SECURITY ISSUES IN INTER-CLOUD COMMUNICATION

[1]Er. Ishatpreet Kaur, [2]Er.Ankit Bansal, [3]Er.Khushwant Kaur, [4]Er. Kamalpreet Kaur

[1] Assistant Professor, [2] Head of the Department, [3]Assistant Professor, [4]Assistant Professor
[1]Computer Science Engineering & IT,
[1] Gulzar Group of Institutes, Khanna, India

Abstract: Cloud computing is an emerging and upcoming field of discussion and advancement in computer science. This is mainly due to its popularization in the world of computing which has happened due to its limitless applications like Gaming, education, health care, It enterprises, daily life and many more. Accessing confidential data from cloud is an issue of concern as many users at a time can have access to the same cloud. Moreover, some users accessing the cloud information can be malicious and can destroy the data stored in the clouds which makes cloud computing suspicious and less reliable to use. Users may think that it's more secure to save your data on the personal machine rather than accessing through a common cloud which is accessible to all. Keeping in mind these cons a concern is raised about the security issues in cloud communication. The two ways of accessing data from clouds are intra-cloud i.e. accessing data within the cloud and inter-cloud communication i.e. accessing data from different clouds to fulfill user requirements. Although the intra-cloud communication is secured from outside threats, there are still prevailing security risks due to the transferred data between two services could potentially be 'visible' to the cloud provider. It is possible for a malicious neighbors for instance within the same physical machine or LAN to sniff the transferred data. However, inter-cloud communication raises an even higher security risk than that in intra-Cloud communications because the transferred business data goes through multiple cloud infrastructures and the entrusted public Internet. Considering the above points a review paper on various security issues in inter-cloud communication is written in which various reasons of security threats posed to inter-cloud communication are discussed with their potential solutions.

Index Terms **- Inter-cloud computing, security, IPSec, IoT.**

I. INTRODUCTION

To address various issues concerned with the inter cloud communication we need to first understand the basic architecture of the cloud computing. According to NIST[3] the characteristics of a basic cloud to do communications are On-demand self-service, Broad network access (BNA), Resource pooling (RP), Rapid elasticity (RE), Measured service (MS) and there are 3 service models defined by NIST Software as a Service as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

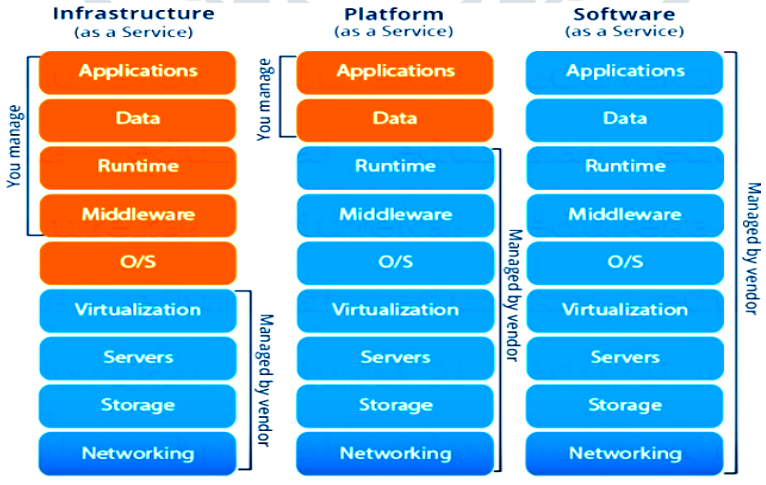

Fig. 1: Service models of cloud computing

Further, there are also four deployment models that are defined by the same Institution and these are Private cloud, Public cloud, and Hybrid cloud.

