

Survey on Security issues in Cloud Computing

Arun A.G
6th sem, Dept. of ISE
Sai Vidya Institute of Technology
Bangalore, India

Darpan.A.Jain
6th sem, Dept. of ISE
Sai Vidya Institute of Technology
Bangalore, India

S.N.Kamala
6th sem, Dept. of ISE
Sai Vidya Institute of Technology
Bangalore, India

Mahesh.Pai
6th Sem, Dept. of ISE
Sai Vidya Institute of Technology
Bangalore, India

Abstract— Cloud computing is the latest effort in delivering computing resources as services. It is based on sharing resources between multiple users. It provides software, data storage space, computation facility. The facilities provided by Cloud computing doesn't require an end user to have the knowledge on, where the data is stored, how the data is accessed etc. Since all the data stored in a public cloud can be accessed by multiple clients (organizations) data stored on a cloud is vulnerable to attacks. It is necessary for the cloud service provider to provide security to the user's data. To increase the adoption of cloud for business environment the cloud services being provided to the customers must be highly secure. In this paper we discuss about few security issues faced by a user.

Keywords— Cloud computing, Definition of cloud Computing by NIST, cloud computing security issues.

I. INTRODUCTION

According to NIST, the definition of cloud computing[1] is "Cloud computing is a model for enabling ubiquitous, 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 the sharing of computing resources rather than having local servers to handle applications. The user uploads the input data to the cloud which is a user's data which is in unencrypted form. This poses some security and privacy challenges. Because the service provider can access the data any time which is in cloud, there is a possibility that the user's private data is leaking to other tenants. User could knowingly or unknowingly alter or delete the data or some unauthorized intruder may get the user's data by breaching into the cloud. Therefore there are various security concerns in cloud computing.

II. COMPONENTS AFFECTING CLOUD SECURITY

There are many security issues for cloud computing as it encapsulates many technologies such as virtualization, databases, load balancing, memory management, transaction management etc.

Virtualization -As per [2], virtualization is a technique in which a single resource or application is shared among

multiple users (organization). Virtualization is done by assigning a logical name to a physical resource and by pointing a pointer to that resource on demand for that particular resource. Several security concerns are due to Virtualization exemplar. For example, mapping of physical machines has to be carried out securely.

Resource allocation-According to V.Vinothina et.al[3], resource allocation is the technique of assigning available resources among the applications which require its services. If resource allocation is not done properly then the services may get stalled or may not work properly due to insufficient resource allocation or improper resource allocation.

Load balancing-Rajesh George Rajan et.al[4] tells that load balancing means to share a work among different nodes in a collective system so as to get best responses time and to utilize the resources to the fullest. Hence resource allocation algorithms must be secure and accurate.

Memory management-The act of managing memory is called as memory management. In a cloud we need to have good management algorithms to maintain proper memory management. The best example in this field according to Harithan Reddy Velagala[5] is the Amazon's Elastic Compute Cloud (EC2).

III. SECURITY ISSUES FACED BY CLOUD COMPUTING.

Cloud is hit badly when it comes to security. A cloud service provider must also make sure that data stored/ being used by a user is not lost or corrupted or misused. The service provider must make sure that all the data in the cloud is secure. There are chances that a malicious user may try to access the data in a cloud by impersonating a legitimate user and thereby infecting the cloud and its end users.

A. Data Access control:

A typical user may store his files on a cloud to access them elsewhere on internet may not bother much about security but, in case of companies which store highly confidential data on a cloud they should be confident that their data on a cloud is secure. But since cloud offers services to multiple clients and therefore data stored in a cloud is vulnerable. Young-Gi Min et.al[6] says that insider attacks is a

huge risk in cloud computing. An unethical hacker may hack into a cloud and retrieve sensitive and confidential data of other clients of the cloud. So the cloud service providers must provide features to make sure that the data in a cloud is well secured.

B. Data theft

Cloud computing makes use of external data server for various operations as a result of which chances of data being stolen from external servers is more. A client is always worried about his data being stolen from the cloud. It is the duty of the cloud service provider to ensure that the data of clients is not stolen, for which he may have to apply certain algorithms, procedures etc.

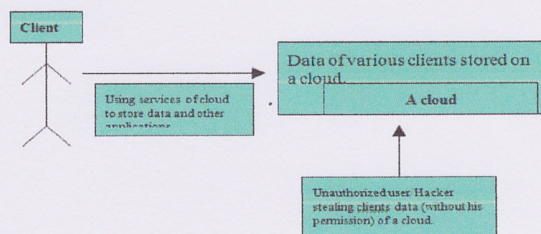


Fig 1: figure explaining Data theft.

C. Data integrity.

Anitha Y[7] in her paper tells that, data integrity means assuring accuracy and consistency of data over its life cycle. It is possible that a user may make a mistake while entering certain data or it is possible that an error may arise while data is being transmitted from source to destination. Due to virus or bug data may get corrupted. Therefore there arises need for certain data integrity methods in cloud computing.

