*IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*
*e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 15, Issue 1 Ver. II (Jan-Feb. 2020), PP 74-76*
*www.iosrjournals.org*

# Security Mechanism to handle Data in Cloud Computing Environment

Anil Kumar Mishra[1], Chinmaya Ranjan Pattanaik[2]
*1(Department of Computer Science & Engineering, Gandhi Engineering College, India)*
*2(Department of Computer Science & Engineering, Gandhi Institute For Technology, India)*

***Abstract:*** *Cloud computing is an Internet-based computing. It has received attention in recent years but security issue is one of the major inhibitor in decreasing the growth of cloud computing.*
***KeyWord****: Data Security, Cloud Computing*

## I. Introduction

Cloud Computing and Its Security Challenges: An Overview. These days, data, resources, and applications can be shared and accessed through the internet whenever one requires. This has been made possible due to the introduction of cloud computing. The cloud helps in storage and retrieval of the resources over the internet than storing them in hard drives or any other storage devices.
Instead of managing information through local servers, resources can be shared through the clouds. A cloud server mainly comprises software applications and services for the end users within cloud servers.
India.

## II. Cloud Computing

Nowadays, cloud computing is at a peak in its implementation. The top cloud service providers in the recent market include Google Drive, Microsoft Azure, etc. These companies help in providing cloud users in keeping files or develop applications in it. From the cloud, the data and the applications can be accessed by the user anywhere and at any time. If a user chooses cloud services, he/she will be able to store their local data remotely. According to Ravichandiran, "the data stored in the remote server can be accessed or managed through the cloud services provided by the cloud service providers (2014)."

Since working through the cloud is easy and simple, businesses, industries, students, communities are storing and accessing their data as well as hosting their applications in the cloud. This is because the cost associated with cloud storage and hosting is way cheaper than traditional methods of storage and local server hosting. In recent years, the cloud market is rising like never before. In the upcoming years, the usage of the cloud is expected to rise even further.

## III. Cloud Services

The working of the cloud is simple as the user sends a request to the cloud and in response; the cloud provides access to the user. According to Cyril and Kumar, "Cloud computing utilize the networks of a huge group of servers naturally brings a low rate data processing with a specialized connection. (2015)" Hence, cloud computing provides a new and interesting model of information technology services and support which benefit the user by helping them drive up their productivity. The same service is provided to multiple users making it flexible for the users to choose their service according to their requirements.

There are a variety of service models that are provided by cloud services around the globe. According to Gorelik, "the cloud service models describe how cloud services are made available to clients (2013)." These service models are briefly described as below:

- Software as a Service (SaaS): This cloud service model provides software solutions to its users. The user can access and work with the software and its features even from a remote location, which is offered by the cloud service providers. The major examples include emailing tools like Gmail, online word processing, presentation tools and spreadsheets, WhatsApp, etc.
- Infrastructure as a Service (IaaS): In this service model, the cloud service provider offers network, memory, storage, firewalls to the clients. The top IaaS service providers include Amazon Web Services (AWS), Windows Live SkyDrive (Microsoft One Drive), etc. In the IaaS model, the user just needs to pay for the storage and resources he/she has consumed.
- Platform as a Service (PaaS): Through this service model, the cloud providers offer their users a readymade platform for placing and delivering their own applications and services. Hence, Platform as a Service (PaaS) helps the user in managing their local servers and developing new applications where the users do

not need to buy expensive software platform tools. The top cloud providers that work on the Platform as a Service (PaaS) model include Microsoft Azure, Hadoop, Google Apps, etc.

Apart from being very easy to use and powerful, cloud computing has not been able to expand as the service providers have expected initially. This is due to a few security reasons. People don't think the cloud is fully reliable since they hardly have any idea about what goes on inside a data center that runs a cloud. Data confidentiality and integrity can also be broken by an eavesdropper, even if the cloud service producer is honest. Furthermore, data availability and privacy issues might not be handled properly by the cloud service provider. Security Challenges in Regard to Cloud Computing.

When multiple organizations share the resources offered by the cloud providers, there is a high chance that the data is handled improperly or the data might even get misused, due to a variety of reasons. Hence, securing the data in the clouds has turned out to be an important aspect as more and more people are using the facilities provided by cloud computing.

