A Study of Security Threats and Issues in Cloud Computing

Nidhi Grover*

Abstract

Cloud computing is an emerging technology gaining popularity in IT industry. In a cloud computing environment, the entire data is distributed over a set of networked resources so as data is accessible through virtual machines. Cloud computing offers potential advantages and provides many enterprise applications. With different cloud deployment models available data are migrating from public to private or hybrid cloud. There are various concerns that need to be addressed with respect to security and privacy in a cloud computing environment. In this paper we have analyzed various security risks and threats in cloud computing environment. The paper also presents various schemes and approaches available to mitigate the security challenges and ensure data security, confidentiality, privacy and availability in cloud environment.

Keywords: Reference architecture, Software as a Service, Platform as a Service, Infrastructure as a Service, RSA, AES, DES

Introduction

The definition of cloud computing as proposed by the US National Institute for Standards and Technology (NIST) in 2009 is as follows: "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" [15]. The fundamental behind cloud computing is to use remote services over a network using various resources. It is meant to maximize computing capability while minimizing the hardware requirements at the user end. Cloud computing deals with network-based services seem to be provided by real server hardware but in reality are served up by virtual hardware with software running on one or more real machines. Virtual servers exist conceptually and not physically so they can be moved around and scaled up just as a cloud, without affecting the user at the other end. In essence, cloud aims to consolidate the economic utility model with the evolutionary development of many existing approaches including distributed applications, services and information infrastructures consisting of pools of computers, networks, and storage resources [2]. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services [11]. The flexibility of cloud combined with the potential of a "pay-per-use" model makes it an attractive solution to the enterprises [9]. The essential characteristics of cloud computing that differentiates it from other computing paradigms are as follows [5, 7, 3]:

1. **On-demand self-service:** NIST has identified on-demand self-service as a chief characteristic of cloud environment. With this feature the resource capacity of a cloud infrastructure appears to be infinite to the user. Users can dynamically provision computing resources like server time and network storage as required without human intervention.
2. **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms

Nidhi Grover*
IITM, GGSIPU

(e.g., mobile phones, laptops, and personal digital assistants (PDAs)).

3. **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with dynamically assigned physical and virtual resources. In general the subscriber has no control or knowledge over the exact location of the provided resources but may be able to specify location at the country, state, and datacenter level of abstraction. Some such resources are storage and memory, processing, virtual machines and network bandwidth.
4. **Rapid elasticity:** Capabilities can be rapidly and automatically provisioned to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
5. **Measured Service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be examined, reported and controlled by providing transparency for both the provider and consumer of the utilized service.
6. **Scalability of infrastructure:** With this feature new nodes and physical servers with little modifications to infrastructure can be added or dropped from the network. Cloud architecture can scale horizontally or vertically as per demand.
7. **Location independence:** Location independence exists as the customer generally has no control or knowledge over the exact location of the resources but may specify location at a higher level of abstraction (e.g., country, state, or datacenter).
8. **Reliability:** Reliability may improve through the use of multiple redundant sites that make cloud computing suitable for business continuity and disaster recovery.
9. **Sustainability:** Sustainability comes about through better resource utilization, enhanced security and more efficient systems.

Cloud Reference Architecture

The cloud reference architecture as shown in figure-1 [17], describes the important security-relevant cloud components and also provides an abstract overview of cloud computing environment for security issue analysis.

The services provided by cloud computing environment can be classified on the basis of the capabilities and resources provided and the service model of providers: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The details are as follows:

1. **Software as a Service (SaaS):** In SaaS model applications are hosted and delivered online via a web browser offering traditional desktop functionality [17]. In SaaS model a software provider licenses a software application to be used and purchased on demand. Applications can be accessed through networks from various clients (web browser, mobile phone, etc.) by application users [6].
2. **Platform as a Service (PaaS):** In PaaS model the cloud provides the software platform for systems (as opposed to just software) [13]. PaaS differs from SaaS as it offers a development platform for both completed and underway cloud applications while SaaS hosts completed cloud applications only.
3. **Infrastructure as a Service (IaaS):** In IaaS model a set of virtualised computing resources, such as storage and computing capacity, are hosted in the cloud; customers deploy and run their own software stacks to obtain services [13]. It delivers computer infrastructure (typically a platform virtualization as environment) as a service, along with raw storage and networking. Rather than purchasing servers, soft wares, data-center space or network equipment clients

