International Research Journal of Multidisciplinary Sciences **ISSN:Awaited**
Volume 1 issue 1 jan 2025 PP 19-31

RESEARCHSTUDYONCHALLENGESIN CLOUD COMPUTING

PriyaGupta
Computer Science,
ChristUniversity,Bangalore.
priya.gupta@mca.christuniversity.in

Abstract
Cloud computing is a recent development in the world of Information Technology offering IT capabilities as services. It involves parallel computing, distributed computing, grid computing, and virtualizationtechnologies. The current method of storing data and other essential resources that organizations wish to easily and securely access is called cloud computing. Innovative investing options are provided by this. The best part is that you may create a firm and take over IT operations without incurring significant upfront fees. Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations.Cloud computing has potential, but it also has a number of security flaws. Among them include account theft, data breaches, malware injections, data recovery, harmful insider attacks, data segregation, a lack of investigative help, and general vulnerabilities. Security and privacy, applicationproblems,accessibility,constantchange, interoperability problems, service level agreements, and data center problems are just a few of the difficulties that cloud computing faces.

Keywords
Datasecurity,cloudcomputing,dataprivacy,data breach,security issues, data availability, data integrity.

INTRODUCTION
Cloud computing is a new generation technology that provides the users access to storage, infrastructure,software and environment deployment.Byallowingthirdpartiestohostalldata and application storage devices, cloud computing is a cutting-edge method of storing data and application software. By simply connecting to the

Internet,newtechnologieshaveenabledusto access our information and resources fromanywhere in the globe.Cloudcomputingisthecontemporarymethod of storing data and other vital resources that organizations wish to access securely and conveniently, from small firms to major corporations. Innovative investment opportunities are provided by cloud computing, particularly for startups. Now, it's possible to take over IToperations without having to pay a lot up front. Other important advantages of this breakthrough include robustness, high flexibility and scalability, andtheopportunityforbusinessestooutsourcenon-core operations.One of the other largest outward uses of Cloud calculating is the mobility that it brings,Bothtothepleasurableuser,aswellastothe commercial and business user. The most famous cloud computing services are including Amazon Web Services, Google Cloud platform and Microsoft Azure. Cloud-based services are models for businesses with increasing or changeable bandwidth demands. If your requirements increase, it’s easy to rule up your cloud capacity, drawing on the service’s remote servers.

CHALLENGESINCLOUD COMPUTING

TheauthorsofResearchPaper[1]providean overview of the difficulties and possibilities associated with cloud computing. These difficulties have been divided by the authors into six key categories. Despite the fact that cloud service providersoffer Iaas, Paas, andSaasservices, serious difficulties and challenges have been identified. Domains include things like resource distribution, load balancing, data management, accessibility, scalability,compatibility,andinteroperability.These elements reduce the cloud's effectiveness.

In paper[2]theygoovermanybenefitsandlimitless

informationmechanismsbutitalsohasseveralissues and problems like Government grant and assistance towards cloud based models is an emerging issue. Connection and speed in MB and GB format is an emerging issue. It needs front and backbones infrastructure and appropriate quality of services. Cloud computing needs high quality broadband connectionotherwisethewholeeffortwillbevalued less.Manycloudcomputingservicesarecostlysofor developing countries like India this is an emerging issue.

The Research Paper [3] discusses different challenges related to cloud computing. The researchers have discussed the evolution of cloud services, different types of clouds, deployment models, relationships between SOC and Grid Computing and Cloud Adoption Challenges. The paperspeaksindetailaboutthecloudinteroperability issue. Sincethe main focus isonchallenges, let'sgo through specific cloud adoption challenges and terminologies based on interoperability issues.The paperdiscussesdifferentcloudcomputingplatforms like AbiCloud, Eucalyptus, Nimbus, OpenNebula.

Inpaper[4]discussestheCloudComputingAccess Control, Secure Data Destruction.
Access control is an important security strategy in cloud computing to assure data protection. It guarantees that onlyauthorized users have access to the requested cloud-based data. There are several security mechanisms available in cloud computing that enable effective access control. Intrusion detection systems, firewalls, and separation of responsibilities can be placed on distinct network andcloudtiers. Becauseofthe firewall, onlylimited contentispermittedtoaccessthecloud.Thefirewall is often set in accordance with the user's security policies.Secure Data Destruction: When it comes to data destruction, it must be done carefully. If data deletion is not safeguarded, there is a danger ofdata leaking. When data is not properly erased, it can be recovered by anybody. When classified andsensitive data is stored in the cloud and the vendor fails to properly remove the data from dead equipment, the data is unnecessarily jeopardized.
The goal of the data deletion service is to entirely erasesensitiveorcriticaldata.Thisisaccomplished through the use of third-party or proprietary

software. Following this procedure, it is assumed thatthedatacannotberetrievedandutilizedforany illegal or fraudulent reasons.

