2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)
Department of Electrical & Electronics Engineering, Galgotias College of Engineering and Technology, Gr. Noida, India

Security Threats and Challenges in Public Cloud Storage

1st G Nagarajan
Assistant Professor
School of Computing Science and Engineering
Galgotis University
gnagarajan@galgotiasuniversity.edu.in

2nd Dr K.Sampath Kumar
Professor
School of Computing Science and Engineering
Galgotias University
k.sampath@galgotiasuniversity.edu.in

2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-7281-7741-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICACITE51222.2021.9404641

Abstract: **Cloud computing is a modern way for many businesses to offer computing tools and services that have transformed their business at a low cost. But the main concern is protection and privacy in cloud computing using a security program, encrypted file systems, and data loss software the problem and threats decreased. But the safety risks still exist in current days. Many cloud computing organizations and consumers also do not trust cloud providers to store their confidential data in public cloud storage because of the scarcity of accuracy in the protection of information sharing. This paper focuses primarily on security risks and problems that different cloud platforms face (Education, Enterprise, and Healthcare).**

Keywords: Public Cloud Storage, CSP, Security Threats, Cloud technology

I. INTRODUCTION

Data storage in cloud space is more important than a physical computer in the real world. Because of the events of their technological or personal lives, people have to compromise with millions of Mb of data throughout the day. [1]. All this information takes a lot of storage space and flexibility in its time around the 24-hour numerous appliance that is widely used and linked by users to get their job done [14]. However, the physical storage space is at a loss because of the expenses associated and a variety of other factors such as the device model or technologies used to operate. A Many companies have developed fast and inexpensive infrastructure; to address the problems of data collection and accessibility for consumers, worldwide known as the cloud computing system [2]. It may be appropriate, or at least possible, for a person to store data on remote cloud servers in particular circumstances. These include the following three critical states or situations that are specific concerns within the cloud computing operational context:

1. The transmission of confidential, non-public data to a cloud server,

2. Transmitting information from the cloud server to the operating systems of the customer and

3. Storage of non-public data from clients on cloud servers that are remote servers that are no longer owned by buyers.

All cloud storage is severely vulnerable to a violation of security that makes analysis and investigation a fundamental one within the safety factors of cloud computing practice users connect their data files to the cloud. They leave the information in a position to be unable to do so. Typical cloud threats include misuse of information, malicious insiders, unstable interfaces, and APIs with technologies gain understanding, loss of data or leaks, account or service hijacking, and unknown profile danger [2].

[I] Customer security problems

Cloud provider companies provide services such as software, platforms or networks [2]. The provider must ensure that data and applications are secured against security problems faced by its clients. The customer must ensure that security steps have been taken by the provider to protect their information.

[II] Traditional data storage VS Cloud data storage

The conventional data centers include several hardware components, such as a desktop computer, connecting to the network via a web server. The server is usually mounted on the premises and provides connection to the gathered information and app of the business to all employees using the hardware.

To serve more customers, companies with that kind of IT framework must purchase new resources and upgrades to ramp up their storage space and facilities. In addition, mandated technological improvements are needed for conventional IT infrastructure to ensure that secure services are applied in the event of a hardware breakdown. The hardware for many IT data centers must be designed and managed by the internal IT agency. To install and manage the hardware, an in-house IT department is essential for many companies with IT data centers.

A simple IT architecture that allows users to take complete care of the apps and data processing on your local server is one of the safest solutions for hosting your files. For businesses that need to run a variety of app types, the customized, dedicated platform is suitable.

Cloud Computing is much more abstract than available by physical devices as a virtual storage solution. The cloud holds both server software and networks. You will lease data storage space from cloud hosting providers on a cost-effective pay-per-use basis, rather than wasting funds on purchasing physical servers in-house. It is a simulated environment of real-time hosting simultaneously between several separate servers.

Cloud infrastructure is an alien approach for data collection and data transmission that is less secure than local data hosting, which can impact the provision of information. The stored information and apps can be penetrated and used in the cloud by anyone with access to the server; anywhere a web link is available. When going into the cloud, the cloud infrastructure provider should be chosen, and hosting cloud

services should be completely open to guarantee that optimal security mechanisms are applied. By using strategies such as firewalls and virtualization, the Cloud Service Provider (CSPs) has vowed to guarantee data protection over client stored data. These mechanisms would not give complete data protection because of their vulnerabilities' over the network, and CSP has full command of cloud applications, hardware, and client data.

