SECURITY CHALLENGES ENCOUNTER BY CLOUD USER AND CLOUD SERVICE PROVIDER (CSP)

Vaishali Chauhan[1], Anil Singh[2]

[1]Student of Master of Technology, [2]Assistant Professor,

Department of Computer Science and Engineering, AP Goyal Shimla University, (India)

ABSTRACT

As cloud has becomes the tool of choice for every organization who wants to reduce their computing operational cost. Cloud Computing provides various services (SaaS, PaaS, IaaS) to their cloud consumer. The cloud guarantees about its environment that it is reliable, dynamic and assure about good quality of service. One of the most significant challenges in cloud computing is security and oversight to enhance security. Cloud computing is exposed to novel security threats due to the multiple users across a large domain. This paper mainly focused on identifying the challenges associated with cloud security.

Keywords: Cloud Computing Security, Malware, Security Threats, Transparency, Zombie.

I. INTRODUCTION

Cloud computing, as defined by the National Institute of Standards and Technology (NIST) in Special Publication 800-145, is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1]. Formally cloud computing [13] can be defined as— “It is a model for enabling ubiquitous , convenient, on-demand, network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.” NIST goes even further to list what are deemed as five "essential characteristics" which are used for the composition of a cloud model, these five characteristics, in no particular order, are - On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [1]. Cloud computing is a computational model which provide the efficient and seamless connectivity to its users. Cloud computing are pay-per-use model for authorize convenient, on-demand network access to a shared pool of configurable computing resources that can be swiftly provisioned and released with minimal management effort or service provider interaction [3].

The three service type of model achieved in cloud: software-as-a-service, platform-as-a-service, and infrastructure-as-a-service [5]. Software-as-a-service (SAAS) administrates, control and provide the cloud subscribers to approach the software which is running on the cloud infrastructure. For example, Google Docs relies on JAVA Script, which runs over the Web browser [5].

Platform-as-a-service (PaaS) isdelivery model, in which the user can make their own application and deploy them on the providers cloud infrastructure. Example is the Google App Engine, a service that lets developer to write programs to run them on Google's infrastructure [5].

Infrastructure-as-a-service (IaaS) This service basically delivers virtual machine images as a service and the machine can contain whatever the developers want [5]. Instead of purchasing servers, software, data center resources, network equipment, and the expertise to operate them, customers can buy these resources as an outsourced service delivered through the network cloud [6] For example, host firewalls [5].

The main dissimilarity between these service models lies in how responsibilities are split between Cloud Service Provider (CSP) and Cloud Consumer. This paper is organized as follows. In section 2, we discuss the security requirements in cloud computing. Section 3 reviews the security problems in cloud computing. Finally, we conclude this paper in Section 4, and briefly discuss future work in Section 5.

II. SECURITY REQUIREMENTS IN CLOUD COMPUTING

The security is a major concern in the computing resources. The resources are provided to its users in cloud computing, all the security measurements that needed in traditional computing are applicable in cloud environment also [2]. Virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm[2]. There are numerous security issues in cloud computing but are associated with the cloud service provider and users. The cloud service providers manage the remote server where the data has been stored by the users. They give surety to the users that their data is been stored safely over cloud. The cloud service provider should ensure the user (client) that they are using a strong infrastructure which will provide them proper security measures. The user (client) should check the standard compliance guideline to protect the data. Therefore, more and more users and organisations have moved their data to the cloud to save cost utilise resources and have worldwide access [15]. The concerns are arises by the CSU whether their data has been accessed by the unauthorised person since there are many user sharing the resources over the cloud. This has also been supported by the Cloud Security Alliance (CSA) in their statistical overview of vulnerabilities. It has been reported by CSA [16] that the major concerns on security issues are confidentiality, integrity and availability.

III. SECURITY PROBLEM IN CLOUD COMPUTING

The cloud computing field is a flourishing industry with its own new security challenges. The users and organisations store sensitive information such as customer information and corporate information into the cloud service provider platforms to reduce the cost economically by giving up the control of some data [7]. But the worry arises by the user or organization is data security in cloud. This issue leads to the leakage of the data or the data may be corrupted by attackers. To identify the top most security threats impending in cloud computing, Cloud Security Alliance conducted a survey of industry experts to compile professional opinion on the greatest vulnerabilities within cloud computing. In this most recent edition of this report, experts identified the following critical threats to cloud security [8].