This paper [5] is about a cloud infrastructure called C-CLOUD that allows people to rent out computing resources,includingresourcesthatarenotpartofany cloud infrastructure. C-CLOUD enables a huge amount of resources to be rented out, which allows resource owners to earn money from idle resources, andclouduserstohaveacheaperalternativetolarge cloud providers. C-CLOUD has two keychallenges: ensuringthattheresourcesarereliableandproviding an incentive for people to share their resources. C-CLOUD is designed to work like modern cloud infrastructure-as-a-service, but it is hosted on resourcesthatmaynotbereliable.Majorproblemsin deployment are based onthe interactionbetweenthe C-CLOUD and the shared resources for periodically checking the resource status such as capability, reliability,availability,etc.Thiscanbeovercome by volunteer computing.

In paper [6], the authors discuss a case study on the company that was trying to figure out if they could use cloud storage to help them better understand oil fieldsand howto get hydrocarbonsout ofthem. The pilot project involved developing a secure software model that can be used by different vendors, which would be more efficient and reliable. The project faced delays in getting buy-in and agreement on intellectual property rights, as well as design challengesdueto securityrequirements.Politicswas the most common issue mentioned by interviewees, with 66.7% of respondents saying it was an issue. Project management was the second most common issue, with 37.5% of respondents saying it was an issue. Contracts and processes were tied for third, with 20.8% of respondents saying they were issues. Otherkeyissuesmentionedincludedthecapabilityof staff, lackofclear KPIstomeasure, and information security.

In paper [7], the authors propose a new solution for pricingcloudservices,basedonvalue-basedpricing. Thismeanstakingintoaccountnotonlyhowmuchit costs the service provider to offer the service (intrinsic value), but also how much the customer is willing to pay for it (extrinsic value). They demonstrate that this can capture the value of non-marketablefeatures,whichtraditionalpricingmodels oftenignore.Theyalso showthattheaverageannual growthrateofAmazonWebServicesisfarslower

than Moore's Law. The primary goal of the research is to provide a less biased pricing model for cloud decision makers to develop their optimizing investment strategy.

In paper[8] the author discusses the End to End Availability of Cloud Computing. The general requirements for Cloud Computing is service availability , service reliability and quality assurance.The main purpose ofthis paper is to draw more attention to clarify the definition of service availabilityandtoevaluateend-to-endavailabilityof cloud service infrastructure. And the general consideration will be detailed for cloud service "Desktop as a Service"(DaaS). DaaS is a cloud computing service category in which capabilities providedtothecloudservicecustomeraretheability tobuild,configure,manage,storeandexecuteauser's desktop function remotely.

SECURITYCHALLENGESINCLOUD COMPUTING

The Research Paper [9] centered on the privacy and security of private data stored in the cloud.
The authors provide a succinct description of cloud computingandoutlineitsfeatures.Next,theydiscuss difficulties with cloud security and privacy.
Data leaks and loss are two securityrisks associated with cloud computing. The main causes of these dangers are problems like multi-tenancy. Cloud computing security challenges include multi-tenancy, loss of control, and trust chain.
Additionally, they looked into how handling sensitive data affects privacy. Concerns about privacyhavearisenasaresultofsecuritydifficulties.
There have been numerous attempts to work around the privacy issues.
The authors have also researched solutions that can enhance the security of the data stored on the cloud.These solutions include, Authentication and Authorization, Identity and Access Management, Confidentiality, Integrity and Availability, Security Monitoring and Incident Response, Security policy management,Data Transmission, Network Security, Data Segregation and Patch Management.These are some solutions that can be effective in terms of effectiveness in order to secure the data.

This Research Paper [10] focused on Security and PrivacyIssuesinCloudComputing.Theauthorgives a brief intro to cloud computing. After a brief introduction, theauthorexplainsthecharacteristics of cloud computing. Theyexplainthe cloud computing models, i.e., Iaas, Paas, and Saas.

[11] Cloud service providers need to inform their customers on the level of security that they provide on their cloud.One of the biggest security worries with the cloud computing model is the sharing of resources In this paper, we first discussed various models of cloud computing, security issues and research challenges in cloud computing and later on discussedabouttheattacksrelatedtotheproblemlike Release of Message Contents, Traffic Analysis, ProblemRelatedtoActiveAttacks,Problemsrelated toSessionLevelDOS,ProblemrelatedtoDictionary Attacks.DenialofService attacksare deeplyanalyzed in port, session and service levels by making either server service is temporarily stopped or making service slow.

