International Journal on Emerging Technologies **10**(2): 195-199(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

A Security Risk on Data Storage in Cloud based System –Survey

G. Nagarajan and K. Sampath Kumar

School of Computing Science and Engineering,
Galgotias University, Greater Noida, Uttar Pradesh, India

(Corresponding author: G. Nagarajan)
(Received 03 May 2019, Revised 10 July 2019 Accepted 17 July 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Organizations sketchy to enjoy the benefits of cloud computing are having the option to use the services and resources from a public cloud or to make their own private cloud infrastructure. Public clouds are using proprietary cloud software and security is usually maintained by issuing organizations. However, many organization and users of the cloud technology still do not trust the cloud entirely for their sensitive data storage, mainly due to the lack of transparency in the security of data sharing in the cloud. There are many security risks involved that may compromise the data stored in cloud applications, the data stored on cloud the third party who can do anything to our data like change it, corrupt it, delete it, and give access to others. So, the data security on the cloud based application becomes a major issue. This paper mainly focuses on security vulnerabilities and issues in confidentiality and privacy over client data storage.

Keywords: Data Storage, Security, Cloud, Organization.

I. INTRODUCTION

In the modern world, data storing in cloud space becomes essential rather than physical device, with the assistance of cloud computing, we are able to work simply and effectively. Now we have a tendency to store various information within the cloud server and may facilitate remote area's individuals by storing their vital data is stored in the cloud [8]. People get to deal with thousands of megabytes of data every day because of the activities in their professional or personal life. All this data needs a lot of storage space along with consistency in its availability round the clock across various devices that the users commonly use and connect to get their work done. However, the physical storage space has a limitation because of the cost involved and a few other factors like the device type or the technology they use to function. Many companies have come up with a new, fast, and low-cost technology to overcome the challenges regarding storage and availability issues of data for the users which is commonly known as Cloud Computing to the world [1] in particular situation, it might be required or at least possible for a person to store data on remote cloud servers. These give the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing [5]:

1. The transmission of non-public sensitive data to the cloud server,
2. The transmission of information from the cloud server to client's computer systems and
3. The storage of clients' non-public data in cloud servers which are remote server no longer owned by the purchasers.

All the over three state of affairs of cloud computing are severely prone to protection breach that makes the research and investigation within the safety factors of cloud computing practice an fundamental one, when user add their data files onto the cloud, they are leaving the information in a location where is out of their control [2]. Typical cloud risks cover information abuse, malicious insiders, insecure interface and APIs, shared technology issues, data loss or leakage, account or service hijacking, and unknown threat profile [3].

[I] *Security issues faced by customers*

Cloud providers organizations provide software, platform or infrastructure as a service. Security issues faced by their customers, the provider must ensure that data and applications are protected.

Customer must ensure that provider has taken security measures to protect their information.

[II] *Traditional data storage VS Cloud data storage*

Traditional data centers consist of various pieces of hardware, such as a desktop computer, which are connected to a network via a remote server. This server is typically installed on the premises, and provides all employees using the hardware, access to the business's stored data and applications.

Organizations with this IT model must purchase additional hardware and overhauls in order to scale up their data storage and services to support more users. Mandatory software upgrades are also required with traditional IT infrastructure to ensure safe systems are in place to in case a hardware failure occurs. For many businesses with IT data centers, an in-house IT department is needed to install and maintain the hardware. On the opposite hand, a standard IT infrastructure one among the foremost secure information hosting solutions and permits you to take care of full management of your company's Applications and data on the local server. As the next generation, Cloud Computing has versional architecture of IT Enterprise. In distinction to traditional solutions the IT offerings are below physical, logical and personnel controls. Current cloud provider is provided accesses to net browser or host deploy utility directly [15]. They are a customized, dedicated system ideal for organizations that need to run many different types of applications.

Cloud computing is far more abstract as a virtual hosting solution, rather than being accessible via physical

hardware, all servers, software and networks are hosted in the cloud, off premises. It's a real-time virtual environment hosted between several different servers at the same time rather than investing money into purchasing physical servers in-house, you can rent the data storage space from cloud computing providers on a more cost effective pay-per-use basis.

