Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis of Various Security Breaches and Its Measures in Cloud Environment

Uzma Ali, Prof. Sulabha Patil, Prof. Neha Mogre
Dept. of Computer Science & Engineering
T.G.P.C.E.T, Nagpur, India

Abstract*— Cloud computing is a versatile technology that can support a broad-spectrum of applications. The low cost of cloud computing and its dynamic scaling renders it an innovation driver for small companies, particularly in the developing world. Nowadays, digital storage of computer data is moving toward cloud computing which is a set of infrastructure provides data storage for organizations and individuals. Due to this large scale, in case an attack occurs in the network of a cloud it would be a big challenge to investigate the cloud. Therefore, digital forensics in cloud computing is a new discipline related to the increasing use of computers, networks and digital storage devices in numerous criminal activities in both traditional and Hi-Tech.This paper focuses on the literature on some challenges in cloud computing forensic investigation, and it is followed by evaluation and analysis of all types of information on cloud computing and its impacts on computer forensic investigations in publishing alliances with the survey was carried out in the field.

Keywords*— Cloud Computing, Digital forensics, Computer forensic, Network attacks, Cloud Security.

I. INTRODUCTION

Recently, cloud computing has become a new paradigm in information technologies. It grants several promising technological and economic opportunities that have a prospective to become an evolutionary point in the new era of computing environment. The evolution of this technology creates various challenges mostly in cybercrime investigations and digital forensics. Therefore, there is a need for digital forensics experts or investigators to extend their knowledge and tools into cloud forensics environments and establish their capability in order to reduce the risks of cloud security. Apart from that, some characteristics of cloud computing such as multijurisdiction, different service models, different deployment models and multitenancy have created a new setting for cloud forensics dimensions [6].

Even though there is many advantage concerned in cloud computing, the organization are slow in accepting it due to security issues associated with it. Security is one of the primary issues in cloud environment. Here there are various security concerns given below which are applicable in cloud computing environment [17]:

- Virtualization
- Network Security
- Policy and Compliance
- Data location
- Data integrity

"Vulnerability" refers to the unauthorized access to the resources within the cloud environment. It may be a service running on a server, unmatched applications or operating system software, or an unsecured physical entrance. There are several significant vulnerabilities that should be considered when an organization is ready to move their critical applications and data to a cloud computing environment [3].

II. RELATED WORK

J.Srinivas, K.Venkata Subba Reddy, Dr.A.Moiz Qyser [14] looked at the basics of cloud. There are interests and concerns in the cloud. From a technology point of view, there are interesting technical problems to solve. From a service or consumer point of view, there are essential usability, stability, and reliability problems to solve. We are at a crossroads with cloud technology. On one hand, there are many stories of problems with clouds, from data loss, to service interruption, to compromised sensitive data. To stay relevant, to remain meaningful, to grow in the service space, the cloud providers must step up their game and produce robust cloud implementations.

H. Guo, T. Shang and B. Jin [12] present the definition of cloud computing and its various models. Further they compare traditional forensic investigations and forensic investigations in cloud and analyze the challenges of forensic investigations in cloud environments.

George Grispos Tim Storer William Bradley Glisson [19] in their paper summarizes the key aspects of cloud computing and analyses how established digital forensic procedures will be invalidated in this new environment. Several new research challenges addressing this changing context are also identified and discussed.

Dominic Birk [20] paper focuses on the technical aspects of digital forensics in distributed Cloud environments. We contribute by assessing whether it is possible for the customer of Cloud Computing services to perform a traditional digital investigation from a technical stand point. Furthermore we discuss possible new methodologies helping customers to perform such investigations and discuss future issues.

Keyun Ruan, Ibrahim Baggili (PhD),Prof Joe Carthy, Prof Tahar Kechadi[16] present the current results and analysis of the survey "Cloud forensics and critical criteria for cloud forensic capability" carried out towards digital forensic experts and practitioners. This survey was created in order to gain a better understanding on some of the key questions of the new field cloud forensics before further research and development information from log files in locations which were determined to have been accessed by the suspect.

