IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

RESEARCH PAPER ON SECURITY ISSUES IN CLOUD COMPUTING

Bohniman Bhuyan	Yash Ravindra Sontakke	Nalin Bisht	Shubhendra Pratap Singh	Mayank Adtani
Department of computer science and engineering	Department of computer science and engineering	Department of computer science and engineering	Department of computer science and engineering	Department of computer science and engineering
Lovely Professional University, Phagwara, Punjab, India	Lovely Professional University, Phagwara, Punjab, India	Lovely Professional University, Phagwara, Punjab, India	Lovely Professional University, Phagwara, Punjab, India	Lovely Professional University, Phagwara, Punjab, India

Abstract

Cloud computing is the way of utilizing a system of remote servers available on web to store, oversee and run information on request and pay depending on utilization. It gives access to a pool of shared assets rather than nearby servers or PCs. As it doesn't obtain the things genuinely, it spares overseeing cost and time for associations. Distributed computing is a totally web subordinate innovation where customer information is put away and keep up in the server farm of a cloud supplier like Google, Amazon, Microsoft and so forth. Cloud computing is a rising space and is acclaimed all through the world. There are some security issues sneaking in while utilizing administrations over the cloud. This examination paper presents a survey on the distributed computing ideas just as security issues characteristic inside the setting of distributed computing and cloud framework. This paper also thoroughly checks the key research and problems that presents in cloud computing and offers best practices to experts' co-ops just as endeavours wanting to use cloud administration to improve their main concern right now atmosphere and lift up its use. The principle accentuation of our examination dependent on existing writing and to comprehend the idea of multi-occupancy security issue.

Keywords: Cloud Computing, Cloud security, Distributed Computing, Framework

1. INTRODUCTION

Cloud computing is an appropriate design which concentrates server assets on a versatile stage in order to give on request figuring assets and administrations. Cloud Service Providers (CSP's) offer cloud stages for their clients to utilize and make their web administrations, much like Internet Service Providers (ISP's) offer costumers fast broadband to get to the web. CSPs and ISPs both offer administrations. Cloud computing is a gear which is a useful, on-request order access also a customary pool of processing assets, for example, server, system, stockpiling, applications which can be providing and discharged with minimal administration exertion or specialist co-op's communication.(Abbadi et al., 2011) Clouds are the new pattern in the development of the dispersed frameworks. Prior to Cloud we utilized Grid. In Cloud Computing, the client doesn't require information or skill to control the foundation of clouds; it gives just deliberation. It tends to be used as a help of the Internet with high versatility, higher throughput, nature of administration and high figuring power. Cloud computing suppliers transfer basic online business applications which are gotten to from servers through internet browser.[3]

Ongoing improvements in the field of Cloud figuring have massively changed the method for registering just as the idea of processing assets. In a cloud-based figuring foundation, the assets are regular in another person's reason or organize and got to remotely by the cloud clients.[1] At times, it may be required or if nothing else workable for an individual to store information on remote cloud servers. These gives the accompanying three delicate states or situations that are of specific worry inside the operational setting of cloud computing:

- The conveyance of individual private information to the cloud server.
- The conveyance of data from the cloud server to customers' PCs.
- The stockpiling of customers' very own information in cloud servers which are remote servers not claimed by the customers.

All the above three conditions of cloud computing are seriously inclined to security break that makes the exploration and examination inside the security parts of cloud computing practice a basic one.[15]

The viewpoints introduced right now sorted out so as to examine and identify the way to deal with distributed computing just as the security issues and worries that must be considered in the sending towards a cloud-based processing foundation. Conversation on the mechanical ideas and ways to deal with distributed computing including the design delineation has been thought about inside the setting of conversation right now. Security issues in distributed computing approach have been talked about a while later. The investigation in the innovative and security worries of distributed computing has prompted the finishing up acknowledgment on the general parts of cloud computing.[3]

2. LITERATURE SURVEY

The journal 'Trustworthy middleware services in Cloud' written by Abbadi, Cloud infrastructure should be capable of supporting Internet-scale critical applications (e.g., hospital systems and smart grid systems). Without clear guarantees that their specifications will be met, essential infrastructure providers and companies will not outsource their critical applications to the public Cloud. The consumer should be presented with proof of the Cloud elements' trustworthiness, which is at the heart of this issue. Establishing a Cloud confidence model is critical, but the sophistication and dynamism of the Cloud's architecture make it difficult to do so. One of the main goals of the EU-funded TClouds (Trustworthy Clouds) project is to establish trust in the Cloud. TClouds focuses on developing trust models with varying degrees of transparency in the sense of technological complexities and trust establishment. These trust models benefit not only Cloud users, but also Cloud vendors, partnering Clouds-of-Clouds, and third-party auditors. In this paper, we look into this issue and summarise some of the most recent TClouds project findings in the sense of trust establishment.[1]

