Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.123 – 125

SURVEY ARTICLE

Security and Privacy in Cloud Computing: A Survey

Shachindra Kumar Dubey[1], Prof. Ashok Verma[2]

[1]Computer Science and Engg, Department, Gyan Ganga Institute of Technology and Sciences, Jabalpur

[2]HOD, Computer Science and Engg, Department, Gyan Ganga Institute of Technology and Sciences, Jabalpur

[1] sachindrakumar000@gmail.com; [2] ashokverma@ggits.org

Abstract— Cloud computing is envisioned as the next-generation technology. It is an Internet based technology where quality services are provided to users including data and software, on remote servers. The phrase cloud computing originated from the diagrams used to symbolize the Internet. Cloud computing is not a completely fully new concept; it has intricate connection to the grid computing paradigm, and other relevant technologies such as utility, cluster and distributed systems. Here we present an analysis of security issues in a cloud environment. This paper introduces the background and service model of cloud computing. Along with this, few of security issues and challenges are also highlighted.

Key Terms: - Cloud Computing; Security; Trust

I. INTRODUCTION

A broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are "cloud-based" (also known as security as a service).

In this paper, we investigate the security concerns of current cloud computing systems. As cloud computing referred to both the applications delivered as services over the Internet and the infrastructures (i.e. the hardware and systems software in the data centers) that provide those services. More concerns on security issues, like authentication, confidentiality, integrity, non-repudiation, access control and availability.

NIST definition of cloud computing:

"*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, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*"

Buyya defined cloud as follows:

"A cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers."

II. CLOUD COMPUTING

Cloud computing, to put it simply, means "Internet Computing." The Internet is commonly visualized as clouds; hence the term "cloud computing" for computation done through the Internet. With Cloud Computing users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources.

Depending on the type of service provided, there are three types of cloud services also termed as delivery models; Infrastructure as a service, (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).

(i) IaaS refers to delivering IT infrastructure as commodity to customers. These resources meet the end user requirements in terms of memory, CPU types and power storage.

Examples:

Amazon Simple Storage Services (Amazon S3): which customer pay based on storage capacity.

Amazon Elastic Compute Cloud (Amazon EC2): which customer pays for compute resources by the hour.

(ii) PaaS provides an application or development platform in which users can create their own application that will run the cloud.

Examples:

Microsoft's Azure: Application platform that allows applications to be hosted and run at Microsoft datacenters.

Google's App Engine (App Engine): Let customers built virtual Java or Python Web application on Google servers.

(iii) SaaS means a customer runs software remotely via tha Internet. SaaS solutions provide end users with an integrated service comprising hardware, development platforms and applications.

Examples:

Yahoo!, Gmail, Google Docs, Flickr, Facebook, etc.

III. SECURITY IN CLOUD COMPUTING

In cloud computing paradigm, a cloud provider creates, deploys and manages the resources, application and services. Major types of security threats in the context of cloud application are briefly described below:

A. Confidentiality

The principal of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access a message.

For Example, the user of A sends a message to user B. Another user C gets access to this message, which is not desired, and therefore, defeats the purpose of confidentiality.

B. Authentication

Authentication mechanism helps to establish proof of identities. The authentication process ensures that the origin of an electronic message or document is correctly identified.

For Example, Suppose that user C sends an electronic document over the Internet to user B. However, the difficulty is that user C has posed as user A when he sent this document to user B. How would user B know that the message has come from user C, who is posing as user A?

C. Integrity

When the data of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of a message is lost.

For Example, suppose you write a check for $1000 to pay for the goods bought from the US. However, when you see your next account statement, you are startled to see that the check resulted in a payment of $10000. This is the case for loss of message integrity.

D. Non-repudiation

There may situations where a user sends a message, and later on refuses that he had sent that message.

For Example, User A could send a funds transfer request to Bank B over the Internet. After the Bank Performs the funds transfer as per A's instructions, a could claim that he never sent the funds transfer instruction to the Bank. Thus, A repudiates, or denies, his funds transfer instruction.

E. Access control

The principle of access control determines who should be able to access what.

For Example, We can specify that user A can view the records in a database, but cannot update them. However, user B might be allowed to make updates as well. An access control mechanism can be used to ensure this.

IV. RELATED RESEARCH IN TRUST

Trust is an important aspect of decision making for Internet applications and particularly influences the specification of security policy. It implies depth and assurance of confidence based on some evidence. The trust ability of entity can be defined in a particular regard like security, reliability, availability or any property.

Trust addresses security issues in various collaborative environments. We have identified techniques and methods of incorporating trust in various collaborative environments.

Various sub sections are identified depending on the way of obtaining trust in such environments as below:

A. Data privacy

A trust based approach has also applied to control privacy exposure in ubiquitous computing. Trust values are used to provide fine-grained control over the exposure of personal information. Trust decisions in terms of trust metrics are used to provide security and privacy of data.

B. Agent based Trust Evaluation

An automated Agent based trust negotiation scheme for dynamic trust establishment is proposed in. Agent centric approach for intelligent environment is proposed in. Agent based solution for calculating trust metric in complex environment is achieved by checking user behavior and actions.

C. Trust for service selection

A trust space in terms of vector form stores the attribute value of the particular service. These vector values are calculated and updated to measure trust. It includes systematic and adjusted subjective logic evaluation as well as evolutionary based approach for composite and individual service.

D. Identity based solutions

Identity management solution using trust is achieved by measuring authentication and access control. Trust based solution by developing a security policy, assigning credentials to entities, delegating trust to third party, and reasoning about user access rights. Trust calculation, updation, reputation evaluation are carried based on experience and recommendations. A trust based solution comprising of trusted computing also provides access control.

E. Application security

Integrity requires that application code is not tampered with, prior to or during execution, by a rogue user or a malicious software agent. The integrity of the application that is executed by the remote machine will be maintained by the continuous replacement during run time. The integrity check is done using tag generated by the respective machine to prove its authenticity.

V. CONCLUSION AND FUTURE WORK

Cloud computing is a kind of computing paradigm that can access conveniently a dynamic and configurable public set of computing resources (e.g. server, storage, network, application and related service), provided and published rapidly and on-demand with least management and intervention. However, the prevalence of cloud computing is blocked by its security to a great extent. Trust based solution also exists for cloud but not directly addressing all security issues discussed.

In the future, we will give and implement some security strategies with technology and management ways.

REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing_security.
[2] National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.
[3] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing (v2.1). Decemeber,2009.
[4] Jensen, M. Schwenk, J. Gruschka, N. Iacono, "On technical security issues in Cloud" IEEE International Conference on Cloud Computing, 2009, pages 109-16, Germany.
[5] Diana Kelley," Cloud computing security model overview: Network infrastructure issues", http://searchcloudsecurity.techtarget.com/tip/, 2009.
[6] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009.
[7] IBM Corporation, Enterprise Security Architecture Using IBM Tivoli Security Solutions, Aug 2007.
[8] Carl Almond, "A Practical Guide to Cloud Computing Security", http://www.avanade.com/Documents/Research%20anad%20Insights/practicalguidetocloudcomputingsecurity574834.pdf, August 2009.
[9] http://es.slideshare.net/iaeme/reliable-security-in-cloud-computing-environment-23456
[10] Descher, M. Masser, P. Feilhauer, T. Tjoa, A.M. Huemer, D., "Retaining data control to the Client in Infrastructure Cloud", International Conference on Availability, Reliability and Security, 2009, pages 9-16, Dornbirn.

