CLOUD SECURITY REQUIREMENTS

BY

POONAM RAWAT * NEHA RAWAT ** SHIKHA SINGH ***

AWANTIKA ****

*-**** Students, Govind Ballabh Pant University of Agriculture and Technology, Pantnagar.

ABSTRACT

Cloud computing brings new opportunity and challenges for IT industry. Basically, Cloud computing provides you to access your information from anywhere at any time. So, Cloud computing security is a major concern for cloud service providers, developers and also for users who are using this technology everyday. And ensuring cloud security has become a burning topic in IT industry and research era. The goal of this paper is to provide all the cloud security requirements which should be properly understood for giving cloud its full potential. Taking those requirements, cloud service providers will be able to deliver an efficient and secure service on cloud to individual customers and enterprise. This will encourage the adoption of cloud computing not only on small enterprises, but all over the world on large scales also.

Keywords: Cloud computing, security requirements.

INTRODUCTION

Cloud computing is a maturation of grid computing, cluster computing, distributed computing, parallel computing and virtualization. Client and server computing is the first step in computing in which all the software applications, data and control resides on a sever (a huge mainframe), and then peer to peer computing came with equalizing concepts. Distributed computing provides more computing power than previous computing techniques. Then the need for multiple users to work on the same computer based project simultaneously gives birth to collaboration computing. The next step in collaboration computing is cloud computing [9].

Cloud computing provides you to access your information from anywhere at any time. It uses computing resources for e.g. Storage, server, data files, network, runtime environment etc which are delivered as a service over internet. According to National Institute of Standards and Technology (NIST) [7], 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".

With the help of cloud computing, you can access all your applications and documents from anywhere in the world at anytime, you just need an internet connection. In the front end of the cloud system, we have the client's device and some application which is needed for accessing the cloud computing system. And at the back end, there are various computing machines, data storages and servers. Cloud computing is available in various service models.

Software as a Service

It is also known as SaaS, In which cloud provider installs and operates application software in the cloud. Cloud user does not need to worry about the infrastructure and platform on which the application is running [1]. So cloud computing gives subscribers to access both resources and applications. Some examples of SaaS are Google docs, salesforce.com, Microsoft office 365 etc.

Platform as a Service

PaaS is the delivery of computing platforms which include operating systems, database servers, web servers and runtime environment as a service. So PaaS provides the facility to run software solutions on cloud platforms written by application developer. Microsoft Windows Azure, Force.com, Google App Engine, flexisacle, Heroku, and Engine Yard are some of the examples of PaaS.

Infrastructure as a Service

IaaS provides you the facility to run your computing task on virtually unlimited numbers of machines. Paas is the sharing of infrastructure resources such as processing, storage, networks [1] and other fundamental computing resources for running software applications in the cloud that would ordinarily be deployed and operated on-premise. Amazon EC2 and S3, IBM SmartCloud, Rackspace and OpenStack are examples of commercial IaaS.

1. Cloud Service Models

The cloud service models exhibit certain characteristics like devices and location independence, multi-tenancy, measured service, rapid elasticity, on-demand self-service and resource pooling [8] which are shown in the top of Figure 1(According to NIST). Cloud computing has four types of deployment models:

1.1 Public cloud

Public cloud can be accessed by any public user or subscriber, who just requires an internet connection and access to the cloud space. Public cloud is managed by a third party on off-premises and so, access may be insecure [4]. Google, Amazon, Rackspace are some examples of public cloud.

1.2 Private cloud

Private cloud is dedicated for a specific group and organization and access is limited to just that organization. It can be a simple normal data center within an organization. It is managed by an organization or a third party on on-premises or off premises which provides you trusted access [4].

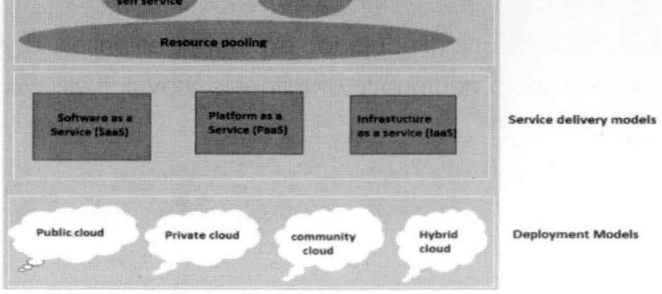

Figure 1. Cloud Computing

1.3 Community cloud

Community cloud deployment model is sharing of a cloud among two or more organizations having some same requirements and share same context.