Deoyani Shirkhedkar, Sulabha Patil [3] paper proposes a digital forensic technique for cloud environment. The propose system will address the issues in cloud forensics like live forensics. It also detect two attacks the DDos attack and unauthorized file sharing.

U. Oktay and O.K. Sahingoz [9] describe the definitions and properties of different attack types in cloud computing and to introduce intrusion detection and prevention models to resist these types of attacks. In this paper, they had introduced the security issues of cloud computing and in terms of attack types and their defense mechanism by means of intrusion detection and prevention systems.

Shams Zawoad and Ragib Hasan [10] describe the technical challenges of executing digital forensic investigations in a cloud environment and presented the requirements to make clouds forensics-friendly. Creating a secure model for cloud forensics is very important as it will lead to more trustworthy clouds, allowing their adoption in sensitive application domains such as defence, business, and healthcare.

Patrick Honer [11] describes literature review on cloud computing security requirements and solutions provided a comprehensive overview, which not only targets fellow researchers following up investigating on one or more security sub-factors, but also addresses the interest of consultants or developers: the identified gaps within (under-researched) security requirements make it clear that currently very little useful evidence exists on well-thought out solution designs.

Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem [15] explored the importance of the cloud computing; but still there are a number of risks associated with the cloud computing procedure and process. This paper also illustrated the data privacy problem in cloud computing environment. Different data protection models and techniques have been defined that show their contribution in cloud computing. This paper will provide a base for future research work in the field of data security of cloud computing system. The defined models in the paper have a lot of challenges and issues, which open a new way for more research in this area.

Ashalatha R [13] aims to provide a comprehensive review on the essentiality of Security- as- Service in cloud computing scenario. The paper also presents the significance of data security and the various existing security techniques for the cloud. In addition, a number of regulatory, jurisdictional, and public policy issues remain to be solved in order for online computing to thrive.

Khaled Salah, Jose M. Alcaraz Calero, Sherali Zeadally, Sameera Al-Mulla and Mohammed Alzaabi [8] proposed and analysed a cloud-based security overlay network that offers an integrated set of security services. They focus on the most popular types of security software, including intrusion detection systems (IDSs), distributed denial-of-service (DDoS) prevention, and security management in protected endpoints—antivirus (AV), firewall, and email protection.

Zhifeng Xiao and Yang Xiao [5] have identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Beginning with these attributes, they present the relationships among the above attributes, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defence strategies in a cloud scenario.

Chun-Jen Chung, Tianyi Xing, and Dijiang Huang [4] presented NICE, which is proposed to detect and mitigate collaborative attacks in the cloud virtual networking environment. NICE utilizes the attack graph model to conduct attack detection and prediction. The proposed solution investigates how to use the programmability of software switches-based solutions to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks.

Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen [7] proposed a design and implementation of a cloud-based security centre for network security forensic analysis. They propose using cloud storage to keep collected traffic data and then processing it with cloud computing platforms to find the malicious attacks. By this type of close-loop control, the collaborative network security management system can identify and address new distributed attacks more quickly and effectively.

Le Xu, Dijiang Huang, Wei-Tek Tsai [1] presents a cloud-based virtual laboratory education platform called V-Lab that provides a contained experimental environment for hands-on experiments using virtualization technologies (such as Xen or KVM Cloud Platform) and OpenFlow switches. The system can be securely accessed through OpenVPN, and students can remotely control the virtual machines (VMs) and perform the experimental tasks.

Zahid Anwar and Asad Waqar Malik [2] explore the extent to which the vulnerabilities plaguing the Internet, particularly susceptibility to distributed denial-of-service (DDoS) attacks, impact the Cloud. It demonstrates how a network simulator can study the interplay of the communication and thermal properties of a network and help prevent the Cloud provider's worst nightmare: meltdown of the data centre as a result of a DDoS attack.

