Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review Paper on Virtualization and Security in Cloud Computing

Yogesh Bhardwaj[1], Dr. Manju Kaushik[2]
M.Tech, Department CSE, JECRC University, Jaipur, India [1]
Associate Professor, Department CSE, JECRC University, Jaipur, India [2]

Abstract— ***Cloud computing is an emerging software technology based on the network and it is a technique that provides access to data from server. It describes extremely scalable computing assets provided as an external service via the internet on a pay- as- you-go basis. We all know about cloud computing but there are many factors on which we have to focus on like "Virtualization "and "Security". In this paper we give a survey on cloud computing on virtualization and possible threats and attacks on cloud computing as well as their solution.***
***Keywords*— Cloud Computing, virtual, virtualization, Security, Threats, Attacks**

I. INTRODUCTION

In the early days the mainframe computer was very large or bulk in size and the computing platform was centralized with limited resources & power, CPU, memory so used by limited no of users. The origin of mainframe computer was 1920s so it gives the concept of cloud computing where all data of user stored on server and user access the data from anywhere at any time. There is no hard drive or special system required only his account required. We can understand the concept of cloud computing with an example "when we store our photos or data online (Internet) instead of our home PC or we use our webmail or social networking sites then it is CLOUD COMPUTING".

In simple language it refers to the delivery of information of user or resources over internet. Cloud services used for individual and business purpose which managed by third party. So "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (example:- Network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST).

The service model of cloud computing are SAAS, PAAS, IAAS. SAAS refers to Software as a Service in this a system with operating systems, hardware & network provided or we can say a pre developed system. PAAS refers to Platform as a Service in this the operating system, hardware & network are provided and customer/ user install or develop its own software. IAAS refers to Infrastructure as a Service in this customer has the knowledge about all the stuff. Now after services the well known concept Virtualization came. Basically virtualization is a concept of operating system. It came from word "Virtual" which means "Not Actual" or "Imaginary". So in cloud computing virtualization is the emulation of one of more workstations/servers with in a single physical computer. So by using virtualization the use of hardware resources is increased, cost of resources and management is reduced, business flexibility is improved & security also improved. So by using cloud services it is also valuable or useful that the sensitive information of user remain trustworthy or secured but there are many possible attacks like man in middle attack, denial of service attack etc. So we have to minimize these types of attacks.

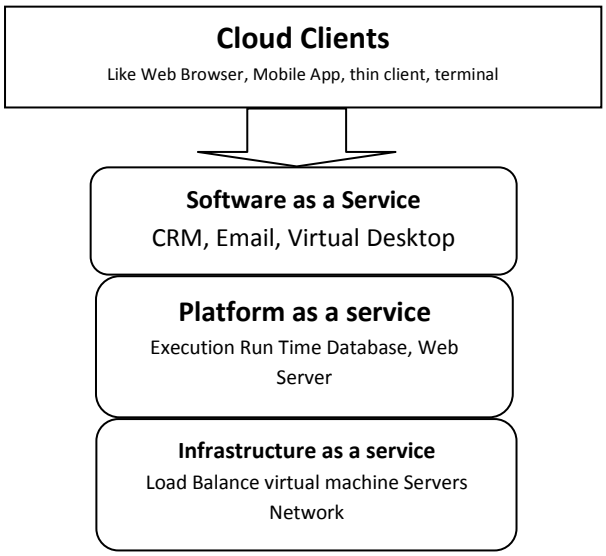

Fig. 1 Cloud Computing Services

Cloud computing has lots of technical as well as legal issues. The presence of internet in the cloud computing rises the same legal and technical issue of internet. The issues are like conflict of jurisdiction, online IPR infringement, application of law, data protection, security, privacy and finally management of the big data which generated through the cloud computing. This paper is structured as follow: - In section 2 discusses work related closely to us. Section 3 presents the actual definition of cloud Section 4 about brief description of Virtualization, Section 5 represent security threats & attacks, Section 6 give the idea about handling those type of attacks, Section 7 gives short detail of challenges of cloud computing and Conclusion and future work are summarized in section 8.

II. RELATED WORK

In this section study or review of the other author resources and write about their research. It is not a new technology the trend towards cloud computing initiated in the late 1980s with grid computing. On that particular time a large no of systems were used for a single problem also by using parallel computing. It is basically used in Europe for long distance optical network for educational area [1].

After grid computing the concept of cloud computing is used. In a cloud computing environment, computing and extended IT business resources such as server, storage, network, applications and processes can be dynamically shaped. In the 1990s the concept related to cloud computing means virtualization was used or came in form in this the virtual servers to higher levels of abstraction [2]. In cloud computing SAAS [3] has raised the level of virtualization to the application. There are many companies like Google, Microsoft, Amazon; IBM etc used cloud computing & build data centre based application over the internet and offering various types of services. Today there are many changes in trends of cloud computing according to business and providers. It used mainly in enterprises and social networking. Today hybrid cloud [4] used for business solutions and big data analytics because of its scalability.

