integrity is assuring that data can not be changed or edited by other drugs, designed in a vicious way or by mistake. In a decentralized cloud calculating structure, data isn't variable by anyone except the stoner that uploaded the data. This assures that data holds its integrity as far as content, rather than physical integrity. [3] Since every sale on a decentralized cloud structure that's erected on a blockchain network is recorded considerably, druggies can see exactly when data was modified by themselves and track changes and edits, assuring that no bone differently has changed or penetrated their data.

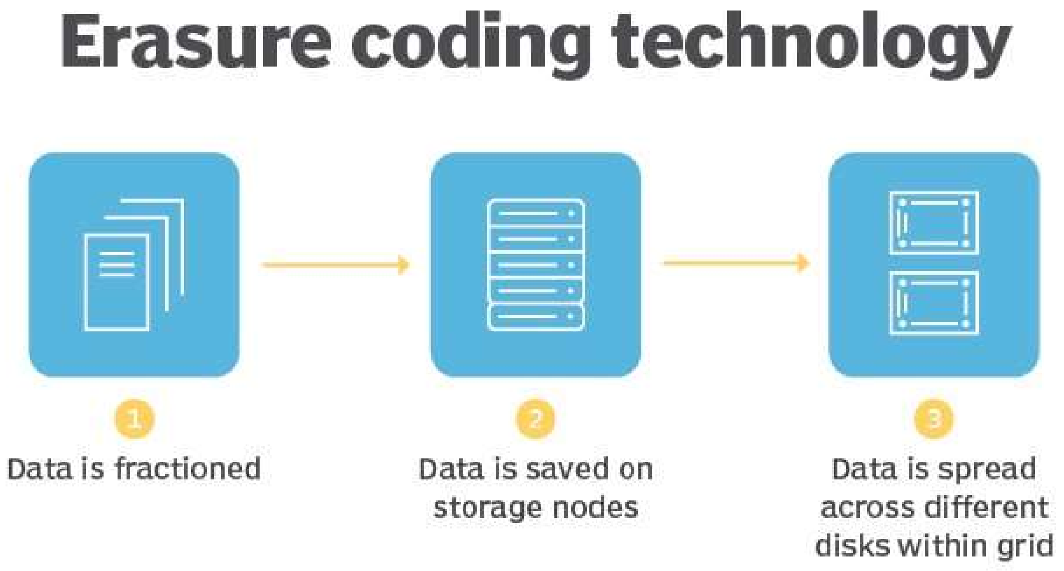
Erasure coding technology
1
Data is fractioned
2
Data is saved on storage nodes
3
Data is spread across different disks within grid

Figure 2: Visual representation of erasure coding technology.

7. 预期的成果 expected results:

Centralized Cloud Computing structure Stability:

Centralized cloud calculating architectures are fluently affected by geographical outages or disasters, performing in the cloud structure being offline for a period of time. In December of 2021, numerous diligence and enterprises suffered losses due to an outage of the Amazon Web Services US East 1 region. This outage affected companies Similar as Netflix, Disney, and thousands of others. This outage caused numerous to question the stability of the cloud calculating structure and look into other options for their data storehouse and resource hosting.

Decentralized Cloud Computing structure Stability:

A decentralized cloud calculating structure doesn't provoke the same stability enterprises that the centralized cloud calculating model does. Decentralized cloud computing architectures use geo-spare coffers, which means that if one resource or region goes down, business is routed to another region where data and coffers are still accessible and available. [3] This is because decentralized cloud calculating replicates coffers and data across different locales automatically, barring outages unless a significant quantum of the locales are passing outages. Each position is frequently located in dramatically different places than the other locales, similar as in entirely different locales rather than just different structures. This means there's no single point of failure for a decentralized cloud calculating structure, giving decentralized cloud computing high stability in comparison to traditional centralized cloud calculating architectures. Cloud Computing structure Administration With any resource or service, the administration of the service or resource is always an area for concern. Cloud computing is frequently employed for storing hundreds of thousands of petabytes of data per enterprise, which frequently includes vital business records similar to profit, client data, and duty data. Storing this kind of data on a cloud Calculating structure requires that the enterprise trusts the administration of the cloud provider since they've the means to pierce or modify that data. Cloud structure directors would not by good heart do commodities of that nature, but if their accounts were to be compromised due to poor security practices or cybersecurity attacks similar to phishing, their accounts could be used for vicious exertion. For this reason, numerous cloud providers have heavy security and security training for their directors to avoid this script, though it remains a concern of druggies and enterprises likewise. This concern, still, isn't applicable to a decentralized cloud calculating structure. Blockchain networks aren't centrally conducted or managed, and no individual stoner has access to further warrants than another on a blockchain network. This provides peace of mind and increased data security, along with the Forenamed data security measures similar as erasure coding and data encryption.