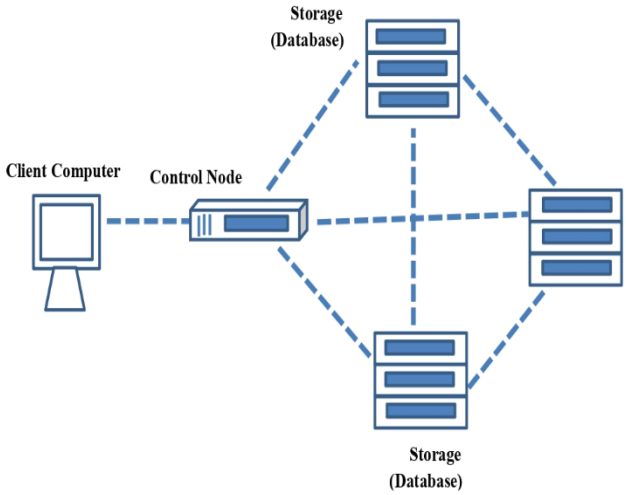

Fig.1: Working of Cloud Data storage

Traditional Security VS Cloud Security

Cloud safety	***Traditional IT safety***
Data Centers by Third Party	Data Centers in-house
Poor readiness technology facilities.	Strong expenses for readiness.
Rapidly extensible	Unrushed scalable
Productive system utilization	Performance reduction
Cost based on data storage usage	Higher cost to preserve data

Table 1: Traditional Security VS Cloud Security

II. VARIOUS CLOUD COMPUTING PLATFORM SECURITY ISSUES

A. Education Cloud Platform

Now a day's remote education is extensively used in the education department resource sharing and resource integration are a huge concern, with the prevalent use of the cloud for learning. Security challenges are now becoming more relevant for the educational cloud, the data loss, the educational cloud, because of the need for a large-scale school awareness and quality, is highly competitive and reliable[3]. Cloud services vendors are using some common technology for data storage, such as encoding and access protection, to secure information from any data violations and breaches[1]. In addition to the information theft, losses, and security assaults in an educational cloud network, we discovered that students must take care of their privacy concerns and increase the efficiency of their teaching. [3].

B. Enterprise Cloud Platform

To manage the infrastructure and cope with any crises, e-commerce or state-owned banks with huge data need a large number of operating and maintenance staff. However, the operating team with the most relevant authority can quickly access all confidential information from their cloud offering [1]. Another security challenge overlooked by most people here is the use of the community wireless Internet connection to access their privacy. Most cities have free urban wireless networks. Before beginning to use them, most individuals do not care whether it is safe and safe or not. Both the information will be exchanged without encryption. Clients can connect to the internet and use their telephones to access vulnerable data from their accounts, for example, financial or payment platforms. Hackers will quickly use customers' careless habits to capture their payment contacts [1, 3].

The bandwidth, which is still incredibly small, is one more problem with the free network. During their business transactions, potential users may lose touch and become more vulnerable to future attacks on their private accounts. In addition, the Application Programming Interface (API) is used by both traditional and start-up finance institutions mostly for offering their customers third-party applications. Hundreds of online retailers and businesses sell separate non-stable third-party APIs; This is a highly insecure area in which hackers repeatedly strike [1].

C. Mobile Phone Data

Human beings are becoming increasingly aware of a new stage of record sharing in which data stored in the cloud and mobile devices are used to store/return cloud data, with the rise in cloud storage and the popularity of intelligent mobile devices. The growth of cloud computing and the popularity of intelligent mobile devices increasingly allow us to learn more about a new stage of record sharing; where data is stored on the cloud and mobile devices are used in the cloud for storing/recovery of data[4]. Mobile computers typically have no ability for storage and computation, and the cloud has enormous power. The Cloud space is used to store and exchange data in order to achieve good results. [4].

Different cloud mobile apps have widely used at this time. Individuals (Information Holder) can use these applications to transfer their photos, pictures, records and other documents to the cloud and share data with other people (data users) they are willing to appoint[15]. CSPs provide information owners with data processing capabilities. Because private data is open to owners the user can choose whether or not to reveal their statistical data or only to other users. In addition, due to the vulnerability of the smartphone information stored on the server, the protection of personal data is a major issue for several clients.