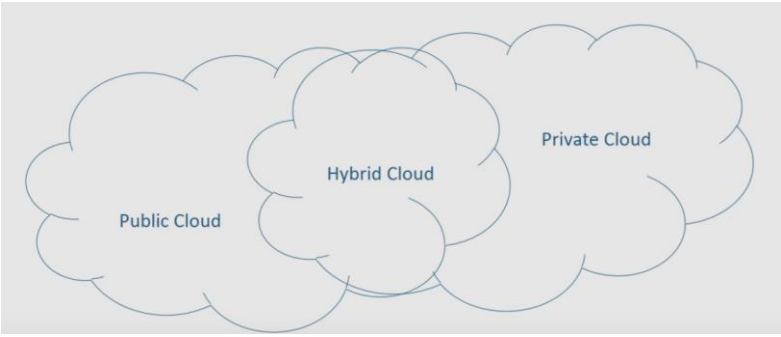

Fig. 2: Deployment models – cloud computing

Cloud entities as explained in [4] are cloud users, cloud service providers, cloud brokers and cloud resellers. The security factors due to inter cloud communications are preferred are Data integrity, Data Intrusion, Service Availability. Furthermore, the protocols used for Inter-cloud communication are Extensible Messaging and Presence Protocol (XMPP) used for basic communication, Transport Layer Security (TLS) is used for communication security over the Internet.

While discussing about the service providers of cloud computing rockspace, digital ocean, terremark, Amazon web services (AWS), Microsoft azure, joyent, vmware and Google cloud platform are some of the main service providers for cloud computing. AWS and Microsoft azure are the top 2 service providers in the industry for cloud computing. Security management areas for cloud computing as discussed in [4] are as follows: Identity Management, Credential Management, Attribute Management, Digital Policy Management, Configuration Management, Cryptographic Key Management, Metadata Management, Audit Management, SM Information Management.

II. SECURITY THREATS AND SOLUTIONS

While communicating on different clouds the data gets transferred though various untrusted paths which may lead to spoofing and sniffing of confidential data which can lead to serious issues like Denial of Service [1]. One method to prevent this is by making a hierarchy of priority of cloud computing services. In this model every cloud service provider will provide a specific service based on priority of the end user and service will be provided by different clouds even in case of data intrusion or service unavailability [6]. Due to this the acceptance of trust issue in cloud computing environment will always be maintained. For data integrity we can use cryptographic methods to prevent the integrity of data [5]. In this solution data intrusion is still a problem but with this remedy the facility of service availability is always maintained because if there is any malicious attack in one cloud then other cloud service provider will provide uninterrupted services to the end users.

Second security concern that occurs in inter-cloud communication is the leakage of the data or the data may be corrupted by attackers [6]. This issue can be overcome by reconsidering the in network communications, data is passed from the highest to the lowest layer, with each layer adding more information. Security controls exist at many layers of the TCP/IP cloud communications like Data Intrusion and Data to encrypt e-mail messages at application layer, TLS is a well-tested protocol used at transport layer that has several implementations that have been added to many applications, so it is a relatively low-risk option compared Authentication and Security Layer (SASL) is used for authentication purpose, SAML is particularly used for authentication and authorization between identity provider and service provider, RDF protocol is used for adding protection at the application layer.

Also, in many environments, network layer controls such as IPSec provides a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. However, IPSec was originally designed for trusted site to site connectivity. IPSec based VPN requires compatible hardware or software – almost always from a single vendor on each ends of the network. This is impractical for cloud environments, because cloud customers have little control to the underlying network infrastructure. This issue can be solved by developing a secure extranet service through an electronic contract. Because the electronic contract acts as a specification for not only contributions, negotiations and policies of resource services but also for configuration, it brings the benefits of establishing secure communication channels with little or no configuration effort [10].

Third security threat arises with the advancement of cloud computing when it's being collaborated with other upcoming technologies like internet of things to provide better and vast user accessibility [2]. However due to other technologies coming into picture Security and privacy will become more of an issue with the kind of ubiquitous computing we are going to have in future? Data security would be an issue on IoT side as well as on cloud side. Similarly, in terms of privacy, more concern would be there. A solution to this security threat is to store sensitive and private data in a virtual storage server located inside the user's country or trusted geographical domain and this can be a friendly country as well [8].

