ISSN 2229-5518

Security and Privacy Shortcomings in Cloud Computing Environment

Rutba Maqsood, Divya Upadhyay

Abstract— Cloud computing is a developing concept with remarkable impetus and therefore it is a major area of interest in both academia and industry. It aims to merge the economic utility model with many existing approaches and computing technologies, including distributed services, applications, and information infrastructures consisting of pools of computers, networks, and storage resources. Understanding the security and privacy risks in cloud computing and developing efficient and effective solutions are vital for its success. Although clouds allow customers to avoid start-up costs, reduce operating costs, and increase their agility by immediately acquiring services and infrastructural resources when needed, their unique architectural features also raise various security and privacy concerns.

A major security challenge on the Internet is the existence of the large number of compromised machines; they have been progressively used to launch various attacks counting spamming and spreading malware, DDoS, and identity theft. DDoS attacks through the compromised zombies. Moreover the cloud users may install vulnerable applications on their virtual Machines which make the detection of zombie attacks extremely difficult.

A survey is conducted in this paper which illustrates various security and privacy challenges of the cloud computing environment and some of the techniques which have been developed in order to overcome these challenges.

Index Terms — CSA, Ddos, IDS, NIST, VM, VPC, VMI.

I. INTRODUCTION

The US National Institute of Standards and Technology (NIST, http://csrc.nist.gov) defines it as follows:
Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, measured service, all of which are geared toward using clouds seamlessly and transparently, three delivery models which are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), and four deployment models which include public, private, community, and hybrid clouds.

According to CSA (Cloud Security Alliance) [1] over the years the number of cloud vulnerability incidents has risen (see figure 2). In fact from 2009 to 2011 the number of cloud vulnerability incidents more than doubled - from 33 to 71, most likely due to the phenomenal growth in cloud services [2].

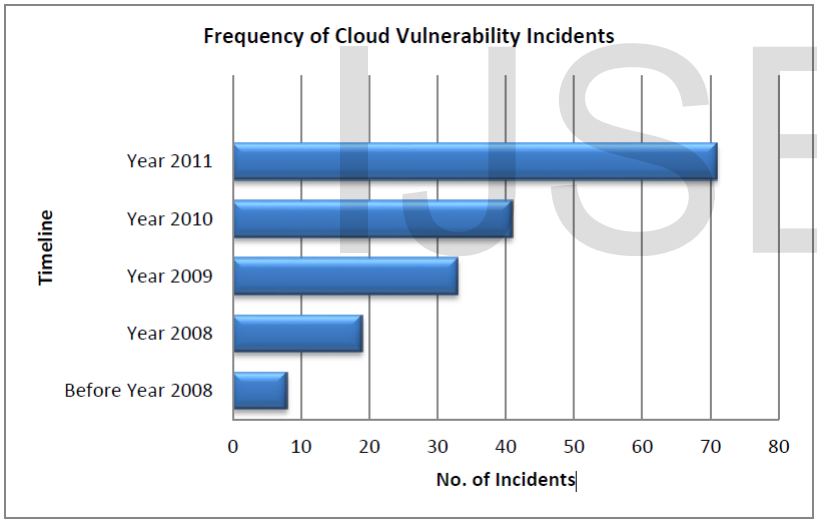

Fig 1 [1]

- *Rutba Maqsood is currently pursuing masters degree program in computer science engineering in Amity University, India, PH-9910126228. E-mail: rutbamaqsood@gmail.com*
- *Divya Upadhyay is currently working as an Assistant Professor in Amity University, India, E-mail: upadhyay.divya@gmail.com*

applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics which include on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and

In 2009, the Cloud Security Alliance propounded the Top Seven Threats to Cloud Computing in all cloud computing environments [1], they are as follows:

1) Abuse and nefarious use of cloud computing
2) Insecure Interfaces and API s
3) Malicious Insiders
4) Data Loss or Leakage
5) Account or Service
6) Hijacking
7) Unknown Risk Profile

II. CHALLENGES IN CLOUD COMPUTING

A. System reliability

Business data is enormous nowadays so it will be stored in the cloud, and the data may include private and other valuable information, so the cloud data centre is prone to be attacked. The attacks may be launched by malicious attacker stealing service or resources external to the cloud or inside staff of the cloud computing operators. Large scale attacks may lead to the breakdown of the cloud computing system, rendering the system useless. So cloud computing operators should integrate the current security technologies to prevent all kinds of attacks [3].

B. Privacy and data protection

Privacy is an important issue amongst all the challenges. The users' data is stored in the shared infrastructure all over the world, and users don't know the accurate position in which their data is stored. So users' private information faces high risk of exposure. After the data delivery from the terminal users to cloud computing providers, the privilege to access the data has changed, namely cloud computing providers have the priority to access the data, so the risk of potential unauthorized access will be faced. [4]

Therefore privacy-protection mechanisms are mandatory in all security solutions. It's becoming important to know who created the data, who modified it, when modified and how, and so on. Balancing between data protection and efficiency is a significant challenge in clouds.

C. Data isolation

Virtualization is an important technology to implement the sharing of resources and services. Therefore multiple virtual resources are likely to be connected to the same physical servers, so use of such technology also increases the occurrence of attack [3]. If malicious users access virtual machine by unfair means, it may be a risk to other virtual machine in the same physical server. In order to prevent this kind of threat the data isolation is a necessary means. The cloud computing environment must realize the effective isolation between one user's data and the others' data; otherwise it will be difficult for the cloud services to persuade the terminal users to believe their data is secure.

D. Other challenges

The cloud platform has its difficulties in the spheres of security management because there are many managers involving resources, and there are conflicts of interest among them, so that unified security management measures are hard to be realized.