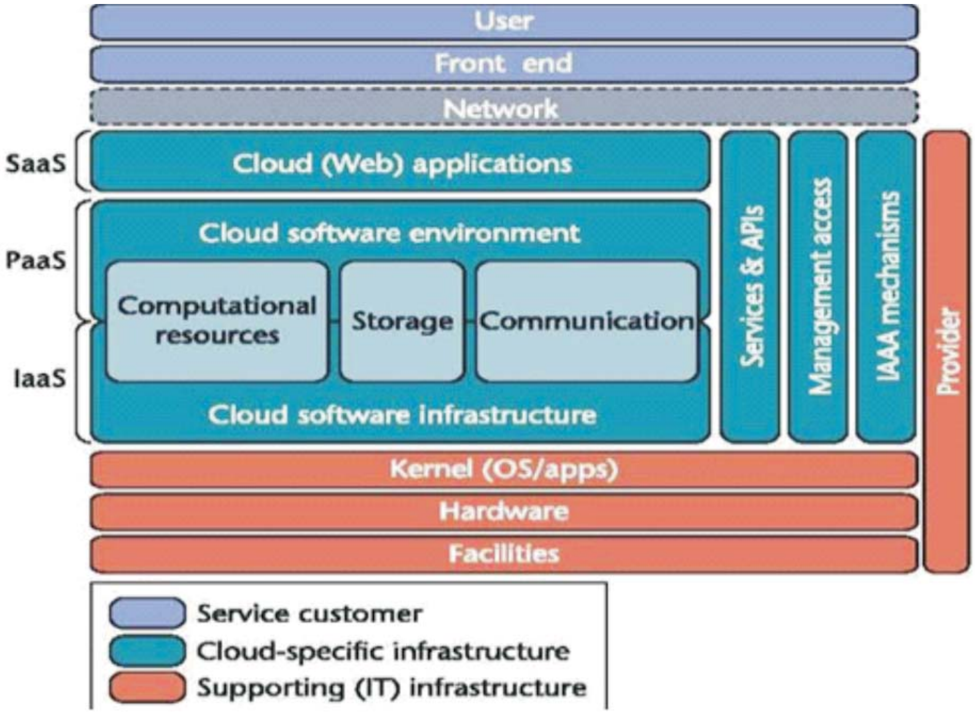

Fig. 1: Cloud Reference Architecture [17]

instead buy those resources as a fully outsourced service [4].

4. **Hardware as a Service (HaaS):** In HaaS model the cloud provides access to dedicated firmware via the Internet [13].

Deployment Models in Cloud Architecture

There are four deployment models that have been identified for cloud architecture solutions as described below [5, 16]:

a. Private cloud: Here the cloud infrastructure is operated only for a private organization. It may be managed by the organization or a third party and may exist on premise or off premise.

b. Community cloud: In this cloud deployment model the infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It can be managed by the organizations or a third party and may exist on premise or off premise.

c. Public cloud: Here the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

d. Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Security Issues and Threats

Cloud Computing is the key powerhouse in many companies that are shifting their data to the cloud environment. With continuously rising number of users looking for the services of cloud computing, the big deal is the protection of their data in the cloud. Providers such as Google, Microsoft, and Amazon have the existing infrastructure to deflect and survive cyber-attacks, but not every cloud has such capability [13]. Thus, ensuring data security and privacy in cloud computing is very important considering its critical nature and the amount and complexity of data that it carries. By their architecture's inherent nature, clouds offer the opportunity for simultaneous attacks to numerous websites, and without proper security, hundreds of websites could be compromised through a single malicious activity [13]. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services [14]. Various issues related to the security of information in cloud environment are as follows:

1. **Privacy and Confidentiality:** When client hosts data to the cloud it is important to ensure that access to that data will be limited to the authorized user access only. Unauthorized access to sensitive user data by cloud personnel is an important risk that may pose a potential threat to cloud data [14]. In order to ensure privacy for sensitive information in the cloud requires specific steps to be taken as discussed below to protect cloud data from unauthorized access [16] :

   a) Understand cloud by realizing how the cloud's structure affects the security of data sent into it by having an in-depth knowledge of how cloud computing transmits and handles data.

   b) Ensure Transparency by guaranteeing that the cloud provider supplies detailed information on its security architecture and is ready to accept regular security audit that should be done by an independent body or federal agency.

   c) Strengthen Internal Security by ensuring that the cloud provider follows strong internal security practices and user access controls such as firewalls.

   d) Legal Implications should be known to understand how the laws and regulations may affect what user sends into the cloud.

   e) Constant monitoring of development or changes in the cloud technologies that may affect data security.