III. PROPOSED WORK AND METHODOLOGY

From the above analysis, security is the major concern in cloud environment. Various security breaches and its measures also taken. The objective of this paper is to design and develop the system for detection of network attack and reporting

the attack using hypervisor even maintains the data integrity of packets in network. The methodology used will be all virtual machines will be SSH unabled. NTP server is configured for this cloud. Each VM can be accessed by using three ways terminal, browser and GUI. The attacks will be performed by attacker machine on victims and monitor, will monitor them. The system state can be recorded before and after attack by system monitor. We can get Log information from WireShark.

IV. CONCLUSIONS

As we know Cloud computing is a versatile technology and security is the crucial issue in cloud environment. In this paper we studied several literature reviews of various security breaches and its prevention in cloud environment. The paper also includes the review of various attacks in the cloud and how it is detected its several measures are also given. Future scope of this paper is that attack whose solution is not taken out cloud is referred for further study.

REFRENCES

[1] Le Xu, Dijiang Huang, Wei-Tek Tsai," Cloud-Based Virtual Laboratory for Network Security Education" IEEE Transactions on Education, Vol. 57, No. 3, August 2014.

[2] Zahid Anwar and Asad Waqar Malik," Can a DDoS Attack Meltdown My Data Center? A Simulation Study and Defence Strategies" IEEE Communications Letters, Vol. 18, No. 7, July 2014.

[3] Deoyani Shirkhedkar, Sulabha Patil," Design of digital forensic technique for cloud computing" Volume 2, Issue 6, June 2014 International Journal of Advance Research in Computer Science and Management Studies.

[4] Chun-Jen Chung, Tianyi Xing, And Dijiang Huang," NICE: Network Intrusion Detection And Countermeasure Selection In Virtual Network Systems" IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.

[5] Zhifeng Xiao and Yang Xiao," Security and Privacy in Cloud Computing" IEEE Communications Surveys & Tutorials, Vol. 15, No. 2, Second Quarter 2013.

[6] Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, Nor Fazlida binti Mohd Sani, Solahuddin bin Shamsuddin, Farhood Norouzizadeh," A Survey About Impacts of Cloud Computing on Digital Forensics" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 77-94The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012).

[7] Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen," Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System" TSINGHUA SCIENCE AND TECHNOLOGY ISSN 1007-0214 05/12 pp40-50 Volume 18, Number 1, February 2013.

[8] Khaled Salah, Jose M. Alcaraz Calero, Sherali Zeadally, Sameera Al-Mulla and Mohammed Alzaabi January/February. 2013 Copublished by the IEEE Computer and Reliability Societies 1540-7993/13/$31.00©2013IEEE

[9] U. Oktay and O.K. Sahingoz," Attack Types and Intrusion Detection Systems in Cloud Computing", 20-21 September /Eylül 2013 | Ankara / TURKEY / Proceedings/Bildiriler Kitabı pp 71-76 2013.

[10] Shams Zawoad and Ragib Hasan, "Digital Forensic in the Cloud", CrossTalk—September/October 2013 pp17-20, 2013.

[11] Patrick Honer," Cloud Computing Security Requirements and Solutions: a Systematic Literature Review" University of Twente, 2013 - referaat.cs.utwente.nl.

[12] H. Guo, T. Shang and B. Jin, "Forensic Investigations in Cloud Environments,"International Conference on Computer Science and Information Processing (CSIP), pp 248-251, August 2012.

[13] J.Srinivas, K.Venkata Subba Reddy, Dr.A.Moiz Qyser,"Cloud Computing Basics"International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 5, July 2012.

[14] Ashalatha R," A Survey On Security As A Challenge In Cloud Computing" ISSN No: 2250-3536 Volume 2, Issue 4, July 2012.

[15] Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem,"A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 1, Issue 3 (May-June 2012), PP 28-36.

[16] Keyun Ruan, Prof.Joe Carthy, Prof.Tahar Kechadi, Ibrahim Baggili (PhD)," Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary Analysis"Jounal of Network Forensics vol.3, Issue 2011.

[17] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, Vol. 1, No. 2, December 2011.

[18] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE, vol. 9, no.2, pp. 50-57, 2011.

[19] George Grispos Tim Storer William Bradley Glisson" Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics".

[20] Dominik Birk, Christoph Wegener," Technical Issues of Forensic Investigations in Cloud Computing Environments".