Cloud computing is an extrinsic form of data storage and software distribution, which can influence it to appear to be less secure than local data hosting. Anybody with access to the server can view and use the stored data and applications in the cloud, wherever web connection is available. Picking a cloud service provider that is totally transparent in its hosting of cloud platforms and guarantees optimum security measures are in place is crucial when transitioning to the cloud. The Cloud Service Provider (CSPs) has promise to ensures the data security over stored data of cloud clients by using methods like firewalls and virtualization. These mechanisms would not give the complete data protection because of its vulnerabilities' over the network and CSPs have full command on cloud applications, hardware and client's data [5].

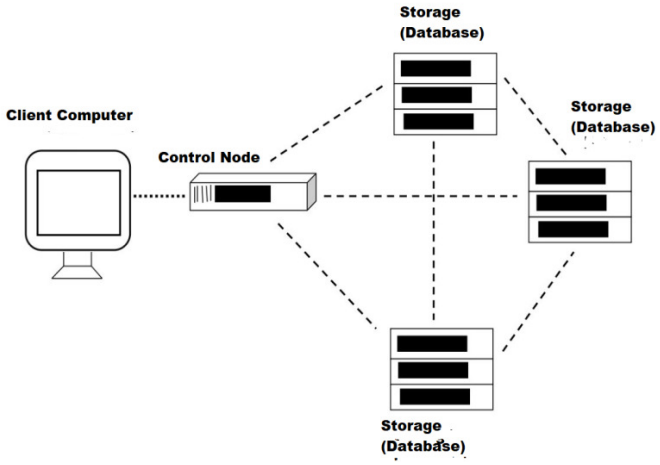

Fig. 1. Working of Cloud Storage.

Traditional Security VS Cloud Security

While demands for on-line storage may be on the increase, each traditional and cloud security has their pros and cons. Both demand terribly high level of observation and there should be redundant systems in situ for simple data accessibility. So, Gartner is of the opinion that merely using the cloud technologies isn't enough as you must be troubled a lot of with however you employ cloud services. It's necessary to optimize applications for the cloud with the thought of obtaining most price from them at minimum prices. Not like the chance of a lockdown for a personal network using firewalls, there's not a one-size-fits-all tool for cloud security. So, cloud security extremely depends on the enterprise.

Table: 1 Traditional Security VS Cloud Security.

Cloud security	Traditional IT security
Third party Data Canters	In-House Data Canters
Low in readiness Infrastructure investment's	High in readiness costs
Rapidly scalable	Unrushed scalable
Productive Resource utilization	Lower efficiency
Cost based on data storage usage	Higher cost to preserve data
Offers security as services	Responsible for data center security
You need to include more physical on-site hardwar This hardware, however, will be costly.	A cloud provider permits you to include the internet as a storage location that allows efficient scaling. However, you're additionally dependent on the service provider's security controls.

II. DIFFERENT CLOUD COMPUTING PLATFORM FACING SECURITY THREATS

A. Education Cloud Platform

Now a day's remote education extensively used in education department, the resource sharing and resource integration is huge concern, with the widespread use of education cloud, the security issues are also growingly important, such as data loss, According to the cloud computing platform, education cloud platform an inheritance and development. Due to the requirements of large-scale education management and education and teaching, the educational cloud has the characteristics of large-scale, high concurrency and high reliability. Education Cloud computing security management is the development trend of information security management [6]. Cloud service providers use some basic data security techniques like encryption and access control to protect their data from potential data breach and data loss. We discovered the existence of data leakage, loss and security attacks on education cloud platform and require take care of the personal privacy issues of various education departments and teachers and students and improve teaching quality.

B. Enterprise Cloud Platform

E-commerce business or state-owned banks with immense data need a significant number of operations

and maintenance personnel to help them maintain the system and deal with any emergency. However, the operations team with the most considerable authority can easily access all the confidential information from their cloud product. Another security issue the majority of citizens ignore here is the use of the public wireless internet connection to access their susceptible personal information. In India, most of the cities provide the free urban wireless networks. Most people do not even care if it is safe and secure or not before starting to use them. The public Wi-Fi connections allow people to have internet access without asking for any authorization. This means that all the information gets transmitted without any encryption. The clients are likely to access the internet and use their phones to access their accounts with vulnerable data like banking or online payment systems. Hackers can easily utilize these careless habits of clients to steal their payment authentication keys.

One more issue with the free network is the bandwidth, which is always extremely limited. It is very likely for the users to lose connectivity in the middle of their financial transactions which could leave their private accounts more susceptible to potential attacks. Besides, both traditional and start-up financial companies are also using Application Programming Interface (API) to provide third-party services to their clients. India has hundreds of online retailers, and each company provides different third-party APIs that are not completely safe. It is a very susceptible area to get frequent attacks from the hackers.

