



Security Challenges and Issues in Cloud Computing

Monika Hire¹, Nilesh Uke²

¹PG Scholar, Pimpri Chinchwad College of Engineering, Pune, India

²Professor, Pimpri Chinchwad College of Engineering Pune, India

Abstract Cloud computing has been developed as a standout amongst the most energizing standards in IT industry and is increasing more significance, as it offers stockpiling of information at bring down expenses and is accessible all the time on net. Despite the fact that cloud computing gives information at bring down costs, less demanding support, and accessibility of administrations anyplace, whenever, a key test is the means by which to guarantee that cloud can secure client's information productively. Security in cloud identifies with the hazard regions in a similar way with outside capacity of information, absence of control, multi-client accessibility and consolidating these variables with inside security. The fundamental motivation behind this paper is to concentrate on the security issues of ensuring client's information in cloud.

Keywords Cloud Computing, Security, and Security issues

1. Introduction

Cloud computing is perceived as another option to customary data innovation because of its inborn asset sharing and low-upkeep qualities. In the distributed computing the cloud specialist organizations (CSP) give diverse sorts of administrations, for example, Infrastructure, information stockpiling, programming and so on. As the interest for cloud computing expands, security and protection will turn out to be more basic. Cloud security and protection gives expansive scope of terms and definition to help both IT and Information experts. There have been many endeavors to comprehend distributed computing and delineate the security issues required with such innovations. By using the cloud, the workplace staffs can be totally discharged from the troublesome nearby information stockpiling and upkeep. Be that as it may, it additionally represents a huge hazard to the classification of those put away documents. In particular, the cloud servers oversaw by cloud suppliers are not completely trusted by clients while the information documents put away in the cloud might be delicate and classified, for example, marketable strategies. To safeguard information security, an essential arrangement is to encode information records, and afterward transfer the scrambled information into the cloud. Outlining a productive and secure Data sharing plan for assemble in the cloud isn't simple errand because of some reasons. Cloud computing attracts people for various services provided by it at lower costs. In cloud computing, services are provided to users according to their needs. Service providers can adjust the content to be offered according to user's requirements. For instance, user can seek disparate amount of storage, degree of data encryption, speed of transmission, and other services. Cloud computing provides on demand access to shared pool of resources such as servers, storage, network and applications that can be granted and unleashed with minimal management effort and reduced service provider interaction [1]. The review of threats is done by considering various parameters, such as the threat exploits internally or externally through the outsider of cloud [13].

Characteristics of cloud computing

- On demand self-service – computer services like the e- mails, applications, or server service can be provided without requiring human interaction with each service provider.



- Broad network access – Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
- Resource pooling - The provider's in the computing resources where pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources which are dynamically assigned and reassigned according to consumers demand. The resources comprise among others storage, processing, memory, virtual machines and the email services. Pooling altogether of the resource builds economies of measure.
- Rapid elasticity – the Cloud service scan be expeditiously and flexible provisioned, in some cases automatically, to immediately scale out and rapidly released to immediately scale in. To the client, the capabilities existing for formularization often appear to be unbounded and can be purchased in any amount at any time.
- Measured service – the Cloud computing resource usage can be controlled, measure and reported by providing transparency for both the provider and the consumer of the utilized service. Cloud computing services can use a metering capability which enables to control and optimize the resource. This may implies that just like electricity or municipality water IT services are charged as pay per use. The more you utilize the higher will be the bill.
- Multi Tenacity - it is the 6th characteristics of cloud computing advocated by the Cloud Security intimacy. It relates to the need for policy-driven origination, detachment, segmentations, governance, service levels, and chargeback/billing models for different client constituencies [2].

2. Service Model

Three types of cloud services and user can use any services which are mentioned below:

IAAS –the term IaaS implies framework as an administration this model give framework fixings or segments to customers. IaaS by and large gives the assets which are overseen and effectively scaled up. Segments in the IaaS incorporates virtual machines, stockpiling, systems ,firewalls, stack balancers and other crucial processing assets where the customer can send and run self-assertive delicate product's which incorporates the working frameworks and applications. The customers of IaaS can coordinate access to the most minimal level programming in the stack. One of the biggest IAAS suppliers is the Amazon web administrations.

