Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# A Review of Services on Security in Cloud Computing

**Amar Nath Bhargava, Asst. Prof Neha Bhardwaj**
Department Cyber Security, MITS Gwalior,
Madhya Pradesh, India

***Abstract— Cloud computing is the process of delivering the resources through the internet. In cloud computing resources can be utilized with efficient cost. When data is stored in the cloud there should be standards and procedures to secure the information. Security in the cloud is a major challenge as many threats and risk are associated with this computing model. This paper deals with the issues in cloud deployment models like public, private, community, hybrid clouds. Cloud computing provides mainly 3 cloud service models where each model has their own security issues.***

***Keywords—Cloud Computing, Security, Saas, Paas, Iaas.***

## I. INTRODUCTION

A new computing prototype cloud computing is a new delivery model which has grown rapidly in recent years. According to NIST, "Cloud computing is generally an enabling Convenient model, on-demand network use of a shared pool of configurable computing Assets that may be swiftly provisioned and launched with minimal administrative effort or seller interplay". The cloud computing mannequin composed with five principal characteristics [1]. The cloud computing accessories include front end, back end and communication. The front end is a computer interface involves client's network, through web browser person can access the applications. The communication channel acts because the mediator between front end and back end. The again back end is cloud itself consists of data storage contraptions, servers [2]. Knowledge and applications are the belongings to install in the cloud. Determine the suitable deployment model and right cloud service model to preserve the information [3]. Privacy and security is a major challenge [4].

Nonprofit institution like Cloud Security Alliances (CSA) is a solution provider. CSA speaks about on quality approach and future approach for securing cloud [5].

This paper is organized as follows: Section 2 illustrates about cloud computing security. Section 3 illustrates about security issues posed by Deployment models. Section 4 illustrates about security issues posed by cloud service models. Section 5 literature survey and last conclude the paper.

## II. CLOUD SECURITY

When the sensitive data is stored in cloud the main concerns are how it is secured, what are the rules and procedures to protect the data. Consumer when migrating to the cloud they trust the third party vender who ensures the requirements like confidentiality, authenticity and integrity of information [6].

### *A. Confidentiality:*

The capability of accessing the confidential data by the authorized users refers to confidentiality [7]. Unauthorized access loads of data privacy risks and leakage of data.

### *B. Authentication:*

Authentication is identifying the credentials of the individual and verifying whether they are legitimate users or not [8].

### *C. Integrity:*

For the period of the information transmission capacity to the defend knowledge from no longer being destroyed or manipulated by unauthorized persons refers to integrity [6].

## III. DEPLOYMENT MODEL

In a cloud environment there are four deployment models based on NIST [1].

### *A. Public cloud*

This cloud infrastructure provides access to public [7]. The adopting public cloud environment has many risks as it is used by everyone and there are more security considerations.

*1) Multi tenancy:*

Sharing of the same resources by many tenants who are not related to each other leads to multi tenancy. Multi tenancy has its own advantages and a number of protection threats. Both the cloud consumer and cloud infrastructure endure with privacy vulnerabilities [9]. Within the multitenant environment, there are advantage privacy dangers, facet-channel attacks to cloud user's knowledge.

 

*2) Malicious insiders:*

Malicious insider is an attacker who has entry to the data in cloud knowledge center, could also be developer who develops code which is exploited by way of outsiders, may inject virus to the system etc.

*3) Access Control:*

Access Control is a strategy allows or restricts the user to access the system. Attempting to access the data by the unauthorized users can also be identified by this mechanism. In this process various steps are involved like identification, authentication and authorization [10]. User needs to know how many can view your data? How many are having privileged access to the data? Can private keys be shared among multiple tenants? For privileged users what type of authentication is required? All the above information needs to be known to the user for the assurance of data protection by the cloud service provider.

*4) Virtual Exploits:*

Cloud customer does now not have the capabilities about what type of virtualization application the vender is utilized. Purchaser needs to query about what version the vender is making use of? Patches in the virtualization are done by way of whom and when? Who is monitoring, logging the every virtualization host and guest? There are numerous virtual exploits such as visitor to host, visitor to guest, server host only, host to the server, which are unknown chance models not known by using individuals.

