Academic Guru Publication House

Advances in Cloud Computing Security
Techniques and Applications
Volume 1
Year: 2021

AG PH Books

Review On Data Security Technology Based on Cloud Storage

Dr. Surender Kumar[1*]

[1]*Head/Assistant Professor, P.G. Department of Computer Science, Sri Guru Teg Bahadur Khalsa College, Sri Anandpur Sahib, (An Autonomous College) Punjab (India), drsurender.sgtb@gmail.com*

Abstract

Data security has become a major concern as cloud storage systems have been more widely used in a variety of complicated environments. It is possible that data may be incomplete due to node failures or other external intrusions, but it is also possible that cloud service providers actively hide or other circumstances make it difficult for the user to be aware of the change.

Approaching the issue of security with more prudence is necessary There have been several techniques created to safeguard files and other information as computer and communication technologies have evolved. The term "computer network security" refers to a combination of tools, processes, rules, and solutions that are used to prevent and respond to assaults on a network. All of these ideas must be defined and learned in order to properly assess an organization's security posture. Some of the methods and dangers to the network and computers are discussed in this document, along with possible programmes.

Keywords: Big Data, Cloud Computing, Data Security, Technical Analysis.

1. INTRODUCTION

Many firms consider data security to be a top priority. For cloud users, this means first identifying the data objects that need to be safeguarded, classifying the data according to its security implications, and defining the data protection policy and enforcement procedures. When it comes to most cloud-based applications, data objects would include not just bulky data stored in the cloud (e.g., a user database

* ISBN No. 978-81-955340-6-7

and/or a filesystem), but also data in transit between the cloud and the user(s) (In many circumstances, it would be more cost-effective and convenient to move large volumes of data to the cloud by mobile media like archive tapes than transmitting over the Internet.). It's possible that additional types of application data, such as user IDs or service audit data generated by the auditing model or service profiles or transient runtime data generated by the service instances, may also be included in data objects. The security implications for cloud users will vary according to the value of the data and the kind of data that is being stored in the cloud. Such as a user database at rest on the cloud servers, cloud users need robust security to ensure the confidentiality of their data as well as the integrity and availability of their information. The privacy of a user's identification information might be jeopardised if it contains any personally identifiable information (PII). Therefore, only authorised users should have access to the user's identification data. Data from service audits give proof of compliance and SLA fulfilment and should not be intentionally distorted. In order to prevent attackers from finding and identifying service instances, attackers need to keep their hands off the service profile information. During runtime, temporary runtime data should be separated from vital user business data and safely removed.

