National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Cloud Security Issues and Implications

Shruthi M G
Assistant Professor, Maharani Lakshmi Ammani College for Women, Bengaluru, Karnataka, India

ABSTRACT

In the recent days the data security is a big issue. Cloud security is one of the most prominent tasks for data security. Cloud security is mainly used for protection of data that has been stored in cloud from theft, leakage and unauthorized access. Different methods have been adopted for cloud security like tokenization, Virtual private network, Firewalls, obfuscation and avoiding public internet connections. Many threats to cloud security has been raised like account hijacking, data hijacking, service traffic hijacking, Application Programming interfaces in-security which leads to duplication of data in different fields and insecure way of data life. In Companies security of data has become a major issue where huge amount of data is stored in cloud and protection of these data is been high challenge. Many threats to cloud security has been raised like account hijacking, data hijacking, service traffic hijacking, Application Programming interfaces in-security which leads to duplication of data in different fields and insecure way of data life. In focus is mainly on Cloud security issues and the different ways of implications on these issues. An incredible increase in hacking of data leads to less productivity to application users, Companies etc. By applying different methods, the main aspect of security of data is been done. Some of the risks have been raised by "Week Cloud Security" is also discussed.

Keywords : Cloud Security, Cloud Threats, Data hijacking, intellectual property, Compliance violation.

I. INTRODUCTION

Cloud Security is the data securing from unauthorized theft, duplication and deletion. Cloud security is very essential for safe guarding data for many users and company's confidentiality. Security of data is most prominent than cloud itself, as cloud users need to protect the access to the cloud as access may be gained using other devices like mobile phones, tab etc.

Cloud security is also known as Cloud computing security as it contains a set of policies, controls, procedures and technologies which is going to protect cloud system entirely along with data and also infrastructure.

II. LITERATURE SURVEY

In recent days the survey about hijacking of data, different applications have become very crucial.
Xiaodong Lin, Xiahui Liang, Shen have proposed the new way of security model for the data forensics and also for the examining cloud computing. Mainly to provide privacy and security of huge data that has been stored in the cloud.

Amazon has provided Infrastructure Security also called as Amazon Web Services (AWS) by providing capabilities and services to increase privacy and to control network access. Wenchao has presented in his paper alternative perspective and also proposed data centric about Cloud security. They also guided security properties mainly to secure data sharing among the applications hosted on Clouds. Also, have discussed different ways of data management issues to process the query, Forensic as well as system analysis and query correction guaranteed. The proposal of new security platform to perform Cloud computing, it was named as Declarative Secure Distributed Systems.

III. Issues and Implications

Issue 1: Loss of intellectual property Many companies increasingly store the sensitive data in the cloud. Cyber criminals gain access to this sensitive data as 21% of files are sensitive data. Absence of breach and certain services can pose a risk by claiming ownership of the data uploaded.

Issue 2: Compliance violations and regulatory actions Most companies are operating some kid of regulatory controls for their information including government and industry issues. BYOC (Bring Your Own Computer) often violates these tenets by putting the company in a state of non-compliance which leads to serious problems.

Issue 3: Loss of control over end user actions Companies using cloud services, employees working may be doing work without noticing until it's too late. For instance, a salesperson who is about to resign from the company could download a report of all customer contacts, upload the data to a personal cloud storage service, and then access that information once she is employed by a competitor.

Issue 4: Malware infections that unleash a targeted attack Cloud security services are used as a vector of data ex-filtration. Skyhigh uncovered a novel data ex-filtration when the attackers loaded sensitive data into video files and also uploaded the videos online they detected malware that ex-filtrates sensitive data using a private Twitter account 140 characters at a time cyber criminal used file sharing services to deliver the malware to targets using phishing attacks.

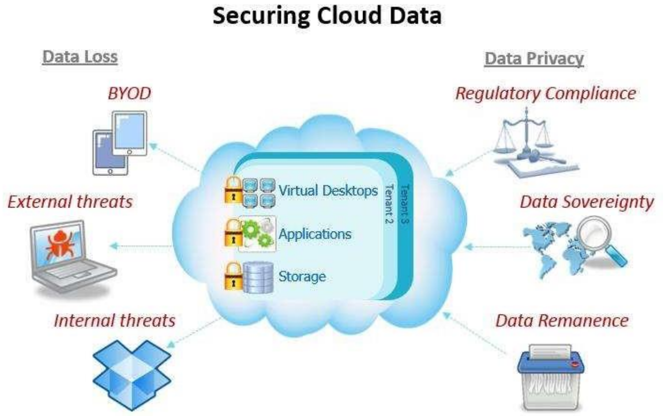
Issue 5: Contractual breaches with customers or business partners Contracts among business parties often restrict how data is used and who is authorized to access it. Consider the example of a cloud service that maintains the right to share all data uploaded to the service with third parties in its terms and conditions, thereby breaching a confidentiality agreement the company made with a business partner.

Issue 6: Diminished customer trust Data breaches inevitably result in diminished trust by customers. Cyber criminals stole over 40 million customer credit and debit card numbers from Target.

Issue 7: Data breach requiring disclosure and notification to victims The company may be required to disclose the breach and send notifications to potential victims. Certain regulations such as HIPAA and HITECH the healthcare industry and the EU Data Protection Directive require these disclosures.

Issue 8: Increased customer churn If customers even suspect that their data is not fully protected by enterprise-grade security controls, they may take their business elsewhere to a company they can trust.

Issue 9: Revenue losses News of the Target data breach made headlines and many consumers stayed away from Target stores over the busy holiday season, leading to a 46% drop in the company's quarterly profit.



IV. Measures taken for Cloud Security

To ensure you put in place proper security measures when beginning your cloud venture, here are five actions every small business owner should take.

1. Creation of unique usernames and passwords: Login credentials represent one of the cloud's main security vulnerability.
2. Usage of industry standard encryption and authentication protocols: IP sec (Internet Protocol Security) is a reliable technology choice.
3. Encryption of data before uploaded to the cloud: Once data is ready hide the data by encryption and only decrypt when reached the destination.
4. Checking IT providers what cloud security policies have been adopted: The most important security measure that can be adopted by finding a trusted IT person and also have signed cloud security policies.
5. Physical cloud server address know: Some cloud servers may be in different locations wherever they are, it's wise to make sure they're located in a safe data center area with proper security afforded to them.

V. CONCLUSION

The biggest cloud security challenge is the sharing of resources. Level of security should be given the most importance prominence.

In this paper I have highlighted the issues and implications of security when data stored in cloud. As Amazon had adopted new cloud security measures need to be developed and implemented in further days.

VI. REFERENCES

[1]. Hassan Takabi.et.al.(2010). "Security and Privacy Challenges in Cloud Computing Environments". IEEE security and privacy. w ww.computer.org/security.

[2]. Rongxing Lu. et.al (2010). "Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing". ASIACCS '10 Proceedings of the 5th ACM Symposium on Information. Computer and Communications Security. pp. 282-292.

[3]. Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; (2010), "Cloud Computing Research and Development Trend", 2nd International conference on Future Networks, 2010. ICFN ' 10. pp 23, 22-24 Jan 2010.

[4]. Basit Ali; (2009), "Ufone Launches Uconnect", published in TelecomPK.Net,12 August 2009.

[5]. Xue J; Zhang J.J; (2010),"A Brief Survey on the Security Model of Cloud Computing",2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.

Cite this article as :

Shruthi M G, "Cloud Security Issues and Implications", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 107-109, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194718