A Review on Issues and Solution to Cloud Computing Security

[1]DEBABRATA SAHU, *Gandhi Institute of Excellent Technocrats, Bhubaneswar, India*
[2]SANTANU MEHER, *Indus College of Engineering, Bhubaneswar, Odisha, India*

Abstract

Cloud computing is the next generation of networks that will change computing in the near future. It has a lot of flexibility, such as on-demand resources and services. In the cloud computing paradigm, security is still a major issue. These issues include user secret data loss, data leakage, and personal data privacy disclosure. This study presents a detailed review of the available literature on cloud computing security issues and solutions. The authors suggest a paradigm for cloud computing security towards the end of this study.
Key words: Cloud computing, cloud computing security, IaaS, PaaS, SaaS

1-Introduction

Cloud computing is a new paradigm for hosting and delivering services over the Internet that has recently evolved. Cloud computing is an internet-based system that allows us to access software, data, and services from any location on any web-enabled device via the internet [3]. Cloud computing is defined by the researchers in the studies [8, 10, 9] as "a form of computing in which massively scaled IT-enabled capabilities are supplied "as a service" to external clients via Internet technology."

Companies and organizations regard cloud computing as the first among the top ten most significant technologies, with a brighter future in coming years [2]. According to [4,] analysts expect that from 2011 to 2016, 12 percent of the software business will migrate to cloud computing, with the market growing to $95 billion. Cloud computing offers a variety of services, each of which is divided into three tiers. Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are two infrastructure models. PaaS (Platform as a Service) and SaaS (Software as a Service) [5, 11].

Physical, virtual, and additional storage networking devices are available from IaaS cloud computing companies [13]. Amazon Elastic Compute Cloud (EC2), GoGrid, and Rackspace Cloud are examples of IaaS provider services. (PaaS) includes Infrastructure as a Service, as well as operating systems and server applications like web servers [22]. Google App Engine, Force.com, Amazon Web Services Elastic Beanstalk, and the Microsoft Windows Azure platform are examples of PaaS vendor services.

Customers can get an application as a service on demand via SaaS [12]. Salesforce.com Customer Relationship Management (CRM), Google Docs, and Google Gmail are examples of SaaS vendor services.
Due to the sensitive and crucial information held in the cloud for consumers, security and privacy are considered a critical issue in a cloud computing environment [6, 7]. Cloud computing, critics contend, is insecure since data leaves firms' local area networks. This paper provides an overview of cloud computing security, with an emphasis on security concerns and solutions for cloud computing layer models. The remainder of this document is structured as follows: Section II discusses the security issues with Infrastructure as a Service. The security challenges for Platform as a Service are discussed in Section III. The security problems for Software as a Service are discussed in Section IV. Section V proposes a cloud computing security proposal model. The paper finishes with Section VI.

II- Infrastructure as Services (IaaS) security challenges

Cloud Service Provider (CSP) outsources storage, servers, hardware, networking components, etc. to the consumer in IaaS model. CSP owns the equipment and responsible for housing, running and maintaining it. In this model, consumer pays on per-use basis. Characteristics and componentsof IaaS include [14]:

- Service Level Agreement (SLA)
- Dynamic scaling
- Automation of administrative tasks
- Utility computing service and billingmodel
- Internet connective
- Desktop virtualization

The virtualization risks and vulnerabilities that affect particularly IaaS delivery model are:

1- Security threats sourced from host a- Monitoring VMs from host

The control point in virtual environment is the hostmachine there are implications that allow the host to monitor and communicate with VM applications up running. Therefore, it is more necessary to strictly protect the host machines than protecting distinctive VMs [25]. VM-level protection is crucial in cloud computing environment. The enterprise can co-locate applications with different trust levels on the same host and can defend VMs in a shared multi-tenant environment. This enables enterprises to maximize the benefits of virtualization. VM-level protection allows VMs to stay secure in today's dynamic data centers. Also, as VMs travel between different environments – from on-premise virtual servers to private clouds to public clouds, and even between cloud vendors. [15]

b- Communications between VMs and host

The data transfer between VMs and the host flow between VMs shared virtual resources; in fact the host can monitor the network traffic of its own hosted VMs. This can be considering useful features for attackers and they may use it such as shared clipboard which allows data to transfer between VMs and the host using cooperating malicious program in VMS [17].

It is not generally considered a bug or limitation when one can initiate monitoring, change, or communication with a VM application from the host. The host environment needs to be more strictly secured than the individual VMs.

The host can influence the VMs in the following ways[16]:

- The host can Start, shutdown, pause, andrestart VMs.
- Monitoring and configuration of resources which are available to the VMs, these include: CPU, memory, disk, and network usage of VMs.
- Adjust the number of CPUs, the amount of memory, the amount and number of virtual disks, and a number of virtual network interfaces which are available toa VM.
- Monitoring the applications which are running inside the VM.
- View, copy, and possibly modify, data stored on the VM's virtual disks.

