ISSN:0975-9646

Parul Chachra / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1066-1068

A Survey of the Existing Security Issues in Cloud Computing

Parul Chachra
Department of Computer Science, College of Vocational Studies
University of Delhi, New Delhi

Abstract: **Cloud Computing is the buzzword in the field of networking. It brings many networking concepts and other benefits under one umbrella. Cloud Computing is the technology that allows the users to commission computing resources according to their requirements. The users are majorly shifting towards the Cloud for their business requirements as it offers many benefits. However, Cloud Computing also pose security risk to the user's data. The major drawback of Cloud Computing is the security issues in storing data in the Cloud. Another fact that hampers the success of Cloud is the reluctance of users to accept Cloud for their business requirements.**

I. INTRODUCTION

Cloud Computing is the new trend in the field of networking. Cloud Computing is the technology which allows the users to commission computing resources according to their requirements. However, Cloud Computing also pose security risk to the user's data. The Cloud offers its users many different advantages that lead to it being adopted in different fields.

Cloud Computing has been defined by varied organizations as they see it. Thus, there are many different definitions of Cloud Computing, which are in use by the industry. Some of the most used definitions are given below:

"Cloud Computing is a model for enabling convenient, on-demand network access to 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." [NIST: National Institute of Standards and Technology][1]

"It is a style of computing in which massively scalable IT-related capabilities are provided 'as a service' using Internet technologies to multiple external customers." [Gartner][2]

"Use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption." [Cloud Security Alliance][3]

A. KEY FEATURES OF CLOUD COMPUTING

According to the definition of Cloud Computing, the following key features surface:

- On-demand service – The services provided by the Cloud can be utilized according to the demands of the cloud user. This facilitates ease of use of the computing resources.
- Network access – the computing resources are placed on a network which can be accessed using "anytime, anywhere" model. The user has the flexibility of connecting to the Internet to use these resources.
- Shared resource pool – cloud users can share these resources with other users. Also, the cloud service provider can also share computing resources with many cloud users. This enables optimum utilization of resources from the perspective of both cloud user and cloud service provider.
- Rapid allocation and de-allocation – the cloud user can increase/decrease the resources according to its own requirements rapidly, that is without much delay. This is possible as no administrative intervention is required.

B. DEPLOYMENT MODELS

A deployment model means the actual positioning of resources to reap maximum benefits.

The deployment models for the cloud are as follows:

- Public Cloud – the cloud infrastructure is available for public use. The cloud infrastructure and resources are owned and managed by an organization dealing with cloud services.
- Private Cloud – the cloud infrastructure is specifically for the use of an organization. The cloud infrastructure and resources can be owned and managed by this very organization or a third party.
- Hybrid Cloud – is a combination of public and private cloud. Generically, organizations are outsourcing public clouds for functions which are not confidential or which may not come under scanner, such as

C. SERVICE MODELS

A service model is a way in which the services are given to the cloud user. The cloud offers the following service models:

- Infrastructure as a Service (Iaas) – refers to a service model in which infrastructure is lent out to the cloud users. IT resources such as servers, storage, operating systems, network devices, etc. are provided to the users for hiring. These resources are placed onto the cloud so that the users can avail their services as per their requirements.
- Platform as a Service (PaaS) – refers to a service model in which the application development

toolkit is lent out. The cloud users hire these services to develop and deploy their own applications as per their own requirements. Here the user is not required to own these deployment tools and development environment.

- Software as a Service (SaaS) – refers to a service model in which the applications are lent to the cloud user for his requirements and specifications. The examples of such applications include Sales Management, Finance and Accounting and Payroll Systems amongst others.

II. SECURITY ISSUES

Cloud Computing is a promising area providing computing and other services to the cloud users. It provides the users with many advantages primarily increasing or decreasing the number of resources according to user's requirements. As the saying goes, "Every Coin Has Two Sides", Cloud Computing also has its own share of problems and challenges.

Cloud Computing is not a new technology; just the existing technology restructured in a new format thereby providing new mode of communication. Thus, it suffers from all inherent issues the earlier networking technologies suffered. Networking between two computers has always been plagued with security and privacy issues. The data and communication channel had to be secured from intrusion; however, there can never be foolproof security.
Cloud Computing has to face many issues and challenges as it is still in its infancy. Much research is being done in this field to better the structure and functioning of the cloud.

The cloud computing suffers from the following drawbacks:

- Data Security and Privacy
- Compliance Issues
- Funding
- Lack of Standardization
- Identity and Access Management
- Reliability and Continuity of Service
- Loss of Internal Control

A. DATA SECURITY AND PRIVACY

Data is stored in the cloud shared by multiple tenants. The data location is mobile, that is, it can move from one location to another. The cloud users may not be aware of the data location or about the access log of their data. The confidential information is stored away from its owner, which increases its vulnerability. This raises serious questions about the security of user's data. Since many people are managing the cloud at the same time, the privacy of cloud data cannot be guaranteed. Any number of people can eavesdrop over the data.

B. COMPLIANCE ISSUES

Cloud Computing provides a challenging environment for the cloud service providers, as they have to comply with different rules and regulations. The cloud is an amalgamation of many different facets such as varied computing resources, cross-border locations, multiple tenants of the same computing resource, etc. Each different dimension provides different set of rules and regulations for the service provider to follow. Cloud data needs to be secured, as it is stored away from the user, the cloud service providers have to comply with regular audits. Many cloud providers may not be willing to get regular audits done, as they have to bear extra costs to achieve that.

