Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-10, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

An Overview of Security Issues For Cloud Computing

Mrs. Varsha Anup Jujare
Assistant professor, Sharad Institute of Technology, College of Engineering
Yadrav, Ichalkaranji

Abstract: *Cloud computing is a complete, reliable package for the users. Instead of using local servers and personal computers to handle resources cloud computing is the best way for utilizing it. Cloud computing is present everywhere and is available as soon as or whenever required with minimum efforts for management. The basic goal of cloud computing is to perform larger number of computations in minimum time, provide faster internet facility and easy accessibility.*

1. Introduction

The necessity and importance of cloud computing is growing rapidly. Now-a-days it is considering as one of the most famous technology among all as it is the best way used for information management. It does not require local server or personal computer to gain access to the data. Again it doesn't require that user should present at only one place all the time to access the data. It is a model in which all the information technology services are provided on internet by using some tools and applications. All the information and resources are present on the web server and one has to use it remotely as per the necessity by paying amount for only used data and resources. Cloud computing is a data processing and data distribution architecture. Its main goal is to provide safe, fast and efficient storage of data for all the resources on the web [2].

2. Types of cloud computing:

It is generally classified in two broad categories

1) Based on the location

a) Public cloud:
Public cloud is a standard on which service provider makes resources like applications, data storage available on overall network. These services may not cost anything that means free or it has cost on pay-per-uses basis.

b) Private cloud:
Private cloud is a standard which provides similar service like public cloud with some added features like scalability, self-service. It is used for single architecture.

c) Hybrid cloud:
Hybrid cloud is the combination of private cloud and third party, public cloud with middleware between two different architectures.

2) Based on the service provided

a) Infrastructure-as-a-service:
This provides services related to hardware by considering all the features of cloud computing. For e.g. database, disk storage, virtual server.

b) Platform-as-a-service:
This is a model which provides services on the web. It provides all the tools which are needed for the development of any application in the form of service.

c) Software-as-a-service:
This model provides complete software package so that user can access the same things on web [1, 2].

3. Security Issues:

As cloud computing works on different areas such as database, network, resource sharing, project scheduling, concurrency control, memory management it needs security.

Security is the key element in cloud computing. Security is measured in some terms like confidentiality, integrity, availability, accountability, assurance, resilience [3].

1) **Confidentiality:** Confidentiality is keeping the data behind scenes. Not only the system or organization data is kept private but all the data of system itself can be remained safe.

Confidentiality can be provided by giving access permissions to the users who are accessing the particular system.

2) **Integrity:** It is the actual measurement for righteousness of data. As cloud uses large amount of database integrity is essential front faceplate for it.

3) **Availability:** It is the factor which defines whether data is available to authorized user or not.

4) **Accountability:** Accountability is the term in which access is permitted to the user can be mapped by using different transactions, auditing logs using a particular system by an authorized user.

5) **Assurance:** Assurance means trust that user will get the things needed over the cloud. This does not include only hardware and software but everything which user wants to access the data over cloud. It includes all the technical details to legal documentation procedure.

6) **Resilience:** Resilience is preventing the system from security threats. Cloud computing increasing resilience by keeping backup of data over the cloud. It does not only protect the data but deals with the problems too.

4. Threats in cloud security

1) **Data rupture:** Due to large amount of data storage over the cloud server, it is the main target for the attacker. The cloud server may contain some sensitive data like financial information, defense information, and health information. Companies are responsible for the security of data [4].

2) **Hacking account:** Attackers can hack a particular account and can change the data, transactions from the account. To prevent these types accesses owner should supervise every transaction by its own.

3) **Permanent data loss:** Sometimes it might be possible to delete the whole data from the cloud server and it can be done by malicious software's by unauthorized persons to harm the organizations. To stop this type of threat cloud service provider must keep the data backup to two to three different places.

4) **DOS attacks:** These are the denial-of-service attacks done on cloud data; this affects the huge amount of data over cloud. This can be controlled by sending a message to administrator before attack happens. So that administrator will keep control on it.

5) **Sharing:** This is the key aspect of cloud computing. It can send data t user as per the necessity of user. Cloud service provider will share all the services such as platform, infrastructure and applications. This will lead to ambiguous use of data over cloud and simultaneously problematic to the other users of the system.

5. Solutions to security issues

1) **Support to investigation:** There are some tools provided to cloud users for checking how the data is stored onto cloud and who is going to use it. It is very difficult task to identify unauthorized use of data because it is spread over data centers. But by using audit tools users can get whether their data is safe or not [6].

2) **Algorithms:** The large numbers of algorithms are provided to secure data over the cloud. The technique of conversion of plain text to cipher text is encryption. And this technique comprises encryption algorithms to keep the data safely. The only disadvantage of this technique is that, the data should not be available for all the users. It will only be accessed by technical persons [6].

3) **Storing the data at another side:** This is the way of keeping backup for user's data on another side always. Any kind of disasters might result in data loss.

4) It is very important for cloud service provider that data must be kept secret, safe and avoid vulnerabilities along with unauthorized access. To maintain quality of data, and customer satisfaction, data service providers must work on this phenomenon.

6. Conclusions

Cloud Computing is a new and emerging concept with providing number of benefits to the user. Though it is having some security issues which are harming the whole system or degrading the performance of system, it is coming up with new power day-by-day. As it includes much

functionality in it; it will overcome all the problems, threats, vulnerabilities in it. By providing some authorities to the enterprises flexibility can be maintained. It leads to security of sensitive data and will provide access to the data for concerned user [5].

7. References

[1] Acquisti, Alessandro, Allan Friedman and Rahul Teland. "Is There a Cost to Privacy Breaches? An Event Study," International Conference of Information Systems (ICIS), 2006.

[2] Blumenthal, Marjory, "Is Security Lost in the Clouds?", Telecommunications Policy Research Conference, Oct 2, 2010.

[3]1026_cloud_computing_friedman_west

[4]http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html
wp_addressing-security-challenges-in-the-cloud

[5] CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD Monjur Ahmed1 and Mohammad Ashraf Hossain2

[6] An Overview and Study of Security Issues & Challenges in Cloud Computing **Rajesh Piplode*** *Department of Computer Science Institute Of Computer Science Govt. Holkar Science College Indore-India.* **Umesh Kumar Singh** *Vikram University Ujjain-India*