Security Challenges In Cloud Computing

*A. N. Suresh, Asst professor CSE, Vignan institute of engineering for women,Visakhapatnam,

**Ch. Sailaja, Asst professor CSE, Visakha institute of engineering and technology,Visakhapatnam,

***G. Gayatri, Asst professor CSE, Visakha institute of engineering and technology,Visakhapatnam,

****D.V.S. Deepak, Asst professor CSE,Avanthi Institute of engineering and technology, visakhapatnam.

ABSTRACT- *One of the emerging technologies in the present world is Cloud computing.Many of the individual users and organisations have profound usage of cloud computing as they can access data base resources through internet from any where. This computing model is beneficiary as far as the terms cost reduction and data accessibility are concerned. But there is a need to consider the security concept in cloud computing as the users store the sensitive data on the cloud storage providers which can not trusted always. In this paper we want to discuss how we can provide security in cloud computing by moving from single cloud providers to inter-clouds which has emerged recently. This paper is mainly aims at the factors that reduce the security risks in cloud computing, an emerging technology in computing world.*

1. INTRODUCTION

In cloud computing model we see the users or the organisations plug into "cloud "in order to access resources that are provided by the cloud service providers. This cloud computing allows the people to share the resources among them as it replaces an organisations data centre or server providing the same service.

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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Fig 1 : Cloud computing

1.1. Characteristics:

The characteristics of a cloud computing mainly involve on-demand self service (customers can request and manage their personal computing resources) , broad network access(allows services to be offered over the internet or private networks) ,resource pooling (customers form a pool of computing resources specially in remote data centres) ,rapid elasticity and measured service.

•*Shared Infrastructure* — Uses a virtualized software model, enabling the sharing of physical services, storage, and networking capabilities. The cloud infrastructure, regardless of deployment model, seeks to make the most of the available infrastructure across a number of users.

• *Dynamic Provisioning* — Allows for the provision of services based on current demand requirements. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed. This dynamic scaling needs to be done while maintaining high levels of reliability and security.

• *Network Access* — Needs to be accessed across the internet from a broad range of devices such as PCs, laptops, and mobile devices, using

standards-based APIs (for example, ones based on HTTP). Deployments of services in the cloud include everything from using business applications to the latest application on the newest smart phones.

• *Managed Metering* — Uses metering for managing and optimizing the service and to provide reporting and billing information. In this way, consumers are billed for services according to how much they have actually used during the billing period.

1.2. Service models:

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

In Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications.

1.3. Deployment Models

Deploying cloud computing can differ depending on requirements, and the following four deployment models have been identified, each with specific characteristics that support the needs of the services and users of the clouds in particular ways

•*Private Cloud* — The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises.

•*Community Cloud* — The cloud infrastructure is shared among a number of organizations with similar interests and requirements.

• *Public Cloud* — The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.

• *Hybrid Cloud* — The cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, and also the need to offer services in the cloud.

2. SECURITY PROBLEMS IN CLOUD COMPUTING

The users and organisations store sensitive information such as customer information and corporate information into the cloud service provider platforms to reduce the cost economically by giving up the control of some data. There may be cases that whether the individuals or the enterprises of organisations may worry about the data security in cloud as it is shared by many of the individuals and organisations. Some times it may lead to the leakage of the data or the data may be corrupted by attackers. The following are the security issues which have to be considered for while discussing about the reduction of security risks in cloud services providers.

2.1. Data Intrusion:

The most considerable security risk that occurs with a cloud service provider is data intrusion. Some of the

hackers may gain access to accounts by hacking the passwords and they will be able to have access over the accounts and database so that they might copy the data or modify the data or even could be able to erase al the information inside any of the virtual machine instance. As cloud computing provides service that can provide a large amount of information and the computing services to each individual or an organisation. The cloud computing systems as service providers provide many services to so many customers or organisations that are not trustworthy because there might chances of occurrence of threats by various cyber attacks. So there is a need of Intrusion Detection Systems (IDSs) for the protection of virtual machines against threats and that system provides a stronger security service by using many of the rules.

2.2. Correctness of Data:

The users store the data on cloud and despite its advantages there are some security challenges has to be considered. The other security problem in cloud computing is correctness of data which can be termed as data integrity. The cloud storage server has to return the correct data and complete data .In order to solve this problem of data integrity, proof of irretrievability (POR) has to be implemented as it tries to verify a proof of data which is stored on a cloud service provider's data storage devices . I t ensures that cloud data is not modified and checks the data integrity.

