RESEARCH ARTICLE OPEN ACCESS

Cloud Computing: Security Concerns

Jitendra Nath Shrivastava [1], Uvaish Khan [2]
Professor [1], Computer Science and Engineering
Master of Computer Applications [2]
Invertis University
Bareilly (UP) - India

ABSTRACT
The current increased utilization of cloud services need advanced insights into necessary security requirements and its solutions. It is really tough to identify which kinds of necessities have been researched most and which are still–under- researched. The objective of this study was to provide a broad and structured overview of the types of security requirements researched in the area of in cloud computing and the proposed solutions to deal with these requirements. This study thus advise fellow researchers about security requirements in cloud computing and indicate to those types of security requirements that have attained much research effort and those that have been under-researched.

Keywords:- Cloud Computing, Security Issues, Saas, Paas, Iaas.

I. INTRODUCTION

National Institute for Standards and Technology (NIST) (Badger etal., 2011) defines the cloud computing as, "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".

Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Prime goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels. As for as service delivery, is concerned ,NIST has identified three basic types of cloud service offerings. These models are: *Software as a service* (SaaS), *Platform as a service* (PaaS) and *Infrastructure as a service* (IaaS).

These three individual models are often referred to as the "SPI MODEL"[1], where "SPI" refers to Software, Platform and Infrastructure (as a service) respectively (CSA Security Guidance, 2009). NIST has identified three basic types of cloud service offerings.

A. Software as a Service (SaaS)

In SaaS, a complete application is provided to the customer as a service on demand. A single instance of the service runs on the cloud and multiple end users are served. On the customers' side, there is no need to invest in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained. Currently, SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho etc.

B. Platform as a Service (PaaS)

In this model, a layer of software is encapsulated and offered as a service, upon which other higher levels of service are built. The customer has the freedom to build their own applications, which run on the provider's infrastructure. Although the customer does not manage or control the underlying infrastructure, network, servers, operating systems, or storage, but they control over the deployed applications. Some examples of PaaS are: Google's App Engine, Force.com, etc.

C. Infrastructure as a Service (IaaS)

Servers, storage systems, networking devices, data centre space etc. are pooled and made available to handle workloads. The capability provided to the customer is to rent processing, storage, networks, and other computing resources where the customer is able to deploy and run software. Some examples of IaaS are: Amazon, Go Grid, 3 Tera etc.

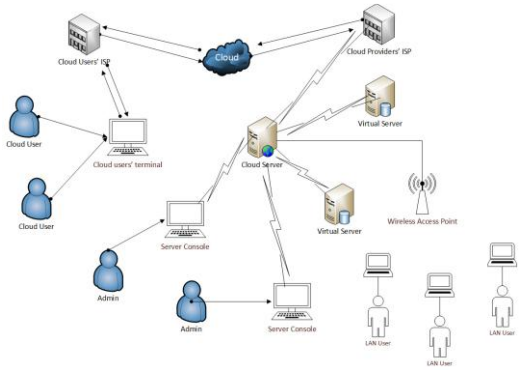

Figure 1: A Typical Cloud Architecture[1]

Figure 1 Shows a typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud computing architecture.

All the above three stages of cloud computing are severely prone to security breach.

II. CLOUD COMPUTING SECURITY ISSUES

There are several security issues for cloud computing. It encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. Data mining techniques may be applicable for malware detection.

As shown in Figure 2, there are six particular areas of the cloud computing environment where equipment and software require appropriate security attention (Trusted Computing Group's White Paper,2010). These six areas are: (1) security of data at rest, (2) security of data in transit, (3) authentication of users/applications/ processes, (4) robust separation between data belonging to different customers, (5) cloud legal and regulatory issues, and (6) incident response.

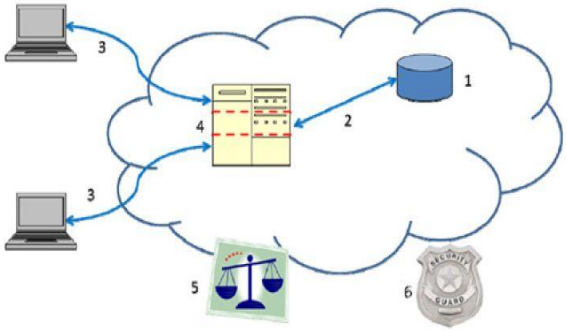

Fig 2: Areas of security concerns in cloud computing[5]