D. Healthcare Cloud Storage

Personal patient health information is costly property of different health-related technologies such as remote detection, illness control, and mature individuals, for example for mobile phones, smart clocks, smart bands and smart cups, etc., [6]. Through these gadgets, vast quantities of private health records are generated, and these statistics are useful sources for healthcare research and industrial apps. The ownership and maintenance of the personal information should be the responsibility of the respective users[8]. Different insurance providers, sources of products, or delivered in different

healthcare networks typically control health records. Generally speaking, it creates challenges to data sharing and places data protection at risk as these consolidated data stores and service providers represent tempting cyber threat targets[7, 8].

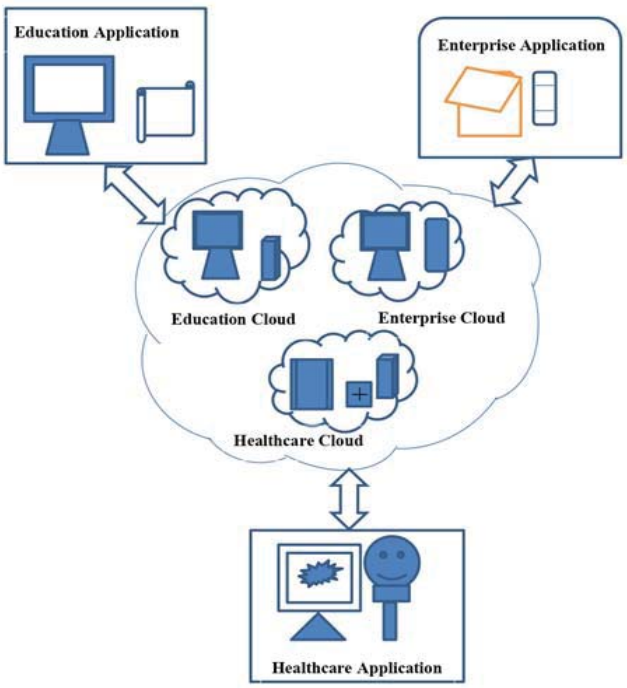

Fig.2: Cloud Storgae model

III. CLOUD STORAGE ISSUES

No wonder businesses have hopped on the cloud car with the rising pace and availability of cloud computing. A cloud server may be a versatile tool that not solely satisfies storage and process necessities however additionally helps to avoid wasting thousands of dollars in IT investment for the enterprise data[9].

The following are significant threats that need to be discussed while using company cloud space and document distribution applications.

A. Out of control data

Organizations have had to take care of more recent privacy concern, such as the lack of hypersensitive information management, with cloud offerings such as "Google Drive, Dropbox, and Microsoft Azure" being a routine part of industry growth[7]. The concern here is that when third parties have exploited file-sharing systems, the information is always taken out of the IT atmosphere of their business, which means that the security of information is far removed from the management of the company.

B. Data Out flow

Today's, organizations are now putting more data and base in the public cloud. The public cloud has rendered it much more effective, flexible and also much easier for companies to adopt emerging technologies. Any organizations that are back from the cloud have done so in fear of their information leakage. This fear is due to the cloud being a multi-user system in which all services are distributed [5, 15]. It is also a trusted third-party service that implies that the vendor risks viewing or mismanaging information potentially. The competences of a third party are solely human to be questioned. Various external risks, like cloud-based hacking, or intrusion on cloud user accounts, can lead to data leakage[12].

C. Snooping

Cloud files are among the most insecure without the possibility of hacking security mechanisms in place. Additionally, fact hangs on and transmitted over the net is a significant risk problem, and information; can still be caught on the path to its end [5]. The excellent security structure of threats would have encrypted documents and transmitted over a tightly closed network it prevents outsiders from accessing metadata from the cloud[10].

IV. SECURITY CONTROVERSY IN CLOUD STORAGE SYSTEM

Cloud computing firms continue to take advantage of promises to improve performance, greater robustness, and better agility at a fast rate. In this mutual accountability model, the 2019 Cloud security review illustrates what is and what doesn't succeed for security teams in protecting their cloud records, applications and services. The findings continue the problems of the past [13]:

1. The highest risk among cyber-security experts is 64 percent data retention and leakage.
2. 42 percent improper access detection and misuse by unauthorized access; the most considered risk to cloud protection this year is top one in the study.
3. 42% occupy cloud platform mis-configuration.
4. Two of the SOC team's most challenging defense activities are enforcement (34%) and infrastructure safety visibility is 33%.

Security issues	**Percentage of security issues**
Data loss and leakage	64%
Access control	42%
Interface and API	42%
Platform Mis-configuration	40%
Infrastructure visibility	33%
Compliance	34%

Table: 2 Percentage of issues based on cloud storage system security

Large companies consider a range of key benefits in identifying cloud-based security solution; respondents may prefer cost reduction and pace up implementation and efficiency to choose cloud-based security mechanisms [14].

