A Comparative Approach for Security Issues In Cloud Computing

Shweta Vasant Shinde
Assistant Professor, Dept of Computer Engineering
Vadodara Institute of Engineering, Kotambi, Vadodara, India

Abstract- *Cloud computing has drastically changed everyone's perception of infrastructure architectures, software delivery and development models. The transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective, a number of risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. The aim of this paper is just to review the issues related to the security in cloud computing*.

Keywords- Cloud computing, Threats, Security Issues, Service Models

I. INTRODUCTION

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Due to the unprecedented success of internet in last few years, computing resources are now more easily available. And it enabled realization of a new computing concept called cloud computing. Cloud Computing environment requires the traditional service providers to have two different ways. These are infrastructure and service providers. Infrastructure providers manage cloud platforms and lease resources according to usage. Service providers rent resources from infrastructure providers to serve the end users. Cloud Computing has attracted the giant companies like Google, Microsoft, and Amazon and considered as a great influence in today's Information Technology industry. Business owners are attracted to cloud computing concept because of several features.

These are as follows:

- Lower initial investment Easier to manage Scalability
- Deploy faster Location independent Device independent
- Reliability Security
- Although cloud computing has shown considerable opportunities to the IT industry of today's world, but still there are number of challenges that requires to be carefully addressed. In our paper, we present a survey of cloud computing and state of- the-art research challenges. Our aim is to provide a better understanding of cloud computing and focus on the research ongoing in this tremendously flourishing arena of computer science.

II. WHAT IS CLOUD COMPUTING?

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Due to the unprecedented success of internet in last few years, computing resources Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services),which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

Advocates claim that cloud computing allows companies to avoid up-front infrastructure costs (e.g., purchasing servers). As well, it enables organizations to focus on their core businesses instead of spending time and money on computer infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables information technology (IT) teams to more rapidly meet resources to meet fluctuating and unpredictable business demand. Cloud providers typically use

a "pay as you go" model. This will lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

In 2009, the availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease.

In 2013, it was reported that cloud computing had become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Some cloud vendors are experiencing growth rates of 50% per year, but being still in a stage of infancy, it has pitfalls that need to be addressed to make cloud computing services more reliable and user friendly.

III. SERVICES PROVIDED BY CLOUD

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). These are sometimes called the cloud computing stack, because they build on top of one another. Knowing what they are and how they are different makes it easier to accomplish your business goals.

Infrastructure-as-a-service (IaaS)

The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis.

Platform-as-a-service (PaaS)

Refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

Software-as-a-service (SaaS)

Is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC.

IV. SECURITY ISSUES IN CLOUD COMPUTING

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds. We have extended the technologies and concepts we have developed for secure grid to a secure cloud. We have defined a layered framework for assured cloud computing consisting of the secure virtual machine layer, secure cloud storage layer, secure cloud data layer, and the secure virtual network monitor layer (Figure 1). Cross cutting services are provided by the policy layer, the cloud monitoring layer, the reliability layer and the risk analysis layer. For the Secure Virtual Machine (VM) Monitor we are combining both hardware and software solutions in virtual machines to handle problems such as key logger examining XEN developed at the University of Cambridge and exploring security to meet the needs of our applications (e.g., secure distributed storage and data management). For Secure Cloud Storage Management, we are developing a storage infrastructure which integrates resources from multiple providers to form a massive virtual storage system. When a storage node hosts the data from multiple domains, a VM will be created for each domain to isolate the information and corresponding data processing. Since data may be dynamically created and allocated to storage nodes, we are investigating secure VM management services including VM pool management, VM diversification management, and VM access control management. Hadoop and MapReduce are the technologies being used. For Secure Cloud Data Management, we have developed secure query processing algorithms for RDF (Resource Description Framework) and SQL (HIVE) data in clouds with an XACML-based (eXtensible Access Control Markup

Language) policy manager utilizing the Hadoop/MapReduce Framework. For Secure Cloud Network Management, our goal is to implement a Secure Virtual Network Monitor (VNM) that will create end-to-end virtual links with the requested bandwidth, as well as monitor the computing resources.