III. CURRENT SECURITY TECHNOLOGIES

Cloud computing security products and solutions are constantly emerging nowadays. Sun released open-source cloud security tools including the OpenSolaris VPC Gateway software [3]. The OpenSolaris VPC Gateway software will allow an OpenSolaris-based system to be used as an Amazon Web Services Virtual Private Cloud (VPC) Customer Gateway. And the software can help customers to set up the communications channel to the Virtual Private Cloud (VPC). Meanwhile Sun company designed the security enhanced Virtual Machine Images (VMIs) for Amazon Elastic Compute Cloud (EC2). [5, 6]

IT company	Security Technology	Application
SUN	OpenSolaris VPC	For Amazon Elastic Compute Cloud (EC2)
Microsoft	"Sydney"	For windows Azure
Intel	Execution Technology	Trusted Cloud Architecture
VMware	Virtual Isolation Technique	Trusted Cloud Architecture
RSA	EnVision	Trusted Cloud Architecture

Fig 2 [3]

Besides the trusted execution technology of Intel, virtual isolation technique of VMware and enVision of RSA are combining for trusted cloud system architecture [5].

IV. STRATEGIES THAT HELP IN COMBATING SECURITY CHALLENGES

Some strategies that help cope up with the security challenges are enumerated ad follows [8]:

A. Security Governance

A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies [9].

B. Security Management Standards

Standards that are relevant to security management practices in the cloud are: 1) Information Technology Infrastructure Library (ITIL), 2) ISO/IEC 27001/27002 and 3) Open Virtualization Format (OVF) [9].

C. Data-centric Security

Data security becomes very important in cloud computing services. In mobile environment, data collection happens all over the place, the final channel that deals with the data will be in a central place. Since mass data is uploaded by the customer themselves, data needs to be self-describing and defending, regardless of its environment, and it also needs to be encrypted and packaged with a usage policy [10].

D. Privacy-enhanced Business Intelligence

The encryption of data is very important, however, encryption will limit data use. In particular, customers' searching and indexing of the data will become problematic when encryption is too harsh. How to allow customers to access data in a controlled manner requires privacy-enhanced business intelligence [10]. The development of intelligent encryption has opened up new possibilities for cloud computing security and it also leads to more reliable access to data.

E. Market-oriented Service Management

A high-level, market-oriented, cloud architecture will release a high-level of Cloud utility so that the power of cloud computing can be realized but some cloud computing services do not align their management with the market demands. There are several ways to achieve high-level, market oriented cloud architecture, especially to cope with the security and access challenges [11].

Cloud computing leads to new challenges due to consistent development of new techniques thus new security mechanisms need to be developed for resolving these challenges. There are some obstacles in the way of developing new security mechanisms. Solution providers need to have access to different components of a cloud environment so they can study them and also propose and develop proper solutions. Open environments should be available so others can do the same. Open source platforms, like Eucalyptus, are the way to address that requirement [7]. Additionally, the security model is not mature yet, and monitoring mechanisms need extensive development. Open communities are working on standards for components in the model which help us not only in securing the model, but also in clarifying the common understanding of security requirements.

V.CONCLUSION

Cloud computing brings with it new deployment and associated models and vulnerabilities, it is important that security taken into consideration. Moreover, cloud computing services are being used for e-commerce applications, medical record services, and back-office business applications, all of which require strong confidentiality guarantees. In order to take complete advantage of the power of cloud computing, end users need comprehensive security solutions to attain assurance of the cloud's treatment of security issues. In the process of cloud computing application, new security challenges occur, which makes enterprise users, cloud computing operators and regulators pay more attention to the cloud security. Many enhancements in existing solutions as well as more mature and newer solutions are urgently needed to ensure that cloud computing benefits are fully realized as its adoption accelerates. In this literature, we reviewed characteristics of cloud computing, and analysed security challenges along with some strategies which help us combat these challenges and current security technologies.

.

REFERENCES

[1] Ryan Ko, Stephen S G Lee ,Cloud Security Alliance, "Cloud Computing Vulnerability Incidents", 2013 .

[2] C. Babcock. (2009, 7th April 2012). Cloud Implementation To Double By 2012.

[3] Xiao Nie, Hui Suo*,"Security in the Cloud Computing: A Review",2nd International Conference on Computer Science and Network Technology, 2012.

[4] Bernd Gro Bauer,ToBias Walloschek. "Understanding Cloud Computing Vulnerabilities", IEEE Security and Privacy, v9, 2011,pp.50-57.

[5]Feng DG, Zhang M, Zhang Y, Xu Z. "Study on cloud computing security", Journal of Software , 22(1),2011,pp. 71−83.

[6]George Pallis. "Cloud Computing The New Frontier of Internet Computing", IEEE Internet Computing, v14, 2010, pp.70-73.

[7]Aryan Taheri Monfared, Martin Gilje Jaatun, "Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments", Third IEEE International Conference on Coud Computing Technology and Science , 2011.

[8] Xianghui Zhao , Hui Liu , Jin Yi, Wen Tian, Ning Luo, Lin Ye, " Cloud Computing Service Security and Access: From the Providers and Customers Perspective", International Conference on Information Technology and Applications,2013.

[9] Popovic, K. and Z. Hocenski: Cloud computing security issues and challenges. in MIPRO, 2010 Proceedings of the 33rd International Convention, 2010.

[10] Chow, R., et al.: Controlling data in the cloud: outsourcing computation without outsourcing control, in Proceedings of the 2009 ACM workshop on Cloud computing security, ACM: Chicago, Illinois, 85-90, 2009.

[11] Buyya, R., C.S. Yeo, and S. Venugopal.: Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities, IEEE, 2008.