3.1 Identification and Authentication

Researchers have said that long, random passwords are tough to crack but they are hard to remember. Security is not just a technical issue but also a behavioural issue involving users, mostly untrained ones [17] built a Cloud-based storage free BPM designed to achieve a high level of security with desired CIA [18]. Generation of password structure at highest probabilistic order to make password-cracking harder using the right word-mangling rule [19] is said to be able to assist users in selecting their own memorable password even though it is argued that as long users are able to choose their own passwords, the attacks can break password more easily than through a brute-force attack.

3.2 Data Loss

Even if both consumers and businesses, don't know where their data is the prospect of permanently losing one's data is terrifying. Data stored in the cloud can be lost due to reasons other than malicious attackers like physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers' data. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders [2].

3.3 Shared Technology Issues

IaaS, PaaS, or SaaS are the service model which is been provided by the Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms, and applications. In a shared infrastructure, the security experts acclaimed In-profundity Defensive System [22]. The issue is that a single vulnerability or wrong configuration can lead to a problem across an entire provider's cloud.

3.4 Denial of Service

Denial of Service (DOS) attacks are nothing new and they've been a thorn in the sides of data center managers and IT staff for more than a decade now. Through DOS, a hacker doesn't need to attack the entire infrastructure anymore. They can simply choose the most resource intensive app that the user is running on the cloud and use simple low band width attacks to take out that service [2].

3.5 Zombies

One of the fastest growing threats in malware world is botnet. A zombie is a computer connected to the Internet that has been attacked by a hacker, computer virus or Trojan horse and can be used to perform malicious tasks. A zombie can be a VM instance in the Cloud. An estimate that 40% of the 800 million computers that connect to the internet on a daily basis are Zombies that are part of a botnet [21].

3.6 Malicious Insiders

Cloud computing as a process is governed, managed, and maintained by site administrators. By default, they hold the key to managing all the data, files and privileged company resources and files. These administrators sometimes because of some personal differences can leak out the important data of a client or can distribute confidential financial or official data of the organization [2].

3.7 Flooding Attacks

Cloud Computing enables a dynamic adaptation of hardware requirements to the actual workload requirements [4]. Though this feature of providing more computing power on demand is appreciated in the case of valid users, it poses severe issues in the presence of an attacker. One such attacking scenario is ―flooding attacks [9]. To elaborate flooding attacks on Cloud, two security experts David Bryan and Michael Anderson conducted a research and they warned that "Cloud-based denial-of-service attacks are looming on the horizon with $6 and a homemade Thunder Clap" program, they managed to take down their client's server by using the Amazon's EC2 Cloud infrastructure itself [10].

3.8 Transparency

Transparency allows an organization to more easily identify potential security risks and threats and also create and develop the right countermeasures and recommendations for its enterprise [14]. Transparency of data privacy, data security, anonymity, telecommunications capacity, liability, reliability, and government surveillance ensures strong security on the client’s data [14]. The third party manage the data and security which is the cloud-specific challenge.

3.9 Account Hijacking

Account hijacking is not a new threat to computing. It is a type of identity theft in which the attacker uses stolen account information to carry out malicious or unauthorized activities [2]. Typically account hijacking is carried our through phishing, sending spoofed emails to the user, password guessing or a number of other hacking techniques. In many cases, an email account is linked to a person’s social networks and financial networks etc. and by impersonating the account; a hacker can gain access to these confidential data for illegitimate activity [2].

3.10 Insecure APIs and Interfaces

The era of cloud has realized the inconsistency of attempting to make services accessible to millions while restricting any harm to a great extent unnamed clients may do to the service [4]. The response has been an open confronting application programming interface, or API, that characterizes how an outsider associate an application to the administration and giving confirmation that the outsider delivering the application is who he says he is. Heading web engineers, including Twitter and Google, teamed up on pointing out Oauth [11], an open approval administration for web benefits that controls outsider access. Oauth turned into a web designing team standard in 2010 and form 2.0 is utilized for a few administrations by real multi-occupant associations such of Facebook, Microsoft and Google. Anyway security masters caution that there is no superbly secure open API, and Oauth, in spite of its insurance and controls, is liable to break [12].