The topic in paper[12] enlightens that deploying data-centric applications in a multi-user cloud environment presents a number of challenges, includingmakingsurethatallqueryprocessingand data sharing are done securely. To accomplishthis, participating parties must be authenticated and authorized, and user-specified access control policies must be strictlyenforced. Furthermore,the access control language should be sufficiently flexible to meet the needs of a large range of applications.

The topic in paper[13] presents that the usage of outdated cryptographic algorithms by a developer may expose important data that was encrypted but could be hacked due to an algorithmic flaw. This poses a problem for the cloud provider in the event ofdataleaks involvingconsumer datathathasbeen harmedbyalgorithms.Sensitivedataisdeliveredin a huge number of packets while data in the cloud goes across a specialized network to and from a particular location.Amalicioususercanusepacket sniffing to intercept and examine the data included in the packets carried across this network.

Inpaper[14]theyarediscussingabout CLOUD COMPUTING SECURITY THREATS

Databreaches:Themostessentialthingistoavoid data breaches. The difficulty in dealing with the

concerns of data loss and data leaking is that "solutions put in place to ameliorate one might aggravate the other." Data is encrypted to mitigate the consequences of a violation, but if theencryption key is lost, the data is destroyed.Data Loss/Leakage:Some methodsofcompromisingdata owing to poor authentication, authorization, and audit (AAA) measures, such as record deletion or changewithoutabackupoftheoriginalinformation, exist. The loss of an encoding key may result in effective destruction. Unauthorized individuals may obtain access to critical information. A hostile hacker may remove data from a target.Account or service hijacking: Various hijacking tactics, such as phishing, fraud, and exploiting software flaws, are still in use. If an attacker has access to user credentials, he may monitor user activity and transactions, altering data, inserting false information, and redirecting user clients tomalicious websites.APIs with insecure Application Programming Interfaces: These interfaces must be developed to safeguard the user from both unintentional and malicious efforts..Malicious insiders: A supplier may not divulge how it grants workers access to physicaland virtualassets, how it watches these employees, or how it analyzes them. The organization does not need to understand the technicalintricaciesofhowtheservicesaresupplied with cloud computing. The danger is high in these circumstances.Yourfirmmayalso be jeopardized if you do not have complete understanding and control.Unknown risk Profile: In order to determine an organization's security status, some important factors to consider include software versions, code modifications, security policies and applications, vulnerability reports, interference attempts, and securitydesign, as well as information about who is sharing your infrastructure.Cloud abuse: Some services allow free short trial periods. Spammers, harmful code developers, and other criminals are ready to perform their operations with relevant weaknesses, such as password and key cracking, at this moment. A hostile hacker uses cloud servers to launch a Distributed Denial of Service (DDoS) attack,spreadmalware,or distribute illegallycopied software..Shared TechnologyIssues: (IaaS) is based onsharedinfrastructure(e.g.storagepartitions,CPU caches, GPUs, etc.), which was not designed to provide good isolation features for a multitenant architecture. A virtualization hypervisor mediates access between guest operating systems and, as a result, physical computational resources.

[15] Cloud computing has become one of the trendiestsubjectsinthecomputingprofession,with

its progress supporting huge changes in the worlds of both computers and business. However, as cloud computing security concerns become more prominent, they cannot be disregarded, particularly data security and privacy protection in the cloud computing environment. This article presents the ideaanddistinguishingfeaturesofcloudcomputing, as well as security challenges and tactics in the virtual cloud environment. Furthermore, it offers to create a single-line connection between the virtual machine and the client using digital certificate technology and Elliptic Curves Cryptography, examinesthemathematicaltheoryofEllipticCurves Cryptography, and defines the communication process between the virtual machine and the client, so that users' private data may be protected and isolated in the cloud environment, and cloud computing technologycan provide users with much stronger security.

[16] In this paper, they covered all cloud computing security issues and how to possibly avoid them. For them to work with cloud architectures, new security technologies must be developed and old ones fundamentallyoptimized.Theybelievethatindustry is the main application area for cloud services. The reportexaminescloudusageinfivemajorindustries, along with his increase in cloud usage from 2015 to 2017. Last but not least, his entire IT industry is looking forward to the process ofhis automation, so we'll see how our imagination continues, and the basicsofwhat wewillface inthefuture.providedan overview of what the security issues are. Since automation in cloud computing is an ideal process thatneedsmoreclarityandresearch,wehopethatour research will give us a better understanding of the design challenges of cloud computing and will inform future research in this area.

