International Journal of Thesis Projects and Dissertations (IJTPD)
Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013, Available At: www.researchpublish.com

Security Issues in Cloud Computing - A Review

Anitha Y[1]
[1]Department of Computer Science and Engineering, Punjab Technical University
[1]SSCET, Pathankot, India

Abstract: **Cloud computing technology drawn the attention of IT world and is the changing the focus of enterprises. A high percentage of internet users today are already utilizing aspects of cloud computing in their normal daily workflow. Cloud computing gained attention due to the growth of internet technologies, reduced costs of storage and processing, growth technologies of visualization, SOA (Service Oriented Architecture) and advancement in internet security. Cloud computing security is one of the main challenges in cloud computing. An organization can decide to adopt cloud only on based on benefits to risk ratio. This paper is focused on the security issues of cloud computing. Before analysing the security issues, the definition of cloud computing and brief discussion to under cloud computing is presented. Then discusses the components that affect the security of the cloud then it explores the cloud security issues and problems faced by cloud service provider and some solution for security issues.**

Keyword: **Cloud Computing, Cloud Security, Cloud Security Issues, Cloud Legal Issues.**

I. INTRODUCTION

Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts [1]. Cloud computing can be defined as “Cloud is a parallel and distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLA) established through negotiation between the service provider and consumers” [2]. It is a style of computing where IT-related capabilities are provided to consumer as “service” rather than a product using the internet. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels. Many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities [3].

The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to cloud it is more focused upon the frontend and the back end. The front end is the user who requires the data, whereas the backend is the numerous data storage device, server which makes the cloud [4].

The remainder of this paper is organized as follows: A brief review of Cloud Computing is given in section II. Section III describes cloud computing security issues. Section IV proposed cloud computing security issues solution. Paper is concluded in section V.

II. CLOUD COMPUTING

A. Understanding Cloud Computing

Users connect the cloud they seen cloud as a single application, device, or document. All things inside the cloud system like hardware in the cloud and the operating system that manages the hardware connections are invisible. Cloud computing starts with the user interface seen by individual users. This is how users gives their request then gets passed to the system management, which finds the correct resources and then calls the system’s appropriate provisioning services.

Cloud computing is mainly used for data storage. Here the data is stored on multiple third-party servers. The user sees a virtual server; it appears as if the data is stored in a particular place with a specific name, when storing the data. This doesn’t exist in reality. It’s just used to reference the virtual space of the cloud. In reality, the user’s data could be stored on any one or more of the computers used to create the cloud.

B. Cloud Computing Service Models

The cloud service providers provide three different services based on different capabilities such as SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) [5].

1. Software as a Service (SaaS): Software as a Service consists of software running on the provider’s cloud infrastructure, delivered to (multiple) clients (on demand) via a thin client (e.g. browser) over the Internet. Typical examples are Google Docs and Salesforce.com.

2. Platform as a Service (PaaS): This gives a developer the flexibility to develop applications on the provider's platform. Entirely virtualized platform that includes one or more servers, operating systems and specific applications. Main services provided are storage, database, and scalability. Typical examples are Google App Engine,Mosso ,AWS: S3.
3. Infrastructure as a Service (IaaS): The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. IaaS offers users elastic on demand access to resources (networking, servers and storage), which could be accessed via a service API.Typical examples are Flexiscale, AWS: EC2(Amazon Web Services).

C. Cloud Computing Deployment Models

The security issues starts with the cloud deployment models. Depending on infrastructure ownership, there are four deployment models of cloud computing[6].

1. The Public Cloud*:* Which describes cloud computing in the traditional mainstream sense; resources are dynamically provisioned on a self-service basis over the Internet. It is usually owned by a large organization (e.g. Amazon, Google's AppEngine and Microsoft Azure).This is the most cost-effective model leading to user with privacy and security issues since the physical location of the provider's infrastructure usually traverses numerous national boundaries[7].
2. The Private Cloud*:* It defers from the traditional data enter in its predominant use of virtualization. It is a single tenant environment They have been criticized on the basis that users still have to buy, build, and manage them and as such do not benefit from lower capital costs and less hands on management. The private cloud is more appealing to enterprises especially in mission and safety critical organizations.
3. The Community Cloud: Thus refers to a cloud infrastructure shared by several organizations within a specific community. It may be managed by any one of the organizations or a third party. A typical example is the Open Cirrus Cloud Computing Testbed, which is a collection of Federated data centres across six sites spanning from North America to Asia.
4. The Hybrid Cloud: It comprises of a combination of any two (or all) of the three models discussed above. Standardization of APIs has lead to easier distribution of applications across different cloud models.

III. CLOUD COMPUTING SECURITY ISSUES

A. Layered Framework for Cloud Security

There is a layered framework is available that assured security in cloud computing environment. It consists of four layers as shown in Figure 1 [8].