3.11 Job Starvation Due to Some Virus or Worm

Resources starvation takes place when one job takes up a huge amount of resources and other job stay idle. Resources can be reserved in advance by the customer. The priority of the affected tasks/job can be reduced by the customer [20].

3.12 Encryption

It’s unsafe to store plain text data anywhere or over the cloud. If the cloud were to be breached, the information would be directly available to the hackers. The CSPs provide the encryption/ decryption mechanisms over the client data. The cloud specific is CSPs may be responsible for encryption.

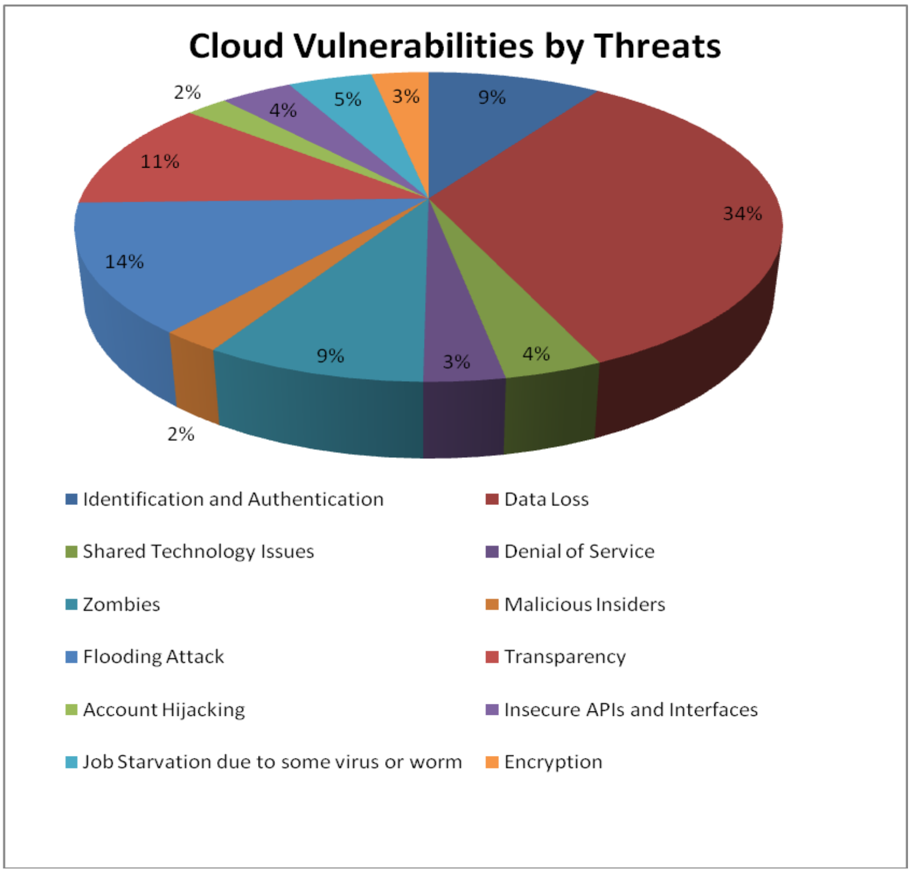

Figure1: Cloud Vulnerabilities Incidents by Threats [16]

This statistical overview also been supported by the Cloud Security Alliance (CSA) in their statistical overview of vulnerabilities [16].

IV. CONCLUSION

This paper explored various challenges unique to cloud security. The cloud is a multi-tenant environment, where resources are shared. Threats can happen from anywhere, inside the shared environment or from outside of it. Since the concept of Cloud Computing was proposed Cloud Security has inevitably become a significant business differentiator. Much of cloud computing targets customers who have extensive business reasons leading them to treat security as an elevated priority. There are several emerging solutions to these challenges in the form of supplements in standards, regulations, new technologies, etc. We are also looking into emerging approaches and technologies that may be potentially continued and improved for future research. Therefore, in our next stage of research, a thorough work will be introduced. An overview of future work is described in the last section.