Security challenges occur in cloud computing when data is lost when an unauthorized user alters or changes various records in a cloud. Other security issues include insecure APIs (Application Programming Interfaces). Here are some of the major security challenges that are prevalent in the world of cloud computing:

1. Attacks on Virtual Machines (VMs): Cloud computing can be subdivided into front-end (client side) and back-end (server side). The front end section includes the client's computer whereas the back end includes the data centers from which the client receives the required services. The data centers consist of virtual machines, through which the data is stored and the cloud services are provided through the servers. As the cloud services heavily depend upon the VMs and the VM-wares, they need to be highly secured and need to be maintained and checked on a regular basis. Otherwise, these VM-wares will be very prone to attacks.
2. Losing Administrative Controls: Attacks in the cloud servers may lead to loss of administrative controls like transferring data to the cloud, location loss, redundancy, etc. These may further lead to data breach and unauthorized access.
3. Insecure Service Models: Cloud providers take the help of web browsers for delivering applications in Software as a Service (SaaS) to a cloud consumer. On the other hand, intruders use the web to hack into the cloud system. Hence, these situations possess "a threat to data because the issues like data leakage, malicious attacks and in the case of disaster backup and storage can lead to unauthorized access of sensitive data (Kaur, 2016)."
4. In PaaS (Platform as a Service), the developers who use the platform to create their software and application services, need to upgrade their PaaS applications on a regular basis.
5. In Infrastructure as a Service (IaaS), physical attacks are very much prevalent and they may lead to a lack of data security and data leaks.
6. Data Leakage: Data may be lost through any device or any storage area. It occurs when the data of an organization or an individual that is stored in the cloud gets leaked or detached due to various factors (both intentional and unintentional).

## IV. Major Steps towards Cloud Computing

The need for using the cloud is increasing day by day. As cloud computing is internet based, hence we need to ensure data security and privacy. High-end security is needed since a minimal data loss or data leakage can have a severe impact on the business' data or the individual's data, which is using cloud services.
Here are the major steps that are needed to be considered to ensure hassle-free and secure cloud computing:

- Protection of Data: A risk always prevails when multiple organizations share the same cloud service provider. Hence, the storage and protection of the data in the storage devices need to be properly handled. To make data secure in a cloud server, proper authentication and authorization are required. This will ensure rightful access to data that is stored in the cloud.
- Data Integrity: According to Ravichandiran, "Most of the web services face a lot of problems with the transaction management frequently as it uses HTTP services (2014)." To maintain personal data or crucial data, it is advised to not store personal information such as username or passwords in the cloud. This will ensure data integrity.
- Data Confidentiality: Data needs to be checked to avoid the vulnerabilities and malicious threats. Hence, to maintain data confidentiality, security tests such as cross-site scripting, access control mechanisms, etc. are needed to be performed on a regular basis.
- Limited Access to Data: If cloud storage contains data within an organization, then limited access is to be given to the employees of that organization and full access will stay with the authorities. In this situation, data encryption is needed to be used. Also, the information stored by an employee cannot be accessed by another person in an organization.

- Data Separation: Since multiple users take the services of the cloud and store their data in the cloud, most data appear to be similar. Hence the data can be accessed with ease just by applying a code. Hence, to avoid such a disaster, the data need to be separated and segregated as per their types and user's demand.
- Data Center Operations: Cloud service providers should make sure that the data of their clients need to be secured at any cost. Proper data center operation will ensure data security and integrity against data breaches.
- Encryption of Data: Encryption is a proven technique to secure data and information from malicious users and hackers. It is better to encrypt the data with some type of code before storing them within a cloud server. As a user, it is suggested that he/she verifies whether their data is backed up on other drives without any changes in the keywords of the file.
- Cryptography: It is a modern technique of the new network security technology. With the help of it, we can send and secure data over an unreliable pathway to protect the cloud user's valuable on the internet and even in the cloud servers.

## V. Conclusion

"Cloud Computing is a disruptive methodology that is rapidly changing how computing is done (Gorelik, 2013)." Cloud computing is fast and easy and presents a high number of benefits to their users, but, on the other hand, it still possesses a threat to the data stored by its users. Business organizations that use cloud services for data storage and access require trusted services to transfer and store their data to the cloud so that a win-win situation is maintained between them and the cloud service providers. Encryption of data is the best option for securing the data in cloud computing systems. In the upcoming years, better and advanced techniques of encryption will be applied to secure the important data of valuable users.

## References

[1]. Cyril, B. Rex, and S. Britto Ramesh Kumar. Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey. International Research Journal of Engineering and Technology (IRJET), 2015, p. 848, https://pdfs.semanticscholar.org/85da/e9a36820dab4a7c1e63dd2c2cf1e31e180dc.pdf. Accessed 22 Nov 2018.

[2]. Ravichandiran, C. Data Security Challenges and Its Solutions For Cloud Computing. International Journal of Advanced Computing, Engineering and Application (IJACEA), 2014, p. 60, https://www.iracst.org/ijacea/papers/vol3no62014/1vol3no6.pdf. Accessed 26 Nov 2018.

[3]. Gorelik, Eugene. Cloud Computing Models. Massachusetts Institute of Technology, 2013, http://web.mit.edu/smadnick/www/wp/2013-01.pdf. Accessed 26 Nov 2018.

[4]. Kaur, Manpreet, and Kiranbir Kaur. A Comparative Review on Data Security Challenges In Cloud Computing. International Research Journal of Engineering and Technology (IRJET), 2016, https://www.irjet.net/archives/V3/i1/IRJET-V3I157.pdf. Accessed 26 Nov 2018.