In the journal "The cloud Grid approach: Security Analysis and Performance", V. Casola, A. Cuomo and M. Rak, said that in both cloud computing and grid computing are paradigms which manage sets of distributed resources which will benefit the scientific community from their convergence. This paper proposes a model known as Cloudgrid, through which can achieve cloud and grid integration. After analysing the security issues involved, a solution is proposed based on fine-grained access control mechanisms and identity federation through which interoperability and cooperation is allowed among untrusted cloud resource.[3]

Zissis and Lekkas, in their publication "Addressing Cloud Security Issues", discussed about how we can increase cloud security in particular infrastructures. They proposed introducing a Trusted Third Party who are tasked with checking specific security characteristics in a cloud environment. The solution used cryptography, which is used to maintain confidentiality of all involved data and communications in the system. This solution is available to all entities.[15]

R. L Grossman, in his publication "The case for Cloud Computing", says that understanding clouds and cloud computing is understanding there are two different types of clouds. They are distinguished by provide on-demand computing instances' and 'provide on-demand computing capacity. Both of them uses similar machines, but the second one is designed as support data- or compute-intensive applications by scaling capacity. Example of the first category is the Amazon EC2 services, and Google's MapReduce is the example of second category. The provide on-demand computing instances uses instance to supply Software as a Service (SaaS) or Platform as a Service (PaaS).[4]

The book by Tim Mather, Subra Kumaraswamy, Shahed Latiff, "Cloud Security and Privacy: AN Enterprise Perspective on Risks and compliance starts with the basic introduction of Cloud Computing and its evolution. It tells us how Computing changed into Cloud computing during a period of time. It introduces the readers with features of Cloud Computing like pay as you go model, elasticity, shared resources, vast scalability, and self-provisioning of resources. It tells us that Cloud Computing is a fast-changing field which have recently came into existence. Cloud can have multiple definitions and this book tries to explain the same in a very easy manner. This book describes some of the most important aspects of Cloud Computing like visualization. In third chapter, we see how Cloud is helpful in providing security to IT infrastructure. We can learn about IT infrastructure security in different levels like network, host and application levels. Fourth chapter introduces us with Data Security and Storage which inspects the data storage and data security of current state in the cloud. It includes features like integrity, confidentiality and availability of services. After Data Security and Storage, we come across Identity and access Management feature of Cloud which is helpful in authentication, auditing and authorization of users accessing the cloud services. Security Management can be seen in

Chapter six which shows various frameworks used in Security Management. We also learn about necessary protocols required for cloud in Security Management. After Security Management we come to know about the privacy control on cloud. It makes us familiar with the privacy points to remember about Cloud Computing and also compares the similarities and differences with traditional cloud models. We also come across legal and regulatory aspects of cloud. These aspects could be helpful while providing as well as using cloud services. Chapter eight deals with Audit and Compliance where we can know the significance of Audit and Compliance functions. Moreover, we get to know about frameworks and protocols to consider in context of Audit and Compliance. After this we get to know about some of the most popular Cloud Service Providers in market and what services they provide. Another emerging feature of Cloud is Security-As-a-Service which is talked about in chapter ten. Here we come to know how security is provided as a service on cloud and how it is becoming more popular day-by-day. We also get to know what are the security services that are provided on cloud. In the final chapter, we go through the Impact of Cloud Computing on the role of Corporate IT. We can know about the perspective of Cloud Service Providers and IT departments towards each other. Cloud Computing is a very important aspect in context of IT but the fact that it replaces much of what IT is cannot be ignored by IT departments. Finally, we come across the conclusion of book, which highlights the important points presented in the book and a brief description about the future of Cloud Computing.[10]

3. CLOUD COMPUTING

3.1 ARCHITECTURE SERVICE MODELS:

- Software as a Service (SaaS)

Software as a service (Saas): It is also known as a delivery model where the software and the data which is associated with is hosted over the cloud environment by a third party known as cloud service provider, just like your Gmail account, you use that application on someone else's system.

- Platform as a service (PaaS)

Platform as a service (Paas): Right now, it can utilize Web-based apparatuses to create applications so they run on frameworks programming which is given by another organization, similar to Google App Engine.

