International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 7, ISSN No. 2455-2143, Pages 156-158
Published Online May - June 2016 in IJEAST (http://www.ijeast.com)

INFORMATION ASSURANCE AND SYSTEM SECURITY IN CLOUD COMPUTING

Brahm Prakash Dahiya
Ph. D. Scholar, CSE Department,
I.K. Gujral Punjab Technical University,
Jalandhar, India

Balkar Singh
Ph. D. Scholar, CSE Department,
Thapar University,
Patiala India

***Abstract*— Cloud Computing is most emerging Technology that is used by Information Technology Industry Now a days. It is easily used by the peoples who are having internet facilities in their Computers. The service availing is either pay or free services. Generally used deployment models of Cloud Computing are Public based, Private based, and Community based and most important is Hybrid based. The major problems of information assurance and system security is arising with public based cloud computing. The major security issues facing while working with public based cloud computing is confidentiality of the data, quality assurance of the availability of data online detection of faults attached with data and online recovery of available data. Thus, it's upon the people how to use cloud computing, when to use cloud computing and various circumstances for using cloud computing. This paper provides an overview of various facilities of Cloud Computing and their major challenges based on public based cloud computing. It also discusses major challenges facing by various cloud providers and their users. The paper enhances some security measures and solutions based on public based cloud computing.**

Keywords—**Cloud Computing; Public based Cloud Computing; Challenges; Online Detection; Cloud Providers; Security Measures.**

I. INTRODUCTION

In Computer Industry, Cloud Computing is an important way through which Computer Networks can send their data from source computer to destination computers [1]. Cloud Computing is totally a computer based networking method which is widely used for data communication. We know about various types of cloud are – Private, Public, Hybrid, Community and Distributed cloud. As we know with the help of cloud computing network, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications [2]. This facility is when used in Public Cloud Computing then it creates a major problem of Security of the data. So, this paper is focused on the major security issues based on Public cloud Computing.

By public cloud we mean a service which is available to the public openly and with proper benefit [3]. When any service is available publically then the security of the service and data both are affected. We already know public clouds are only be used by the peoples via internet. Internet services are available in the form of connection oriented and connectionless to the users. Public cloud providers provide services in all types of cloud services.

II. LITERATURE REVIEW AND PROBLEM FORMULATION

Now days, Internet becomes an important part of our daily life. Everybody uses internet for their personal, professional and commercial purposes [4]. Peoples used to keep their personal data, professional data and commercial data as attachments in their e-mail accounts or somewhere else but keeping online available so that it must be easily available at the time of need. Public cloud is a most general way which is used by big companies to facilitate various services to their users. So, their arises the need of security in public cloud. We are already using some methods like Encryption, Decryption or some application based protection in our software's but the main problem arises when any service is available publically like e-mail, facebook or any other social services then how to keep our data secure [5].

The solution for this question is we are providing security to our application, architecture, infrastructure, data or information's in four levels of security in public cloud. This will be in the form of the following forms:

1) Design based security in cloud computing
2) Application based security in cloud computing
3) Service based security in cloud computing
4) User level security in cloud computing

1) **Design based security in cloud computing**: This means the security will be available in the architecture level. We design the architecture in such a way that various devices be deployed which will maintain security at the entry level of the data or information. This will happens in the form of filtering the data with the help of algorithms and it's design architecture. It provides the security by filtering the operations

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 7, ISSN No. 2455-2143, Pages 156-158
Published Online May - June 2016 in IJEAST (http://www.ijeast.com)

like reading, writing, modifying or updating the data or information online. Generally, if we are providing security through devices and algorithms at the entry level of the data or information then it will reduce the chance of hacking at little extent in cloud computing [6].

2) Application based security in cloud computing: when any user enters in their application, first it must be verified that whether it is a valid user or not. Afterwards, when the user works in the software the data will be in alphanumeric but internally it will be represented in come converted form like ciphers or some symbols or some signs etc so the data will be managed internally in converted form. This helps us when any outsider hacked our data our information then first the data will come in converted form and providing security answers the data will come in the original form. Another solution to security option at application site is we develop an interface in the application to punch the thumb expression of the user as security because now touch screen mobile are widely used by the peoples and this lead to a drastic change and provides convenient security at application's end [7].

3) Service based security in cloud computing: This will be provided by the service providers of cloud computing like SaaS, PaaS, and IaaS. This is achieved by using special protocols which are designed for providing services to the users, customers, workstations, clients etc. The new protocol first checked the authenticity of the user, reliability of the service and acceptability of the request. In this way the cloud service providers provides value aided services to their users [8].

4) User level security in cloud computing: This security provides a ease to the user at end level while using the software. Users have an interface to give various security options at the time of working in the software like passwords, block any paragraph, and hide the content, encryption and decryption within the software etc at the time of normal working of the software. We will see in all software's user security is maintain with username and password but inspired of that in cloud applications it is maintain through thumb expression [8].