2. **Data integrity:** In the cloud system there should be some means to preserve information integrity i.e., not lost or modified by unauthorized users. Since data is the base for almost all cloud computing services, such as Data as a Service, Software as a Service, Platform as a Service, preserving data integrity is a necessary task [17]. The cloud provider should let the client know about data being hosted on the cloud, its origin and the necessary integrity mechanisms taken.

3. **Data location and Relocation:** Due to data mobility provided by cloud environment, consumers do not always have the knowledge about the location of their data. In case when an enterprise has some sensitive data kept on a storage device in the cloud, they may want to know the data location and specify a preferred location. This requires a contractual agreement between the Cloud provider and the consumer to make sure that data should stay in a particular location or reside on a given known server [14]. The cloud providers must ensure the data security and follow robust authentication techniques. Second issue is the data movement as data is initially stored at an appropriate location but is often moved from one place to another because cloud providers enter into contracts with each other to share and use resources.

4. **Data Availability:** The main aim of availability for cloud computing systems is to ensure its users can use them at any time, at any place. Customer data is normally stored in different locations or in different Clouds systems. The cloud system must be scalable for any number of users and for this two approaches namely, hardening and redundancy, are used to ensure the availability of the cloud system and applications hosted on it [17].

5. **Audit:** Audit adds an additional layer in the virtualized application environment hosted on

the virtual machine to enable to watch and keep track of all the activities happening in the cloud system. Auditing is difficult because for auditing purpose sufficient transparency in the cloud provider operations is required. This transparency is achieved through manual audits and documentation. The real challenge lies in conducting an on-site audit in a dynamic computing environment distributed all over the globe [11].

6. **Online Data Storage, Backup and Recovery:** Data storage online is becoming popular now-a-days because it allows enterprises to maintain huge volumes of data without setting up the required architecture. The backup and recovery procedures of a cloud service should be effective and robust since copies of data are stored and maintained in varied geographical locations. Thus, cloud services may serve as an offsite backup storage for an organization's data center instead of tape-based offsite storage [19]. At the same time the amount of data involved and network performance issues may hinder the restoration mechanism.

7. **User interface attacks:** A Web browser that provides a user interface for accessing Web applications on network is also an important security factor. For instance: An attacker may use fake HTTPS lock icons to fool the user pretending that he is visiting a real website instead of a fake one [8].

Security Attackers in Cloud Environment

Each of the threats hindering the efficiency of cloud computing service delivery models are done by the attackers that can be divided into two groups as [11, 10]:

a. **Malicious Inside attacker:** An internal attacker is the one who has the following characteristics:

   - ➢ Is internal to the organization i.e. employed by cloud service provider, customer or other supporting third party provider supporting cloud service operations.
   - ➢ Has authorized access to customer data, cloud services in use, infrastructure supported and other cloud applications.
   - ➢ May be using on hand privileges to achieve further access beyond present privileges.
   - ➢ May be supporting third parties in executing attacks to breach confidentiality, integrity and availability of information within the cloud service.

b. **External attacker:** An external attacker is the one with the following characteristics:

   - ➢ Is not employed by the cloud service provider, customer or other third party provider i.e. he is not internal to the organization.
   - ➢ Does not have authorized access to customer data, cloud services, infrastructure supported and applications
   - ➢ Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization
   - ➢ He propagates attacks against the confidentiality, integrity and availability of information to gain further access.

In the context of the cloud environment, attackers can be categorized into four types as described below [18]:

c. **Random Attackers**- They are the most common type of attackers using simple tools and techniques. They mainly attack by randomly scanning the Internet to find out vulnerable components and deploy common tools and techniques that can be detected easily.

d. **Weak Attackers** - These are the semi-skilled attackers who target specific servers or cloud providers by customizing freely available tools or specific targets. Since they try to customize their attacks and use available tools so their methods are more advanced.

e. **Strong Attackers** - They are the well organized skilled groups of attackers with necessary finance and are interested in targeting particular applications and users of the cloud.

f. **Substantial Attackers** - They are the most motivated and strong attackers who are not easily detected by the organizations they attack or even by the investigative organizations specializing in eCrime or cyber security.