- Infrastructure as a service (IaaS)

Infrastructure as a service (Iaas): It offers types of assistance to the organizations with processing assets including servers, systems administration, stockpiling, and server farm space on a compensation for every utilization premise.[15]

3.2 DEPLOYMENT MODELS

- Public Model

Public Model: This framework is accessible to all the people. As the name proposes, public cloud is where assets are commonly accessible to everybody at anyplace.

- Private Model

Private Model: This model is created for the private associations like one house and an association and they can utilize it for their own uses. This sort of a help isn't gotten to by everybody.

- Hybrid Model

Hybrid Model: Hybrid Clouds are blend of public and private cloud in an equivalent network. This should be possible if private cloud needs some significant administrations from the public cloud like Private cloud can store some data on their private cloud and we can utilize that data on public cloud.[9]

4. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing comprises of utilization, stages and framework portions. Each section performs various activities and offers various items for organizations and people the world over. There are various security issues for cloud computing as it envelops numerous advancements which incorporates systems, databases, working frameworks, virtualization, asset booking, exchange the executives, simultaneous control and memory the board. Accordingly, security issues for a significant number of these frameworks and innovations are material to cloud computing. Information security includes scrambling the information just

as guaranteeing that proper strategies are upheld for information sharing. The given underneath are the different security worries in a cloud computing condition.[10]

DATA SECURITY

It is the protection of data which is stored online via different platforms from leakage, theft and deletion. Data can be protected by including firewalls, virtual private networks (VPN), penetration testing, and by avoiding public internet connections.[2]

DATA TRANSMISSION

It is the way toward sending advanced or simple information over a correspondence medium to at least one processing system. In Cloud condition the majority of the information isn't encoded in the handling time. To process data for any app that information must be decoded. In homomorphism encryption which permits the information to be prepared without being unscrambled. The assault is completed when the assailants place themselves in the correspondence's way between the clients. Here there is the likelihood that they can hinder and change interchanges.[6]

DATA AVAILABILITY

It is the reliability of access to and timeliness and use of data. This includes accessibility of data. Availability requires continuity of information and accessibility.[7]

VIRTUAL MACHINE SECURITY

The term Virtual Machine (VM) portrays sharing the assets of one single physical PC into different PCs inside itself. VM's give spryness, adaptability and versatility to the cloud assets by permitting the merchants to duplicate, move and control their VM's. Remembering this, malevolent programmers are discovering approaches to get their hands on significant information by controlling shields and rupturing the security layers of cloud conditions. The cloud computing situation isn't as straightforward as it professes to be. The administration client has no clue about how the information is handled and put away and can't straightforwardly control the progression of information stockpiling and preparing. Having VM's would by implication permits anybody access to the host circle of the VM to take an unlawful duplicate of the entire framework.[14]

DATA PRIVACY

One should always have the right to control his/her own data, whether its private, public or professional. As one does not know how processing of data is configured or the physical location of the server, users use cloud services regardless of any knowledge about processes involved.[5]

DATA INTEGRITY

Defilement of information can occur at any degree of capacity. So, Integrity checking is should in cloud storage. Information Integrity in a framework is kept up by means of database requirements and exchanges. Exchanges ought to follow ACID (atomicity, consistency, disengagement, toughness). Information created by cloud computing administrations are kept in the cloud. Keeping information in the mists, clients may lose control of their information and depend on cloud administrators to authorize get to control.[13]

DATA SEGREGATION

It is the division of information of one user to information of another user. This ensures that one user cannot compromise or interrupt the data service of another user which ensures that the cloud provider is executing controls effectively which separates users from each other reducing the risk.[8]

DATA LOCATION

Cloud clients don't know about the specific area of the data-center and furthermore they don't have any command over the physical access to that information. A large portion of the cloud suppliers have data-centers around the globe. In numerous nations' specific sorts of information can't leave the nation as a result of conceivably delicate data. Next in the multifaceted nature chain there are circulated frameworks in which there are different databases and numerous applications.

In light of the investigation, we found that there are numerous issues in cloud computing however security is the significant issue which is related with cloud computing.[11]

Seven security issues in cloud computing environment according to “Cloud Security Alliance” CSA are:

4.1 MISUSE AND INEXCUSABLE USE OF CLOUD COMPUTING

Programmers, spammers and different crooks exploit the appropriate enrolment, basic strategies and relatively vague access to cloud administrations to dispatch different assaults, for example, key breaking, secret phrase and so forth.

4.2 INSECURE APPLICATION PROGRAMMING INTERFACES (API)

Clients deal with and communicate with cloud benefits through API's. Suppliers must guarantee that security is incorporated into their administration models, while clients must know about security dangers.