D. Data loss.

Data loss may happen as a result of deleting data without having a backup or due to unauthorized access. Anitha Y[7] tells that if banking transactions, sharing research ideas are all taking place online then unauthorized people will be able to access those data and may cause harm to that data or may delete the data. If at all a server goes down or is attacked by a virus, the data in the server may be lost.

E. Privacy issues.

Privacy is an important issue when it comes to cloud computing. A client stores his personal information on a cloud. Most of the servers in cloud computing are external so the cloud service provider must ensure that the data in the cloud is secure and the privacy of client's data is ensured. Therefore, the job of software engineers while developing a cloud is that, they should develop a cloud in such a way that it has all the criteria that maintain the privacy of the user's

data and reduces the risk of a user losing his privacy over the data he has stored on a cloud.

F. Phishing attack.

Phishing is the way of acquiring sensitive information of a user such as username, password, research data, bank transactions etc by fake (untrustworthy) users via emails, advertisements and messages. Shilpa.D et.al[8] tell that the links through which a user is targeted may appear authentic but will ultimately lead to fake access locations.

According to [9], the various types of phishing are:

G. Deceptive phishing.

Account theft using instant messaging, is referred to as Phishing. But, today the most common method of phishing is by Deceptive email messaging. Messages such as verify your account, system failure requiring users to re-enter their information and many such scams are broadcast to large number of recipients with the hope that a unaware user will respond to the mail where their data is collected without the knowledge of the authorized user.

H. Malware based phishing.

Running a malicious software on the user's machine, consequence of which is the data collection of the authorized user by the unauthorized user is called as Malware based phishing. The malware can be introduced to a user by sending it through mails as an attachment or by introducing it as a downloadable file exploiting its security vulnerabilities.

I. Content injection phishing.

By inserting malicious content in a legitimate website that leads the user to a malicious website or may install malicious software on to the machine of the user and this software may redirect user's data to the phishing server.

J. Man-in-the-middle phishing.

The type of phishing that is not very easy to detect is the man-in-the-middle phishing. Here the hacker/unauthorized user settles himself between the user and the Cloud, records the details without the knowledge of both the user and the cloud service provider and passes the details entered by the user to the server of the cloud normally. Later the man-in-the-middle sells or uses the recorded information of the user.

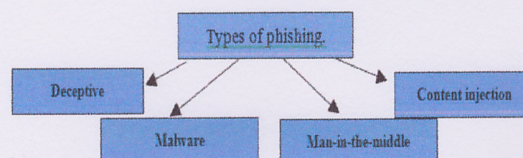


Fig 2: Types of phishing.

L. Denial-of-service attacks (DOS).

If a fake user increases the traffic of the cloud services to such an extent that all the authentic users cannot make use of the services of the cloud, this situation is called as Denial-of-

service attacks. T.Poornachandar and D.Jaya Prakash[10] in their paper have told that in cloud, multiple users make use of services of cloud. Attacker first establishes a network of computer that will be used to generate high volume of traffic which is needed to deny services to legitimate users. As a result, the legitimate customers face a decrease in performance.

CONCLUSION

In this paper we have discussed about various security threats that arise when a user makes use of cloud. A cloud service provider must ensure the client about the security of the data being stored in the cloud or else the client may stop using the services of the cloud. Methods, algorithms must be implemented where ever necessary to ensure that the data of clients in a cloud is not compromised with.

REFERENCES

- [1] National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.
- [2] http://www.tutorialspoint.com/cloud_computing/cloud_computing_virtualization.htm
- [3] V. Vinothina ; Dr .R.Sridaran;Dr. PadmavathiGanapathi , “ A Survey on Resource allocation Strategies in Cloud Computing” published in International Journal of Advanced Computer Science and Applications Vol. 3, No.6, 2012.
- [4] Rajesh George Rajan ; V.Jeyakrishnan , “A Survey on Load Balancing in Cloud Computing Environments” published in International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013.
- [5] Harithan Reddy Velagala, “Dynamic memory management in Cloud Computing”.
- [6] Young-Gi Min; Hyo-Jin Shin; Young-Hwan Bang; “Cloud Computing Security Issues and Access Control Solutions. http://www.serse.org/journals/IJSE/vol9_no2_2012/1.pdf
- [7] Anitha Y, “Security Issues in Cloud Computing – A Review”, published in International Journal of Thesis Projects and Dissertations(IJTDPD) Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013.
- [8] Shilpa D; Nagashree C; Divya C; Spoorthi G S , “Survey on Security attacks and Solutions in Cloud Infrastructure”, published in International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue xx, Xxxxx 2014.
- [9] Types of Phishing Attacks <http://www.pcworld.com/article/135293/article.html>
- [10] T. Poornachandar ; D.Jaya Prakash, “Denial of Service(DoS) Attack Detection in Cloud Computing” published in Indian Journal of Research, Volume : 2, Issue : 11, Nov 2013.