PAAS – the term PaaS implies stage as a benefit. The PaaS display conveys a pre-fabricated application stage for the customer. The PaaS can naturally arrangements and scales required framework parts depending on the applications necessities. The PaaS factors are execution database, web server, sending apparatuses execution runtime and so forth it gives the ability to send the cloud framework purchaser made or obtained application made by utilizing the libraries, programming dialects and the instruments upheld by the suppliers.

SAAS- the term SaaS implies programming as a benefit the SaaS gives the ability of the customers to utilize the applications running on the cloud framework. The SaaS suppliers has finish control of use programming. Online mail, and undertaking administration framework, are the cases of SaaS applications.

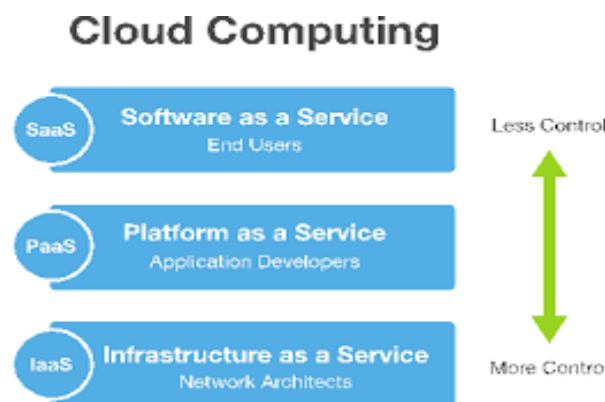


Figure 1: Service Model of Cloud Computing



3. Deployment Model

There are three Deployment Models and are described below:

Public Model: This infrastructure is available to the general public. As the name suggests, public cloud is a model in which resources are generally available to everyone or anywhere.

Private Model: This model is developed for the private organizations like one house and an organization and they can use it for their own purpose. This kind of a service is not accessed by everyone.

Hybrid Model: Hybrid Clouds are combination of public and private cloud in a same network. This can be done if private cloud need some important services from the public cloud like Private cloud can store some information on their private cloud and we can use that information on public cloud [3].

Advantages of Cloud Computing

1. **Accommodation** - You can influence your information anywhere you can also meet to the Internet.
2. **Security** - Most companies use industrial level security software which make it harder for hackers to get at your information.
3. **Backups** - You have a backup of your material in case your local computer crashes.
4. **Collaboration** - With your permission, others can approach, view, and modify your documents.
5. **Environmentally friendly** - It takes fewer resources to cloud, thus excepting energy. Some dealing take it a step further and incorporate cloud computing into their telecommuting strategies.
6. **Easy Approach to data** - Once you register yourself in the cloud, you can accessible the data's and information's.
7. **Fast Deployment** - it gives you the advantage of fast deployment. Once you operate for this method of functioning, your whole channel can be fully dynamic in a minutes. The amount of time taken here will depend on the exact kind of technology that you need for your business.
8. **Availability**- we can Access the information anytime and where ever we want. The Internet cloud infrastructure maximizes enterprise productivity and efficiency by ensuring your application is always acquirable. This permits for simple Complicity and communion among users in multiple locations.
9. **Flexibility for development** - The cloud is easily scalable so companies can add or subtract resources based on their needs. As companies develop, their system will develop with them.
10. **Efficient improvement**- Cloud computing delivers faster and more accurate retrievals of demand and data. With certain time, it is the most achieved improvement plan.

Disadvantages of Cloud Computing

1. **Security breaches**- remote server security makes it difficult, but not tedious, for hackers to access your data. If there is understanding among the servers where your data is collected, your private data may be disclose to the world. There is also a good opportunity that more than just your data may be affected— we are talking possibly millions of other users.
2. **Storage limits** - There is also a foundation being on a THE magnitude of the data and information that can be stored.
3. **Slow speeds** - It is slow. The process of Uploading and downloading of big documents or articles may take a long period of time.
4. **Limited features** - If you use remote software that's provided by the storage service to manipulate and convert your data, it usually decreases the features of a program running locally.
5. **Security and privacy** – the security and privacy in the cloud computing is not so good. The data and application might not be very safe on the public cloud.
6. **No longer in control** - When the services are being moved to the cloud, you manage your information's and the data.
7. **May not get all the features** - All the cloud services are same. Some cloud providers tend to offer limited versions and enable the most prevalent features, so you may not accept every feature you want. Before signing up, make sure you may know that what your cloud service provider is offering.