Besides all services of cloud computing security is also a major issue. There are many threats for user's data and information so many authors give the solution of these threats.

III. WHAT IS ACTUALLY CLOUD?

Thus so far we all know about cloud computing. So now actual definition of word "cloud" is a set of different types of hardware and software that work collectively to deliver many aspects of computing to the end user as an online service. According to cloud providers there are public cloud for all users, private cloud for specific organizations, and community cloud for the service shared by several organizations and made available to those groups [5]. Hybrid cloud is combination of different clouds like public, private and community clouds.

IV. VIRTUALIZATION

Basically the term virtualization refers to the emulation of hardware within a software platform. This allows a single computer to take on the role of multiple computers. Now the need of virtualization is that in a file or a web server purchase, maintenance, depreciation, floor space & energy usage is high or we can say double. But when we create a virtual web or file server than all of our objectives are fulfil like maximum use of hardware resources, reduce cost, increase flexibility in business environment and improvement in security. There are many benefits of virtualization like easier manageability, elimination of the compatibility issues, fault isolation, increased security, efficient use of resources, portability, problem free testing, rapid deployment, reduce costs etc. Virtualization in cloud computing is many types like data storage virtualization for combining local & network resources, storage virtualization for grouping physical storage devices into a single unit, improving availability using virtualization for reaching high level of availability, improving performance using virtualization using stripping and caching and also capacity improvement [6].

V. SECURITY THREATS AND ATTACKS

1. **Threats for Cloud Service Users: -** There are some threats related to cloud user. They are-
   - **1.1. Responsibility Ambiguity: -** Cloud service users use delivered resources through service models. The customer-built IT system thus relies on the services. The lack of a clear definition of responsibility among cloud service users and Providers may evoke conceptual conflicts.
   - **1.2. Loss of Governance: -** This loss of governance depends on the cloud service models. For instance, IaaS only delegates hardware and network management to the provider, while SaaS also delegates OS, application, and service integration in order to provide a turnkey service to the cloud service user.
   - **1.3. Loss of Trust: -** It is sometime difficult for a cloud service user to recognize his provider's trust level due to the black-box feature of the cloud service. There is no measure how to get and share the provider's security level in formalized manner.
   - **1.4. Service Provider Lock-in: -** Cloud provider relies on non-standard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.
   - **1.5. Unsecure Cloud Service User Access: -** Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.
   - **1.6. Lack of Information/Asset Management: -** When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers such as location of sensitive information, lack of physical control for data storage, reliability of data backup, Disaster Recovery and so on.

1.7. Data loss and leakage: - The loss of encryption key or privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information such as encryption keys, authentication codes and access privilege will heavily lead sensitive damages on data loss and unexpected leakage to outside.

2. Threats for Cloud Service Providers: - There are some threats related to cloud service providers. They are-

2.1. Responsibility Ambiguity: - Different user roles, such as cloud service provider, cloud service user, client IT admin, data owner, may be defined and used in a cloud system. Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance etc. may induce business or legal dissention (Especially when dealing with third parties. The cloud service provider is somehow a cloud service user).

2.2. Protection Inconsistency: - Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules.

2.3. Evolutional Risks: - Conventional risk assessment methodology can no longer match such an evolution. A system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

Some of the threats are business discontinuity, supplier lock in, license risk, bylaw conflict, bad integration, unsecured administration API, shared environment, hypervisor isolation failure, service unavailability and data unreliability.

3. Attacks on cloud computing: - We all know denial of service attack and man in middle attack etc. Besides all these types of attacks some others attacks are-

3.1. Side Channel Attack: - Infrastructure as a Service(IaaS) model in cloud computing provides infrastructures like a collection of multiple computers, virtual machines(VMs) and other resources to its users to store their application, file, confidential information, documents and so on. So there are two virtual machine one is instantiate and one is target virtual machine. So placing instantiate to target VM and extracting sensitive information from target VM is called "Side Channel Attack" [7].

3.2. Wrapping Attack: - When a user makes a request from his VM through the browser, the request is first directed to the web server. In this server, a SOAP message is generated. This message contains the structural information that will be exchanged between the browser and server during the message passing. For a wrapping attack, the adversary does its trick during the translation of the SOAP message in the TLS (Transport Layer Service) layer. The body of the message is duplicated and sent to the server as a legitimate user. The server checks the authentication by the Signature Value (which is also duplicated) and integrity checking for the message is done. As a result, the adversary is able to intrude in the cloud and can run malicious code to interrupt the usual functioning of the cloud servers.