C. Mobile phone data

The development of cloud computing and the popularity of smart mobile devices, human beings are gradually getting acquainted to a new stage of records sharing model in which the data is saved on the cloud and the mobile gadgets are used to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider (CSP) to store and share the data.

At the present time, various cloud mobile applications have been widely used. In these applications, people (data owners) can upload their photos, videos, documents and other files to the cloud and share these data with other people (data users) they like to allocate [7]. CSPs also grant data management functionality for information owners. Since private data documents are sensitive, records owners are allowed to select whether or not to make their statistics files public or can solely be shared with unique records users clearly, data privacy of the personal sensitive data is a big concern for many data owners, from this observed mobile data stored on cloud has vulnerability.

D. Health care data storage

Personal health data are valuable resources for healthcare research and commercial projects such as Smartphone, smart watch, smart band and smart glasses etc, to realize various health-related applications, such as remote diagnosis, disease monitoring and mature people. Large quantity of private health records are produced by way of these gadgets and these statistics are precious sources for healthcare lookup and industrial applications. Properly sharing personal health data will benefit all related stakeholders including the device users, patients, researchers, companies and even the whole public healthcare system [10]. As personal asset, the health data should be owned and controlled by the respective users themselves, while in reality they are usually controlled by different service providers, device manufactures or scattered in different healthcare systems. In general, it brings barriers for the data sharing and puts data security and privacy at risk as these centralised data stores and authority providers are attractive targets for cyber-attacks.

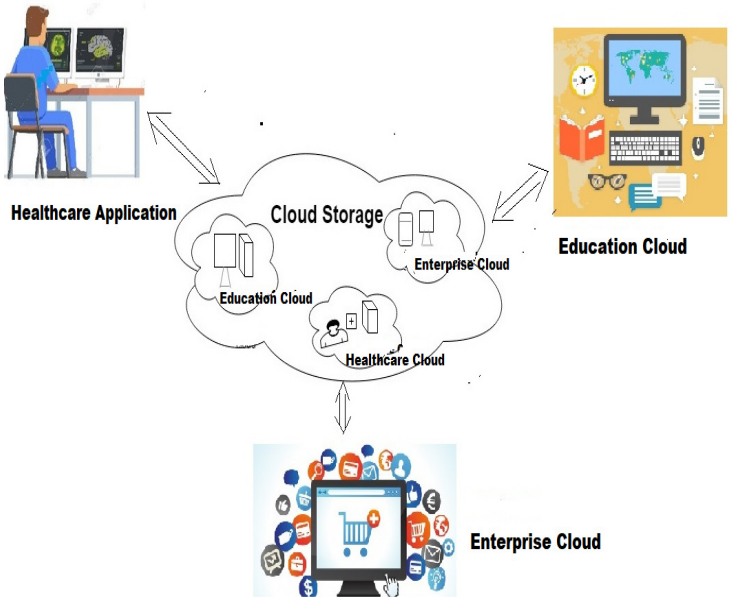

Fig. 2. Storage Model.

III. CLOUD STRORAGE ISSUES

With the rising popularity of cloud storage, and its ever-increasing versatility, it's no surprise that enterprises have jumped on the cloud bandwagon. This powerful tool not only meets storage and computing needs, but also helps saves business thousands of dollars in IT investments. This high demand for storage has nurtured the growth of a booming cloud service industry that offers affordable, trouble-free and remotely-accessible cloud services.

The following are top risks that must be addressed when using cloud storage and file sharing apps for business.

A. Out of control data

With cloud offerings like Google Drive, Dropbox, and Microsoft Azure turning into a regular phase of commercial enterprise processes, organizations have to deal with more recent safety issues such as loss of control over sensitive data. The problem here is that when using third-party file sharing services, the data is typically taken outside of the company's IT environment, and that means that the data's privacy settings are beyond the control of the enterprise.

B. Data Outflow

Today, organizations are placing more data as well as infrastructure in the public cloud. Public cloud has made it possible for organizations to be much more efficient, agile, and to integrate new technologies much more quickly. Most of the companies that have held returned from adopting the cloud have achieved so in the worry of having their data leaked. This feat stems from the fact that the cloud is a multi-user environment, wherein all the resources are shared. It is also a third-party service, which means that data is potentially at risk of being viewed or mishandled by the provider. It is solely human nature to doubt the competencies of a third-party, which seems like an even greater chance when it comes to businesses and touchy commercial enterprise data. There are also a number of external threats that can lead to data leakage, including malicious hacks of cloud providers or compromises of cloud user accounts.