C. FUNDING

A cloud alone comprises of many components and services requiring adequate funding. As a result of lack of funding, there are limited numbers of players in the market providing cloud services. A cloud service provider has to set up large data centers to store data and provide other services such as IaaS, etc. This might not be feasible for each service provider entering the market.

D. LACK OF STANDARDIZATION

Cloud technology is fairly a new concept and there are advancements in the technology every now and then. Every Cloud Service Provider has its own implementations, which leads to a lack of standardization in its implementation. There should be standardization of cloud's hardware, operating system, all technical layers, software stacks, etc. to provide standardized services to all clients and processes as well.

E. IDENTITY AND ACCESS MANAGEMENT

Data in the cloud is stored at multiple locations, that is, the location of data in the cloud is mobile. The cloud user may or may not be aware of his data's location. The cloud being multi-tenant in nature, the cloud user may have to logon using different user credentials for different providers. This poses potential threat to data as any individual may fake as the original owner in case the credentials are lost/leaked outside the system. A cloud needs to have a strong and sturdy identity and access management system in place so as to attract more transfers to the cloud.

F. RELIABILITY AND CONTINUITY OF SERVICE

Any user decides to shift to the cloud environment considering the benefits offered by the cloud computing, namely cost effectiveness. The cloud users need not invest in the in-house computing resources, thereby cutting on costs drastically. When the user shifts to the cloud, he expects continuity of service. In the absence of reliability and continuity of service less number of people would be willing to shift to the cloud environment.

G. LOSS OF INTERNAL CONTROL

Data in the cloud is stored with the cloud service provider, which is generally away from the data owner. The owner of data will have to forego the control over its security, as the data is not stored within the owner's premises. This is a major challenge in the acceptance of cloud computing as the owner feels threatened with respect to the security and usage of data. As the data is managed and administered by many personnel, data security and privacy issues pose a threat to the data owner.

III. RELATED WORK

Deyan Chen and Hong Zhao[6] have proposed the data life cycle stating that data undergoes various stages during its lifetime in the cloud-computing environment. The data life cycle consists of stages such as Data Generation, Transfer, Use, Share, Storage, Archival and Destruction. They have discussed the security issues with respect to these stages.

Deepa Krishnan and Madhumita Chatterjee[7] have proposed Cloud Security Management Suite as the Security as a Service Model. This model works with three modules namely, Identity and Access Management, Trust and Privacy Management and Accountability and Auditability Management. The user credentials are checked with the records maintained with the cloud service providers. The trust managers manage the trust with the cloud users and cloud service providers. The operations performed on the cloud need to be audited and checked with the logs maintained with the cloud service providers.

Venkatesa Kumar V. and Poornima G[12] have studied the problems of data security in cloud data storage. They have proposed an effective and flexible distributed scheme to ensure the correctness of users' data in the cloud servers; this task can also be delegated to Third Party Auditor based on some special conditions. The tokens used in their scheme can be stored at either user's local device or cloud server in an encrypted format.

Mohammed Hussain and Hanady Abdulsalam[9] have introduced a new architecture, namely Security as a Service (SECaaS) that addresses the security issues for cloud-based applications. SECaaS is a user-centric architecture that provides security means for cloud computing on its different levels namely SaaS, PaaS, and IaaS. SECaaS is mainly proposed to control security issues in cloud-based applications. It provides security means for both cloud users and providers.

IV. CONCLUSION

Cloud computing presents a set of technologies in a new format giving the users complete control of the resources; they can increment or decrement resources according to their requirements. Computing resources can be virtualized and accessed by many users from any location. It also promotes sharing of resources amongst many users.

Considering the benefits of cloud computing, it is the key to inducing major shifts towards the cloud. It can also be seen as a new trend attracting more users towards it and changing the future of computing. However, cloud computing comes along with its share of problems and challenges. Much research is being done into securing the cloud and its services. Security issues are posing a major threat to the adoption of cloud. Data Security and Privacy are being seen as big hurdles in the shift towards the Cloud. There is a lot being done and a lot that still needs to be done.

REFERENCES

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," *21. Aug 2009*, 2009.

[2] http://www.gartner.com

[3] http://www.cloudsecurityalliance.org

[4] Tharam Dillon and Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", 2010.

[5] Jianfeng Yang and Zhibin Chen, "Cloud Computing Research and Security Issues", 2010.

[6] Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", 2011.

[7] Cloud computing security, http://en.wikipedia.org/wiki/Cloud_ computing_security.

[8] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering, IEEE-2012.

[9] Deepa Krishnan and Madhumita Chatterjee, "Cloud Security Management Suite – Security as a Service", IEEE-2012.

[10] Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07-02. http://www.infoworld.com/d/security-central/gartner-seven-cloud- computing-security-risks-853.

[11] Mohammed Hussain and Hanady Abdulsalam, "SECaaS: Security as a Service for Cloud-based applications", ACM – 2011

[12] Venkatesa Kumar V. and Poornima G, "Ensuring Data Integrity in Cloud Computing", Journal of Computer Applications, 2012.

[13] "Data Protection Challenges in Cloud Computing", study report by DSCI