3.3. Malware-injection Attack: - In a malware-injection attack, an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping.

3.4. Flooding Attack: - In a cloud system, all the computational servers work in an internal communication between them. Whenever a server is overloaded or has reached the threshold limit, it transfers some of its jobs to a nearest and similar service-specific server to free from itself. This sharing approach makes the cloud more efficient and faster executing requests. When an adversary has achieved the authorization to make a request to the cloud, then he/she can easily create bogus data and pose these requests to the cloud server. This is called "Flooding Attack".

3.5. Data Stealing Problem: - The user account and password are stolen. As a result, the succeeding stealing of confidential data or even the destroying of data can hamper the storage integrity and security of the cloud.

3.6. Accountability Check Problem: - It is related to "pay as per you use" means "no pay no use" [8].

VI. HANDLING THE ATTACKS

Many authors give solution of above defined attacks. So by using those solutions the security aspect of cloud computing is fulfilling.

1. **Side Channel Attack Solution: -** The solution of side channel attack is given by Amazon EC2. This is done by co-residence checks of virtual machine and virtual firewall appliance and patching.
2. **Wrapping Attack Solution: -** Since an adversary can intrude in the TLS layer, the increment in security during the message passes from the web server to a web browser by using the SOAP message. Specifically, as the signature value is appended and a bit called STAMP bit is appended. This bit will be toggled when the message is interfered with by a third party during the transfer. When it is received in the destination, the STAMP bit is checked first and if it is found toggled, then a new signature value is generated in the browser end and the new value sent back to the server as recorded to modify the authenticity checking. This is used for authentication checking.
3. **Malware-injection Attack Solution: -** In this storing the OS type of the customer in the first phase when a customer opens an account. As the cloud is totally OS platform independent, before launching an instance in the cloud, cross checking can be done with the OS type from which the instance was requested from with the account holder's OS type.
4. **Flooding Attack Problem: -** Organizing all the servers in the cloud system as a group of fleet of servers. Each fleet of servers will be designated for specific type of job. In this approach, all the servers in the fleet will have

internal communication among themselves through message passing. So when a server is overloaded, a new server will be deployed in the fleet and the name server, which has the complete records of the current states of the servers, will update the destination for the requests with the newly included server.

5. **Data Stealing Problem Solution: -** At the end of every session, the customer will send an e-Mail about the usage and duration with a special number to be used for log in next time. In this way, the customer will be aware of the usage and charges as well as be availed with a unique number to be used every time to access the system.
6. **Accountability Check Problem Solution: -** Investigation should take place by1) Identities, 2) Secure Records, 3) Auditing and 4) Evidence for accountability checking of customers.

VII. CONCLUSION AND FUTURE SCOPE

This survey give the brief idea about cloud computing and concepts related to cloud computing like virtualization and security. Cloud computing is a technology for information and the services for revolution, but the revolution always comes with new problems. We have depicted some crucial and well known security attacks and threats and have proposed some potential solutions in this paper. In the future, we will extend our research by providing implementations and producing results to justify our concepts of security for cloud computing. The concepts we have discussed here will help to build a strong architecture for security in the field of cloud computation for improving customer satisfaction.

REFERENCES

[1] Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations", Proceedings of the ITI 2008 30th Int. Conf. on Information Technology Interfaces, June 23-26, 2008, Cavtat, Croatia

[2] R. Buyya, C. S. Yeo, and S. Venugopa, "Marketoriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities" In Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08, IEEE CS Press, Los Alamitos,CA, USA) 2008.

[3] Lijun Mei, W.K. Chan, T.H. Tse, "A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues", To appear in Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference (APSCC 2008), IEEE Computer Society Press, Los Alamitos, CA

[4] An Introduction to Virtualization, http://www.kernelthread.com/publications/virtualization/

[5] M.A. Vouk, "Virtualization of Information Technology Resources", in Electronic Commerce: A Managerial Perspective 2008, 5th Edition y Turban, Prentice-Hall Business Publishing, to appear.

[6] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[7] BhruguServak, "Security Against Side Channel Attack in Cloud Computing", *International Journal of Engineering and Advanced Technology (IJEAT),* **2(2),** P.No.- 183-186, (2012).

[8] KaziZunuurhain, SusainV.Vrbsky, "Security attacks and solutions in clouds".

[9] AlexaHuth, James Cebula, "The Basics of cloud computing".

[10] Lewis, Grace. *Basics About Cloud Computing*. http://www.sei.cmu.edu/library/abstracts/whitepapers/cloudcomputingbasics.cfm (2010).

[11] Lewis, Grace. *Cloud Computing: Finding the Silver Lining, Not the Silver Bullet*. http://www.sei.cmu.edu/newsitems/cloudcomputing.cfm (2009).