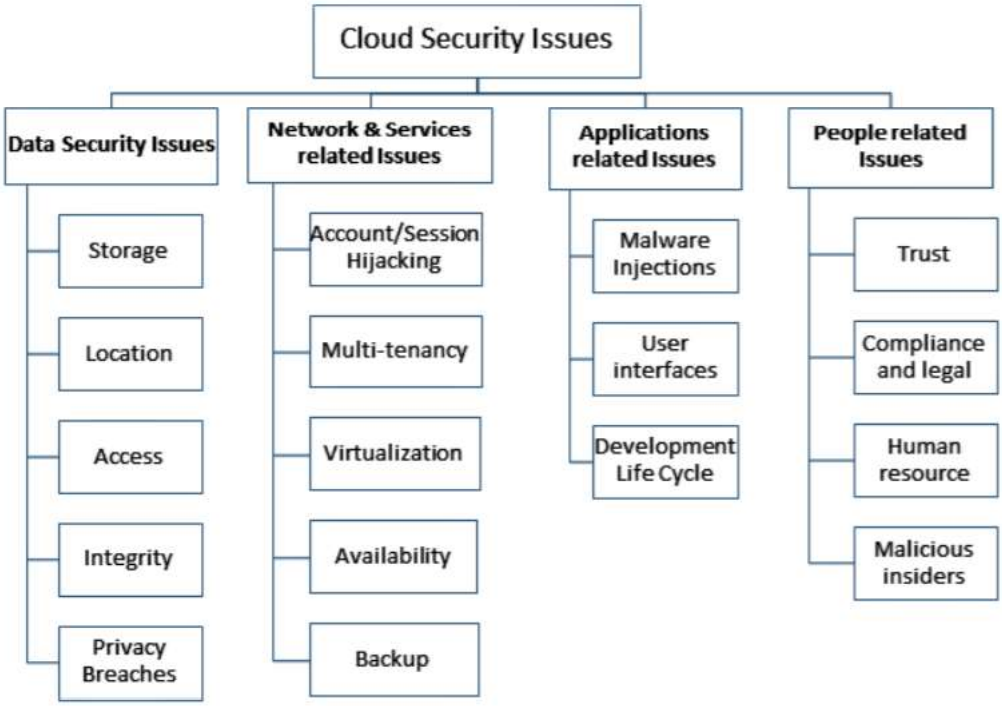

Figure 1. Summary of security issues in each category of Cloud Computing

2. Data Security Technology in Big Data Cloud Computing Environment

Improved data security in a cloud computing environment is dependent on thorough study and analysis of different data security technologies, which must be based on an understanding of cloud computing's huge data security challenges in order to increase data security protection technology's efficiency. It is now possible to significantly increase data security in the cloud computing environment by using the following data security protection technologies:

a) Data Encryption Security Technology

China's economic growth may be considerably accelerated if the full potential of cloud computing is used. However, there are a number of security issues that will impair the cloud platform's application effect in the big data cloud computing environment. Data leakage and theft have become an issue with the implementation of cloud storage and transmission. Big data security privacy must be examined more thoroughly in the research of data security technology, and attention must be paid to the successful implementation of data encryption security technology. The following elements of data encryption technology may be used to verify its efficacy as a security measure. In order to protect personal information, some users may encrypt and process it using the cloud platform's storage service. To a certain degree, this may increase the level of security of information. Cloud computing platforms, on the other hand, may encounter mistakes in data analysis as a result of the framework's inherent irrationality, reducing the effectiveness of encryption processing. Data encryption is a major concern for cloud computing workers, therefore they must be aware of it. The integrity of data must also be taken into consideration while transmitting data via the internet. Because it is necessary to adhere to the applicable criteria while transmitting data. When uploading data, however, the integrity of the data may be compromised. Users' ability to make effective use of the data will be severely hampered if it is not uploaded in its entirety. In addition, it will have an influence on the performance of cloud service platform applications. Third, while calculating data, we should be mindful of safeguarding user privacy. Data computing information and outcomes must be monitored by relevant departments, and the cloud computing platform's security must be regularly improved. Data leakage may be reduced by doing this. Data encryption technologies must be bolstered in order to secure the safety and privacy of information.

One of the large data cloud computing environment's data security methods is data encryption. This data protection technology's primary goal is to keep personal information private and secure. In order to avoid different data security difficulties, the system platform must properly optimise the data encryption technology. Traditional information encryption technology and innovative cloud server configurations are often used in data encryption processing. There must be a download of data to the local before encryption and combination work can be done using typical encryption techniques. To complete the encryption process, the cloud server setting technology may employ cloud server operations to establish relevant keywords. The old technique of data encryption is difficult to use and has a poor fault tolerance rate. It is possible that the new data encryption approach will significantly enhance the effectiveness of data search operations. However, we must be aware that data security cannot be completely ensured

during the use of the new encryption technology. Because of this, we must constantly optimise and develop data encryption technology in order to limit the frequency of sensitive information and increase data security [1].

b) Data Access Security Technology

Big data access security privacy protection technology and data destruction technology are two of the most important components of data access security protection technology. To begin, there is the issue of data security and privacy protection for large datasets. Cloud computing is required for the application process in order to store large amounts of huge data, which may be classified into public and private clouds. As one of them, the public cloud has a big storage capacity and is accessible to everyone. There is a large number of internal data resources that may be accessed via public cloud services because of the data's great openness. In most cases, private clouds are built on top of existing business infrastructure. There is a certain amount of privacy with private clouds. During the course of company growth and practical implementations, private data will be generated. This data must be stored and protected in order to guarantee that the company's regular and steady growth continues. Because of its uniqueness, a private cloud may make use of more sophisticated technology to safeguard its data resources. However, the expense of using private cloud data access security protection technologies must also be taken into account. If you want to assure data security and decrease costs, most firms will employ a combination of public/private cloud solutions. Second, the use of data erasure tools. Data collection, data administration, and data storage all play a role in the big data operation. Big data's destruction connection is also one of its most important linkages. The application value of the data will be directly impacted by the data deletion procedure. The research on data destruction technology must be strengthened to guarantee the soundness and comprehensiveness of data screening techniques in order to assure prompt and effective data destruction and avoid destroyed data surviving or being leaked. Furthermore, we must guarantee that data can be erased swiftly and properly to avoid harmful use of data and harm to the interests of businesses [2].