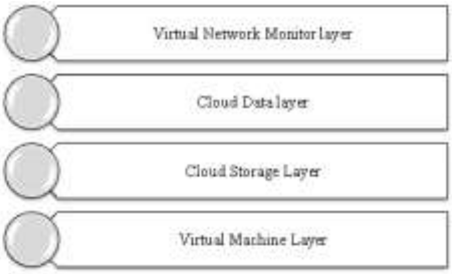

Fig. 1. Layered Framework of Cloud Security

First layer is secure virtual machine layer. Second layer is cloud storage layer. This layer has a storage infrastructure which integrates resources from multiple cloud service providers to build a massive virtual storage system. Fourth layer is virtual network monitor layer, this layer combining both hardware and software solutions in virtual machines to handle problems.

However, there are several groups working and interested in developing standards and security for clouds. The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups. The Cloud Security Alliance (CSA) is one of them. CSA gathers solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. Another group is Open Web Application Security Project (OWASP). OWASP maintains a list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes. The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers.

B. Components Affecting Cloud Security

There are numerous security issues for cloud computing as it encompasses many technologies including virtualization, resource allocation, transaction management, cloud networks, databases, operating systems, load balancing, concurrency control and memory management.

For example, security in cloud network that interconnects the systems in a cloud has to be secure. Load balancing algorithms has to be executed securely. Virtualization paradigm in cloud computing results in several security concerns[9]. For example, mapping the virtual machines to the physical machines has to be carried out securely. Concurrency control involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. Resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

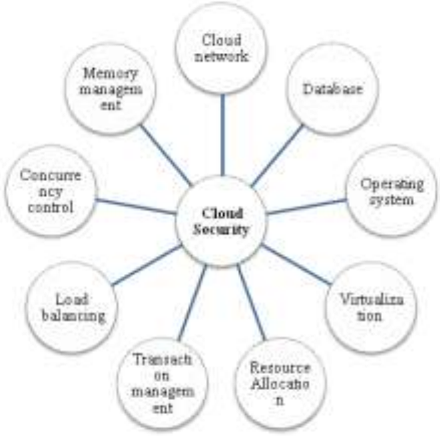

Fig. 2 Components affecting Cloud Security

C. Security Issues Faced By Cloud Computing

Cloud allows users to achieve the power of computing which beats their own physical domain. It leads to many security problems. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. Cloud computing infrastructures use new technologies and services, most which haven't been fully evaluated with respect to security. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. The security issues faced by cloud computing are discussed below.

1. Data Access Control*:* Sometimes confidential data can be illegally accessed due to lack of secured data access control. Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Data exists for a long time in a cloud, the higher the risk of unauthorized access [10].
2. Data Integrity*:* Data integrity comprises the following cases, when some human errors occurs when data is entered. Errors may occur when data is transmitted from one computer to another , otherwise error can occur from some hardware malfunctions, such as disk crashes. Software bugs or viruses can also make viruses. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing.
3. Data Theft: Cloud computing uses external data server for cost affective and flexible for operation. So there is a chance of data can be stolen from the external server.
4. Data Loss: Data loss is a very serious problem in Cloud computing. If banking and business transactions, research and development ideas are all taking place online, unauthorized people will be able to access the information shared. Even if everything is secure what if a server goes down or crashes or attacked by a virus, the whole system would go down and possible data loss may occur. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. The customers won't be able to access those data's because data is no more available for the customer as the vendor shut down.
5. Data Location: Consumers do not always know the location of their data. The Vendor does not reveal where all the data's are stored. Cloud Computing offers a high degree of data mobility. The Data's won't even be in the same country of the Customer, it might be located anywhere in the world. They may also wish to specify a preferred location (e.g. data to be kept in the USA) then requires a contractual agreement between the Cloud service provider and the consumer that data should stay in a particular location or reside on a given known server [11].

6. Privacy Issues: Security of the Customer Personal information is very important in case of cloud computing. Most of the servers are external, so the vendor should make sure that is well secured from other operators.
7. Security issues in provider level*:* A Cloud is good only when there is a good security provided by the vendor to the customers. Provider should make a good security layer for the customer and user .And should make sure that the server is well secured from all the external threats it may come across. The cloud computing service provider has.
8. User level Issues: User should make sure that because of its own action, there shouldn't be any loss of data or tampering of data for other users who are using the same Cloud.
9. Infected Application: Service provider should have the full access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

D. Legal Issues In Cloud Computing Contracts

The following is a brief summary of the most common and significant legal issues that can arise in contracts with customers for cloud computing services.

1. Protection of information.

Privacy: Information about the privacy obligations for Commonwealth contracts can be found on the Office of the Indian Information Commissioner's (OIIC) website. Providers are also strongly advised to consider the "Better Practice Guide – Privacy and Cloud Computing for Indian Government Agencies" before entering into any cloud computing arrangement.

Security: Providers should refer to the Defence Signals Directorate's 'Cloud Computing Security Considerations" for detailed guidance on issues to consider from a security perspective.

Compensation for data loss: Due to technical or operator error as well as fire or other disasters there may be a chance that data could be permanently lost by a cloud computing services provider. Misuse of data by external parties has the risk of data change.