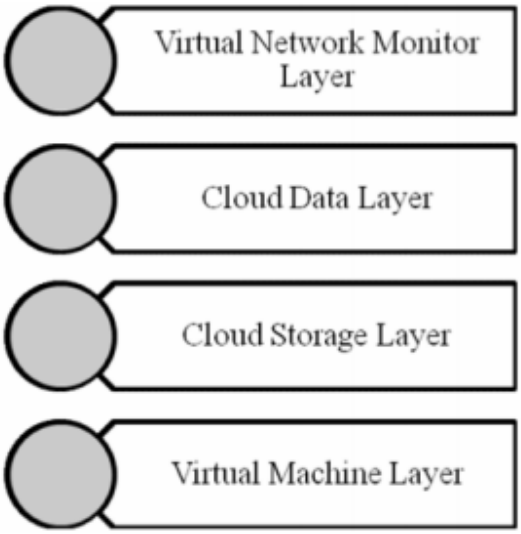

Fig. 1.Layer of assured cloud

V. SOLUTION FOR THE ISSUES

There is need for advanced and extended technologies, concepts and methods that provide secure server which leads to a secure cloud. For this a layered framework is available that assured security in cloud computing environment. It consists of four layers as shown in the above figure.

First layer is secure virtual machine layer. Second layer is cloud storage layer. This layer has a storage infrastructure which integrates resources from multiple cloud service providers to build a massive virtual storage system. Fourth layer is virtual network monitor layer. This layer combining both hardware and software solutions in virtual machines to handle problems such as key logger examining XEN.

There are some tips and tricks that cloud security solution providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution.

Verify the Access Controls

Set up data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by cloud service consumer. To implement access control methods for consumer side, the cloud service provider must describe and ensure that the only authorized users can access the user or consumer's data.

Control the Consumer Access Devices

Be sure the consumer's access devices or points such as Personal Computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. The loss of an endpoint access device or access to the device by an unauthorized user can cancel even the best security protocols in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features.

Monitor the Data Access

Cloud service providers have to assure about whom, when and what data is being accessed for what purpose. For example many website or server had a security complaint regarding snooping activities by many people such as listening to voice calls, reading emails and personal data etc.

Share Demanded Records and Verify the Data Deletion

If the user or consumer needs to report its compliance, then the cloud service provider will share diagrams or any other information or provide audit records to the consumer or user. Also verify the proper deletion of data from shared or reused devices. Many providers do not provide for the proper degaussing of data from drives each time the drive space is abandoned. Insist on a secure deletion process and have that process written into the contract.

Security Check Events

Ensure that the cloud service provider gives enough details about fulfillment of promises, break remediation and reporting contingency. These security events will describe responsibility, promises and actions of the cloud computing service provider.

VI. CONCLUSION

Cloud computing is a cost, time and performance effective technology. Of course the usage of cloud computing will surely increase more in coming years. In this paper we have discussed and surveyed basics of cloud computing and security issues prevailing there in and also some of the solutions that can be considered for security. Some security issues are the key concern in the cloud computing. Especially privacy and integrity of data are the key concern security issues. In the cloud data is stored publically and we don't have

the idea where the data is being stored, due to this data stored in the cloud has a higher risk of being accessed by unauthorized person during storage as well as transmission.

REFERENCES

[1] Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information security issue of enterprises adopting the application of cloud computing", IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM),pp 645, 16-18 Aug. 2010.

[2] Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z; (2010),"Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), pp 105, 1-3 Nov. 2010.

[3] Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2, accessed on 2012.

[4] Amazon Simple Storage Service (Amazon S3), http://aws.amazon.com/s3, accessed on 2012.

[5] Y. Chen, V. Paxson, RH. Katz, "Whats new about cloud computing security," Tech.Rep.UCB/EECS-2010-5, EECS Department, University of California, Berkeley, 2010.

[6] S. Ramgovind, MM. Eloff and E.Smith, "The Management of Security in Cloud Computing," Information Security for South Africa (ISSA), IEEE, 2010.

[7] Open Security Architecture, http://www.opensecurityarchitecture.org/ ,access on 2012.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, Saint Malo, France, Sep. 2009.

[9] P. Saripalli, and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security," 2010 IEEE 3rd Intl. Conf. on Cloud Computing; Miami, FL, July, 2010.

[10] D. Zissis, D. Lekkas, ''Addressing cloud computing security issues,'' Future Generation Computer Systems, 1--10, 2010.