### *B. Private cloud*

Because of many security issues in public cloud many firms migrate to private cloud deployment model [11]. This cloud infrastructure is efficiently owned by one organization [6]. Underlying hardware can have more control in a private cloud than in public cloud because of its multi tenancy environment, to meet the organization's functional need private cloud affords better customization of the infrastructure. But in private cloud there are some security considerations:

*1) Defining responsibilities*:

In this deployment model operational security changes from hands, i.e. from one group to another or the cloud vendor. So, who's liable for what need to be outlined. Extraordinary policies and set of stakes are managed by means of one-of-a-kind departments, customers and domains. To avoid data leakage care must be taken when responsibility changes from the hands.

*2) Elastic and changing perimeters:*

The private cloud infrastructure is elastic, i.e. delivery of assets is carried on demand from a pool of resources. Scaling out happens when required and security desires to be maintained for the changing perimeters additionally [12].

*3) Ineffective device-specific controls:*

Virtual machines are not restricted to particular hardware. So there is not any device specified controls like conventional IT. Intelligent and adaptive security policies ought to be initiated based on physical hardware [12].

### *C. Community cloud*

For multiple organizations this cloud infrastructure functions with a set of shared cooperatives and domain specific concerns [6]. The cloud environment is managed by any third party vendors or hosted by the organizations [7]. Community cloud can be either on-site or off-site [13]. Community clouds are used in healthcare, public sector and media. Below techniques and processes are to be followed:

*1) Identity management:*

Identity management in community cloud involves in accessing the data by whom, when as well as where and how are monitored by service providers. Identifying management needs supervising, enforcement, and provisioning.

Auditing, accounting and forensics tools are required for supervising. In enforcement, access privileged is determined by the user and devices, according to the policy. [14].

*2) Data protection and Integrity:*

With high utilization and greater density the goal of cloud computing is to secure the data. Without affecting data integrity refined software need to be provided by a cloud vendor for hardware breakdown. It is highly critical in virtualization of network and storage resources [14].

*3) Data governance:*

Cloud providers who are responsible for stewards of the data in multitenant environment need mandatory certification and regulations. Around the data lifecycle from creation to disposition governance policies need to be established by cloud service providers. Related to data governance cloud service providers need to set up platforms and systems to support regulations [14].

### *D. Hybrid cloud*

This infrastructure combines two or more clouds [15]. By allowing intercommunication between the cloud models the hybrid cloud remains unique entities and bound together. In hybrid cloud due to separation of resources into multiple clouds the complexity of software and configuration increases while migrating resources of an enterprise. There are possible threats to the enterprise data.

*1) Lack of data redundancy:*

In hybrid cloud environment, lack of redundancy may become a security risk when copies of data are not distributed across data centers. There is a risk of data failure when running your application in single data center to another. Using multiple data centers from single cloud provider mitigates risks and save cost effectively.

 

*2) Security management:*

There are security requirements like identity management, authentication, and authorization for both public and private cloud [8].

*3) Compliance:*

In a hybrid cloud environment, maintaining and demonstrating compliance can be more difficult. In hybrid cloud ensure the moving data between private and public [16] is protected. Ensure prevention of data leakage from private cloud to less secured public cloud.

*4) Poorly Constructed SLAs:*

In service level agreement Public cloud can consistently meet expectations, but private cloud may not. Based on two clouds create SLAs on expectations of insignificant one, possibly private cloud. While integrating both clouds there may be potential risks that could disrupt service. If in private cloud the confidential and sensitive data are on –premise, then SLA should reflect the limits in public cloud.

.

## IV. CLOUD SERVICE DELIVERY MODEL

In cloud computing cloud service delivery models are in classified into three services [1].

Table I Services managed by cloud delivery models

| **Delivery models** | **Managed by users** | **Managed by cloud providers** |
|---|---|---|
| **Software as a service** | Nothing | Networking, storage, server HW, virtualization, servers, databases, security & integration, runtime applications |
| **Platform as a service** | Application | Networking, storage, server HW, virtualization, servers, databases, security & integration, runtime applications |
| **Infrastructure as a service** | Servers, databases, security, integration, runtime applications | Virtualization, server HW, storage, networking |

### *A. Software as a service*

In this SaaS the software is delivered to the customer as a service. From numerous client devices applications are accessible over the web browser. The underlying infrastructure network, server, storage, operating system is not managed or controlled by customer [6].

