*ISBN: 978-93-92995-10-1*

# CLOUD COMPUTING SECURITY

**TANNIRU PRABHU**

**ESHWAR S**

**ALLEN BASTIAN**
*Email ID: allenbastian1207@gmail.com*

**Abstract**
*In this paper, we have focused on cloud computing security and to develop the data security. Cloud computing security is one of the technologies which is fast developing and also should be developed in case of security. Recent technologies and people demand more security for data which they want to store safely in some forum. So, cloud computing must be secure enough to store data. Virtualisation is the key aspect which works behind the cloud security. We have even discussed the advantages of cloud computing along with the security issues faced by the users. You can even find out about the security operating organization which ensures the security of data to some extent.*
***Keywords:*** *virtualization, scalability, infrastructure, cloud service providers, storage security.*

## Introduction

Cloud computing security often referred to as cloud security is a set of policies and control-based technologies that protect any kind of data, application and the infrastructure related to the data of cloud computing. Like internet service is provided by Internet service providers (ISP), this cloud service is provided by the cloud service providers (CSP). It gives us a platform for the user to get access to the cloud computing in a very efficient way. With this cloud computing, the client can easily communicate with server-side application or service by the use of the internet infrastructure. The security process i.e. the process of protecting the data from the unknown user involved here is mainly controlled and managed by the IaaS (Infrastructure as a service).

Cloud computing mainly focus on IT sector and most business fields, as no special hardware is required; updates and patches are very fast, as they are directly done by the virtual server over a secure internet connection. It also helps an individual to work and transform data remotely from any corner of the world.

However, we people do not own the infrastructure physically, still, we can access those resources by paying a subscription fee or some without a fee. The main thing behind this is basically to reduce the burden of paying money for the software licence, the storage hardware and other things like e-mail, etc. as the whole resource is provided by the cloud service provider. So this makes the cloud computing more users friendly.

As soon as the introduction of cloud computing took place, there was a massive reduction in the budget by about 18% in the IT sector, while data centre power costs got reduced by 16%.

## Literary Survey

[1]This cloud computing is the communication between the server and the client. This service is provided by the CSP i.e. cloud service provider. There are many technologies like cloud computing but there are 5 aspects that make it more advantageous than other. Those are (i)Multitenancy, (ii)Massive scalability, (iii)Elasticity, (iv) Pay as you go, (v)Self-provisioning of resources. Cloud

computing is initiated by three different models Public Cloud-It involves the usual thing like the default one. Second is the Private cloud- it allows the user to build how the information is stored. The third is the Hybrid cloud- it includes both the private and the public in the same interface. The main thing is that the CSP must intimate every facility and tell every user about the deployment in it.

[2] Cloud security is the main key for the cloud success. There are two technologies which are mainly used in cloud computing, one is the Multi-tenancy and second thing is the virtualization. IaaS (Infrastructure as a service) is mainly dependent on the virtualization technology. This enhances the security and isolation process in the cloud computing. Multi-tenancy can be achieved through the use of the virtualization. The thing is virtualization allows the user to run any OS (operating system) on the same physical device. Cloud computing has 2 types of virtualization Para-virtualization and full virtualization. The notable difference between these two things is the full virtualization; the complete system has to be emulated. But for the paravirtualization modification is done to OS so that the work is performed easily.

[3] The security issues in cloud computing which came into limelight because of certain academics and black hats were considered as fundamentally new but it is relative to the traditional way of cloud computing and these kinds of problems already received attention. Even though after the exponential growth of cloud computing still the security issues in cloud computing possess as a threatto its development. In the present economic case even, the security issues will not prevent it from becoming a consumer commodity. Cloud computing forms the basis for large-scale computation business. Cloud computing made large-scale computations become universally accessible, affordable, and useful.

[4]Cloud computing is considered the latest and exponential growing technology as seen in the past few years. It gives a user to access their data cheaply with minimum cost to increase their potential in data storage. The user can assess their data through the network. There is increasing concern about the security along with the development of cloud across the world. As it exposes the secrets of different companies and industries to the wrong hands which affect them a lot. Their self-reputation could also be damage it exposes to the public. In some, the organisation could not access to their own data but gets spread with many copies. For this, a security organisation is present to ensure the security i.e., Information Technology Infrastructure Library (ITIL). This helps the user to be safe up to a limit but not completely.

[5] With cloud computing, the IT field has reached higher limits in data storage with less cost. While the concern of security arises when an individual goes deeper into the data storage and programming which could be revealed to the public. Cloud computing offers a user to store their data with a reasonable lower cost. It is a service orientated application with the aim of helping the people but it should have security. Cloud can be classified into different types -public cloud, private cloud, and hybrid cloud. Cloud is further divided on the basis of delivery models – infrastructure as a service (IaaS), software as a service (SaaS), platform as a service (PaaS). For the cloud to be user-friendly it should have certain security requirements such as identification and authentication, authorisation, confidentiality, integrity, non-reputation, and availability.