2.3. Availability of the services:

The later security issue that has to be considered is service availability. The individual's web host or web service may terminate at any time if any of files has got corrupted or effected by data intrusion or data security problems then the service may be unavailable for time to time. Hence considering this as a reason the cloud computing has emerged from single cloud to multi-cloud computing (inter cloud or cloud of clouds). The cloud of clouds concept is implemented to identify the layers in the multi-cloud environment. The inner-cloud and the inter cloud are the two layers. The multi-cloud environment controls several clouds and avoids dependency on any one individual so that it can overcome of the security problem denial of service.

3. INTRUSION DETECTION SYSTEMS

This is an important component which can be implemented for protecting computer systems and network against security attacks. The main aim of IDS is to detect the attacks and provide the proper response and it is a technique that detects and responds to intrusion activities from malicious host. There are two types of IDSs, They are Host level and another is Network level.

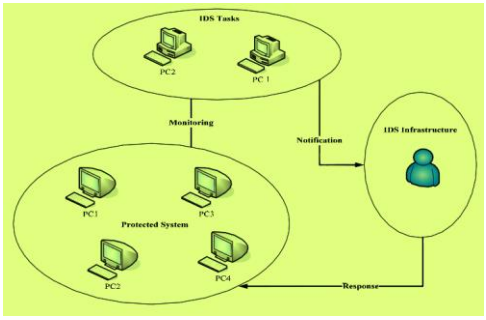

Fig2: IDS architecture

Host based intrusion detection system involves software or agent components, which is run on the server, router, switch or network appliance in detecting and responding to long term attacks such as data thieving. Network based intrusion detection systems captures network traffic packets such as TCP, UDP and IPX/SPX and analyzes the content against a set of rules, signatures to determine if a possible event took place.

4. SYSEM ARCHITECTURE

DEPSKY, a system that improves the availability, integrity and confidentiality of information stored in the cloud through the encryption, encoding and replication of the data on diverse clouds that form a cloud-of-clouds.

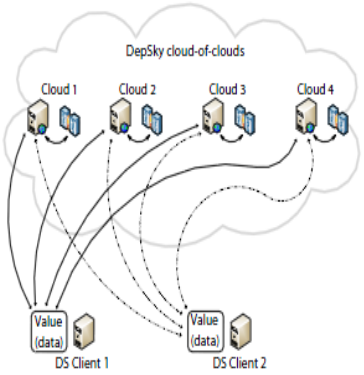

Fig3:DEPSKY architecture

DEPSKY is a virtual storage cloud which can be accessed by its users by invoking operations in several individual clouds. It is intended mainly to address some important limitations of the single cloud storage service providers. The four limitations are denial of service, data integrity and corrupted data.

DEPSKY deals with problem of denial of service attacks by attaining duplicate copy storage on multiple clouds and hence allows access to data as long as a subset of the cloud service provider is available. The correctness the data is attained by the DEPSKY system as it implements Byzantine fault-tolerant replication to store the data on different clouds and gives access to retrieve the data correctly even there is loss of data in some of the clouds. This cloud of clouds service provider system implements a scheme of secret sharing and erasure codes which avoids storing clear data in the clouds and improves the efficiency of storage.

CONCLUSION

As the usage of cloud computing has been increasing rapidly there is need of considering the security concepts in cloud computing service providers as many of the users or customers or the organisations store sensitive data on cloud. If the cloud service provider works only with a single provider then there are many security challenges has to be encountered and the customer has be worried more if there occurs some attacks on the data they have stored on the cloud. Data integrity ,data corruption ,or the unavailability of the data from the cloud service provider could arise many problems for the customers. The main aim of this paper is to ensure a work of the recent research on single cloud storage and multi cloud storage and has to overcome the security issues that are raised during the usage of single cloud storage. It could be more beneficial if the cloud computing has migrated from single cloud to multi clouds in which the DEPSKY system can overcome the limitations of the individual clouds.

REFERENCES

[1] Cloud Computing Security: From Single to Multi-Clouds Mohammed A. AlZain , Eric Pardede, Ben Soh, James A. Thom ,2012 45th Hawaii International Conference on System Sciences

[2] DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds,Alysson Bessani Miguel Correia Bruno Quaresma Fernando Andr´e Paulo Sousa University of Lisbon, Faculty of Sciences, Portugal.

[3] Towards Secure and Dependable Storage Services in Cloud Computing Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE

[4] Intrusion Tolerance: Enhancement of Safety in Cloud Computing, International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012

[5] Intrusion Detection System for Cloud Computing Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande , International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012

[6] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, “A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International

Conference on Parallel Processing Workshops, 2010.
[7] J. Mchugh, A. Christie, and J. Allen, "Defending Yourself: The Role of Intrusion Detection Systems", IEEE Software, Volume 17, Issue 5, Sep.-Oct., pp. 42-51, 2000
[8]http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf
[9]http://www.networkcomputing.com/security/the-biggest-cloud-computing-security-ris/240005337