Security Issues in Public Cloud

In a public cloud there is a shared platform among many existing customers with infrastructure security provided entirely by the service provider. The key security issues in a public cloud are discussed as follows [16]:

a. Data must be protected during the various stages of its life cycle namely- creation, sharing, processing and archiving to satisfy the basic security requirements of confidentiality, integrity and availability. However, this is a very challenging task in a public cloud where we have no control over the service provider's security practices.

b. Since in a public cloud multiple tenants share the same infrastructure so there is a high probability of data leakage between these tenants. Care must be taken while choosing the service provider who can provide security against data leakage.

c. If Cloud Service Provider uses a third party provider to support cloud services then it is necessary to ensure service level agreements between them and necessary contingency plans in case of third party system breakdown.

d. Security requirements such as what level of encryption data should undergo while it is sent over the internet and what are the consequences for the service provider if he fails to provide secure transmission.

Security Issues in a Private Cloud

In a private cloud model the customer has total control over the network and the system provides the flexibility to the customer to implement any security practice. Though security architecture is more reliable in a private cloud still there are certain issues and risks that are needed to be taken care of [16, 10]:

1) Virtualization techniques are very popular in private clouds and so in such a scenario, risks to the hypervisor should be carefully analyzed. There have been cases when a guest operating system has been able to run processes on other guest VMs or host. In order to prevent this it should be ensured that they only communicate with the systems which they are supposed to and for this proper authentication and encryption techniques such as IP level Security should be implemented.

2) The host operating system should be free from any kind of malware threat and constantly monitored to avoid any such risk. Dedicated physical interfaces should be available for the guest virtual machines to be able to communicate with the host operating system and not directly.

3) Users are provided with an option to manage portions of the cloud and access to the infrastructure is provided through a web interface. There are two ways of implementing a web-interface, either by writing a whole application stack or by using a standard applicative stack, to develop the web interface using common languages such as Java, PHP, Python etc.

4) Efficient security measure should be taken to prevent attacks from internal attackers.

The hybrid cloud model combines features of both public and private cloud models and therefore the security issues discussed with respect to both are applicable in case of hybrid cloud.

Security Schemes in Cloud Computing

Several security schemes have been proposed to ensure security and data protection in cloud architecture:

1. **Data Security Model:** User's data can be made secure in a cloud system by using encryption techniques. The major task is to decide which encryption algorithm may be used to encrypt user's data stored in cloud. Several popular algorithms like RSA (Rivest-Shamir-Adleman) [14], Data Encryption Standard (DES) [12], Advanced Encryption Standard (AES) [1] etc. can be used to encrypt user data in cloud architecture.

2. **Authentication and Identity Management:** User-centric Identity Management has become important for handling private and significant identity attributes. In this approach, the user is identified with the help of certain identifiers and attributes that define a user [9]. This approach allows users to manage their digital identities and reduces the complexity of Identity Management tasks. Since users can access the cloud from different places they must be able to export their digital identities and securely transfer them to various computers [9]. The approach uses active bundles scheme in which predicates are compared over encrypted data and multiparty computing and removes the need for trusted third party for the verification of user identity thus freeing TTP for other purposes such as decryption [16].

3. **Access Control Needs:** The role-based access control (RBAC) method is a popular access control model because it is simple, flexible in capturing dynamic requirements, and supports the principle of least privilege and efficient privilege management [9]. Several RBAC extensions—such as credential-based RBAC, generalized temporal RBAC (GTRBAC), and location-based RBAC models— offer necessary modeling constructs and capabilities to capture context-based access requirements. The clouds service providers do not know in advance about their users, so it is difficult to assign users directly to roles in access control policies. Thus, using credential or attribute based policies may help.

4. **Secure Interoperation:** Recent researches have focused on multi domain access control policies and integration issues adopted to build a complete policy management framework in clouds. A centralized approach follows a global policy and is appropriate for a cloud application that consists of various services with different requirements. Specification frameworks are required to ensure that the cross-domain accesses are properly specified, verified, and enforced. Some solutions for achieving this are Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML), and Web services standards [9].

5. **Secure-Service Provisioning and Composition:** Cloud service providers use virtualization techniques separating application services from infrastructure for optimizing resource utilization. In the cloud, service providers and service integrators need to collaborate to provide newly composed services to customers. Secure virtualization uses the idea of an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware [16]. The cloud components behavior can be examined by logging and periodic checking of executable system files.

6. **Trust Management Framework:** To enable policy integration among various domains in cloud environments, a trust-based framework facilitating automated trust-based policy integration is required [9]. The approach separates domains for providers and users, each given a special trust agent and using different trust strategies for service providers and customers. Time and transaction are important factors that are considered for trust assignment. The approach helps the customers to avoid malicious suppliers and also enables the cloud providers to avoid serving malicious users.