4.3 MISCHIEVIOUS INSIDERS

Malevolent insiders make a tremendous risk in cloud computing condition, since buyers don't have an away from of supplier approaches and methodology. Vindictive insiders can increase unapproved access into association and their benefits.

4.4 MUTUAL TECHNOLOGY ISSUES/MULTI TENURE NATURE

This is essentially founded on shared framework, which isn't intended to suit a multi-inhabitant design.

4.5 INFORMATION CRASH

Involved information may incorporate erased or adjusted information without making a reinforcement, un-linking a record from a tremendous situation, loss of an encoding key and unlawful access of delicate information.

4.6 RECORD, SERVICE AND TRAFFIC HIJACKING

Record or administration commandeering is generally done with taken qualifications. Such assaults incorporate phishing, extortion and abuse of programming vulnerabilities.

Assailants can get to basic territories of cloud computing administrations like classification, honesty and accessibility of administrations.

4.7 UNIDENTIFIED RISK REPORT

Cloud administrations implies that associations are less engaged with programming and equipment, so associations ought not know with these issues, for example, inner security, security consistence, reviewing and logging might be neglected.(Tim Mather, Subra Kumaraswamy, 2009)

5. RESEARCH CHALLENGES

Cloud computing research tends to the difficulties of meeting the necessities of cutting edge private, open and half breed distributed computing structures and furthermore the difficulties of permitting applications and advancement stages to exploit the advantages of cloud computing. Many existing issues are yet to be completely tended to, while new difficulties continue rising up out of industry applications. A portion of the difficult research issues in cloud computing are given beneath.

5.1 ADMINISTRATION LEVEL AGREEMENT (SLA's)

Cloud is administrated by administration level understandings that permit a few occasions of one application to be copied on different servers if need emerges; subject to a need plot, the cloud may limit or shut down a lower-level application. A major test for the cloud clients is to assess SLAs of cloud merchants. The greatest part of the cloud sellers SLA's is to make a protective shield against legitimate activity while offering confirmations to clients. So, there are a few issues, for example, information security, blackouts and value structures that must be taken into account by the clients before marking an agreement with the merchant. And furthermore, is there any SLA related with reinforcement, file, or conservation of information? On the off chance that the administration account gets idle, at that point do they keep client information? In the event that truly, at that point to what extent? So, it's a significant research zone in distributed computing.

5.2 CLOUD DATA MANAGEMENT

Cloud information can be enormous, unstructured and ordinarily add just with uncommon updates. As administration sellers don't approach the physical security arrangement of server farms, they should depend on the framework supplier to accomplish full information security. In a virtualized situation like the mists, VMs can powerfully relocate starting with one area then onto the next; subsequently legitimately utilizing remote confirmation isn't adequate. In such case, it is basic to manufacture trust instruments at each structural layer of the cloud. Programming structures, for example, MapReduce and its different executions, for example, Hadoop are intended for conveyed preparing of information serious assignments, these systems commonly work on Internet scale document framework.

5.3 INTEROPERABILITY

It is the capacity of a PC framework to run application programs from various sellers and to interface with different PCs across LAN or WAN free of their physical design and working frameworks. Numerous open cloud systems are arranged as shut frameworks and are not intended to cooperate with one another. To conquer this test, industry guidelines must be created to assist cloud with overhauling suppliers' structure interoperable stages and empower information compactness. Associations need to naturally arrangement administrations, oversee VM occasions, and work with both cloud-based and endeavour-based applications utilizing a solitary instrument set that can work across existing projects and numerous cloud suppliers.[5]

5.4 MULTI-TENANCY

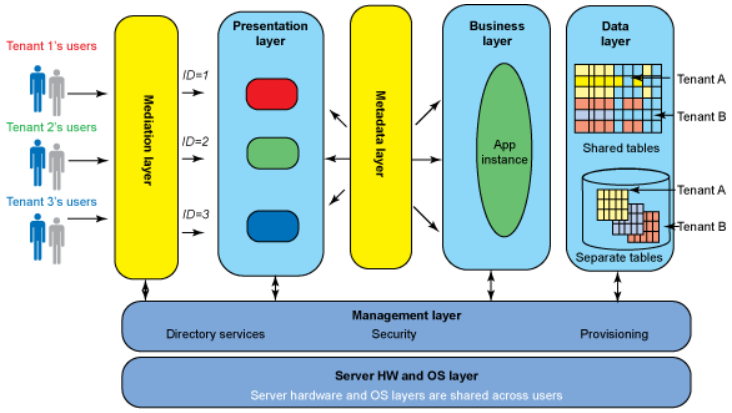
Multi-occupancy is a significant worry in distributed computing. Multi-tenure happens when various buyers utilize a similar cloud, same working framework, on a similar equipment, with similar information stockpiling framework to share the data and information or runs on a solitary server.

