A SURVEY ON CLOUD SECURITY ISSUES IN CLOUD COMPUTING

Santhosh R[#], Pavithra R[*], Subhasri A[$]

ABSTRACT

In the past 30 years, the world's computational change has been centralized. Client Server technology plays a vital role in the field of computation. Now people are moving back to the virtual process called cloud computing[1]. As cloud computing is fetching the location and given date, this process differs entirely from realm computation. In cloud computing one person has complete control over the data and process of a computer , and another person has the service and maintenance of data provided by some vendor. The client here are not aware of how and where the processes are running. Also, where the data is stored . So, the technical talk is that the client does not have any control on their hands. Cloud computing uses the internet as a tool to communicate with the media. When the provider gives assurance to the customer on security issues, the organization fulfills the quality of service by examining the security and confidentiality of the critical insensitive issue[4]. "Cloud" provide different types of service. They can be (SaaS)-Software as a service, and Infrastructure as a services (IaaS). For each server, any kind of problems can occur. The SLA defines the level of security and complexity based on the services to the customer. To understand the security policy that has been implemented in this paper, we have put forward some of the security issues that have to be incorporated during computation.

Keywords : Cloud, Security, Threat, Malware, Cost, Quality of Services

I. INTRODUCTION

Cloud computing is a model for allowing a convenient and on-demand access from anywhere to a shared pool of computing resources[10]. Traditional business application and platforms are too complicated and expensive. They need a data center, a complex software stack and a team of experts to run them. Cloud computing is a much easier and affordable way to run your business. Cloud computing is the best way to improve your company's bottom line while allowing you to have accessibility from any smart phone or computer anywhere in the world at any time. Any organizations can simply connect to cloud and use the available resources. We can deploy a cloud computing service by using three different models[13]. They are

[#]Associate Professor, Department of Computer Science and Engineering, Faculty of Engineering, Karpagam Academy of Higher Education Coimbatore, Tamil Nadu, India.
Email: santhoshrd@gmail.com

[*]UG Scholar,Department of Computer Science and Engineering, Faculty of Engineering, Karpagam Academy of Higher Education Coimbatore, Tamil Nadu, India.
Email: pavithrarajagopal915@gmail.com

[$]UG Scholar,Department of Computer Science and Engineering, Faculty of Engineering, Karpagam Academy of Higher Education Coimbatore, Tamil Nadu, India.
Email: subhukutty176@gmail.com

private cloud, public cloud or hybrid cloud. A private cloud functions only for one organization or a private network and it is highly secured. A public cloud is owned by the cloud service provider and offers the highest level of efficiency of the resources[22]. A hybrid cloud is a combination of private and public deployment models.

II. CLOUD COMPUTING

Cloud computing is the process of many issues. The details about the data in these issues is called information technology (IT). The higher-level information services which has a vision of the computing cloud uses a metaphor to the internet after standardizing the cloud shape of the network. The end point of network is connected to the internet[15]. The data and the essential information can be saved in the process .Cloud computing which is a storage device is a network at low cost. It has the provision for hardware ,automation and utility of a computer in cloud computing.

BENEFITS OF CLOUD

Five concepts of cloud

- Cost
- Speed
- Performance
- Reliability
- Productivity

COST

Cloud computing picks out the expense of buying hardware, software making up and loading of the on-site Datacenters[12]. It manages the infrastructure. It adds up fastly.

SPEED

When you get into cloud, you can have any application in a minute. In IT the communications, functionality and customer relationship management of a software is done in a fraction of second[9]. It gives more flexibility to the cloud by providing network.

PERFORMANCE

The largest cloud computing service runs on the worldwide network with more security[20]. Data centers keep upgrading to the latest generation of fast computing hardware. It reduces the delay in the network connections for each application with greater economic scale.

RELIABILITY

Cloud computing makes backup for all the lost data, also recovers any disaster with very less expense[5]. The data can also be mirrored in multiple redundant sites with the use of cloud computing.

PRODUCTIVIY

On-site of datacenters typically requires a lot of racking and stacking in hardware, patching up the software and other time consumption in IT management[14]. IT group can spend time on achieving more essential business goal. It gives more flexibility to the cloud within its own network.

III. CLOUD SECURITY

Cloud security is an efficient architecture, which should recognize the issues arising with the security management. This security management will control all the security issues. In cloud security all the

information are monitored in a safe manner, but are hacked by someone , or some of the data is misused [11] .For each and every purpose even a single data will be verified and the information about the data where collected after undergoing a long process with the data[7] .To secure cloud project it should be analyzed thoroughly. The provision of cloud security is known to many people, but somehow it goes wrong because the data becomes vulnerable. Finally it is lost.