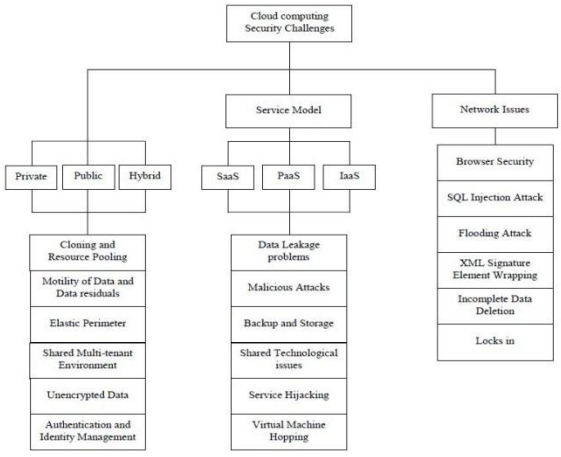

Fig 3: Classification of Security Challenge[2]

Figure 3 represents the hierarchy of the cloud computing, with security challenges. The Deployment model is classified as Private, Public and Hybrid Cloud. The security challenges with respect to network is also shown as for any internet based service, network is considered as the backbone for cloud computing.

The cloud service providers ensure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user. This leads to affects several customers who are sharing the infected cloud. There are four types of issues [3] raise while discussing security of a cloud.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues

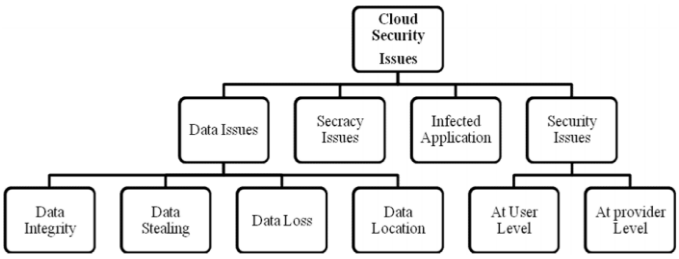

Fig 4: Cloud Security Issues[3]

1. Data Issues

Sensitive data in a cloud computing environment emerge as important issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data. Many cloud computing service consumer and provider accesses and modify data. At the same time, thus there is a need of some data integrity method in cloud computing. Secondly, data stealing is a one of serious problem in a cloud computing environment. Thirdly, Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Fourthly, data location is one of the issues what needs focus in a cloud computing environment. Physical location of data storage is important and crucial. It should be transparent to user and customer both. Vendor does not reveal where all the data's are stored.

2. Private Issues

Service provider must ensure that the customer personal information is well secured from other providers, customer and user. Cloud service provider should ensure who is accessing the data and who is maintaining to protect the customer's personal information.

3. Infected Application

Cloud service provider must have the complete access to the server with all rights of monitoring and maintenance of server. This will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

4. Security issues

Cloud computing security is considered on two levels. One is on provider level and another is on user level. Cloud provider should ensure that the server is well secured from all threats. Even though the cloud service provider has provided a good security layer for the customer and user, the user should ensure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action.

A cloud is good only when there is a good security provided by the service provide to the user.

III. CLOUD SECURITY THREATS

There are several types of security threats to which cloud is vulnerable. Following table provides an overview of the threats for cloud customers categorized according to the *confidentiality*, *integrity* and *availability* (CIA) security model and their relevance to each of the cloud service delivery model.

TABLE I
A LIST OF CLOUD SECURITY THREATS [5]

Threat	Description
Confidentiality	
Insider user threats: • Malicious cloud provider user • Malicious cloud customer user • Malicious third party user (Supporting either the cloud provider or customer organizations)	The threat of insiders accessing customer data held within the cloud is greater as each of the delivery models can introduce the need for multiple internal users: SaaS – cloud customer and provider administrators PaaS- application developers and test environment managers IaaS- third party platform consultants
External attacker threats: • Remote software attack of cloud infrastructure • Remote software attack of cloud applications • Remote hardware attack against the cloud • Remote software and hardware attack against cloud user organizations' end point software and hardware • Social engineering of cloud provider users, and cloud customer users.	The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by external attackers, particularly in private clouds where user endpoints can be targeted. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data. This includes the threat of hardware attack, social engineering and supply chain attacks by dedicated attackers.
Data leakage: • Failure of security access rights across multiple domains • Failure of electronic and physical transport systems for cloud data and backups.	A threat from wide spread data leakage amongst many, potentially competitor organizations, using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise.
Integrity	
Data segregation: • Incorrectly defined security perimeters • Incorrect configuration	The integrity of data within complex cloud hosting environments such as SaaS configured to share computing resource amongst customers could provide a threat against data integrity if system resources are effectively segregated.