*1) Security issues in SaaS:*

SaaS is the dominant delivery model now days. There should be fine grained authorization techniques for access control and encryption techniques for data security [17]. The network layer is responsible for maintaining the network security, providing influential protection against packet sniffing, port scanning, Man-in-Middle attacks, IP spoofing. During the development process of SaaS the security assets considered are data access, data confidentiality, data integrity, availability, data breaches and data segregation [17].

- *Limitations to replicate the organization in the cloud:*

A cloud service provider must create thousands of mirror users on cloud if they potentially have thousands of employees. There is a duct on IT help desk assets and potential security threats when users have multiple passwords.

- *Protect the API Keys:*

Applying REST web services interface, numerous cloud services are accessed which is called as APIs. Organizations access the cloud providers using API keys. For example, if an organization is using a SaaS contribution, it will generally be granted by an API Keys. The security of these keys is very essential. If the keys were stolen then an attacker can acquire control over the confidential data.

- *Backup and recovery:*

A cloud service provider should keep typical backups by way of utilising snapshots and have rapid restoration systems when disaster occurs.

### *B. Platform as a service*

In this PaaS the cloud vender provides the platform to develop and deploy applications [6]. By using a PaaS development tool, user can install and build server environment and run an application which can reduce complexity and cost [18].

*1) Security issues in PaaS:*

PaaS security can be done in 2 ways Firstly security of the PaaS platform itself provided by cloud service provider and secondly security of the deployed customer application on PaaS platform.

- *Data location:*

The PaaS provides storage capacity for resultant output or files. The location of data cannot be on a particular host. It reduces the cost by giving development tools for software buildup. In this environment, performance is achieved through

 

duplication of data which provides high availability of data for users and developers. As the exact location is not known leads to security difficulties.

- *Privileged access:*

To fix a problem in the code developers uses built-in-debug. This enables access for a location and memory place and alters values to scan quite a lot of circumstances. This instrument presents privileged entry not just for builders, but in addition hackers. Programmers request full entry to work in a privileged environment although it is not critical.

- *Distributed systems:*

In a PaaS environment file systems are incredibly distributed. Hadoop disbursed file methods (HDFS) are most used for implementations. The Cloud provider owns the cluster of the namespaces/identify nodes independently managed with the aid of HDFS. Attackers give various inputs to default ports in order to cause failures or DOS (Denial of service) [18]. There may be potential attack vectors for other ports which are used for management and operations. Client is liable to verify the security requirements, but cloud service provider need to provide the necessary security.
Always Physical security, network security and underlying hardware are managed by the cloud service provider.

### *C. Infrastructure as a service*

In IaaS model the cloud service provider provides the storage, server and network resources [6]. A cloud service provider manages the cloud infrastructure and host environment. The customer has the capability to provision network, storage and can deploy and run operating systems and applications [18].

*1) Security issues in IaaS:*

Virtualization is a technique where pooled resources can be accessed in a cloud computing environment [19], [20]. Virtualization is the big security burden in IaaS. Security liabilities are there for both customer and cloud service provider, both have different aspects to control. Data, applications, operating system are controlled by customer [6]. A cloud service provider is responsible for virtualization security, physical security, environmental security [17].

*2) Containerization:*

The effective portability of applications is achieved by the Container. Operating system level virtualization is also known as Containerization. Instead of one instance (container), multiple isolated user space instances are allowed by the operating system kernel. Here, less security isolations is provided by containers than hardware virtualization. If containers provide more isolation it is better than a simple multiuser shared server. Fundamentally container based systems have much larger stack surface [21].
In virtual cloud infrastructure security risks can be divided into three categories [22]:
Hypervisor Attacks, Switch Attacks, Virtual Machine Attacks:

## V. LITERATURE REVIEW

Masky et al [23] introduced OCTAVE Allegro as a novel methodology for risk identification in the Cloud Environment. The biggest improvement of this method compared to others. Through different steps and worksheets, we captured all details of each risk and decided on how to mitigate them. The devised scheme is not specific for Cloud Computing. It can be applied to other systems as well. Possible improvements of this paper can be the consideration of more impact areas for OCTAVE Allegro to meet very large Cloud Computing Infrastructure.