[6] Cloud computing is a platform providing the user with the service through the internet in storage, implementation. It helps in saving the time and cost for the institution. It helps in the improvement of the hospital, banking, and many industries. The data of the user is stored by data centres such as Microsoft, Amazon, Google, and Salesforce. Some of the problems faced by the cloud are leaking of data, resource sharing, availability of data and so on. It gives demand for access

for the users in helping store their data such as photos, videos, etc. there are plenty computing issues as it deals with system operating, scheduling of resources, networks, database, etc. various concerns in security are – data location, data availability, data transmission, data segregation, application and server access.

[7] Cloud computing is regarded as the latest technology in the IT field. In the previous generations, the means of storage is by physical means (hardware) but cloud gives a user to save the data in software means which allows the user to use it from any corner of the world provided there is the availability of the network. There are different types of problem statements such as- system models, adversary model, design goals, notation and preliminaries. The users must ensure that the data that they have stored is secured and not exposed locally. This could be for several reasons maybe the server maybe right or the there are people who will hack the cloud of others. During storage correctness, we could identify data corruption (the servers who are misbehaving could be identified.

[8] As a matter of fact, technology is more boon than bane for the society. Cloud computing is one of the fast-emerging technology in the world. However, one must be cautious and vigilant enough to understand the security issues and challenges faced while using this technology. Few frequent challenges faced are data loss, phishing etc. While this comes as a challenge for many IT companies and Corporates as data is stored ona hard disk without knowledge of how the secure the information is passed and stored. Widely faced security issues are most frequent in public cloud. Generally, cloud consists of three commonly used domains public cloud, private cloud, hyb90-rid cloud. Hybrid cloud is something that uses both public and private clouds, they generally used by IT companies. AS we look into statics provided we can clearly note that issue of security stands on first with 74.6% then stands performance on second with 63.1%. When it comes to hackers they use the cloud as a platform for botnet as cloud services are a low investment for them to do their work. In this paper, you can know the key factors that cause this issue are well described.

[9] In this fast advancing global world, cloud computing plays a major role in the digital platform. On the other hand, there is a great threat to this fast emerging service, that is security. So, one must be cautious enough while using this technology, as no one knows where the information is stored, how securely it is stored and transferred during the time of access by the individual. The technical issue arises when the user's data has to be released by the cloud in order to reach the user, this issue arises. Whether the data is transferred securely or data leaks may have taken place while sending to the user's server. You can also know the varied reasons that there behind this technical issue in cloud computing.

[10] The main aim of this article is to classify and organise the main security concerns that are associated with cloud computing, also helps in finding concerns that are unanswered. In this article, you can know information related to cloud security references mentioned below - network security, transfer security,firewalling, security configuration. The three fundamental security principles that play a major role in the security of cloud are compliance, privacy, architecture. CSA is an organization which helps in providing security for the cloud computing platform.

1

**Findings**

Cloud computing is regarded as the fastest, accessible and conventional means of storing data to the users via the internet. It replaced hardware to software which brought a huge profit to the IT industry not only in case of money but also in time consumption as a user can access their data from any

corner of the world provided there is a good bandwidth. Cloud computing is facing a series of challenges such as the hacking, phishing etc. It is facing a great issue as it exposes the identity and privacy to the public. The security of the cloud must be increased and strengthened drastically so that no hacker can access the valuable data of the user and ensure the privacy of the users. There are institutions that ensure the security of these but it is still not up to the mark. There are technologies like virtualization and Multi-tenancy which is used to develop the cloud security and its interface. These are developed in order to increase the data security and isolation process.

**Conclusion and Recommendation:**

One can infer details about cloud computing and mainly its security. The cloud service is provided by the CSP i.e. cloud service provider. The main focus is to improve and ensure cloud computing security. Virtualization and Multi-tenancy are the key technologies that are used to develop and run the cloud security. The users must understand more about the cloud and must know about its transparency which avoids up to a certain extent. So, we recommend the cloud servers to increase the security of the cloud to make the cloud service a more user-friendly. Two-factor authentication or multi-factor authentication should be practised to protect the data. Cache and cookies should be cleared frequently, passwords should never be auto-saved in a pc.

**References**

Carlin, S., & Curran, K. (2013). Cloud computing security. In Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments (pp. 12-17). IGI Global.

Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security. University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010), 2010-5.

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., &Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 1(1)

Mishra, A., Mathur, R., Jain, S., & Rathore, J. S. (2013). Cloud computing security. International Journal on Recent and Innovation Trends in Computing and Communication, 1(1), 36-39.

Padhy, R. P., Patra, M. R., &Satapathy, S. C. (2011). Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), 136-146.

Popović, K., &Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In MIPRO, 2010 proceedings of the 33rd international convention (pp. 344-349). IEEE.

Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In Information Security for South Africa (ISSA), 2010 (pp. 1-7). IEEE.

So, K. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks, 3(5), 247-55.

So, K. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks, 3(5), 247-55.

Wang, C., Wang, Q., Ren, K., & Lou, W. (2009, July). Ensuring data storage security in cloud computing. In Quality of Service, 2009. IWQoS. 17th International Workshop on (pp. 1-9). Ieee.