C. Snooping

Files in the cloud are among the most susceptible to being hacked without security measures in place. The fact that they are stored and transmitted over the internet is also a major risk factor. And even if the cloud service provides encryption for files, data can still be intercepted on route to its destination. The excellent structure of security towards this threat would be to make certain that the records is encrypted and transmitted over a tightly closed connection, as this will stop outsiders from getting access to the cloud's metadata as well.

D. Cloud credentials

The fundamental value proposition of the cloud is that it presents near-unlimited storage for everyone. This means that even an enterprise's data is usually stored along with other customers' data, leading to potential data breaches via third parties. This is mitigated - in theory - by the fact that cloud access is restricted based on user credentials; however those credentials are also stored on the cloud and can vary significantly in security strength based on individual users' password habits, meaning that even the credentials are subject to compromise. While a credential compromise may not give attackers access to the data within your files, it could allow them to perform other tasks such as making copies or deleting them. The only way to overcome this security threat is by encrypting your sensitive data and securing your own unique credentials, which might require you to invest in a secure password management service.

IV. CONCLUSION

From this study, we can conclude the cloud sector is rapidly increasing, today's world cloud computing is very necessary for businesses and organizations for storing their large data, as the data is very vast and that has to be stored at some place, if we do it by ourselves lot of hardware has to be purchased, lots of space have to be there on computers, it will take more costs and time to manage them. But we cannot compromise with security as nobody wants that someone else is using or misusing their data. Data storage in cloud is more advantageous than traditional storage because of its availability, scalability, performance, portability and its functional requirements, The data centers and cloud service providers given certain security on client data to business and organizations even though more security required on client data storage in the aspects of confidentiality and privacy of data storage.

CONFLICT OF INTEREST

The authors declares that there is no conflict of interest.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my Research guide and research coordinator who encouraged and supported me to complete research paper. I would also thank to our University (Galgotias University) for providing me with all the facility that was required.

REFERENCES

[1]. Chandel, S., Tian-Yi Ni and Yan, G. (2018). Enterprise Cloud: its Growth & Security Challenges in China. *5th IEEE International Conference on Cyber Security and Cloud Computing.* DOI 10.1109/CSCloud/EdgeCom.

[2]. Chauhan, N., Ahuja, L., & Khatri, S.K. (2018). Secure Data in Cloud Computing Using Face Detection and Fingerprint. In *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 231-234). IEEE.

[3]. Xiaotong Sun. (2018). Critical Security Issues in Cloud Computing: A Survey. 4th IEEE International Conference on Big Data Security on Cloud. DOI 10.1109/BDS/HPSC/IDS18.2018.0005.

[4]. Kumar, K., Sampath, G.K.D. Prasanna, Venkatesan (2015). A Novel Approach to Enhance DNS Cache Performance in Web Browser using SPV Algorithm. *Indian Journal of Science and Technology,* **8.15**: 54635.

[5]. Rao, B.T. (2016). A study on data storage security issues in cloud computing. *Procedia Computer Science*, **92**, 128-135.