2. Liability

Limitations on liability: In traditional information technology agreements, cloud service agreements typically seek to minimize the provider's liability for any loss that arises from the provision of the service. The Commonwealth will accept a list of exceptions agreed by the provider. These exceptions are*:*

- Injuries including sickness and death.
- Tangible property's damage or loss.
- Violation of privacy, security or confidentiality responsibilities.
- Intellectual property contravention.
- Illegal act or exclusion.

In addition to the standard exceptions, agencies should consider whether the risks of their procurement justify additional protection including the following as exceptions :

- service interruption losses.
- data loss.
- misuse of data.

Decisions made by agencies about the amount of any liability should be informed by a risk assessment that examines all the cases.

3. Performance management

Service levels: Service levels ensures that a provider meets the level of service expected by the agency. This is particularly important where the cloud computing service is critical either to the functioning of an agency or to the agency's clients [12].

IV. SOLUTION FOR CLOUD SECURITY ISSUES

There are some cloud security solutions, that providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution.

Trust between the Service provider and the customer is one of the main issues cloud computing. Service Level Agreement (SLA) is the only legal document between the customer and service provider. Which contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do.

Legal Issues is also one of the major problems, the laws vary from country to country, and users have no control over where their data is physically located. Regulatory measures likes, privacy laws and data security laws that cloud systems need to follow.

Preserving confidentiality and Integrity is one of the major issues. data encryption preventing the improper disclosure of information.

Authenticity may varies with varying amount of users rights. Sometimes there would be a user with a limited set of rights might need to access a subset of data, and might also want to verify that the delivered results are valid and complete Solution for such problems is to use digital signatures. Then the problem with digital signatures is that not all users have access to the data superset, therefore they cannot verify any subset of the data even if they're provided with the digital signature of the superset; and too many possible subsets of data exist to create digital signatures for each. Solutions to this problem is to provide customers with the superset's signature and some metadata (verification objects) along with the query results[13].

Data Splitting is also a solution for cloud security issues. Here the data split over multiple hosts that cannot communicate with each other; only the owner who can access both hosts can collect and combine the separate datasets to recreate the original.

Data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by cloud service consumer. To implement access control methods for consumer side, the cloud service provider must describe and ensure that the only authorized users can access the user or consumer's data.

Make sure the consumer's access devices or points such as personal computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. Access to the device by an unauthorized user can cancel even the best security protocols loss of an endpoint access device in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features.

Data Access Monitoring have to assure about whom, when and what data is being accessed for what purpose. Cloud service provider must share diagrams or any other information or provide audit records to the consumer or user. Provider must verify the proper deletion of data from shared or reused devices. Cloud service providers must gives enough details about fulfillment of promises, break remediation and reporting contingency.

V. CONCLUSION

Cloud computing by itself is in evolving stage and hence the security implications in it aren't complete. It is emerging as the various organizations that are developing cloud services are evolving. It is evident that the Even the leading cloud providers such as Amazon, Google etc are facing many security challenges and are yet to stabilize. Achieving complete solution for legal issues is still a question. With this level of issues in cloud computing, decision to adopt cloud computing in an organization could be made only based on the benefits to risk ratio.

Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. The largest comes when the differences between actual cloud security and virtual machine security comes. Research should be center on these gaps and differences and its removal. Main goal of cloud computing is to securely store and manage the data in cloud.. One solution for cloud security issues is to produce the framework might be developing a way to monitor the cloud's management software, and another might be development of isolated processing for specific clients' applications. It is useful to track the client's behaviour and monitored for instance whether client allow the updating anti-virus software definitions , or ,automated patching software to run, or whether client understand how to make safe their virtual machines in the cloud.

REFERENCES

[1]. Peter Mell, Timothy Grance "The NIST Definition of Cloud Computing" NIST Special Publication 800-145.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 25:599616, 2009.

[3] Tackle your client's security issues with cloud computing in 10 steps, http://searchsecuritychannel.techtarget.com/tip/Tackle-your-clients-security-issues-withcloud-computing-in-10-steps.

[4] Lord CrusAd3r,"Problems Faced by Cloud Computing", , dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

[5] R. Buyya, S. Pandey, and C. Vecchiola, Cloudbus toolkit for market-oriented cloud computing, in Proceedings 1st International Conference on Cloud Computing (CloudCom 09), Beijing, 2009, pp. 3_27.

[6] Tharam Dillon, Chen Wu and Elizabeth Chang, Cloud Computing: Issues and Challenges, 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 1550-445X/10.

[7] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A 32Berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.

[8] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51, University of Texas, USA, April-June 2010.

[9] Problems Faced by Cloud Computing, Lord CrusAd3r,dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

[10] ZiyuanWang , “Security and privacy issues within the Cloud Computing” ,International Conference on Computational and Information Sciences , 2011

[11] Zaigham Mahmood , " Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web Technologies, 2011.

[12] Negotiating the cloud – legal issues in cloud computing agreements Commonwealth of Australia 2012, ISBN 978-1-922096-05-0

[13] Joshua Kissoon, Cloud Computing Security Issues and Solutions, 2013 Gountis and A. G. Bakirtzis, “Bidding strategies for electricity producers in a competitive electricity marketplace,” IEEE Trans. Power System, vol. 19, no. 1, pp. 356–365, Feb. 2004.