[17] Thepaperexplainsterminologiesrelatedtocloud and cloud security attacks. Attacks include Guest-hopping attacks, SQL injections, Side Channel Attacks, Malicious Insider, Data Storage Security and ARP Cache Poisoning. Cloud Service Providers (CSP)mustmaintainahighlevelofphysicalsecurity, includingaccesscontrollimitedtoauthorizedpeople. Cloud computing primarily relies on the infrastructureofLAN, MAN, andWAN. Man-in-the-

middle attacks, domain squatting, and ARP cache poisoning are some types of attacks.
Attacks against cloud users include phishing, fraud, and the use of software flaws. There should be varioussolutionstominimizethedrawbacksofcloud computing platforms

[18] Cloud computing includes numerous levels of abstractionand technology, whichcomplicates system integrityanddrawsonesecurityproblemafteranother. Each layer of the cloud has its own set of vulnerabilities, therefore any flaw in software or hardware poses severe problems with cloud computing. In a distributed computer system, vulnerabilities are relatively widespread. To solvesuch issues, strong security policies must be implemented that are globally standard and generalized across all layers of cloud services and deployment types. Security and privacy remain key concernsincloudcomputing,withseveraldangersand obstacles that require considerably more attentionfrom academics and business.

This Research Paper [19] is about data security and its solution in cloud computing. The author talks about the security issues faced by cloud service providers.The author starts by introducing cloud computing and then moves to challenges in cloud computing. He addressesthe challenges byreferring to pictures, facts, and flowcharts.
Dataprotectionisthemost essentialandchallenging step incloud computing. The securityofdata should be done with utmost care. By mentioning the issues or challenges, the author also provides some solutions.Itisessentialtoprovideadifferentlevelof security to enhance the security in a cloud. Starting from authentication, authorization, and access control for the data stored on the cloud.
There are three main areas in data security: **Confidentiality**, a measure that the dataisprotected from any attacks. **Integrity**: is a measure that deals withproviding securitytothe client'sdata,i.e., users should not storetheirdata,suchaspasswords,onthe cloudsothatintegritycanbeassured**Availability**:as the user requests their data, it should be readily available without downtime, lag, or anyother issue.

[20] ISSUES WITH SECURITY Cloud service models not only give various sorts of services to customers, but they also divulge information that contributes to the security challenges and vulnerabilities associated with cloud computing systems.IaaSisabottom-layerservicethatdirectly

delivers the most powerful capabilities of a whole cloud. IaaS also enables hackers to carry out attacks thatneedalargeamountofcomputationalpower,such asbrute-forcingcracking.IaaSsupportsseveralvirtual computers,makingitanexcellentplatformforhackers to undertake attacks that need a large number of attacking instances. Another security issue associated with cloud models is data loss. Data in cloud models may be easily accessible by both unauthorized inside personneland external hackers. Internalpersonnelcan readily get unintentional or purposeful access to data. External hackers may use hacking techniques such as session hijacking and network channel eavesdropping to get access to databases in such setups. Viruses and Trojans can be uploaded to cloud systems and inflict harm . It is critical to identify potential cloud risks in order to create a system with improved security procedures to secure cloud computing environments.

CONCLUSION

The main finding ofthe researchpapers isachieving high availability requires redundancy, in particular, fornetworkconnectionsanddatacenters;thecostof this redundancy must be taken into account when conducting a feasibility study for cloud services. Organizations, businesses, and even private parties all host their services inthe clouds. Thishas made it easier to use the innovative technology's many amazing benefits, including high scalability, cheap cost, and easy access. Businesses today, particularly those providing e-commerce services and software firms, benefit greatly from cloud computing. But there are several reasons to exercise caution while using cloud computing. In order for the cloud computing service providers to guarantee adequate security and high performance, strong policies and agreements must be implemented. This essay examined the main cloud computing security concerns as well as other customer concerns about these issues. storage and networks are the biggest security concerns in Cloud Computing. Virtualization that allows multiple users to share a physical server is a major concerns for cloud users

REFERENCES

[1]B.Furht,andA.Escalante,Handbook of Cloud Computing.NewYork:Springer,2010.Availableat: http://searchcloudcomputing.techtarget.com/definition/private-cloud

[2]T.Dillon,C.Wu,andE.Chang,“Cloud Computing:Issues and Challenges,” 2010 24th IEEE International ConferenceonAdvanced

InformationNetworkingandApplications(AINA), pp. 27-33,DOI=
20-23April2010

[3] FarazFatemiMoghaddam,Mohammad Ahmadi, SamiraSarvari,MohammadEslami,AliGolkar," Cloudcomputingchallengesandopportunities:A survey, 2015 1st International conference on Telematics and Future Generation Network(TAFGEN)",DOI:10.1109/TAFGEN.2015.7289571.