Unfortunately, the system admin or any authorized user who has privileged control over the backend can misuse these procedures.[17]

2- Security threats sourced from otherVM

a- Monitoring VMs from other VM Monitoring VMs could violate security and privacy, but the new architecture of CPUs, integrated with a memory protection feature, could prevent security and privacy violation. A major reason for adopting virtualization is to isolate security tools from an untrusted VM by moving them to a separate trusted secure VM [14, 15].

b- Communication between VMs

One of the most critical threads that threaten exchanging information between virtual machines is how it's deployed. Sharing resources between VMs may strip security of each VM for instance collaboration using application such as shared clipboard that allow exchanging data between VMs and the host assisting malicious program in VMs, this situation violate security and privacy. Also, a malicious VM can has chance to access other VMs through shard memory [16].

c- Denial of Service (DoS):

A DoS attack is a trying to denial services that provide to authorize users for example when tryingto access site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error. This happens when the number of requests that can be handled by a server exceeds its capacity, the Dos attack marking carting part of clouds inaccessible to the users [26]. Usage of an Intrusion Detection System (IDS) one of the useful method of defense against this type of attacks[27].

3- Networks & Internet Connectivity attacks

Practical solutions and techniques for eliminating these attacks or reducing their impacts are listed asfollows:

1- Logical network segmentation 2- Firewalls implementing
3- Traffic encryption
4- Network monitoring

III- Platform as Services (PaaS) security challenges

PaaS is a way to rent hardware over the Internet, PaaS provide capability to manage application without installing any platform or tools on their local machines, PaaS refers to providing platform layer resources this layer including operating system support and software development frameworks in which it can used to build higher – level services. [23], developer gets many advantages from PaaS these are:

- OS operating system can be changed and upgraded as many time as need.
- PaaS allow geographically distributed teams to sharing information to develop software projects [14].

The use of virtual machines act as a motivated in the PaaS layer in Cloud computing. Virtual machines have to be protected against malicious attacks such as cloud malware. Thereforemaintaining the integrity of applications and well enforcing accurate authentication checks during thetransfer of data across the entire networking channels is fundamental[18]

PaaS security threat can be summarize as:a- Data location

The actual platform is not in a single host, the platform can be thought as group of cluster hosts, in fact the location of your data cannot be isolated to specific sector on specific host, this will add more security over head as far as a single location is easier to secure than many.

Another security issue is that the duplication of data creates high availability of data for developers and users this distributed data remains like other data the big difference in this case in the exact location is unknown [24].

b- Privileged access

One of the most popular features in PaaS is the advertised software developers to use debug. Debug grants access to data and memory locations in order to allow the developers to modify values to test various outcomes we consider the debug provide the desired tool for both developers and hackers. [20]

c- Distributed systems

The PaaS file system is often highly distributed. The nodes can be independent while cloud service provider (CSP) owns the cluster so most likely to standardized configuration paths will be in place. The CSP should be able to provide the necessary security, but the responsibility for verifying this belongs to the client [1].

Practical solutions and techniques for eliminating these attacks or reducing their impacts are listed asfollows:

- Encapsulation Encapsulating access control policies with objects can be one ofthe solutions to resolve Privileged access
- Policy enforcement points (PEPs) A Policy Enforcement Point (PEP) is the logical entity or place on a server that makes admission control and policy decisions in response to a request from a user wanting to access a resource on a computer or network server. And thisconsider solution for distributed system[20]
- Trusted Computing Base (TCB) is a collection of executable code and configuration files that is assumed to be secure. TCB is thoroughly analyzed for security flaws and installed as a layer overthe operating system and provides a standardized application programming interface (API) for the user objects, encryption seems to be the best possible solution.[21]

IV- Software as Services (SaaS) security Challenges

SaaS also called "software on demand" using SaaS provider licenses an application to customers either on demand through a subscription or at no charge and this consider part of utility computing model, where all technology in the cloud accessed over internet as service. SaaS was basically widely deployed for sales force automation and Customer Relationship Management (CRM). Now, it has become common place for many business tasks, including computerized billing, invoicing, human resource management, financials, document management, service desk management and collaboration [14]. Software as a service applications are accessed using web browsers over the Internet. Therefore, web browser security is vitally important. Information security officers willneed to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet [18]

The service provider has to verify that their multiple users do not violates privacy of the other users, also it is very essential for user to verify that the right security measures are in place mean whileit is difficult to get an assurance that the application will be available when needed [19].

SaaS security threat can be summarize as

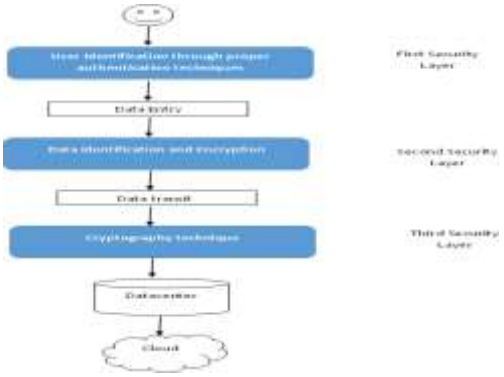
- Authentication and authorization
- Data confidentiality
- Availability
- Information security
- Data access
- Data breaches
- Identity management and sign on process

Navneet Singh [19] suggested practical solutions to assess the security threats in SaaS in which the customer must be asked:

- What metrics can be used for reporting?
- What is the level of access controls?
- Is the provided data can be easily adapted in the internal monitoring tools?
- How important and critical the enterprise data is?