7. **Data-Centric Security and Privacy:** Although data in the cloud resides in a shared environment

still the data owner should have complete control over who has the right to use the data i.e. who has access permission and what he actually does after obtaining access [9]. To achieve this data control in the cloud a heterogeneous data-centric security approach is required. In this approach, documents must be self-describing regardless of their environments. Cryptographic approaches and usage policy rules may also be considered.

8. **Managing Semantic Heterogeneity:** A key aspect of complex cloud computing environments is semantic heterogeneity among policies. Although XML has been adopted as the preferred language for information sharing but it is inadequate for describing information semantics. RDF provides a facility for describing semantics by supporting element attributes and properties description. Use of ontology is the most promising approach to addressing the semantic heterogeneity issue. For ontology development, we can use both XML Schema and Resource Description Framework Schema (RDFS) to accommodate the domain specific concepts.

Conclusions

The cloud techniques are gaining popularity and IT market is expected to take a major shift towards the cloud in the coming times. Although cloud computing has emerged as a revolutionary technology but still it is prone to various security threats from different attackers. In order to ensure the Cloud security these security threats need to be prevented and handled appropriately. Data residing in the cloud is prone to a number of security risks such as confidentiality breach and integrity loss of data. In this paper we have discussed various security issues associated with cloud architecture. We also discussed the solutions available to ensure cloud data security such as data encryption, role based authorization and user identification, secure virtualization, trust management framework etc. In future, extensive work needs to be done to ensure data security in cloud computing such as efficient use of third party auditors, implementing data encryption algorithms and their combinations to encrypt data, exploring new security techniques and upgrading older techniques to provide security in cloud architecture.

References

1. Abha Sachdev, Mohit Bhansali, “Enhancing Cloud Computing Security using AES Algorithm”, International Journal of Computer Applications (0975 - 8887) Volume 67– No.9, April 2013
2. Amani S. Ibrahim, James Hamlyn-Harris and John Grundy, “Emerging Security Challenges of Cloud Virtual Infrastructure”, In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 Nov 2010.
3. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011.
4. CSA Security Guidance For Critical areas of focus in Cloud Computing v3.0 available at: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
5. Dimitrios Zissis and Dimitrios Lekkas, “Addressing cloud computing security issues”, Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece
6. Eeva Savolainen, “Cloud Service Models Seminar – Cloud Computing and Web Services”, Helsinki 10.2.1012 UNIVERSITY OF HELSINKI Department of Computer Science.
7. G. Reese, “Cloud Application Architectures: Building Applications and Infrastructure in the Cloud”, Theory in practice, O’Reilly Media, 2009.

8. Harmeet Kaur, Comparison Of Data Security In Grid And Cloud Computing, IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

9. Hassan Takabi and James B.D. Joshi, “Security and Privacy Challenges in Cloud Computing Environments”, University of Pittsburgh Gail-Joon Ahn Arizona State University , copublished by the ieee computer and reliability societies, november/december 2010 IEEE.

10. Information Security Briefing 01/2010 Cloud Computing ,Center for the protection of National Infrastructure, March 2010

11. Jaydip Sen, “Security and Privacy Issues in Cloud Computing”, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

12. Mandeep Kaur, Manish Mahajan, “CSA Security Guidance For Critical areas of focus in Cloud Computing”, v3.0 available at: Using encryption Algorithms to enhance the Data Security in Cloud Computing Department of Information and Technology Chandigarh Engineering College, Landran Mohali, India

13. Neil Robinson, Lorenzo Valeri, Jonathan Cave & Tony Starkey (RAND Europe) Hans Graux (time.lex) Sadie Creese & Paul Hopkins (University of Warwick), “The Cloud: Understanding the Security, Privacy and Trust Challenges”, Final Report TR-933-EC 30 November 2010 Prepared for Unit F.5, Directorate-General Information Society and Media, European Commission

14. Parsi Kalpana, Sudha Singaraju , “Data Security in Cloud Computing using RSA Algorithm”, International Journal of Research in Computer and Communication technology (IJRCCT), ISSN 2278-5841, Vol 1, Issue 4, September 2012.

15. Peter Mell Timothy Grance, “The NIST Definition of Cloud Computing”, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145

16. Rohit Bhadauria, Sugata Sanyal, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques”.

17. Santosh Kumar and R. H. Goudar, “Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey”, International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012

18. Security in Private Database Clouds, Oracle White paper, July 2012

19. Wayne Jansen, Timothy Grance, Draft NIST Special Publication Guidelines on Security and Privacy in Public Cloud Computing, January 2011