8. **No Redundancy**-A cloud server is not dispensable nor is it covered up. As technology and techniques may fail here and there, debar getting burned by purchasing a redundancy scheme. Though it is an extra cost, in most cases it will be well worth it.
9. **Bandwidth issues**- For idealistic adherence, clients have to design accordingly and not pack big amounts of servers and storage devices into a small set of data centers.
10. Storing information in the cloud could make your company penetrable to outer hack attacks and remedies. As you are conscious, nothing on the Internet is absolute, safe and hence, there is always the lurking feasibility of fraud of the sensitive data.

4. Security Issues

In spite of the fact that distributed computing has been broadly embraced by the business, yet the cloud processing research is comfortable beginning time. A few unchangeable issues are not been completely tended to, while new difficulties keep rising up out of industry applications. In the cloud security is an evolutionary subdivision of domain of computer security network and, more considerably, information security. It concludes to a huge set of, techniques, and controls deployed to secure data, applications, and the associative infrastructure of cloud computing [2].

4.1. Security and privacy

Unmistakably the security issues play the vital part in ruining Cloud figuring acknowledgment. There are numerous security dangers which originates from inside or outside of cloud suppliers/customers air which has arranged into the pariah dangers, and the insider troublesome assaults, information misfortune, issues worried to multi-occupancy and loss of control. In a cloud situation the security highlights needs to take ownership to protect cloud fanciful framework. Execution and Availability, outside assaults, antagonistic Insiders, Loss of Control, Service Deterioration and Multi-tenure are the assaults that must be for the most part tended to.

Security issues like the phishing, botnet, information misfortune posture genuine dangers to association's information furthermore, programming, the common processing and the multi-tenure model assets in cloud registering has delegate new security challenges that require novel strategies to manage. For ex, programmers can utilize Cloud to oversee botnet as Cloud much of the time gives more true foundation administrations at a generally less expensive cost for them to begin an assault. Cloud customers' information stores in information focuses that cloud suppliers diffuse everywhere the globe inside several servers that convey through the Internet have a few surely understood potential dangers inside them. Since cloud administrations are utilizing the Internet as their correspondence foundation, cloud registering includes a few sorts of security dangers.

4.2. Resource Availability / Reliability

Unwavering quality indicates how regularly assets are accessible without disengage and how frequently they come up short. Unwavering quality remains a test for cloud specialist co-ops wherever Cloud suppliers still need round-the-clock benefit. It is imperative to screen the administration being given utilizing inner or third-work gadget. It is basic to have plans to deal with control, execution, and business reliance of these administrations. The critical stage that frames strong issues for the dependability of distributed computing is down time. One approach to get dependability is unimportant asset use.

Availability can be comprehended as the probability of getting the assets at whatever point they are required with the thought to the time it takes for these assets to be provided. Despite elevating arranging having property for high unwavering quality and openness, the administrations in the distributed computing can encounter disavowal of support surge, stuff blackouts and normal mischance.

4.3. Interoperability and Portability

Interoperability is the capacity to utilize the same apparatuses or application there on different cloud specialist organizations programs. A conceivable answer for the assets accessibility issue is the utilization of various mists to guarantee the required measure of assets.

Transportability and interoperability both are relate to the office to fabricate frameworks from re-usable segments. Convenience and interoperability of foundation segments are accomplished by equipment and virtualization structures. The real sorts of distributed computing movability to be application compactness, stage convenience what's more, information convenience. These are the movability in a specific order of utilization



stage and information factors. Cloud clients must have the adaptability of relocating in and out and changing to mists at whatever point they need without no merchant secure time. The purpose behind the present awful compactness furthermore, constrained interoperability between mists is the absence of institutionalized API's.

4.4. Performance

Execution is the second greatest issue in cloud condition. The cloud give upgraded execution when a client moves to distributed computing framework. Execution is generally deliberately by abilities of applications dealing with the cloud framework. Flawed execution and non-accessibility of data to an end client implies the same as the administrations required are not in working request. Featured a few factors responsible for terrible execution in distributed computing air. These include: constrained data transfer capacity, plate space, memory CPU cycles, web association and most mightily postpone which decreases the end to end response time. Ordinarily clients lean toward to utilize administrations from more than one cloud where a few applications are situated on private mists while some different realities or execution being on open or system.

