An Analytical Overview of Cloud Storage Security Issue

Srinivas Reddy Baddam[1], Dr. M. Raghvender Sharma[2], Retired Prof. M V Ramana Murthy[3]

[1]Department of Computer Science, University College of Science, Osmania University
[2]Department of Statistics, University College of Science, Osmania University
[3]Retd Prof & Chairman in Mathematics and Computer Science, Dept of Mathematics, Osmania university, Hyderabad

Abstract:
The ability of cloud computing, an emerging paradigm, to lower computer costs, has made it the hottest research field of the day. The most intriguing and alluring technology of the present day is that which provides customers with services on demand via the internet. Security has emerged as the primary barrier preventing the development of cloud settings because cloud computing stores data and its distributed resources in the environment. Many users save their personal information on the cloud, necessitating the need for data storage security on the storage medium. Security when uploading data to cloud servers is the main worry in a cloud system. Many diverse communities have given cloud data storage a great deal of thought or attention. Data outsourcing requires the involvement of a third party. Third parties are crucial for preventing and managing unwanted access to cloud storage of data. The security concerns with cloud storage are covered in this study article

Keywords: Cloud service provider (CSP), cloud data storage, security issues, policies & protocols.
DOI: 10.24297/j.cims.2023.7.6

1. Introduction

With little management overhead, cloud computing allows on-demand access to computing and data storage resources that may be tailored to each client's specific needs. For customers with limited computing or storage capabilities who are reluctant or unable to purchase and operate their own computing infrastructure, the recent increase in the availability of cloud services makes them appealing and economically practical. The steadily rising popularity of businesses providing cloud services can be attributed to the constantly growing demand for computer capacity and storage. Clients can simply execute apps straight from the cloud and outsource enormous amounts of processing and data to distant places.

Cloud-based internet security is an outsourced solution for storing data. Instead of saving data onto local hard drives, users store data on Internet-connected servers. Data Centers manage these servers to keep the data safe and secure to access. Anytime you access any file that was stored remotely, you are accessing the cloud. How is cloud storage any different from local storage? The primary contrast is that the cloud vendor uses internet for data transfer, from secure data centers to individual devices that the cloud is accessed on. Hence, this makes cloud centralized" [1]. Both consumers and businesses utilize cloud storage extensively. Users don't take any care with the data they store on their hard drives, and nobody knows where the data is actually preserved. Data security has become a top issue for the user as the majority of the data will be kept in a network computing system on top of the cloud. The same cloud system may be used by various customers, including businesses and individuals. The cloud computing system should have different levels of data protection prepared for different users since different users require varied levels of data security and have varying financial means. It does represent the idea of on-demand cloud computing services.

Using online apps and web services like Amazon E2/S3, resources are dynamically provisioned on a fine-grained, self-service basis through the Internet. This is known as public cloud computing. Both internal cloud and private cloud have been called neologisms. However, it merely refers to using and managing hybrid systems. All cloud users collaborate as a single, sizable group. And the cloud that belongs to the group, like IBM's Blue Cloud and EMC's Doli Projects.A hybrid cloud infrastructure is made up of services from many internal and/or external sources. Given that you have less control over many aspects of the public cloud and that you must share machines with strangers, security concerns have grown. In a private cloud, all users can be seen as trustworthy individuals, and all servers and storage devices are under your control, much as in corporate security.

Fig.1: Cloud data storage model

Cloud Storage

One of the main applications of cloud computing is cloud storage. Cloud storage can be summed up as the online archiving of data on the cloud. A cloud storage system is viewed as a distributed data center that offers some sort of interface for storing and accessing data. These data centers often leverage cloud computing technology. Data stored in the cloud appears to be kept in a specific location with a distinct name.

There are four main types of cloud storage

Personal Cloud Storage:

It's also referred to as portable cloud storage. In this sort of storage, a person's data is kept in the cloud and is accessible from any location.

Public Cloud Storage:

The enterprise and storage service provider are separate in public cloud storage, and no cloud resources are kept in the company's data center. The enterprise's public cloud storage is entirely managed by the cloud storage provider.

Private Cloud Storage:

Private cloud storage integrates the enterprise's data center with the cloud storage provider. In private cloud storage, the infrastructure is often maintained by the storage provider and is located in the company's data center. Private cloud storage maintains the benefits of cloud storage while assisting in resolving any security and performance issues.

Hybrid Cloud Storage:

It is a hybrid cloud storage solution where certain vital data is stored in the private cloud of the business and other data is stored and accessed from a public cloud storage provider.

