International Journal of Current Research in Multidisciplinary (IJCRM) *ISSN: 2456-0979*
Vol. 3, No. 4, (April'18), pp. 06-09

SECURITY ASPECTS OF CLOUD COMPUTING: AN OVERVIEW

Dr. G. Rajitha Devi
Asst. Prof. in Computer Science

ABSTRACT:
Cloud computing is the latest effort in delivering computing resources as a service. It represents a shift away from computing as a product that is purchased, to computing as a service that is delivered to consumers over the internet from large-scale data centers. Cloud computing is architecture for providing computing service via the internet on demand and pay per user access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. This paper is the first systematic review of peer-reviewed academic research published in this field, and aims to provide an overview of the swiftly developing advances in the technical foundations of cloud computing and their research efforts. This overview gives the basic concept, defines the terms used in the industry, and outlines the general architecture and applications of Cloud computing. It gives a summary of Cloud Computing and provides a good foundation for understanding.

Keywords: *Cloud, Grid, Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform, Grid Computing.*

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. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. Cloud computing has recently reached popularity and developed into a major trend in IT. While industry has been pushing the Cloud research agenda at high pace, academia has only recently joined, as can be seen through the sharp rise in workshops and conferences focusing on Cloud Computing. Cloud computing provides the facility to access shared resources and common infrastructure, offering services on demand over the network to perform operations that meet changing business needs. The location of physical resources and devices being accessed are typically not known to the end user. It also provides facilities for users to develop, deploy and manage their applications 'on the cloud', which entails virtualization of resources that maintains and manages itself. Clouds are the new trend in the evolution of the distributed systems, the predecessor of cloud being the grid. The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser [1].

BUILDING BLOCKS OF CLOUD COMPUTING

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). *Software-as-a-Service (SaaS):* SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support. SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data center space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SaaS features a complete application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps. *Platform as a Service (PaaS):* "PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure[2].

Infrastructure as a Service (IaaS):

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new

equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid. There are also four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below. *Private cloud:* Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems [3].

Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud include Microsoft Azure, Google App Engine [4].

Hybrid Cloud:

A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds[5].

CLOUD COMPUTING ARCHITECTURE

Cloud computing architecture, just like any other system, is categorized into two main sections: Front End and Back End. Front End can be end user or client or any application (i.e. web browser etc.) which is using cloud services. Back End is the network of servers with any computer program and data storage system. It is usually assumed that cloud contains infinite storage capacity for any software available in market. Cloud has different applications that are hosted on their own dedicated server farms. Cloud has centralized server administration system. Centralized server administers the system, balances client supply, adjusts demands, monitors traffic and avoids congestion. This server follows protocols, commonly known as middleware. Middleware controls the communication of cloud network among them. Cloud Architecture runs on a very important assumption, which is mostly true. The assumption is that the demand for resources is not always consistent from client to cloud. Because of this reason the servers of cloud are unable to run at their full capacity. To avoid this scenario, server virtualization technique is applied. In sever virtualization, all physical servers are virtualized and they run multiple servers with either same or different application. As one physical server acts as multiple physical servers, it curtails the need for more physical machines. As a matter of fact, data is the most important part of cloud computing; thus, data security is the top most priority in all the data operations of cloud. Here, all the data are backed up at multiple locations. This astoundingly increases the data storage to multiple times in cloud compared with a regular system. Redundancy of data is crucial, which is a must-have attribute of cloud computing [6].

SECURITY ISSUES IN CLOUD COMPUTING

The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. 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 and mapping the virtual machines to the physical machines has to be carried out securely [7].

Data Transmission
• Data Security
• Data Privacy
• Data Integrity
• Data Location
• Data Segregation

Data Transmission: In Cloud environment most of the data is not encrypted in the processing time. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

Data Privacy:
A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks[8].

Data security:
To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption. In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host [9].

Data Integrity:
Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control [10].

Data Location:
Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications [11]. In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manger. Each application in the distributed system should be able to participate in the global transaction via a resource manager.

Data Segregation:
Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

CONCLUSION

After so many years, Cloud Computing today is the beginning of "network based computing" over Internet in force. It is the technology of the decade and is the enabling element of two totally new computing models, the Client-Cloud computing and the Terminal-Cloud computing. These new models would create whole generations of applications and business. Our prediction is that it is the beginning to the end of the dominance of desktop computing such as that with the Windows. It is also the beginning of a new Internet based service economy: the Internet centric, Web based, on demand, Cloud applications and computing economy.

REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, "*Introducing New Services in Cloud Computing Environment*", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] B. R. Kandukuri, R. Paturi V, A. Rakshit, "*Cloud Security Issues*", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[3] Welcome *to the Data Cloud*, Semantic Web blog, ZDnet, 6 Oct 2008.

[4] Pollette, Chris. "How the Google-Apple Cloud Computer Will work."*Howstuffworks.com.* 2 Mar. 2008

[5] Rubel, Steve. "*The MacBook Air is the Biggest Test Yet for Cloud Computing*." *MicroPersuasion.* 2 Mar.2008.

[6] Weiss, Aaron. Computing in the clouds. *Networker* 4 Dec. 2007.

[7] K. Hwang, S Kulkarni and Y. Hu, "*Cloud security with virtualized defence and Reputation-based Trust management*," Proceedings of 2009 Eighth IEEE International

[8] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "*On technical Security Issues in Cloud Computing,"* Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[9] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O' Reilly Media, USA, 2009.

[10] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "*Research Issues in Cloud Computing* "Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[11] X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, "*Information Security Risk Management Framework for the Cloud Computing Environments*", In Proceedings of 10th IEEE International Conference on Computer and Information Technology, pp. 1328- 1334, 2010.