[6]. Nie, W., Xiao, X., Wu, Z., Wu, Y., Shen, F., & Luo, X. (2018). The Research of Information Security for the Education Cloud Platform Based on AppScan Technology. In *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (pp. 185-189). IEEE.
[7]. Li, R., Shen, C., He, H., Gu, X., Xu, Z., & Xu, C.Z. (2017). A lightweight secure data sharing scheme for mobile cloud computing. *IEEE Transactions on Cloud Computing*, *6*(2), 344-357.
[8]. Singh, I., Kumar, D., & Khatri, S.K. (2019, February). Improving The Efficiency of E-Healthcare System Based on Cloud. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 930-933). IEEE.
[9]. Cheng, H., Rong, C., Hwang, K., Wang, W., & Li, Y. (2015). Secure big data storage and sharing scheme for cloud tenants. *China Communications*, **12**(6), 106-115.
[10]. Yorozu, T., Hirano, M., Oka, K., & Tagawa, Y. (1987). Electron spectroscopy studies on magneto-optical media and plastic substrate interface. *IEEE translation journal on magnetics in Japan*, **2**(8), 740-741.
[11]. Jain, S. and Richhariya, V. (2017). Kerberos based Enhanced Authentication Protocol for Cloud Computing Environment. *International Journal of Theoretical & Applied Sciences*, **9**(2): 25-30.
[12]. Kang, S., Veeravalli, B., & Aung, K.M.M. (2016). A security-aware data placement mechanism for big data cloud storage systems. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 327-332). IEEE.
[13]. Vijayalakshmi, S. and Ranjan, V.G. (2018) A Novel Approach for Human Identification using Sclera Recognition *International Journal of Computer Sciences and Engineering,* Vol. **6**, special Issue-4. 228–235.
[14]. Zhang, Y., Xu, C., Li, H., & Liang, X. (2016). Cryptographic public verification of data integrity for cloud storage systems. *IEEE Cloud Computing*, **3**(5): 44-52.
[15]. Nisha and Dhillon, N.S. (2016). A Novel Approach to Enhance the Security in Cloud Computing using AES Algorithm. *International Journal on Emerging Technologies*, **7**(1): 76-79.
[16]. Kalpana, P., & Singaraju, S. (2012). Data security in cloud computing using RSA algorithm. *International Journal of research in computer and communication technology, IJRCCT,* Vol. **1**, Issue 4.
[17]. Hasan, M.M., & Mouftah, H.T. (2017). Cloud-centric collaborative security service placement for advanced metering infrastructures. *IEEE Transactions on Smart Grid*, **10**(2), 1339-1348.
[18]. Bao, S.D., Chen, M., & Yang, G.Z. (2017). A method of signal scrambling to secure data storage for healthcare applications. *IEEE Journal of Biomedical and Health informatics*, **21**(6), 1487-1494.
[19]. Ramjan, S. (2012). Flexible security rule-based system on cloud service for e-travel agent. In *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*. Vol. **1**, pp. 298-302). IEEE.
[20]. S. Vijayalakshmi and Savita (2018). Fuzzy C-Means Based Automated Technique for Hippocampus Segmentation" *International Journal of Computer Sciences and Engineering.* Vol. **6** Special Issue 4. 243-247.
[21]. Shanthi, K., Murugan, D., & Ganesh Kumar, T. (2018). Trust-based intrusion detection with secure key management integrated into MANET. *Information Security Journal: A Global Perspective*, **27**(4): 183-191.
[22]. Kumar, K. Sampath, G. K.D. Venkatesan (2017). Certain Investigation in DNS Stub Network Performance by using Accelerator System. *Asian Journal of Research in Social Sciences and Humanities,* **7.2**: 72-84.
[23]. Yuzhao, Wu, Yongqiang, Lyu, Yuanchun, Shi, (2019). Cloud storage Computing using AES Algorithm security assessment through equilibrium IEEE *Volume*: **24**, Issue: 6 DOI: 10.26599/TST.2018.9010127.
[24]. Kumar, T. Ganesh, D. Murugan, K. Rajalakshmi, (2015). Image enhancement and performance evaluation using various filters for IRS-P6 Satellite Liss IV remotely sensed data. *Geofizika*, Vol. **32**, Issue 2, 179-189.
[25]. Kaur, R. and Singh, A. (2016). Cloud Computing Services Model and Security Threats. *International Journal on Emerging Technologies,* Vol. **7**(1): 68-71.
[26]. Pandey, V. and Goswami, M.G. (2017). Various Challenges and Trust issues in cloud computing for Improvement the quality and services. *International Journal on Emerging Technologies* (Special Issue NCETST-2017) **8**(1): 324-329.
[27]. Adeppa, S. (2015). Data Sharing in Cloud Storage using Identity Encryption Technique. *International Journal on Emerging Technologies,* **6**(1): 115-117.
[28]. Jain, S. and Richhariya, V. (2017). Data Sharing in *Cloud Storage Using Identity Encryption Technique International Journal of Theoretical & Applied Sciences,* **9**(2): 227-231.
[29]. Pandey, A. and Sharma, S. (2017). Hybrid Encryption Technique for Security of Cloud Data. *International Journal of Theoretical & Applied Sciences,* **9**(2): 283-287.

How to cite this article: Nagarajan, G. and Kumar, K.S. (2019). A Security Risk on Data Storage in Cloud based System –Survey. *International Journal of Emerging Technologies*, **10**(2): 195–199.