ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

An Analytical Study on Security Concerns in Cloud Computing

Radha Ramani Malladi

Visiting Faculty, Martins Academy, Bangalore, India

ABSTRACT: Cloud computing provides the ability to utilize scalable, distributed computing environments via the Internet. Over the years, cloud computing has grown from being a promising business concept to a fast growing sector in IT organizations. It has emerged as a promising hosting platform that allows an intelligent usage of a collection of applications, information and infrastructure comprised of pools of computer, network and storage resources. However, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the key factor which hampers growth of cloud computing. Some of the fundamental security challenges are data storage security, data transmission security, application security and security related to third-part resources. This paper focuses on security issues arising from the usage of cloud services.

This paper presents a comprehensive study, on the challenges and issues of security in cloud computing. We first book into the impacts of the distinctive characteristics of cloud computing, namely, multi-tenancy, elasticity and third party control, upon the security requirements. Then, we analyse the cloud security requirements in terms of the fundamental issues,i.e., confidentiality, integrity, availability, trust, and audit and compliance. Furthermore, we discuss the taxonomy for security issues in cloud computing.

KEYWORDS: Cloud computing security; Trusted Third Party; Security; Cloud Assessment; Availability; Confidentiality; Elasticity; Integrity; Multi-tenancy;

I. INTRODUCTION

Moving to the cloud presents the enterprise with a number of risks which include securing critical information like the protection of intellectual property, trade secrets, personally identifiable information that could fall into the wrong hands.

Making sensitive information available on the internet requires a considerable investment in security controls and monitoring of access to the contents. In the cloud environment, the enterprise may have little or no visibility to storage and backup processes and little or no physical access to storage devices at the cloud computing provider. Moreover, because the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of the access and deletion will be a significant challenge.

In case of a public-cloud computing, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario. A public cloud acts as a host of a number of virtual machines (VMs), virtual machine monitors, supporting middleware. The security of the cloud depends on the behaviour of these objects as well as on the interactions between them. Moreover, in a shared multi-tenant environment enabled by a public cloud, as the number of users is increasing, security risks are getting more intensified and diverse.

Before sensitive and regulated data move into the public cloud, issues of security standards and compliance must be addressed including strong authentication, delegated authorization, key management for encrypted data, data loss protections, and regulatory reporting.

Risk management of information security is the process in which we understand and respond to factors that may lead to a failure in the confidentiality, integrity or availability of an information system; the information security risk is the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information.

Cloud in general provides services at three different levels -
Software as Service (SaaS),
Platform as Service (PaaS) and
Infrastructure as a Service (IaaS).

SaaS is a software development model where applications are remotely hosted by an application or service provider and made available to customer via the Internet. SaaS offers customer with significant benefits, such as improved operational efficiency and reduced cost.

SaaS delivers special-purpose software that is remotely accessible by consumers via the Internet with a usage-based pricing model. Sales force is an industry leader in providing online CRM (Customer Relationship Management) services. Live Mesh from Microsoft allows files and folders to be shared and synchronized across multiple devices.
PaaS offers a high level integrated environment to build, test, and deploy custom applications. Generally, developers will need to accept some restrictions on the type of software they can write in exchange for built-in application scalability.

An example is Google's App Engine, which enables users to build web applications on the same scalable systems that power Google applications.
IaaS provides hardware and software and equipment to deliver software application environments with a resource usage-based pricing model. It changes the way developers deploy their applications. Typical examples are Amazon EC2(Elastic Cloud Computing) Service and S3 (Simple Storage Service) where compute and storage infrastructures are open to public access with a utility pricing model.