Swati Paliwal et al. [24] proposed an Attribute Based Encryption (ABE) and verifiable data decryption method to provide data security in the cloud based system. They've been designed the information, decryption algorithm established on the user requested attributes of the outsourced encrypted knowledge. Probably the most primary efficiency drawbacks of this method is, cloud service providers have extra computational and storage overhead for verification of consumer attributes with the outsourced encrypted information.

Shiv Shakti et al. In [25] discussed the performance of six different symmetric key RSA data encryption algorithms in cloud computing atmosphere. They have proposed two separate cloud servers; one for knowledge server and different from key cloud server and the data encryption and decryption system on the client side. The major shortcoming of this technique is to maintain two separate servers for data security in the cloud, which creates a more storage and computation overheads.

Rewagad et al [26], have chosen to make use of a combo of authentication method and key exchange algorithm blended with an encryption algorithm. This mixture is referred to as "Three method mechanism" considering it ensures all the three defense scheme of authentication, knowledge safety and verification, whilst. Here proposed to utilize digital signature and Diffie Hellman key exchange blended with AES algorithm to the preserve data confidentiality saved in the cloud. Even though the important thing in transmission is hacked, the power of Diffie Hellman key alternate renders it useless, considering the fact that key in transit is of no need without a person's private key, which is constrained only to the respectable consumer. This devised framework of the three means mechanism makes it difficult for hackers to crack the security procedure, thereby protecting information stored in the cloud.

Singh et al [27], proposed cloud storage security model provides a highly secure cloud environment by introducing the three sections to store the user database on the security parameters namely authentication, confidentiality, integrity, availability, non repudiation, security, and privacy. It restricts unauthorized entities to get control of the user's data by implementing double authentication mechanisms. It also provides protection against various security breaches such as a brute force attack, masquerade attack, data tampering, and cryptanalysis of integrity key. It also enables the user to select the encryption techniques in hybrid section, according to the various factors associated with data such as cost, security etc.

 

Shahzad et al [28], presented features of cloud computing, three models of cloud service, and four models of cloud deployment. Research within the at ease cloud storage is compounds with the aid of the truth that users knowledge could also be kept in several places for either redundancy/ fault tolerance or in view that the service is provided by means of a series of service vendors.

Nath et al [29], represents a milestone for the day where cloud computing security issues can be listed in one comprehensive document together with its solutions. This paper identifies top security concerns of cloud computing, these concerns are Data loss, Governance and compliance, Trust, Virtualization vulnerabilities and various attacks. It also summarizes various countermeasures which can be adopted to overcome security issues. This study provides a pillar to the researcher and practitioner where they can stand and further classify issues and improve cloud-computing security.

Kaur et al [30], concentrated on security issues of cloud computing to overcome the data privacy issue. It explores the cloud security issues and problem faced by cloud service provider.

## VI. CONCLUSIONS

In this paper security concerns are discussed at each stage of cloud computing. Security as service model will lead the future as it provides instructions to organizations by classifying different types of security as services. Adoption of cloud computing has rapidly increased because of its efficiency of cost and flexibility. Customized security mechanisms need to be introduced to mitigate the risks and attacks.

## REFERENCES


[1] Meel, P. Et Grance, Timothy. The nist definition of cloud computing (draft).National Institute of Standards and Technology, Gaithersburg, 2011.

[2] Patil, Pradip. Cloud Security Issues. Journal of Information Engineering and Applications, 2015, vol. 5, no 1, p.31-34

[3] Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0

[4] SO, Kuyoro. "*Cloud computing security issues and challenges"* International Journal of Computer Networks, 2011,vol. 3, no 5.

[5] Cloud security alliance https://cloudsecurityalliance.org/(Accessed on: December 15, 2015)

[6] Balasubramanian, V. Et Mala T *"A Review On Various Data Security Issues In Cloud Computing Environment And Its Solutions"* ARPN Journal of Engineering and Applied Sciences. 2015, vol. 10, no. 2.

[7] ZISSIS, Dimitrios et LEKKAS, Dimitrios. "*Addressing cloud computing security issues"*. Future Generation computer systems, 2012, vol. 28, no 3, p. 583-592.