2. Literature Survey

The key scientific challenge around cloud computing is ensuring the privacy of user data in cloud storage. Users' sensitive data is stored by cloud storage providers; it must be protected. Information technology has recently seen success with cloud computing, which will rule the IT sectors in the years to come. Additionally, cloud computing has enormous difficulties. It is more important than ever to secure the necessary physical, logical, and people security safeguards,

especially while storing data in the cloud. Additionally, it's possible that the administration of such massive amounts of data is not completely reliable.

With the improvement in cloud infrastructure, security issues and standards have been on the rise. To this end, multiple research projects have been conducted to exploit and understand the severity of said threats, if any. Some of the examples can be seen as demonstrated" by Zissis et. Al [2].

The paper [3] has provides a "categorization of security issues on the basis of several security topics. The work provides an overview of previous research work. The author present several topics related to cloud security and provide security issues related to each topic. The security landscape in this paper is very wide as compare to other papers. At the end, this paper gives some recommendations of various open challenges that to be solved in the future. The recommendations is very fruitful for future research work in this area".

The paper [4] presents a "detailed study about the cloud security and privacy for cloud service providers. The author describes the security and privacy both term separately. First, focus on security terminologies such as confidentiality, integrity, access control, availability, and auditing characteristic, after that focus on widely used privacy methodology. In addition, the paper contributes some solution on multi-location storage server".

The paper [5] "discusses the security issues and challenges present in the public and private clouds. After the discussion, they discussed some more security issues like service availability, multi-tenant service issues, data storage issues, identity and access control issues. They mainly focus on data utilization management aspects".

The IaaS cloud security [6] "includes security on virtualization, storage, networking, and physical sides of cloud infrastructure networks. Multi-tenancy is a property of the cloud, which allows the users to access the resources in a shared manner. Multi-tenancy is the major property of the cloud that lead many security threats and issues".

Cloud Security

Cloud security is a part of computer security. It outlines a set of rules, safeguards, and technological advancements that are beneficial for protecting data and services. Threats and

attacks have an effect on the cloud system either directly or indirectly. New security issues could arise as a result of the cloud resources' integrity, availability, and confidentiality being compromised, as well as the services offered at different levels.