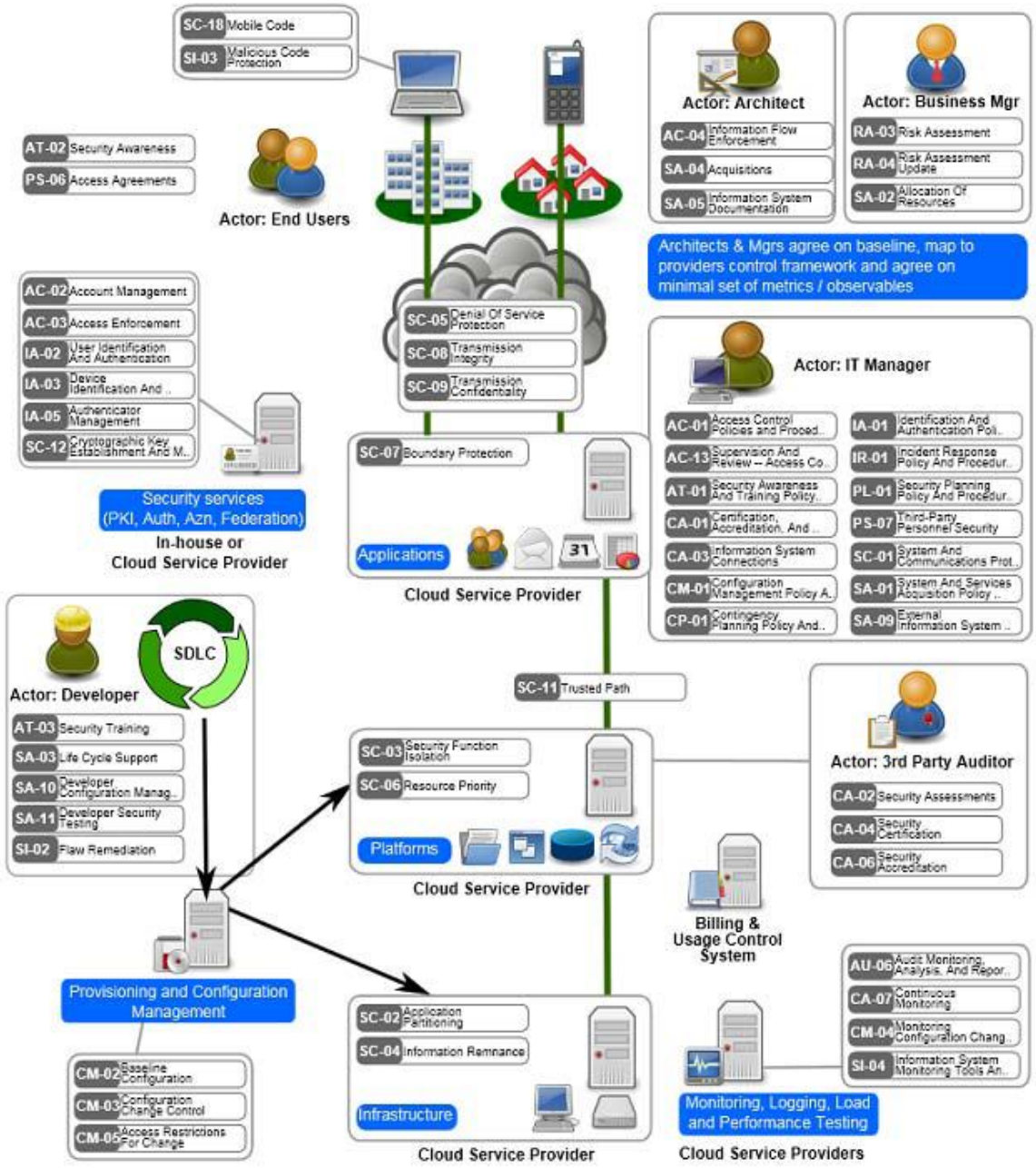
All these levels come with a promise to reduce expenditure and infrastructure. They offer a wide variety of products and advanced capabilities, automated scalability, pay-per-use, and on-demand provisioning. In spite of these advantages, security is most relevant inconvenience for fastening wide spread adoption of the cloud, for many business-critical computations.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015



II. CLOUD CHARACTERISTICS FOR SECURITY

A. Multi-Tenancy

Multi-tenancy, as the term implies, refers to having morethan one tenants of the cloud living and sharing other tenantsthe provider's infrastructures, including computationalresources, storage, services, and applications. By

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

multitenancy, clouds provide simultaneous, secure hosting of services for various customers utilizing the same cloud infrastructure resources.