V- proposed model

The proposed cloud security model is compose of three layers. In the first layer user's identification can be checked through proper authentication techniques. Security in the second layer depends on data identification and encryption. At the last layer cryptography technique is used to secure the transmission of the data. The architecture of the proposed model has been shown in figure (1)



VI-Conclusion

This paper gives a survey of different threats and solutions in cloud computing environment with respect to security and privacy of user's sensitive data in the cloud environment. The paper focusing on the security challenges and solutions for the cloud computing layers models. Authors have proposed model for cloud computing security.

References

[1] M.H.Nerkar, Sonali Vijay Shinkar, "Cloud Computing in Distributed System ", International Journal of Computer Science and Informatics ISSN (PRINT): 2231 –5292, Vol-1, Iss-4, 2012.

[2] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013, 4:5 .

[3] Deepaklal. K. B, " fuzzy keyword search over encrypted data in multicloud ", Discovery, Volume 21, Number 67, July 3, 2014

[4] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications (2011), pp. 1-11.

[5] Hassan Takabi , James B.D. Joshi, Gail Joon Ahn , "Cloud Computing Security and Privacy Challenges in Cloud Computing Environments ", COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES,1540- 7993/10/$26.00 © 2010 IEEE.

[6] Mohammed A. AlZain, Ben Soh, Eric Pardede, "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", JOURNAL OF SOFTWARE, VOL. 8, NO. 5, MAY 2013.

[7] Meenu Bhati, Puneet Rani, "Review of Passive Security Measure on Trusted Cloud Computing", International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-3, June 2015.

[8] M. P. Boss G, Quan D, Legregni L, Hall H. , Cloud computing, White Paper, IBM (2007).

[9] J. Heiser, What you need to know about cloud computing security and compliance, Gartner, Research, ID (2009).

[10] B. Whyman, Cloud Computing, information Security and Privacy Advisory Board (2008), pp. 11–13.

[11] Mahesh U. Shankarwar and Ambika V. Pawar, "Security and Privacy in Cloud Computing: A Survey", Proc. of the 3rd Int. Conf. on Front. of Intell. Comput. (FICTA) 2014.

[12] Harshitha. K. Raj, "A Survey on Cloud Computing ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014.

[13] Nidal M. Turab, Anas Abu Taleb Shadi R. Masadeh, "CLOUD COMPUTING CHALLENGES AND SOLUTIONS", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5, September2013.

[14] P. R. Jaiswal, A. W. Rohankar, "Infrastructure as a Service: Security Issues in Cloud Computing " , International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014, pg. 707-711.

[15] Trend Micro, "Virtualization and Cloud Computing Threat Report.", August 2011.

[16] J. Kirch, "Virtual machine security guidelines," 2007. [Online]. Available: http://www.cisecurity.org/tools2/vm/CISn VMn Benchmarkn v1.0.pdf.

[17] Wesam Dawoud, Wesam Dawoud, Christoph Meinel, "Infrastructure as a service security:

Challenges and solutions Informatics and Systems", (INFOS), 2010 The 7th InternationalConference on Source.
[18] Ibikunle Ayoleke ," Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011
[19] Navneet Singh Patell," Software as a Service (SaaS): Security issues and Solutions ",International Journal of Computational Engineering Research (IJCER) *ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 6 || June – 2014*
[20] Devi T*1, Ganesan R2," Platform-as-a- Service (PaaS): Model and SecurityIssues ", TELKOMNIKA Indonesian Journal of Electrical EngineeringVol. 15, No. 1, July 2015, pp. 151 ~ 161
[21] Mehmet Tahir, Ali Emre, "Security Problems of Platform-as-a-Service (PaaS)Clouds and Practical Solutions to the Problems" International Symposium on Reliable Distributed Systems2012 31st
[22] Australian government department of defense, "Cloud Computing Security Considerations", CYBER SECURITY OPERATIONS CENTRE APRIL 2011, UPDATED SEPTEMBER 2012.
[23] Dr. Jayant Shekhar1," An analysis on securityconcerns and their possible solutions in cloud computing environment ", 3rd International Conference on Role of Engineers as Entrepreneurs in Current Scenario - 2014 (ICREECS-2014) ISBN:978-93-5174-583-9.
[24] Waleed Al Shehri, "CLOUD DATABASE DATABASE AS A SERVICE", International Journal of Database Management Systems (IJDMS) Vol.5, No.2, April 2013 .
[25] Jenni Susan Reuben, " A Survey on Virtual Machine Security", KK T-110.5290 Seminar on Network Security 2007-10-11/12
[26] Rohit Bhadauria, " Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", International Journal of Computer Applications 47(18):47-66, June 2012.
[27] K. Vieira, A. Schulter, C. B. Westphall, C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment", ITProfessional, IEEE Computer Society, vol. 12, issue 4, 2010, pp. 38-43.