III. RESULTS AND DISCUSSION

In this research work the purpose to improve the security of inter-cloud communications was fulfilled by considering the various problem areas like storage and IoT. Furthermore, the possible solutions are discussed keeping in mind the key areas of security in mind. In future, research can be done on other issues in inter-cloud communications with different technology collaborations and its effect on security of inter-cloud communication. Also, a research can be carried out to see model for example Pretty Good Privacy (PGP) [6] which is commonly used Protocol for resource allocation such as storage and processing in inter-cloud environment whereas SPARQL Protocol is a query/matching service used for RDF. Few other features such as Advanced Video Coding (AVC), is one the most commonly used coding scheme for high quality video recording, compression, and distribution when data is accessed from inter-cloud communication.

IV ACKNOWLEDGMENT

I would like to extend my hearty thanks to **S**. Gurcharan Singh Chairman, GECT, Er. Gurkirat Singh General Secretary, GECT, Dr. Honey Sharma Dean Academics, Gulzar group of Institutes, Khanna and Er. Ankit Bansal, HOD Computer Science Engineering & IT, Gulzar group of Institutes, Khanna for providing an opportunity to conduct this research work. I would also like to thank my fellow colleagues who supported me in this research work.

REFERENCES

[1] Bansal A, **"Dark Side of Cloud Computing"** in International Conference on Emerging Trends in computer Science & Information Technology; ETCSIT-2011(001247) 26th feb2011, PP. (349-351)
[2] Rahul Reddy Nadikattu, 2014. Content analysis of American & Indian Comics on Instagram using Machine learning", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.2, Issue 3, pp.86-103.
[3] Bansal A, "**Improve Efficient Storage and Data Authentication in Cloud: A Review"**, International Journal of Advance Research and Innovation (ISSN 2347 – 3258) (2017)
[4] Cachin, Keidar and A. Shraer (2009). **Trusting the cloud**, acm sigact news, 40, pp. 81-86.
[5] Sikender Mohsienuddin Mohammad, "DEVOPS AUTOMATION AND AGILE METHODOLOGY ", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 3, pp.946-949, August-2017, Available at :http:// www.ijcrt.org/papers/IJCRT1133441.pdf
[6] Michael Kretzschmar, Mario Golling and Sebastian (2011). **Security Management Areas in the Inter-Cloud**. Hanigk Universität der Bundeswehr München, Institut für Technische Informatik,Werner-Heisenberg-Weg 39, 85577 Neubiberg, Germany
[7] Mohammad Aazam, Eui-Nam Huh (2014). **Inter-Cloud Architecture and Media Cloud Storage Design Considerations.** Computer Engineering Department Kyung Hee University, Suwon, South Korea
National Institute of Standards and Technology (2009). **The NIST Definition of Cloud Computing, Information Technology Laboratory.**
[8] Rahul Reddy Nadikattu. 2017. The Supremacy of Artificial intelligence and Neural Networks. International Journal of Creative Research Thoughts, Volume 5, Issue 1, 950-954.
[9] Mohammad Aazam, Imran Khan, Aymen Abdullah Alsaffar, Eui-Nam Huh (2014). **Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved**. Innovative Cloud and Security Lab, Department of Computer Engineering Kyung Hee University, Suwon, South Korea.
[10]Mukesh Kant Tripathi I, Vivek Kumar Sehga (2014). **Establishing Trust in Cloud Computing Security with the Help of Inter-Clouds.** Dept. of CSE, Jaypee University of Information Technology, Waknaghat, INDIA
[11]Vaishali Chauhan and Anil Singh (2009). **Security Pitfalls in multi-cloud computing environment.** M.Tech Student Chandigarh university, Assistant Professor Indian Institute of Technology Ropar, Department of Computer Science and Engineering.
[12]R. Thayer, N. Doraswamy, R. Glenn, (November 1998). **IP Security Document Roadmap.** IETF.
[13]Sikender Mohsienuddin Mohammad, "IMPROVE SOFTWARE QUALITY THROUGH PRACTICING DEVOPS AUTOMATION", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.251-256, March 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133482.pdf
[14]Shiping Chen and Surya (2011). **International Conference on Parallel Processing Workshops Secure Connectivity for Intra-Cloud and Inter-Cloud Communication.** Nepal Information Laboratory CSIRO ICT Centre Sydney, Australia