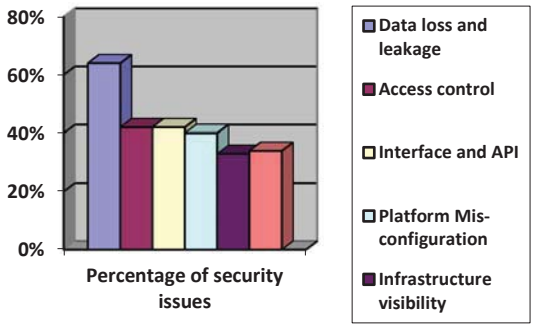

Fig.3: Cloud storage system protection vulnerability

Recent problems include high risks for data loss and leakage, according to the research optimization required to improve the public cloud safety in the context of a current algorithm and model [13].

V. CONCLUSION

From this study, when organizations store data physically, a lot of hardware needs to be purchased and a lot of space required, and it takes more time and expense to handle it. It concludes that today's global cloud computing is increasingly growing in the cloud industry and is necessary for businesses and organizations to store their massive data at a low cost. But we cannot compromise security because nobody wants someone else to use or misuse their data. The affordability of records, scalability, security, accessibility, and functional needs in the Public Cloud are more beneficial than conventional storage. Data centers and cloud service providers have given a certain degree of client security to secure their business and corporate data even though more security is required for client data in public cloud storage in the areas of confidentiality and privacy.

VI. REFERENCES

[1] Sonali Chandel, Tian-Yi Ni, Geng Yang, "Enterprise Cloud: its Growth & Security Challenges in China," 5th IEEE International Conference on Cyber Security and Cloud Computing, 2018.

[2] Nitin Chauhan, Laxmi Ahuja, Sunil Kumar Khatri,"Secure Data in Cloud Computing Using Face Detection and Fingerprint"International Conference on Inventive Research in Computing Applications, IEEE Xplore Compliant Part Number:CFP18N67-ART; ISBN:978-1-5386-2456-2,2018.

[3] Xiaotong Sun, "Critical Security Issues in Cloud Computing: A Survey" 4th IEEE International Conference on Big Data Security on Cloud, 2018.

[4] Hussam Hourani, Mohammad Abdallah " Cloud Computing: Legal and Security Issues" 8th International Conference on Computer Science and Information Technology (CSIT) ISBN: 978-1-5386-4152-1, 2018.

[5] Naresh Data Storage Security Issues in Cloud Computing" 2nd International Conference on Intelligent Computing, Communication & Convergence Elsevier, Procedia Computer Science 92 (2016) 128 – 135.

[6] Wei Nie, Xiangfei Xiao, Zhaohui Wu, Yuanhui Wu, Fang Shen, Xionglan Luo, "The Research of Information Security for The Education Cloud Platform Based on AppScan Technology" 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud) 2018.

[7] Ruixuan Li, Chenglin Shen, Heng He, Ruixuan Li, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu, " A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing" IEEE TRANSACTIONS ON CLOUD COMPUTING.

[8] Xiaochen Zheng, Raghava Rao Mukkamala1, Ravi Vatrapu1, Joaqun Ordieres-Mer "Blockchain-based Personal Health Data Sharing System Using Cloud Storage" IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) 2018.

[9] Hongbing Cheng ; Chunming Rong ; Kai Hwang ; Weihong Wang ; Yanyan L, "Secure big data storage and sharing scheme for cloud tenants", IEEE,ISSN: 1673-5447, DOI:0.1109 , CC.2015.7122469, June 2015.

[10] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[11] More, S. and Chaudhari, S., 2016. Third Party Public Auditing Scheme for Cloud Storage. Procedia Computer Science, 79, pp.69-76.

[12] Dave, D., Meruliya, N., Gajjar, T.D., Ghoda, G.T., Parekh, D.H. and Sridaran, R., 2018. Cloud security issues and challenges. In Big Data Analytics (pp. 499-514). Springer, Singapore.

[13] https://www.ethicalhat.com/2019/08/cybersecurity-insiders-2019-cloud-security-report, 2019.

[14] P.Mell and T.Grance,"The NIST definition of cloud computing",National Institute of Standards and Technology,Tech. Rep.,2009.

[15] Digital Guardian. 2021. Digital Guardian. [online] Available at: <https://digitalguardian.com/> .