8. 结论 Conclusion：

Modern cloud computing has multitudinous benefits, similar as scalability, ease of use, cost-saving pay- as- you- go styles, and universal availability. There are two types of cloud computing architectures, one that's known as the traditional and most extensively used and accepted structure, and another more lately developed and less habituated structure. These are the centralized cloud calculating structure and the decentralized cloud Calculating structure independently. The centralized cloud calculating structure model is more extensively used, but has several security pitfalls, data sequestration and integrity enterprises, and has a single point of data failure. The decentralized cloud calculating structure model has inherent security due to its blockchain network application, increased data integrity and sequestration through encryption and erasure coding, and no single point of failure through geo- redundancy. The decentralized cloud calculating model solves all the excrescences and enterprises associated with the traditional centralized cloud calculating model. Though right now the decentralized cloud is less employed by consumers and enterprises likewise, that's likely to change given the number of benefits that come with the decentralized cloud and its capability to cover and secure data.

9. 参考文献 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://learnumbrella.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.

[8] Statista (2015) Einsatz von Cloud Computing in deutschen Unternehmen bis 2015 Umfrage Statista, Accessed 18 Aug 2016.

[9] IDC (2015) IDC Studie: Hybrid Clouds nehmen angesichts der digitalen Transformation Fahrt auf in deutschen Unternehmen, Accessed 5 Aug 2016.

[10] BITKOM (2014) Wie Cloud Computing neue Geschäftsmodelle ermöglicht, Accessed 18 Aug 2016

[11] Ropohl G (2009) Allgemeine Technologie. Eine Systemtheorie der Technik. Universität Karlsruhe Universitätsbibliothek, Karlsruhe.

[12] BMBF: Die neue Hightech-Strategie: Innovationen für Deutschland (2014).

[13] BMWi, BMI, BMVI: Digitale Agenda 2014–2017. München (2014).

[14] Atzori L, Iera A, Morabito G (2010) The Internet of Things: A survey. Comput Netw 54:2787–2805.

[15] Beetz K (2010) Die wirtschaftliche Bedeutung von Cyber Physical Systems aus der Sicht eines Global Players. In: Broy M (ed) Cyber-Physical Systems. Springer, Berlin Heidelberg, pp 59–66.

[16] Software-Cluster (2015) Emergente Software, Accessed 24 Nov 2015.

[17] Vaquero LM, Rodero-Merino L (2014) Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. SIGCOMM Comput Commun Rev 44:27–32.

[18] TecChannel (2014) Cloud Computing - der deutsche Mittelstand hinkt hinterher - TecChannel-Studie TecChannel.de, Accessed 29 Jan 2016.

[19] Smith M, Szongott C, Henne B, Voigt Gv (2012) Big data privacy issues in public social media. In: 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp 1–6.

[20] Gregory RW, Muntermann J (2014) Research Note—Heuristic Theorizing: Proactively Generating Design Theories. Inf Syst Res 25:639–653.

[21] Venable J, Pries-Heje J, Baskerville R (2014) FEDS: a Framework for Evaluation in Design Science Research. Eur J Inf Syst 25:77–89.

[22] Laudon KC, Laudon J.P, Schoder D (2009) Wirtschaftsinformatik: Eine Einführung. Pearson Studium, München.

[23] Heinrich L.J., Heinzl A, Riedl R. (2010) Wirtschaftsinformatik: Einführung und Grundlegung. Springer, Berlin.

[24] Moore JF (1997) The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems. Harper Paperbacks, New York.

[25] Erklärung von Montreux: Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt. 27. Internationale Datenschutzkonferenz in Montreux, Montreux (2005).

[26] Yeung C-MA, Liccardi I, Lu K, Seneviratne O, Berners-lee T (2009) Decentralization: The future of online social networking. In: In W3C Workshop on the Future of Social Networking Position Papers.

[27] Buchegger S, Schiöberg D, Vu L-H, Datta A (2009) PeerSoN: P2P Social Networking: Early Experiences and Insights. In: Proceedings of the Second ACM EuroSys WS on Social Network Systems. ACM, New York, pp 46–52.

[28] Zhang L, Mislove A (2013) Building Confederated Web-based Services with Priv.Io. In: Proceedings of the First ACM Conference on Online Social Networks. ACM, New York, pp 189–200

[29] Cutillo LA, Molva R, Strufe T (2009) Safebook: A privacy-preserving online social network leveraging on real-life trust. IEEE Commun Mag 47:94–101.

[30] Sharma R, Datta A (2012) SuperNova: Super-peers based architecture for decentralized online social networks. In: 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS), pp 1–10.