[8] Reddy, V. Krishna Et Reddy, L. S. S. Security architecture of cloud computing. International Journal of Engineering Science and Technology, 2011, vol. 3, no 9

[9] REN, Kui, WANG, Cong, et WANG, Qian *"Security challenges for the public cloud"* IEEE Internet Computing, 2012, no 1, p. 69-73.

[10] Khan, Abdul Raouf *"Access control in cloud computing environment"* ARPN Journal of Engineering and Applied Science, 2012, vol. 7, no 5, p. 613-615.

[11] SumitGoyal *"Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review"* I.J. Computer Network and Information Security, 2014, 3, 20-29 Published Online February 2014 in MECS (http://www.mecspress.org/) DOI: 10.5815/ijcnis.2014.03.03

[12] Subramanian Krishnan. Analyst & Researcher *"Private Clouds A whitepaper"* sponsored by Trend Micro Inc.

[13] Fernandes, Diogo AB, SOARES, Liliana FB, GOMES, João V., et al. *"Security issues in cloud environments: a survey"* International Journal of Information Security, 2014, vol. 13, no 2, p. 113-170.

[14] *Securing Government Private and Community Clouds (http://www.cisco.com/web/strategy/docs/gov/c45* 617006_aag.pdf)(Accessed on: December 15, 2015).

[15] Koushik Annapureddy. School of Science and Technology *"Security Challenges in Hybrid Cloud Infrastructures*" Aalto University, T-110.5290 Seminar on Network Security Fall 2010

[16] SEN Jaydip. Innovation Labs *"Security and Privacy Issues in Cloud Computing"* , Tata Consultancy Services Ltd., Kolkata, INDIA

[17] Subashini, Subashini Et Kavitha, V *"A survey on security issues in service delivery models of cloud computing"* Journal of network and computer applications, 2011, vol. 34, no 1, p. 1-11.

[18] Reddy, V. Krishna, Rao, B. Thirumala, et REDDY, L. S. S. *"Research issues in cloud computing*" Global Journal of Computer Science and Technology, 2011, vol. 11, no 11

[19] Kumar, Sarvesh, SINGH, Suraj Pal, SINGH, Ashwanee Kumar, et al.Virtualization "*The Great thing and Issues in Cloud Computing"* International journal of Current Engineering and Technology, 2013, vol. 3.

[20] SABAHI, Farzad. *"Secure Virtualization for Cloud Environment Using Hypervisor-based Technology"* Int. Journal of Machine Learning and Computing, 2012, vol. 2, no 1.

[21] Wheeler, David *"A. Cloud Security: Virtualization, Containers, and Related Issues"*.

[22] Kumar, A., Srinivasulu, C., Kumar, B. Sudeep, et al. *"Emphasis and emerging trends on virtualization of cloud infrastructure with security challenges"* International Journal of Computer Trends and technology (IJCTT), ISSN,2013, p. 2231-2803.

[23] Mackita Masky, Shin Soo Young, Tae Young Choe; *"A novel Risk Identification Framework for Cloud Computing Security"*. IEEE, 2015


 

[24] Swati Paliwal, Ravindra Gupta(2013 February ), *"A Review of Some Popular Encryption Techniques*" International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 2, ISSN: 2277 128X.

[25] ShivShakti etc(2013 January-Febuary). *"Encryption using different techniques: A Review"* international journal in Multidisciplinary and academic research (SSIJMAR) vol.2 No.1 -(ISSN 2278-5973).

[26] Mr. Prashant Rewagad, Ms.YogitaPawar; *"Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing"* International Conference on Communication Systems and Network Technologies, IEEE, 2013

[27] Ranjit Kaur Raminder Pal Singh; *"Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques* . IEEE, 2014.

[28] FarrukhShahzad*; "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions".* The 6th International Symposium on Applications of Ad hoc and Sensor Networks(AASNET'14), Elsevier

[29] Meena Kumari RajenderNath; *"Security Concerns and Countermeasures in Cloud Computing Paradigm".*Fifth International Conference on Advanced Computing & Communication Technologies, 2015.

[30] Randeep Kaur, JagroopKaur*;" Cloud Computing Security Issues and its Solution: A Review".* IEEE, 2015.

 