ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Study on Data Transmission Security Threats in Cloud

Anjali Nigam[1], Vineet Singh[2]

M. Tech Student, Dept. of Computer Science and Engineering, Amity University, Uttar Pradesh, India[1]

Assistant Professor, Dept. of Computer Science and Engineering, Amity University, Uttar Pradesh, India[2]

ABSTRACT: Associations must be aggressive in today's quick paced, online and profoundly interconnected worldwide economy. So they should be fast, adaptable and ready to react quickly to the dynamic business sector situations. Cloud computing gives this profoundly versatile and flexible processing that is accessible on interest. It permits a clever and keen utilization of a gathering of uses, data and framework constituted of pools of PC, system and capacity assets. Cloud computing offers many advantages for the associations. In the same way, there are numerous security issues, as with any new model or innovation. Security is one of the key factors which upset the development of cloud computing. This paper recognizes security threats with special focus data transmission threats with some approaches to resolve them.

KEYWORDS- Cloud Computing; Security; Data Transmission; Security Threats; Open Security.

I. INTRODUCTION

Cloud computing is the deliverance of on-demand computing resources on a pay-for-use basis over the Internet. It furnishes clients with various capacities to store and process their information in third party data centers. It depends on sharing of assets to accomplish solidity and economies of different sizes. Cloud assets are not only shared by a small number of customers but also dynamically reallocated on interest. With cloud computing, numerous clients can access a single server to recuperate and update their information without having to buy licenses for a variety of applications [1]. Cloud computing grants associations to get their applications up and about and work speedily, with less upkeep and enhanced manageability. It also permits IT organizations to all the more quickly adjust assets to deal with dynamic and irregular business requests. Cloud suppliers commonly utilize a pay as you go model. The present handiness of high-capacity systems, low priced computers and storage devices and also the far-flung mixture of hardware virtualization, service-oriented architecture and involuntary and utility computing have prompted the enlargement of cloud computing. Enterprises can scale up or scale down as their computing needs increases or decreases. Figure 1 below depicts some of the benefits provided to customers by cloud computing.

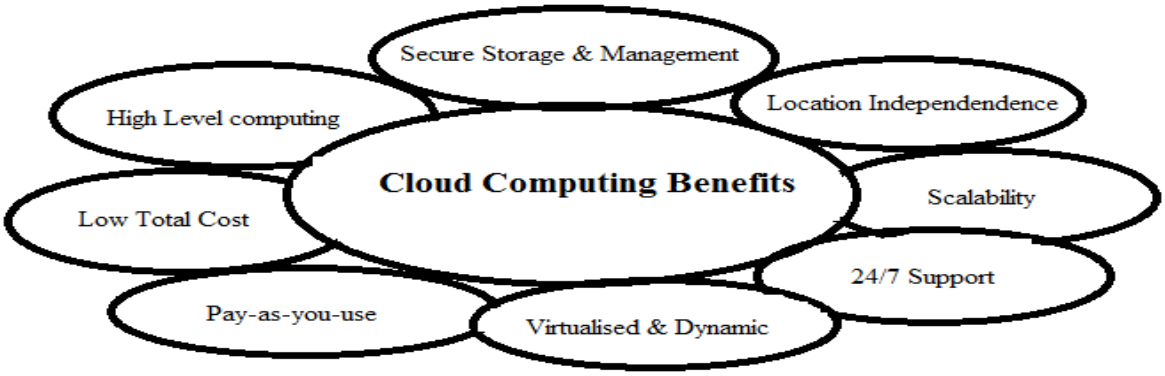

Fig. 1: Cloud Computing Benefits

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

II. DEPLOYMENT MODELS

There are four types of cloud computing deployment models which are described below [12]. A figure is also shown to illustrate the deployment models.

A. *Private cloud*

In this, the cloud infrastructure is operated solely for a single enterprise. It is managed and hosted either internally or by a third-party.

B. Public cloud

In this, the services are delivered over a network that is assailable for public use. Public cloud services may be free. There may be little or no difference between public and private cloud architecture. But security conditions are by a long way different for services that are presented by a service provider to public.

C. Hybrid cloud

This cloud is constituted with two or more clouds (private, community or public) that stay distinguishable entities but are bonded together, providing the profits of various deployment models.

D. Community Cloud

A community cloud is shared among two or more enterprises that have related cloud necessities.