IV. SECURITY ISSUES IN CLOUD

In case of security in cloud there are many security issues faced by cloud but some of the main issues are as follows:

- DATA BREACHES
- INSIDER THREATS
- DATA LOSS
- MALWARE INJECTION
- HIJACKING OF ACCOUNTS

DATA BREACHES

A data breach is an intentional or unintentional release of the confidential information to an untrusted environment[8]. Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill[17]. Incidents range from concerted attack by black hats associated with organized crime, political activist or national governments to careless disposal of used computer equipment or data storage media.

The top five data breaches attack

- T.J. MAX COMPANIES (2007)
- PLAYSTATION NETWORK (2011)
- TARGET (2013)
- HEARTLAND PAYMENT SYSTEMS (2009)
- E-BAY (2014)

Investigations have been launched in the US and UK into a data analysis firm which claimed, harvested all the private information from more than 50 million Facebook users.

INSIDER THREAT

One of the biggest cyber security threats faced by the organizations today is the insider threat[2]. Insiders are employees and trusted partners with authorized access to digital system and organizations. Recent research by FBI has indicated 70% of data leakages are related to insiders. More than 70% organization allocates less than 3% of it's budgets to insider threat. Recent studies reveal that 90% of organization experience at least one insider leakage every month on hundred employees. The trusted natures of insider's access is slightly undetectable by standard cyber security measures such as antivirus, firewall, DLP's.

DATALOSS

The data we put in the cloud may be available to the people according to their needs. Sometimes we are dealing with machines and services managed by other people that are managed by third parties and if we are putting the date out there, that is a possibility of third parties accessing the data[3]. So, if you are dealing with cloud computing, your data is extremely important and sensitive.

No information or data in this world is 100% safe from

the disaster. A big disaster in the year June 2012 was knocking out the Amazon's data center[6]. Only a natural disaster like earthquake, tsunami can loss the data of the users permanently as they cannot be recovered from the loss.

In 2011 amazon organizations suffered from the date loss permanently . And also Google lost data when their power grid was struck by the thunder and lightning by four times

As many organizations are moving to the cloud based storage, many persistent threats may rise up.

MALWARE INJECTION

This malware injection attack focuses on injecting the implementing virtual machine to the cloud. The main aim is to take control of users' data where an image is uploaded and tricks that image to be part of that users cloud[16]. After the implementation of malware injection the user request will start forwarding which causes the vulnerable codes to execute in the cloud. Malware injection has become one of the major security issues in this cloud security.

HIJACKING OF ACCOUNTS

Attackers can gain lots of information through hijacking the accounts of users[19]. The attackers can eavesdrop the activities of users as they can control and manipulate the data in cloud. The information of the users can be stolen by the attackers and it is later used by them. In order to protect the data in the cloud there will be many ways but it is not 100% sure that the data we put in cloud cannot be hijacked by the attackers for their use. Now a days it is not new to hear that of accounts being hijacked.

V. SOLUTIONS FOR SECURITY ISSUES IN CLOUD

DATA LOSS

Data loss prevention is a technology which provides active information can be used, stored and moved. Cloud computing is being widely adopted across different sectors. There are also ways to ensure protection of data loss and privacy. In order to prevent data loss we have to back up our data[20]. In some critical situations of natural disasters like thunder lightning , the data is lost permanently from the cloud. So, to prevent data loss we have to back up our data which are in the cloud.

INSIDER THREAT

One of the biggest cyber security threats faced by the organizations today is Insider threat. We have to control and also access our accounts to minimize the risk. In a recent survey by people, there are number of insider threats increasing rapidly to access our data by the employees in the organization. To avoid this type of threat we need to monitor our accounts in order to protect data in the cloud.

HIJACKING OF ACCOUNTS

Cloud computing is experiencing a significant growth in rapid adoption in various regions in the world[21]. Cloud is cited as a top priority for global financial services CIO. Out of 39% of those surveyed experts more than half of their transactions are processed via cloud infrastructure and software as a service. In order to secure our data in this cloud, we have to create the user ID and password which is critical to detect or analyze for our safer side. Because now a days more

organizations and almost 90% of people in the world are storing information in cloud, in order to ensure prevention of loss of the data of the users in the cloud.

DATA BREACHES

Data residency and data security are the key concerns when moving to the cloud. The main concern with the data residency is who manages and access the data. Data encryption and tokenization are the key solution to overcome data redundancy [6]. Data encryption is the mathematical process which includes changing of text into cypher text which cannot be read by anyone. Tokenization saves from only external threat where as data encryption saves from both internal as well as external threats. To protect our data in the cloud, we have to encrypt the data , so that the stealing of data will be worthless because no one can read the encrypted data.