V. FUTURE WORK

Our future research will be more focused on the existing algorithms complexity applied over the cloud security techniques. There are many practical concerns regarding to security the future work is much concentrated to cloud security techniques which targets to concepts and provide a practical solution for cloud security.

REFERENCES

[1]. Mell, Peter and Grance, Timothy. (2011). The NIST Definition of Cloud Computing. Special Publication 800-145. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2]. Nilotpal Chakraborty et.al,. (Security Challenges in Cloud Computing: A Comprehensive Study) International Journal of Computer Science Engineering and Technology (IJCSET) | January 2014 | Vol 4, Issue 1, 1-4.

[3]. George Reese, “Cloud Application Architectures”, First edition, O’Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.

[4]. Anuradha Thilakarathne, Janaka “Security Challenges Of Cloud Computing”, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 11, NOVEMBER 2014.

[5]. John Viega, McAffee, Cloud Computing and the Common Man,” published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009

[6]. Cisco White Paper, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/white_paper_c11-532553.html, published 2009, pp. 1-6.

[7]. A. N. Suresh, et al., “Security Challenges In Cloud Computing” International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181. Vol. 2 Issue 2, February- 2013

[8]. “The Notorious Nine: Cloud Computing Top Threats in 2013”, Top Threats Working Group, Cloud Security Alliance, February 2013

[9]. Jensen M., Schwenk J., Gruschka N., and Iacono L., 2009. On Technical Security Issues in Cloud Computing. In IEEE International Conference on Cloud Computing, 2009. CLOUD '09. Bangalore, 21-25 September. Bangalore: IEEE. 109 – 116

[10]. Ristenpart T., Tromer e., Shacham H., Savage S., 2009. Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In Proceedings of Computer and Communications Security -- CCS '09. USA, 9–13 November. New York: ACM. 199-212.

[11]. Pai S., et al., 2011. Formal Verification of OAuth 2.0 using Alloy Framework. In International Conference on Communication Systems and Network Technologies (CSNT). India, 3-5 June. USA: IEEE. 655-659.

[12]. Georgiev M., et al., 2012. The most dangerous code in the world: validating SSL certificates in non-browser software. In ACM Conference on Computer and Communications Security. Raleigh, 16-18 October. USA: ACM. 38-49.

[13]. Fang Liu, et.al,. (NIST cloud computing reference Architecture; NIST special publication 500-292, 2011.)

[14]. Pauley, Wayne A. (2010). Cloud Provider Transparency: an Empirical Evaluation. IEEE Security and Privacy. November/December 2010.

[15]. J. JU, J. WU, J. FU, and Z. LIN, “A Survey on Cloud Storage,” Journal of Computers, vol. 6. 2011.

[16]. CSA, “Cloud Computing Vulnerability Incidents : A Statistical Overview,” 2013.

[17]. Y. Bang, D.-J. Lee, Y.-S. Bae, and J.-H. Ahn, “Improving information security management: An analysis of ID–password usage and a new login vulnerability measure,” Int. J. Inf. Manage., vol. 32, no. 5, pp. 409–418, Oct. 2012.

[18]. R. Zhao and C. Yue, “Toward a secure and usable cloud-based password manager for web browsers,” Comput. Secur., vol. 46, pp. 32–47, Oct. 2014.

[19]. M. Weir, S. Aggarwal, B. De Medeiros, and B. Glodek, “Password cracking using probabilistic context-free grammars,” in Proceedings - IEEE Symposium on Security and Privacy, 2009, pp. 391–405.

[20]. Steve Hanna, Juniper Networks, “Cloud Computing: Finding the Silver Lining”, published 2009, pp. 2-30.

[21]. Li C., Jiang W., and Zou X., 2009 Botnet: Survey and Case Study. In Fourth International Conference on Innovative Computing, Information and Control (ICICIC). Kaohsiung, 7-9 Dec. Kaohsiung: IEEE. 1184 – 1187

[22]. Padhy R., Patra M., Satapathy S., 2011. Cloud Computing: Security Issues and Research Challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), 136-146