Multi-tenancy is a feature unique to resource sharing in clouds, especially in public clouds. Essentially, it allows cloud providers to manage resource utilization more efficiently by partitioning a virtualized, shared infrastructure among various customers.

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. To reach the high scales of consumption desired, service providers have to ensure dynamic flexible delivery of service and isolation of user resources.

With a multi-tenant architecture, a software application is designed to virtually partition its data and configuration so that each customer organization works with a customized virtual application instance.

B. Elasticity

In cloud computing, customers need to use resources as faras needed while being able to increase or decrease resources consumption based on actual demands. To meet such needs, cloud services have to be scalable, i.e., the required resources of storage and computing power can be increased or decreased based on customers' needs. Elasticity implies being able to scale up or down resources assigned to services based on the current demand. Scaling up and down of a tenant's resources gives the opportunity to other tenants to use the tenant's previously assigned resources. This may lead to confidentiality issues. Moreover, elasticity contains a service placement engine that maintains a list of the available resources from the provider's offered resources pool. This list is used to allocate resources to services. Such placement engines should incorporate cloud customers' security and legal requirements such as competitors services should be avoided being placed on the same server, data location should be within the tenants' country boundaries. Placement engines may include a migration strategy where services are migrated from one physical host to another or from cloud to another in order to meet demands and efficient utilization of the resources. This migration strategy should take into account the same security constraints. Furthermore, security requirements defined by customers should be migrated with the service and initiate a process to enforce security requirements on the new environment, as defined by cloud customers, and updates the current cloud security model.

C. Multiple Stakeholders

In a cloud computing model there are different stakeholders involved: cloud provider (an entity that delivers infrastructures to the cloud customers), service provider (an entity that uses the cloud infrastructure to deliver applications/services to end users), and customer (an entity that uses services hosted on the cloud infrastructure). Each stakeholder has their own security management systems/processes and their own expectations (requirements)and capabilities (delivered) from/to other stakeholders. This leads to the following issues.

(i) Each stakeholder has their own security management processes used to define their assets, expected risks and their impacts, and how to mitigate such risks;
(ii) Providers and customers need to negotiate and agree upon the applied security properties.
(iii) With regard to the multi-tenant environment, the protection requirements for each tenant might differ, which can make a multi-tenant cloud a single point of compromise. A set of security requirements defined on a service by different tenants that may conflict with each other. So security configurations of each service should be maintained and enforced on the service instances level and at runtime taking into account the possibility of changing requirements based on current customers' needs to mitigate new risks;
(iv). In addition, each tenant could have different trust relations with the provider—and some tenants could actually be malicious attackers themselves— thus generating complex trust issues.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

D. Third-Party Control

The major security challenge is the third-party issue, that is, the owner of the data has no control on their data processing.

A related concern is proper governance of cloud related activity. Just as in traditional IT outsourcing, using cloud services requires the customer to give up control over his IT infrastructure. To make customers take this step easier, cloud providers should make the management and maintenance of cloud services more transparent and auditable by the customers. This should include recording logs and complete administrative sessions affecting the part of the cloud infrastructure used by the customer - and if requested by the customer making these accessible.

On the other side, cloud providers are not able to deliver efficient and effective security controls because they are not aware of the hosted services' architectures. A key issue for cloud computing is that aspects of traditional infrastructure security move beyond an organization's control and into the cloud. This will lead to fundamental changes in the number and roles of security stakeholders as enterprises turn over control of security infrastructure and processes to outside contractors. Trust relationships between various cloud stakeholders (users, corporations, networks, service providers, etc.) need careful consideration as public cloud computing evolves to manage sensitive enterprise data.

Third-Party Control is probably the prime cause of concerning the cloud. Transparency of what security is enforced, what risks exist, and what breaches occur on the cloud platform and the hosted services must exist between cloud providers and customers. This is what is called "trust-but-verify" , where cloud customers should trust in their providers while cloud providers should deliver tools to help customers to verify and monitor security enforcements.

III. CLOUD SECURITY

A. Data Storage Security

The cloud has different architecture based on the services they provided. In cloud computing, customers store their data in the cloud and no longer possess the data locally. Thus correctness and availability of the data file being stored on the cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption. From the perspective of data security, this has always been an important aspect of quality of service.

Verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Secondly, cloud computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.

Distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. Methods of data storage protection, such as redaction, truncations, obfuscation, and other, should be viewed with great concern. The data storage security pattern in cloud is the third part services within the cloud, lead to establishment of necessary trust level and provide solution to security services. The data is stored in a centralized location called cloud storage server, having a large size of data storage. Its processing is somewhere on servers, so the client has totrust the provider on availability as well as data security.

B. Data Transmission Security

Providing secure and efficient transmission of data is an important component of cloud computing and forms the foundation for information management and other operations

Some of the threat events compromising data transmission security are given as follows:

• *Cross site Scripting (XSS):* script executes in victims browsers to hijack user sessions, deface web sites, and introduce worms etc.

• *Injection Flaws:* the data sent by the users to a web application is not properly validated, which can manipulate a query on the server.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

• *Malicious File Execution:* XML or any other framework which accepts a file from the user is vulnerable to this attack, as the file can contain a malicious script.
• *XML corrupt:* XML traffic between the server and the browser is poisoned and corrupted.
• *Insecure Cryptographic Storage:* web applications which do not use cryptographic functions to protect data transmission lead to an attack.
• *Insecure Communication:* failing to encrypt network traffic leads to an attack.

C. Application Security

Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Security measures built into applications and a sound application security routine minimize likelihood that hackers will be able to manipulate applications and access, steal, modify, or delete sensitive data. Security is becoming an increasingly important concern during development, as applications become more frequently accessible over networks and are, as a result, vulnerable to a wide variety of threats.
SaaS is the software developed over the internet to run behind a firewall in local area network or personal computer.
Some of the current application security threats are:
Injection flaw like SQL, Cross-site scripting, Broken authentication, Insecure direct object reference, Cross-site request forgery, Security miss configuration, Insecure cryptographic storage, Failure to restrict URL access, Insufficient transport layer protection and invalidated redirects and forwards. The security requirements at the application level are summarized as follows:
• Privacy in multitenant environment
• Data protection from exposure (remnants)
• Access control
• Communication protection
• Software security
• Service availability

D. Security on Cloud Integrity

When running an application on cloud system, requires configuring a suitable backup routine so that it is safe in the event of a data-loss incident. It does not matter if this is a corrupt entry in a database file, deletion of user data or even amore disastrous data loss. Usually, the data requires to backup to portable media on a regular basis. Cloud system is responsible for determining and eventually instantiating a free-to-use instance of requested service implementation type on request of any user. Then, the address for accessing that new instance is to be communicated back to the requesting user.

Generally, this task requires some metadata on the service implementation modules, at least for identification purposes. Most of these metadata descriptions are usually required by any user prior to service invocation in order to determine the appropriateness of a service for a specific purpose. Thus, these metadata should be stored outside of the cloud system, resulting in a necessity to maintain the correct association of metadata and service implementation instances

E. Security related to Third-Party

In cryptography, a Trusted Third Party (TTP) is an entity which facilitates secure interactions between two parties. The scope of a TTP within the cloud is to provide end-to-end security services, which are scalable, based on standards. The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. Introducing a Trusted Third-party can specifically address loss of traditional security boundary by producing trusted security domains. A Trusted Third Party is an impartial organization delivering business confidence, through commercial and technical security features, to an electronic transaction. It supplies technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means.
The data and applications held by a third party are complex; there is also a potential lack of control and transparency when a third party holds the data. Some of the security requirements on third part are as follows:
• Low and High level confidentiality,