c) Data Sharing Security Technology

Data sharing security protection technology is an essential technology type for enhancing data transmission security. The following three components make up the bulk of shared encryption technology. First and foremost, cloud server encryption. The cloud server encryption technique may utilise public key encryption to retransmit the data to the cloud once it has been downloaded. The efficiency of this method of operation is poor, and it's a lot more difficult to use. Secondly, proxy re-encryption. To complete the data transmission procedure, this encryption technology must be sent from the authorised person to the agent, and finally to the accepting talent. In order to transmit data, there must be a number of steps. As a result, data exchange has a poor effectiveness. Third, conditional re-encryption through a proxy proxy is a possibility. Today's data sharing security protection technology is mostly used

in this manner. The proxy re-encryption approach necessitates the addition of encryption execution conditions throughout the application process. Using this method, not only can you better organise your data and make it easier to share, but it may also increase the safety of your data in transit. However, in the process of implementing data encryption techniques, it is also important to enable consumers to make a suitable choice of encryption methods based on their specific demands. This is the most effective method of ensuring the safety of sensitive data.

3. Security Techniques For Securing Cloud

Cloud data encryption is not a solution for data that has trust in the cloud's ability to protect it. Authentication and identity management, encryption, integrity checks and data masking may all be applied to cloud data using currently available security mechanisms. Here, security approaches are explained in Figure 1.

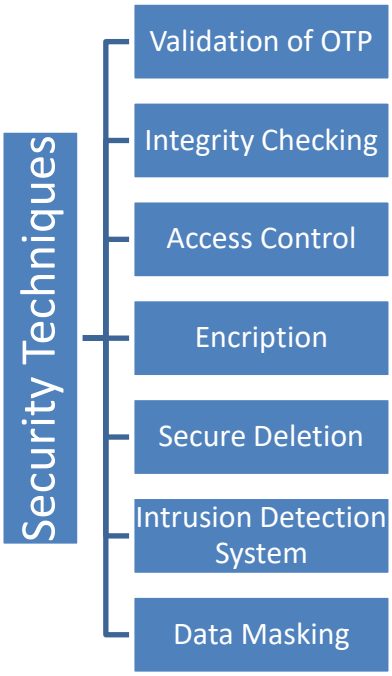

Figure 1 Security Techniques for Securing Cloud

- **Validation of OTP**

To authenticate a cloud user's identity, many banks now employ the One Time Password (OTP) approach, which generates an OTP using a random number generator and is often referred to as system factor authentication (see Figure 2). When used in conjunction with a second authentication factor, it is known as a Multiple Authentication Factor (MAF).

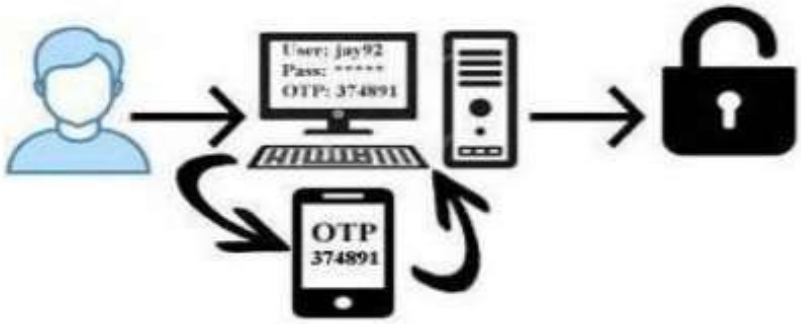

Figure 2 OTP Authentication

- **Access Control**

An authorised cloud data user may see and modify their own data, but an unauthorised cloud data user cannot do so because of access control measures in place at both the cloud service provider and the cloud data owner.