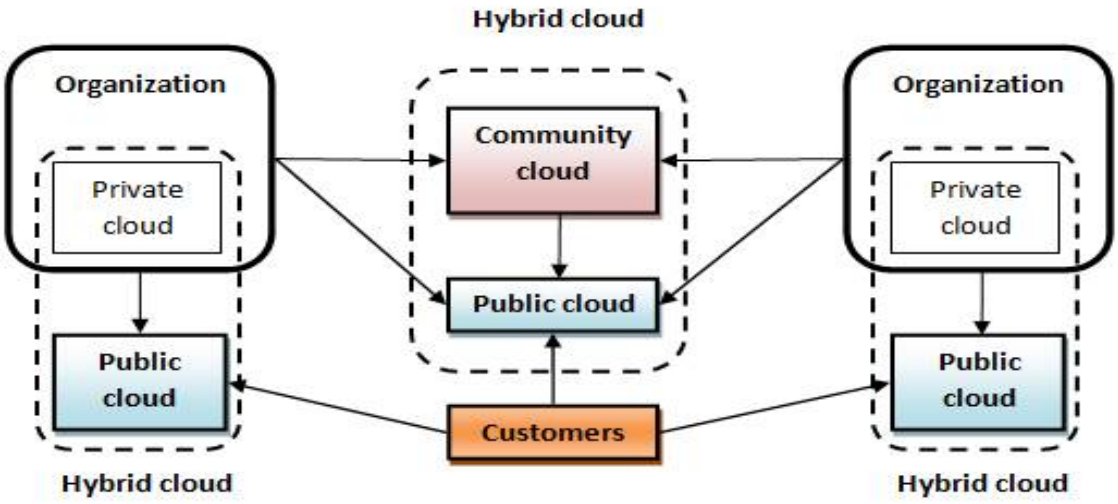

Fig. 2: Cloud Computing Deployment Models

III. CLOUD COMPUTING OPEN SECURITY

Mutum and Anita [2] expressed a few sorts of security threats present in cloud computing. They are as follows:

A. *Data Storage Security*

In cloud computing, information is put away on cloud and not possessed privately. Along these lines, accuracy and accessibility of information must be ensured. One of the key issues is to recognize unapproved data alteration and corruption. Confirmation of right data storage must be led without knowledge of entire information. Storage correctness along with dynamic data update is of paramount significance [7].

B. *Data Transmission Security*

Internet is the correspondence system for cloud clients to exchange their information. An imperative part of cloud computing is to give secure and effective transmission of information.

Some threats trading off data transmission security are given underneath:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

- Cross Site Scripting (XSS): script executes in victims' browsers to steal client sessions, destroy sites, present worms, etc [8].
- Injection Flaws: the information sent by the clients to a web application is not appropriately accepted, which can influence an inquisition on the server.
- Malicious File Execution: as the record can carry a malicious script, any framework which acknowledges a document from the client is powerless against this threat.
- XML corrupt: XML movement amid the server and the program is harmed and tainted.
- Insecure Cryptographic Storage: web applications which don't utilize encryption techniques to ensure information transmission become susceptible to an attack.
- Insecure Communication: failure of encrypting network traffic can lead to an attack.

C. Application Security

It is the process of utilizing software, hardware, and procedural techniques to guard applications from external dangers. Security is turning into an undeniably imperative alarm throughout development. This is because applications are regularly being accessed over networks and are helpless against a wide assortment of threats [9]. The requirements for securing applications should include privacy in multitenant atmosphere, data insurance from publicity, access control, communication protection, software security and service accessibility.

D. *Security on Cloud Integrity*

Information Integrity implies shielding information from unapproved cancellation, alteration or manufacture. To deal with an entity's permission and rights, the organization ought to ensure that important information and administrations are not abused or stole. Integrity preserving techniques renders greater visibility into figuring out whom or what could adjust information or framework data. Information could be encrypted to give privacy. Still there is no way of getting insurance that the information is not being altered while it occupies the cloud.

A cloud computing supplier is trusted to keep up information integrity and accuracy. They are believed to make sure of the reliability and correct operation of the cloud system in support of its legal duties and technical standards. This allows them to react fleetly from intrusions and assaults such that mischief and the times of service outages are insignificant.

E. Security identified with Third-Party

A Trusted Third Party (TTP) is an entity which encourages safe and sound communications between two gatherings. The duties of a TTP involve giving end-to-end security administrations which must be adaptable and surveying all basic exchange correspondences between the clients. The foundation and the confirmation of a trust relationship between two executing parties should be finished up as a consequence of particular acknowledgments, procedures and systems. A Trusted Third Party is a fair-minded association conveying business certainty, through business and specialized security elements, to an electronic exchange. It supplies in fact and lawfully solid method for completing, encouraging, delivering free proof. Its administrations are given and guaranteed by specialized, lawful, monetary and/or auxiliary means [10]. The information and applications being held by an outsider are complex; there is additionally a potential absence of control and straightforwardness when an outsider holds the information.