[4]https://www.researchgate.net/publication/355436710_Cloud_computing_Security_Solutions_and_Privacy

[5] P.Dutta,T.Mukherjee,V.G.HegdeandS.Gujar, "C-Cloud: A Cost-Efficient Reliable Cloud of Surplus Computing Resources," 2014 IEEE 7th InternationalConferenceonCloudComputing,2014, pp.986-987,doi: 10.1109/CLOUD.2014.152.

[6] M. Eldred, C. Adams and A. Good, "Trust ChallengesinaHighPerformanceCloudComputing Project,"2014IEEE6thInternationalConferenceon CloudComputingTechnologyandScience,2014,pp. 1045-1050, doi: 10.1109/CloudCom.2014.21.

[7] C. Wu, A. N. Toosi, R. Buyya and K. Ramamohanarao, "Hedonic Pricing of Cloud Computing Services," in IEEE Transactions on Cloud Computing, vol. 9, no.1,pp.182-196,1 Jan.-March 2021, doi: 10.1109/TCC.2018.2858266.

[8]ITU-T Recommendation Y.3501 (06/2016). Cloud Computing – FrameworkandHigh-LevelRequirements.

[9] M. Armbrust, A. Fox, et al., "A view of cloud computing," IEEE CommunicationsMagazine,vol.53,pp.50-58,April 2010.

[10] CloudComputing: SecurityIssuesandResearch Challenges
Moulika Bollinadi Under Graduate Student, MGIT, Hyderabad, Telangana, India.
VijayKumarDameraAssistantProfessorofIT,MGIT, Hyderabad, Telangana, India.

[11]A.Kundu,C.D.Banerjee,P.Saha,"Introducing New
Services in Cloud Computing Environment", International Journal of Digital Content Technology and itsApplications,AICIT,Vol.4,No.5,pp.143-152, 2010.

[12]Pearson S., Benameur A. Privacy, security and trust issues arising from cloud computing IEEE International Conference on Cloud Computing Technology and Science

[13]P.Alvaro,T.Condie,N.Conway,K.Elmeleegy, J.Hellerstein, andR.Sears.BOOMAnalytics:ExploringData-Centric, DeclarativeProgrammingfortheCloud.InProc. EuroSys,
2010.

[14]M. Almorsy, J. Grundy, and A. Ibrahim. Collaboration-based cloud computing security management framework.Proc.ofCloudComputing, pages 364–371, 2011.

[15]https://www.researchgate.net/publication/292544739_Research_on_security_issues_of_privacy_data_under_the_cloud

[16] Cloud Computing: SecurityIssuesand Research Challenges
Moulika Bollinadi Under Graduate Student, MGIT, Hyderabad, Telangana, India.
VijayKumarDameraAssistantProfessorofIT,MGIT, Hyderabad, Telangana, India.

[17] Nidal M. Turab, Anas Abu Taleb, Shadi R. Masadeh, *Cloud Computing Challenges and Solutions,* International Journal of ComputerNetworks & Communications (IJCNC) Vol.5, No.5, September 2013

[18]https://d1wqtxts1xzle7.cloudfront.net/58220784/AhmadCloudThreats-with-cover-page-v2.pdf?Expires=1666779281&Signature=LeQw6mO1DgAHFMhxyIpDE-DvXZqHMANAwDvu~1svhi25cLFLbD9ZYsPDDdf4fNL0g8~5oIMxDdmDDANzRw8hEi03fkOH1Th5rspPZyQ-UW-L6ydu-uNzRyAmeS1rlJ45aYkKkHmRsGyFtdFKAuNUL3LMP~6iHnENcl3CwT5ItksLkoVGlIyu5-KBJZ7i0r0KUkITbDb1WZXIOmP2Pk0oFHyALK5h5TKuYfd6ZW-q0RTRGDL3ffHmd4KBfYjiF10cCP843xsn5Y4FtX5aJciEDxtexUrspYhMwZJrAi6nForazeg5zFiDizd5KV2JCahNhA5A5Lqu1k8Qi6pOSJlCfQ&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[19]R. Velumadhava Raoa, K. Selvamanib, "Data

Security Challenges and Its Solutions in Cloud Computing",InternationalConferenceonIntelligent

Computing,Communication&Convergence(ICCC-2014) Conference Organized by Interscience InstituteofManagementandTechnology, Bhubaneswar,Odisha,India

[20] https://www.researchgate.net/publication/317908867_Cloud_Computing_and_Security_Issues