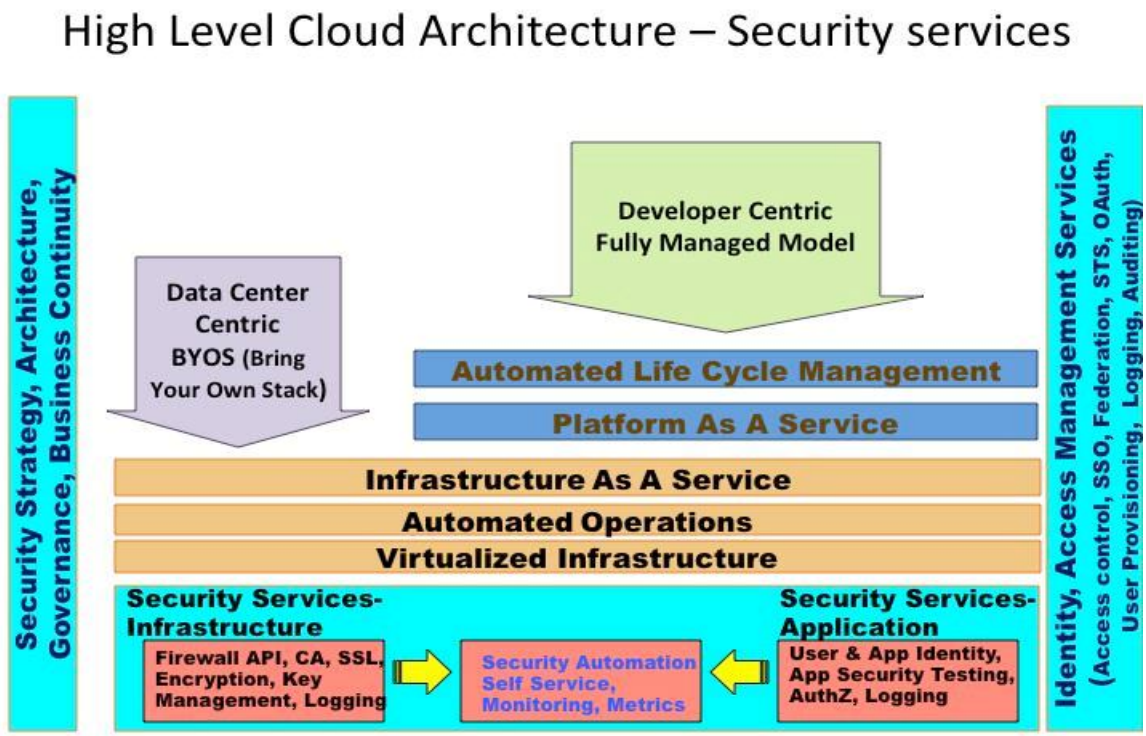
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

• Server and Client Authentication,
• Creation of Security Domain,
• Cryptographic Separation of Data, and
• Certificate-Based Authorization.



IV. CONCLUSION

The focus is on security issues in cloud computing. It is a vital to take security and privacy into account when designing and using cloud computing services. We discussed security challenges such as data storage security, data transmission security, application security, security on cloud integrity and security related to third-part resources. To identify high risk threat on the cloud security, a probability of threat is also derived. We conclude that to enhance the revolutionary of cloud computing in the Internet, it is essential to strengthen the security capabilities.

REFERENCES

[1] S. Ramgovind, MM. Eloff and E.Smith, "The Management of Securityin Cloud Computing," Information Security for South Africa (ISSA),IEEE, 2010.
[2] D. Zissis, D. Lekkas, ''Addressing cloud computing security issues,''Future Generation Computer Systems, 1--10, 2010.
[3] Y. Chen, V. Paxson, RH.Katz, "Whats new about cloud computingsecurity," Tech.Rep.UCB/EECS-2010-5, EECS Department, Universityof California, Berkeley, 2010.
[4] J.-S. Pan, S.-M. Chen, N.T. Nguyen (Eds.), "On cloud Computing Security Issues," ACIIDS 2012, Part II, LNAI 7197, pp. 560–569, 2012.
[5] F.Sabahi, "Cloud Computing Security Threats and Responses,"International Conference on Communication Software and Networks (ICCSN) , IEEE, 2011.
[6] Cloud Security Alliance, Security guidance for critical areas of focus incloud computing, V2.1, 2009.
[7] L. M. Kaufman, Data security in the world of cloud computing, IEEESecurity & Privacy, vol. 7, no. 4, 2009.
[6] S. Subashini, V. Kavitha, A survey on security issues in service deliverymodels of cloud computing, J. of Network and Computer Applications, vol. 34, no. 1, 2011.