VI. CONCLUSION

Cloud security provides secured cloud enablement and deployment. It meets privacy and redundancy regulation globally and is deployable for multiple cloud application in the enterprise. Cloud is used by almost 90% of the organization and almost every people to store their data in cloud. The data we put in cloud is more sensitive and more confidential and it needs more security. Even though cloud has many issues, it also provides security or solutions for that issues in cloud.

REFERENCES

[1] Sox, "Sarbanes-Oxley Act of 2002," p. 66, 2002. [Online]. Available: news.?ndlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf Last accessed: Jan 2017

[2] Crown, "Data Protection Act 1998," 1998. [Online]. Available: http://www.legislation.gov.uk/ukpga/1998/29/contents Last accessed: Jan 2017

[3] A. A. Berle and G.G.C. Means, The modern corporation and private property, 1932. [Online]. Available:https://books.google.co.uk/books?id= mLdLHhqxUb4C Last accessed: Jan 2017

[4] M. C. Jensen and W. H. Meckling, "Theory of the firm: Managerial behavior, agency costs and ownership structure," Int. Libr. Crit. Writings Econ., vol. 3, no. 214, pp. 191-246, 2008.

[5] A. Cadbury, "The financial aspects of corporate governance," HMG, London, Tech. Rep., 1992. [Online]. Available: http://www.ecgi.org/codes/documents/cadbury.pdf Last accessed: Jan 2017

[6] M. C. Jensen, "The modern industrial revolution, exit, and the failure of internal control systems," J. Finance, vol. 48, no. 3, pp. 831-880, 1993.

[7] M.C.Jensen and D.Chew, "US corporate governance: Lessons from the 1980's," Harvard Univ. Press, no. December 2000, pp. 1-47, 1995.

[8] R. Greenbury, "Directors' remuneration - Report of a study group chaired by Sir Richard Greenbury," HMG, London, Tech. Rep., 1995. [Online]. Available: http://www.emeraldinsight.com/journals.htm?articleid=848139&show=abstract Last accessed: Jan 2017

[9] R. Hampel, "Committee on corporate governance," London, Tech. Rep., 1998.

[10] S. Turnbull, "Corporate governance: Theories, challenges and paradigms," SSRN Electron. J., pp. 1-97, 2000.

[11] P. Myners, "Institutional investment in the United Kingdom: A review," HMG, London, Tech. Rep., 2001.

[12] H. Gov, "Transparency in supply chains etc. A practical guide," 2015. https://www.gov.uk/government/uploads/system/uploads/attachment data/?le/471996/Transparency in Supply Chains etcA practical guide ?nal .pdf Last accessed: Jan 2017

[13] R. Bauer, N. Guenster, and R. Otten, "Empirical evidence on corporate governance in Europe: The effect on stock returns, ?rm value and performance," J. Asset Manag., vol. 5, no. 2, pp. 91-104, 2004.

[14] W. W. Bratton, "Enron, Sarbanes-Oxley and accounting: Rules versus principles versus rents," Soc. Sci. Res., vol. 48, no. 4, pp. 1023-1056, 2003.

[15] K. Brickey, "From Enron to WorldCom and beyond: Life and crime after Sarbanes-Oxley," 2003. [Online]. Available: http://heinonlinebackup.com/hol-cgibin/get pdf.cgi?handle=hein.journals/walq81&section =19 Last accessed: Jan 2017

[16] B. Holmstrom and S. N. Kaplan, "the State of U.S. corporate governance: What's right and what's wrong?" J. Appl. Corp. Financ., vol. 15, no. 3, pp. 8-20, mar 2003.

[17] L. E. Mitchell, "The Sarbanes-Oxley Act and the reinvention of corporate governance?" Villanovo Law Rev., vol. 48, no. 4, pp. 1189-1216, 2003.

[18] R. E. Rosen, "Risk management and corporate governance: The case of Enron," Conn. Law Rev., vol. 35, no. 1157, pp. 1157-1184, 2003.

[19] Financial Reporting Council, "The combined code on corporate governance," HMG, London, Tech. Rep. July, jan 2006. [Online]. Available: http://doi.wiley.com/10.1111/1467-923X.00209 Last accessed: Jan 2017

[20] Financial Reporting Council, "The Turnbull Guidance as an evaluation framework for the purposes of Section 404(a) of the Sarbanes-Oxley Act," Financial Reporting Council, London, Tech. Rep., 2004.

[21] G. Clinch, B. Sidhu, and S. Sin, "OECD principles of corporate governance," Organisation for Economic Co-Operation and Development, Tech. Rep. 4, may 1999.[Online].Available:http://www.oecd.org/corporate/ca/corporategovernanceprinciples /33977036.pdf Last accessed: Jan 2017

[22] Financial Reporting Council, "The combined code on corporate governance," Financial Reporting Council, London, Tech. Rep. July, 2006.