1.4 Hybrid cloud

Hybrid cloud is a combination of any two clouds (private, public, and community).For example: a private cloud that can extend to use resources in public clouds. it is managed by organization and third party on on-premises and off-premises, so it provides you a trusted and insecure access[4].

2. Cloud Computing Security

With the huge use of cloud computing services all over the world, security is becoming a major concern which is hampering the growth of cloud computing. With increasing use of cloud computing in every area, there are lots of security requirements, which are considered by cloud service providers to ensure their customers that cloud is safe. The key security requirements of cloud computing are the following:

- Confidentiality
- Integrity
- Access control
- Non-repudiation
- Single sign-on
- Security audit
- Availability

2.1 Confidentiality

Confidentiality means, limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones. This security requirement of cloud computing prevents sensitive information from reaching the unauthorized people, while making sure that the authorized one can get information access. Some time confidentiality is directly connected to requirements of access control [5]. When we apply strict access control, it directly affects the confidentiality. Data encryption are common schemes which provide confidentiality. For security purpose, cloud provider uses Encryption schemes like symmetric encryption and asymmetric scheme to protect sensitive information. Unencrypted data is known as plaintext and encrypted data is known as cipher text. At sender side, Encryption algorithm and cryptographic key is used to encrypt data into cipher text and then data is send to recipient. At the receiver end, cipher text are decrypted into plain text. In this way, data is secured during transmission from eavesdropping, release of message content and traffic analysis.

2.2 Integrity

Integrity is a security requirement which refers to the trustworthiness of information in cloud. In cloud security, integrity includes the concepts of data integrity, hardware integrity, software integrity and personnel integrity. Data integrity ensures that data has not been changed either intentionally or by accident. Integrity can be applied on selected fields within a message, a single message or a stream of messages. For example: Data integrity in database systems, Data integrity in such a system is maintained by database transactions. For ensuring data integrity, transactions should follow ACID (atomicity, consistency, isolation and durability) properties [6]. In database management, there are lots of protocols like two phase commit protocol [2] and three phase commit protocol which are used to maintain the integrity of data. Data integrity assures the accuracy and reliability of communication in cloud.

2.3 Access control

Cloud is a pool of resources which can be accessed by users at anytime from anywhere. So cloud security requirements like Access control ensures only authorized users have the privilege to access those resources, but cannot make improper modifications in cloud. It also ensures that unauthorized access of resources is not allowed. There are three major components of access control: identification, authentication and authorization [5]. Identification activities can be username, account numbers and memory card information. While authentication is the verification of the identity of the users, for example- passwords, pin numbers, cryptographic keys etc. And authorization ensures which user can actually access the resources and what operations they can perform.

2.4 Non-repudiation

Repudiation is the denial by one of the communicating parties involved in a communication of having participated in a part or all of the communication. Communication can be a message, transaction and transmission of data. Such denials can be prevented by non repudiation. Non-repudiation allows a secure communication between two parties in such a way that the parties cannot subsequently deny they communicate. In Cloud computing, non-repudiation can be achieved by applying some traditional e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services [6, 10].

2.5 Single sign-on

Single sign-on is one of the basic cloud security requirements. It is user authentication process to allow a user to use single name and password combination to access multiple applications. Normally, a user requires single sign-in for accessing a single system, but when multiple systems are involved, user has to authenticate each system individually and repeatedly. For secure user authentication to multiple systems simultaneously, cloud provider uses security schemes like RSA crypto system, the subset-sum NP-complete problem, and discrete logarithm problems. These schemes are used to create Proxy certificates. In this process, user has to sign-in only once to create proxy certificates and then this certificate is used for all subsequent authentications.

2.6 Security Audit

Audit is a type of cloud security requirement, in which analysis on security related events is performed by security personnel, who are allowed to audit the status, use and vulnerability of security mechanisms. Audit services keep track of security related events. Auditing is a dynamic verification approach achieved by analyzing the execution of systems and checking and verifying its conformity against a set of rules. There are lots of standards available, but cloud-specific standard has not been introduced yet [5].