IV. SECURING DATA TRANSMISSION

The information correspondence amid the user and cloud server goes through the arrangement, where it can be tainted. Priyanka and Sugata [11] expressed that malicious flooding paths needs to be attended by setting a boundary for each route. The limit of the route is defined by the number of packets it can transfer [3]. To make safe the transmission encryption algorithms i.e. public key and private key encryption are used along with spread spectrum modulation [4]. By utilizing Wired Equivalent Privacy (WEP), SSID for every access point and MAC address filtering wireless transmission can be secured [5].

A. *Tunneling*

The idea of tunneling can be utilized to protect the information in the middle of communication. The packet intended for the cloud server can be bound with a packet containing the address of a different node. When the packets reach this node it will be redirected to the server by the node. This encapsulation stops the assailant to follow down packets meant for the server. As a result it minimizes their likelihood of getting hacked [6].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

B. Utilization of Virtual Circuits

The IP packets when exchanged as datagrams throughout the network take the most model way. While doing so, they may pass through a router which might have been assaulted by an assailant. In such scenarios, the packets can be followed down and misused by the assailant. To prevent this attack a virtual circuit can be executed for routing the datagrams. In this tactic, the server during the connection establishment phase presets a route, which the data packets oblige to take after. This path is in the course of approved routers. By following this way information can be secured. However, it might come up unsuccessful if a router on the path is not working.

V. CONCLUSION AND FUTURE WORK

It is important to consider protection and anonymity when utilizing and planning for cloud computing services. In this paper, figure 1 and figure 2 illustrates the benefits of cloud computing and deployment models of cloud respectively. The emphasis is given on the security issues present in cloud computing. Security threats like data storage security, data transmission security, application security, security on cloud integrity and security identified with third-party assets are talked about. Methodologies such as tunneling and utilization of virtual circuits for securing data transmission in cloud are additionally said in this paper. Cloud environment is a huge help to the IT world and also to singular customers. However, in the event that the efforts to establish safety are lacking then the whole framework's idea will fall flat. That is why all conceivable approaches to build the security ought to be considered. Cloud developers are constantly trying to develop novel and trouble-free methods to secure the information in cloud especially when they are being transmitted between the client and the server. Several works on creating new cryptographic algorithms that will provide better security from the existing techniques are also in progress.

REFERENCES

1. Zaigham Mahmood, “Data Location and Security Issues in Cloud Computing”, International Conference on Emerging Intelligent Data and Web Technologies, 978-0-7695-4456-4/11, 2011.
2. Mutum Zico Meetei and Anita Goel, ‘Security Issues in Cloud Computing’, 5th International Conference on Bio-Medical Engineering and Informatics, 978-1-4673-1184-7, 2012.
3. J. Kataria, P. S. Dhekne and S. Sanyal, ‘A Scheme to Control Flooding of Fake Route Requests in Adhoc Networks’, International Conference on Computers and Devices for Communications, CODEC-06, 2006.
4. S. Sanyal , R. Bhadauria and C. Ghosh, ‘Secure Communication in Cognitive Radio’, International Conference on Computers and Devices for Communications, CODEC-2009, 2009.
5. D. P. Agrawal1, H. Deng, R. Poosarla and S Sanyal, ‘Secure Mobile Computing’, Distributed Computing –IWDC 2003, Springer Berlin/ Heidelberg, pp. 265-278, 2003.
6. R. Bhadauria, R. Chaki, N. Chaki and S. Sanyal, ‘A Survey on Security Issues in Cloud Computing’, arxiv.org, arXiv: 1204.0764, 2012.
7. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, ‘Enabling public verifiability and data dynamics for storage security in cloud computing’, in Proc. of ESORICS'09, Saint Malo, France, Sep. 2009.
8. P. Saripalli, and B. Walters, ‘QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security’, IEEE 3rd Intl. Conf. on Cloud Computing; Miami, FL, July, 2010.
9. D. Zissis, D. Lekkas, ‘Addressing cloud computing security issues’, Future Generation Computer Systems, 1--10, 2010.
10. K.P. Saripalli, N.M Mahasenan, and E.M Cook, ‘Risk and hazard assessment for projects involving the geological sequestration of CO2’, In: Gale, J. and Y. Kaya (eds.) Sixth International Greenhouse Gas Control Conference, Kyoto, Japan, pp. 285–289, Elsevier Ltd. 2003.
11. Priyanka Naik and Sugata Sanyal, ‘Increasing Security in Cloud Environment’.
12. Huaglory Tianfield, “Security Issues In Cloud Computing”, IEEE International Conference on Systems, Man, and Cybernetics- October 14-17, COEX, Seoul, Korea, 2012.