There are numerous sorts of cloud applications that clients can access through the Internet, from little Internet based gadgets to huge venture programming applications that have expanded security necessities dependent on the kind of information being put away on the product merchant's foundation. These application demands require multi-tenure for some reasons, the most significant is cost. Various clients getting to similar equipment, application servers, and databases may influence reaction times and execution for different clients. For application-layer multioccupancy explicitly, assets are shared at every framework layer and have legitimate security and execution concerns. For instance, numerous help demands getting to assets simultaneously expand hold up times yet not really CPU time, or the quantity of associations with a HTTP server has been depleted, and the administration must hold up until it can utilize an accessible association or in a most dire outcome imaginable drops the administration demand.[12]

5.5 ARCHITECTURE

This engineering completely isolates your data from other client's data, while permitting us to turn out quickly the most recent usefulness at the same time. This methodology offers the most configurability and permits you to separate profound understanding from your data.

Prophet conveys a most recent Multitenant design that permits a multitenant compartment database to get a handle on various pluggable databases. An existing database can basically be embraced with no application changes essential.[5]



5.6 WHAT MULTI-TENANCY CAN DO?

Rearrange Data Mining: Instead of being made from different sources, all the data for buyers is put away in a solitary database plot.

Diminishes use: Multi-occupancy decreases the overhead by amortizing it over numerous clients, similar to they can charge for the ensured programming since everybody can run it on a solitary framework, so just single guarantee should buy.

Greater versatility: It gives the adaptability of bringing in and sending out your data.[12]

6. REFERENCE

1. Abbadi, I. M., Deng, M., Nalin, M., Martin, A., Petkovic, M., Baroni, I., & Sanna, A. (2011). Trustworthy middleware services in the cloud. *International Conference on Information and Knowledge Management, Proceedings*, *October*, 33–40. https://doi.org/10.1145/2064085.2064094

2. Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016). Data security in cloud computing. *5th International Conference on Future Generation Communication Technologies, FGCT 2016*, *October 2017*, 55–59. https://doi.org/10.1109/FGCT.2016.7605062

3. Casola, V., Cuomo, A., Rak, M., & Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. *Future Generation Computer Systems*, *29*(1), 387–401. https://doi.org/10.1016/j.future.2011.08.008

4. Grossman, R. L. (2009). The case for cloud computing. *IT Professional*, *11*(2), 23–27. https://doi.org/10.1109/MITP.2009.40

5. Guilloteau, S., & Mauree, V. (2012). Privacy in Cloud Computing. *ITU-T Technology Watch Report*, *March*, 26. http://www.itu.int/ITU-T/techwatch%0Ahttp://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx

6. Naralasetty, T., & Eswar, K. (2013). *Secure Data Transmission Using Cloud Computing*. *2*(11), 1356–1362.

7. Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/jis.2016.73014

8. Solanki, Seema Singh and Nabeel, S. (2014). Cloud Computing : Data Separation Issues. *International Journal & Magazine of Engineering, Technology, Management and Research*, *1*(November), 155–160.

9. Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. *Information Security Technical Report*, *16*(3–4), 102–107. https://doi.org/10.1016/j.istr.2011.08.005

10. Tim Mather, Subra Kumaraswamy, and S. L. (2009). Cloud Privacy and Security. *Governance An International Journal Of Policy And Administration*, 336.

11. Vaish, A., Kushwaha, A., Das, R., & Sharma, C. (2013). Data Location Verification in Cloud Computing. *International Journal of Computer Applications*, *68*(12), 23–27. https://doi.org/10.5120/11632-7104

12. Varsha, V., Wadhwa, A., & Gupta, S. (2015). Framework using Multitenancy Architecture in Cloud Computing. *International Journal of Computer Applications*, *121*(15), 12–17. https://doi.org/10.5120/21615-4883

13. Vijayaragavan, V., & Sivasankar, K. (2014). Data integrity in cloud computing - A survey. *International Journal of Applied Engineering Research*, *9*(23), 23285–23297.

14. Wu, H., Ding, Y., Yao, L., & Winer, C. (2010). Network security for virtual machine in cloud computing. *Proceeding - 5th International Conference on Computer Sciences and Convergence Information Technology, ICCIT 2010*, 18–21. https://doi.org/10.1109/ICCIT.2010.5711022

15. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006