User access: • Poor identity and access management Procedures	Implementation of poor access control procedures creates many threat opportunities, for example that disgruntled ex-employees of cloud provider organizations maintain remote access to administer customer cloud services, and can cause intentional damage to their data sources.
Data quality: • Introduction of faulty application or infrastructure components	The threat of impact of data quality is increased as cloud providers host many customers' data. The introduction of a faulty or mis-configured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing infrastructure.
Availability	
Change management: • Customer penetration testing impacting other cloud customers • Infrastructure changes upon cloud provider, customer and third party systems impacting cloud customers.	As the cloud provider has increasing responsibility for change management within all cloud delivery models, there is a threat that changes could introduce negative effects. These could be caused by software or hardware changes to existing cloud services.
Denial of service threat: • Network bandwidth distributed denial of service • Network DNS denial of service • Application and data denial of service	The threat of denial of service against available cloud computing resource is generally an external threat against public cloud services. However, the threat can impact all cloud service models as external and internal threat agents could introduce application or hardware components that cause a denial of service.
Physical disruption: • Disruption of cloud provider IT services through physical access • Disruption of cloud customer IT services through physical access • Disruption of third party WAN providers Services	The threat of disruption to cloud services caused by physical access is different between large cloud service providers and their customers. These providers should be experienced in securing large data centre facilities and have considered resilience among other availability strategies. There is a threat that cloud user infrastructure can be physically disrupted more easily whether by insiders or externally where less secure office environments or remote working is standard practice.
Exploiting weak recovery procedures: • Invocation of inadequate disaster recovery or business continuity processes	The threat of inadequate recovery and incident management procedures being initiated is heightened when cloud users consider recovery of their own in house systems in parallel with those managed by third party cloud service providers. If these procedures are not tested then the impact upon recovery time may be significant.

IV. TYPES OF ATTACKERS IN CLOUD COMPUTING

Many of the security threats, attacks and challenges of cloud computing are considered by organizations.

TABLE II
A LIST OF ATTACKS ON CLOUD COMPUTING ENVIRONMENTS [5]

Internal Attackers	An internal attacker has the following characteristics: • Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service • May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role • Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service.
External Attackers	An external attacker has the following characteristics: • Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service • Has no authorized access to cloud services, customer data or supporting infrastructure and applications • Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service.

V. CLOUD SECURITY RISKS

The security risks related with each cloud delivery vary and are dependent on a wide range of factors including the sensitivity of information, cloud architectures and security control involved in a particular cloud environment.

Table III summarizes the security risks relevant in the cloud computing paradigm. This table will help us in implementing the appropriate security measures.

TABLE III
A LIST OF SECURITY RISKS IN CLOUD COMPUTING ENVIRONMENTS [5]

Risk	Description
Privileged user access	Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data.
Data location and segregation	Customers may not know where their data is being stored and there may be a risk of data being stored along with other customers' information.
Data disposal	Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during decommissioning is enhanced within the cloud.
e-investigations and Protective monitoring	The ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model in use, and the access and complexity of the cloud architecture. Customers cannot effectively deploy monitoring systems on infrastructure they do not own; they must rely on the

	systems in use by the cloud service provider to support investigations.
Assuring cloud security	Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements.

VI. CONCLUSIONS

This paper gives the detailed description of cloud computing. Many organizations have shifted their business on cloud from traditional systems. Many people are accessing the cloud individually for different purposes. During these access people are concerned about the security. They need a high level of security for their data on cloud. This paper will help us to understand cloud computing concepts and will open the new window to implement security measures.

REFERENCES

[1] Monjur Ahmed and Mohammad Ashraf Hossain, "Cloud Computing And Security Issues In The Cloud" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[2] Ms. Disha H. Parekh and Dr. R. Sridaran "An Analysis of Security Challenges in Cloud Computing" International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013.

[3] Prince Jain "Security Issues and their Solution in Cloud Computing" International Journal of Computing & Business Research ISSN (Online): 2229-6166

[4] Petre, R. (2012). Data mining in Cloud Computing. Database Systems Journal, 3(3), 67-71.

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

[6] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma, "Towards Analyzing Data Security Risks in Cloud Computing Environments", Springer-Verlag Berlin Heidelberg 2010, pp. 255-265.

[7] Open Cloud Computing Interface. Homepage URL: http://occi-wg.org.

[8] Perez R, van Doorn L, Sailer R. "Virtualization and hardware-based security". IEEE Security and Privacy 2008;6(5):24–31

[9] Jamil, D., Zaki, H. "Security issues in cloud computing and counter measures", International Journal of Engineering Science and Technology (IJEST) , Vol. 3 No. 4, pp: 2672-2676.

[10] Mingi Zhou et al., "Security and Privacy in Cloud Computing: A Survey," Proc. 6th Int'l Conf. Semantics, Knowledge and Grids, IEEE Press, 2010, pp. 105–112.

AUTHORS

Prof. Jitendra N. Shrivastava

Presently he is working at Invertis University. His research interests are Data Mining and Artificial Intelligence. He has published three books and many research papers. He is member of board of studies, academic council and University Court of many organizations. He can be contacted by email: jitendranathshrivastava@yahoo.com

Uvaish Khan

Presently he is student at Invertis University. His research interests are in the area of cloud computing and Artificial Intelligence. He can be contacted by email: owaiskhan04@hotmail.co.uk