4.5. Virtualization

Virtualization is a system, which permits to share single physical example of an application or asset among different associations or occupants (clients). It does so by relegating a sensible name to a physical asset and giving a pointer to that physical asset when request. In registering, virtualization intends to make a virtual form of a gadget or source, similar to the capacity gadgets, servers organize or even a working framework where the structure parts the asset into at least one execution conditions. Working framework virtualization is the utilization of programming to permit a bit of equipment to run different working framework pictures in the meantime. Virtualization programming was received speedier than anybody envisioned, including the specialists. In the field of IT there were three ranges where the virtualization is making, arrange virtualization, stockpiling virtualization, head streets and server virtualization. It can be part of a general pattern in big business IT that incorporates autonomic listing, a situation in which the IT conditions will have the capacity to oversee itself in view of saw occupation, what's more, advantage figuring, in which PC preparing power is viewed as an utility that customers can pay for just as required Virtualization makes framework administration more compound, and gigantic mechanization is required in association to help the key perspectives, on-request and adaptability need.

5. Parameter of Analysis

There are certain inherent requirements that must be met by any Security protocol developed for the cloud computing. We present these parameters below:

Access control: The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked [4].

Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation [4].

Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners [4,12].

Efficiency: The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner [4].



Table 1: Comparison of Parameters [4]

Parameters	Access Control	Data Confidentiality	Anonymity & Traceability	Efficiency
Plutus [5]	Y	Y	N	N
Sirius [6]	Y	Y	Y	N
Revocation and Tracing Schemes [7]	Y	Y	Y	N
Improved Proxy Re- Encryption Schemes [8]	Y	Y	N	Y
Achieving Secure, Scalable, and Fine-Grained Data Access Control [9]	Y	Y	Y	N
Secure Provenance: Essential of Bread and Butter of Data Forensics [10]	Y	Y	Y	N
Mona[11]	Y	Y	Y	Y

6. Conclusions

As portrayed in the paper, however there are outrageous favorable circumstances in utilizing a cloud-based framework, there are yet numerous down to earth issues which must be explained. Distributed computing is a troublesome innovation with significant ramifications for Internet benefits as well as for the IT part all in all. All things considered, a few exceptional issues exist, especially identified with benefit level understandings (SLA), security and protection, and power effectiveness. As portrayed in the paper, as of now security has parcel of remaining details which drives off a considerable measure of potential clients. Until the point that an appropriate security module isn't set up, potential clients won't have the capacity to use the upsides of this innovation. This security module should oblige every one of the issues emerging from all headings of the cloud. Each component in the cloud ought to be broke down at the large scale and smaller scale level and an incorporated arrangement must be outlined and sent in the cloud to pull in and captivate the potential purchasers. Until at that point, cloud condition will stay overcast .A coordinated security show focusing on various levels of security of information for an ordinary cloud foundation is under research. This model is intended to be more unique and confined in nature. Our examination inquiries will focus on application and information security over the cloud, and we expect to build up a system by which the security technique shifts progressively starting with one exchange or correspondence then onto the next.

References

- [1]. Samjot Kaur, Vikas Wasson, "Different Data Security Issues of Cloud Computing: A Survey", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 639-643
- [2]. Sangita Das Ankita Chandrakar Reshamlal Pradhan January 2015, "A Review on Issues and Challenges of Cloud Computing" International Journal of Innovations & Advancement in Computer Science, Volume 4, Issue 1 January 2015
- [3]. Varsha, Amit Wadhwa, Swati Gupta, "Study of Security Issues in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 230-234
- [4]. Lal Vikram Singh, Amol V. Bole, Shailesh Kumar Yadav, "Security Issues of Cloud Computing- A Survey" International Journal of Advance Research in Computer Science and Management Studies Volume 3, Issue 1, January 2015 pg. 43-49
- [5]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
- [6]. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp.131-145, 2003.
- [7]. D. Naor, M. Naor, and J.B. Latspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.



- [8]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp.29-43, 2005.
- [9]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
- [10]. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp.282-292, 2010.
- [11]. Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud" IEEE Transactions on Parallel and Distributed System, Vol.24, No.6, June 2013.
- [12]. Priya Dudhale Pise, Nilesh J. Uke, "Efficient Security Framework for Sensitive Data Sharing and Privacy Preserving on Big-Data and Cloud Platforms" in Proceedings of the International Conference on Internet of things and Cloud Computing, ACM, New York, NY, USA, , Article 38 , 5 pages.
- [13]. Arati Koli, Nilesh Uke, Swati Shinde,"A Comparative Analysis on Categorization of Different Threats in Cloud Computing Environment", International Journal of Computing and Technology, Volume 3, Issue 11, Nov 2016