2.7 Availability

In cloud computing, availability are known as an on demand service of cloud. Actually on demand services refer to services or resources (data, software etc) that are available to authorized user upon their demand. That is, services and resources being accessible by authorized user upon demand. Availability is one of the most critical cloud security requirements because it is a key factor when deciding among which are private, public or hybrid cloud vendors as well as in the service delivery models SaaS, PaaS, and IaaS. Cloud provider should guarantee that the information access and processing is available to its client on demand in secure manner.

Therefore, by understanding the cloud security requirements and applying some cryptographic techniques, it will be easy for cloud service providers to deliver a protected, secure cloud environment.

Conclusion

In this paper, our main focus on security requirements in cloud computing. This paper describes the major cloud security requirements like confidentiality, integrity, availability, access control and also some cryptographic techniques (RSA, digital signature) which can be applied on cloud in brief. So when cloud service providers are designing and delivering cloud computing services, they should focus on these cloud security requirements. Although cloud computing is a new and emerging technology in IT industry, security is a key factor which is hampering its growth. We conclude that to ensure cloud security it is very essential to strengthen cloud security requirements.

References

[1]. **Dimitrios Zissis, Dimitrios Lekkas (2012).** "Addressing cloud computing security issues", *Future Generation Computer Systems*. pp.28 583–592.

[2]. **S. Subashini and V. Kavitha (2011).** "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*. pp.34, 1–11.

[3]. **Su Qinggang, Wang Fu and Hang Qiangwei (2012).** "Study of Cloud Computing Security Service Model", *IEEE* 978-1-4577-1964-6/12,

[4]. **Mutum Zico Meetei and Anita Goel (2012).** "Security Issues in Cloud Computing", *5th International Conference on BioMedical Engineering and Informatics. BMEI*.

[5]. **Patrick Höner (2013).** "Cloud Computing Security Requirements and Solutions: a Systematic Literature Review", *19thTwente Student Conference on IT*, June 24th.

[6]. **Ramgovind S, Eloff MM, Smith E (2010).** "The Management of Security in Cloud Computing", *IEEE*. pp.978-1-4244-5495-2/10.

[7]. **Peter Mell, and Tim Grance (2010).** *"The NIST Definition of Cloud Computing,"* Retrieved from http://www.wheresmyserver.co.nz/storage/media/faq-files/clouddef-v15.pdf, Accessed April.

[8]. **Cloud Security Alliance (2009).** *"Security guidance for critical areas of focus in cloud computing"*, V2.1.

[9]. **Michel Miller.** "Cloud computing web-based applications that change the way you work and collaborate online", *Indianapolis*, Indiana

[10]. **A. Priyadharshini (2013).** "A Survey on security issues and countermeasures in cloud computing storage and a tour towards multi-cloud". *International Journal of Research in Engineering and Technology (IJRET)*. Vol. 1, Issue 2, July.

ABOUT THE AUTHORS

Poonam Rawat has received her B-Tech degree in Computer Science Engineering from Dev Bhoomi Institute of Technology (DBIT), Dehradun (U.K.), India in 2012. Currently, she is pursuing M-Tech in Information Technology from Govind Ballabh Pant University of Agriculture & Technology, Pantnagar. Her research areas are Web Search algorithms, Web mining and Cloud computing.

Neha Rawat has received her B-Tech degree in Computer Science Engineering from Dev Bhoomi Institute of Technology (DBIT), Dehradun (U.K.), India in 2012.Currently,she is pursuing M-Tech in Information Technology from Govind Ballabh Pant University of Agriculture & Technology, Pantnagar. Her research areas are Cloud Computing and Computer Networks.

Shikha Singh has received her B-Tech degree in Information Technology from Uttaranchal Institute of Technology (UIT),Dehradun (U.K.), India in 2012 and pursuing M-Tech in Information Technology from Govind Ballabh Pant University of Agriculture & Technology, Pantnagar. Her research areas are Digital Image Processing and Cryptography.

Awantika has received her B-Tech degree in Computer Science Engineering from Apex Institute of Technology, Rudrapur (U.K.), India in 2011 and pursuing M-Tech in Information Technology from Govind Ballabh Pant University of Agriculture & Technology, Pantnagar. Her research areas are Wireless Sensor Network and Cryptography.