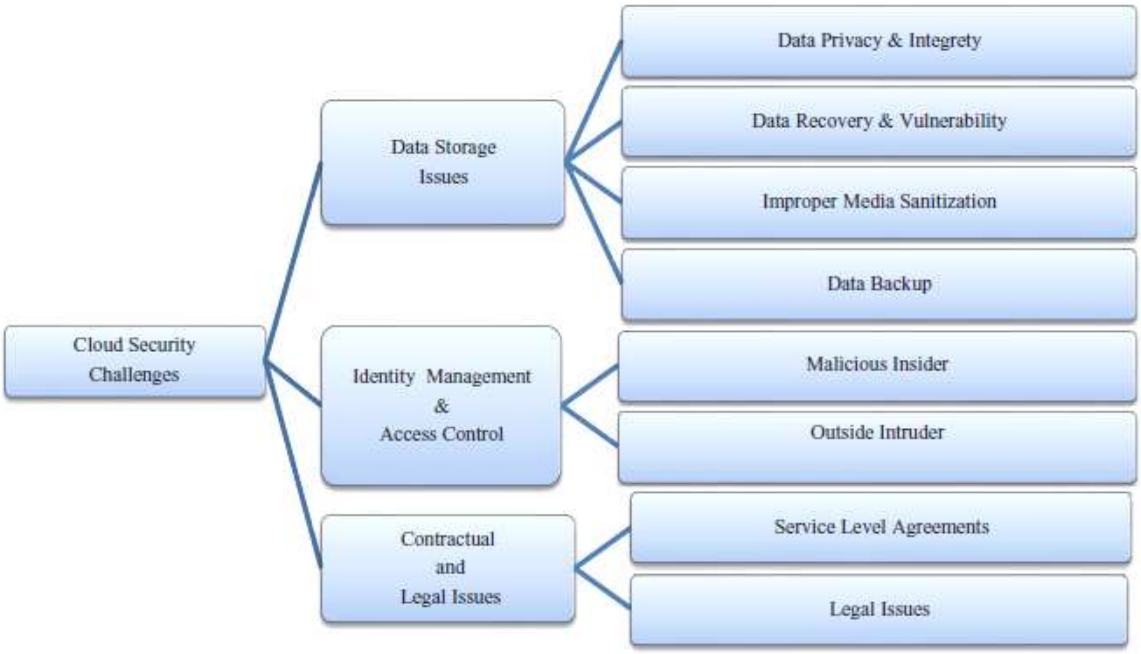

Fig.2: Cloud security Challenges

Data privacy and Integrity : Despite having lower costs and requiring less resource management, cloud computing comes with a number of security vulnerabilities. The cloud computing model must ensure data availability, confidentiality, integrity, and privacy, as we've already stated. However, the cloud computing approach is more vulnerable to security risks as a result of the limitations mentioned above. There are a ton of applications hosted on the cloud because using it is so simple. The security risks to cloud clients are increased by these factors. A data breach will come from any successful attack on a data entity, giving unauthorized access to the data of all cloud users. This integrity violation caused cloud data to lose its multi-tenant nature. There is a high risk of losing technical data, particularly for SaaS vendors. Data processing presents a high risk when data is transformed among several tenants in addition to these issues. Virtualization allows users to share a variety of physical resources. As a result, the CSP and/or organization's malicious insiders start attacking. Due to these situations, a malicious user may be able to handle the data of other clients while attacking their stored data. When the CSP contracts with a third party for data storage, there is even another serious risk. The procedures for key generation and key management in cloud computing Standards for

cryptography are insufficient. However, without standardized and safe key management for the cloud, conventional encryption methods cannot work effectively in a generalized cloud computing context. Cryptography may also ensure any potential risks connected to cloud computing in this way.

Data recoverability and vulnerability: The resource pooling and elasticity aspects of the cloud enable dynamic and on-demand resource provisioning for consumers. The resource given to one user may be transferred to another user at a later time. When it comes to memory and storage resources, a malevolent user may employ data recovery strategies. The data recovery vulnerability may pose a major threat to the sensitive user data.

Authentication: Data stored by cloud users is accessible to all unauthorized users on the internet. From now on, the interchangeability management entity must be present for both certified users and assistance clouds.

Access Control: The cloud must have the proper access control policies in order to verify and promote only authorized users. Such services must be flexible, thoughtfully developed, and conveniently overseen in their allocation. The Service Level Agreement (SLA) must be the foundation for the integration of the approach governor provision.

Policy Integration: End users can access a variety of cloud service providers, including Amazon and Google. Because they employ their own policies and methods, there are very few conflicts between their policies.

Service management: In this, many cloud service providers, including Amazon and Google, work together to create new composed services to satisfy the needs of their clients. To obtain the simplest locally focused services at this point, there should be a purchasing division.

Trust Management: The establishment of a trust management strategy that takes into account the negotiation of trust between user and provider is necessary in the cloud environment as a service provider. As an illustration, for a provider to disclose their services, both the user and the supplier must have some level of trust in each other.

3. Conclusion

Users can save their data in a remote storage location thanks to cloud computing. But the biggest risk to cloud computing is data security. Many businesses are reluctant to adopt the cloud environment as a result. In order to combat this, a CSP's Service-Level Agreement (SLA) to its clients should include provisions for confidentiality, integrity, and availability. Otherwise, make sure that no sensitive data is stored in a public cloud and that, if it is, it is encrypted. Data integrity can also be achieved through the deployment of efficient auditing tools.

References

1. Mladen A. Vouch, ¯Cloud Computing Issues, Research and Implementations‖, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246.
2. D. Zissis et al, - Addressing Cloud Computing Security Issues, Future Generation Systems 2012, Pages 583-592.
3. Fernandes DA, Soares LF, Gomes JV, Freire MM, Incio PR. Security issues in cloud environments: a survey. International Journal of Information Security. 2014 Apr 1;13(2): pp. 113-170.
4. Zhou M, Zhang R, Xie W, Qian W, Zhou A. Security and privacy in cloud computing: A survey. InSemantics Knowledge and Grid (SKG), 2020 Sixth International Conference on 2020 Nov 1 (pp. 105-112). IEEE.
5. Tari Z., Yi X., Premarathne U. S., Bertok P., and Khalil I. Security and privacy in cloud computing: Vision, trends, and challenges. Cloud Computing, IEEE, 2019.
6. Vaquero LM, Rodero-Merino L, Morn D. Locking the sky: a survey on IaaS cloud security. Computing. 2020 Jan
7. Mohammad et. al., - An Analysis of the Cloud Computing Security Problem, 2016, Swinburne University of Technology, Hawthorn, Victoria - Australia.
8. F. –T. Lin, T. –S. Shih, "Cloud Computing: The Emerging Computing Technology", ICIC Express Letters Part B: Applications (ISSN: 2185-2766), vol. 1, (2020) September
9. Latifur Khan and Bhavani Thuraisingham, "Security Issues for Cloud Computing", in Technical Report UTDCS-02-10, February 2020.