- **Integrity Checking**

Cloud data integrity is an assurance that only authorised users may update or access cloud data. Simple cloud-based data verification assures the integrity of the data and that it has not been altered in any way. As a result of PDP and POR, it is possible to secure the integrity of cloud data on a distant server while verifying that the proof that cloud data is saved by the user on the server has not been altered [3].

- **Encryption**

Using cloud storage security encrypts all of your data before it travels from your local computer to the cloud, making it virtually impossible for anyone else to read your private information. Only an authorised user with access to your decryption key can decrypt your encrypted files, making it essential to keep encrypted data separate from the encryption key.

The method of encrypting and decrypting is shown in Figure 3.

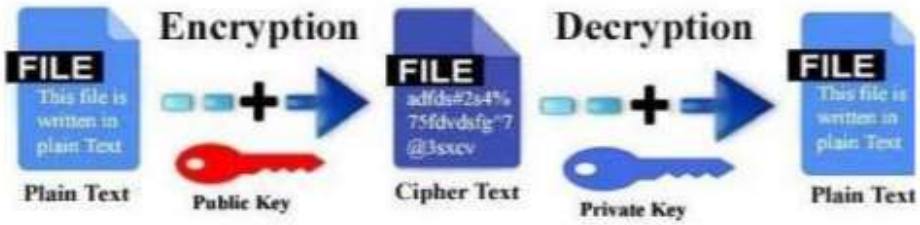

Figure 3 Data Encryption and Decryption

- **Secure Deletion**

It's critical to know how the data on the server gets purged. In this strategy, we destroy the media before it is reused and at the same time give protection for accepting the data that was on the media before to deletion. This sort of data is often transmitted at a lower level of categorization since the security for accepting earlier data is not supplied [4].

- **Intrusion Detection System**

To put it simply, an intrusion detection system (IDS) monitors system activity and network traffic in order to look for any indications of illicit activity. In the modern day, most hackers use a variety of various methods to get access to private information. Any unauthorised or harmful use of IT resources is considered an incursion. It is the goal of the invaders, who want to get access to sensitive information, to wreak damage. An Intrusion Detection System (IDS) may be divided into two categories: a network-based IDS (NIDS) that monitors network traffic and keeps an eye on ongoing assaults, as well as a Host-based IDS (HIDS), which is placed on a single system or server and monitors unlawful activity on that system.

- **Data Masking**

Data masking is a method for protecting cloud data from unauthorised access and theft while also ensuring that the data is replaced with fictitious but plausible data. De-recognition, cleansing, and comprehending the phrase are all terms that are used interchangeably to describe the same muddled process. Not only is data masking an algorithm, but it is also a collection of publicly available data. Static Data Masking (SDM) is utilised by most businesses when developing tests, and this is the only form of masking that is available when utilising outsourced developers in a separate firm or location to create tests. Duplicating the database is the only option in these situations. Based on the user's function in the organisation, Dynamic Data Masking (DDM) allows access to certain information.

4. CONCLUSION:

In the recent decade, businesses, companies, and hackers have all benefited from the widespread use of cloud computing technologies. Cloud computing security has been threatened by the rise of current cloud architectures and high-speed internet with new developments. One benefit of moving to a cloud-based system was that it allowed a company's capacity to adapt and grow with the ever-changing industrial landscape. For a variety of reasons, this rendered their data less secure and more prone to attack. There is a need to focus more on research and use of different data security protection solutions in the cloud computing environment because of its unique properties. Only by improving data transmission efficiency can the security and reliability of data transmission be enhanced.

REFERENCES

1. Zhang Qian, Yang Huibi. Exploration of big data security and privacy protection under cloud computing[J]. Science Popular (Science Education), 2017, 000(010):192-192.
2. Yuan Huihua. Research on Data Security in Big Data Cloud Computing Environment[J]. Information Technology and Informatization, 2019.
3. S. Sharma, "Data Integrity Challenges in Cloud Computing", 4 th international conference on recent innovations in science engineering and management, pp. 736-7436, 2016.
4. DIGITAL GUARDIAN [online] https://digitalguardian.com/blog/what-cloud-encryption (Accessed 25 December 2019).
5. G.K. Ravikumar "Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing", International journal of engineering science and Technology, vol. 3, no. 6, pp. 5150-5159, 2011.