III. TYPES OF CLOUD PROVIDERS

In cloud computing the types of cloud providers are as follows : Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) [9].

1) **Software-as-a-Service (SaaS)** *:* This type of service is based on software used in cloud computing and the facilities provided to them.It's the responsibility of the administrator to update and modify the services which are existing and update according to the requirements or demands of the users.This service is important because it is the backbone of the cloud computing [10].

2) **Platform as a Service (PaaS)** : This type of service is mainly used in social sites by the companies who are working in this field.It is also used by some search engines which is working online in the world of Internet.The users also have controled in the existing softwares based on applications deployed by the users or some settings related with environment [11].

3) **Infrastructure as a Service (IaaS)** : This can be visualised by using various devices,components and resources which are deployed using various algorithms so that it can be used in the cloud architecture.This is changing by application to application used by the users in the internet [12].

IV. MAJOR ISSUES OF SECURITY

At the time of working by the important cloud providers the problem faces are as follows [13]:

1. **Geographical location of the stored data** : As we know about the cloud computing it is used publically so the data is in the form of signals, audio, videos or images and anybody can be easily used it for their operations [13].

2. **Access to data**: Data can be accessed with any place and from anywhere across the world and the security is maintained through thumb expression of the user. Administrators are there to look after the control and management of the accessibility [14].

3. **Agreement**: Service level agreement is needed to look after the services which are required at first party's end and Third party's end [15].

4. **Issues**: Issues are the major concern for the services because it is used by mass of the users at very esteemed companies and organizations [16].

5. **Granted Authentication & Granted Authorization**: Generally the authorization is given by the service providers and the members of the service provider companies. Once it is assured then the authorization is easily provided to the users [17].

V. SOLUTION PROPOSED AND IMPLEMENTATION

When we are using cloud computing either in social sites or in mobile technology we have to provide top level security with the services because in the coming time hackers can use every type of algorithms and actions to hack the service and data. To protect them from hacking we have to use user's thumb expression in every services which are used currently by the users and for this we have to embed some micro chips in the existing devices which protects from hacking and ensure our data to be protected.

VI. CONCLUSION AND FUTURE SCOPE

The main conclusion from this paper is we are using four levels of security in the cloud computing so that it is more secure in the based of software, service and infrastructure which will be implemented for all types of services used in cloud computing with the help of algorithms and deployment of various models in the architecture used by the companies which are working in the field of various services available in the social sites. In future, four levels of security which is proposed by me is implemented in the models of networking. The security proposed is of type design based, application based, service based and user level security in the field of cloud computing. Most important is the implementation of thumb expression in the application and software level so that it is highly secured while use.

VII. REFERENCE

[1] B. Corona, M. Nakano, H. Pérez, "Adaptive Watermarking Algorithm for Binary Image Watermarks", *Lecture Notes in Computer Science, Springer, pp. 207-215, 2004*.

[2] Jansen Wayne Grance Timothy Guidelines on Security and Privacy in Public Cloud Computing NIST Special Publication 800-144

[3] Kumar Ashish **,** World of Cloud Computing & Security , International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.2, June 2012, pp. 53-58.

[4] S.Hemachander Harikrishna, R.Backiyalakshmi, "A Game Theory Modal Based On Cloud Computing For Public Cloud", IOSR Journal of Computer Engineering, Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014).

[5] R. W. Lucky, "Cloud computing", IEEE Journal of Spectrum, Vol. 46, No. 5, May 2009, pages 27-45. [4]. M. D. Dikaiakos, G. Pallis, D. Katsa, P. Mehra, and A. Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research", IEEE Journal of Internet Computing, Vol. 13, No.5, September/October 2009, pages 10-13.

[6] http://www.isaca.org/groups/professionalenglish/cloudcomputing/groupdocuments/essential%20characteristics%20of%20cloud%20computing.pdf .

[7] T.R.V. Anandharajan, Dr. M.A. Bhagyaveni" Co-operative Scheduled Energy Aware Load-Balancing technique for an Efficient Computational Cloud" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011.

[8] Wayne Jansen Timothy Grance" Guidelines on Security and Privacy in Public Cloud Computing" NIST Draft Special Publication 800-144.

[9] B. P. Rima, E. Choi, and I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems", Proceedings of 5th IEEE International Joint Conference on INC, IMS and IDC, Seoul, Korea, August 2009, pages 44-51

[10] A. M. Alakeel, "A Guide to dynamic Load balancing in Distributed Computer Systems", International Journal of Computer Science and Network Security (IJCSNS), Vol. 10, No. 6, June 2010, pages 153-160.

[11] C.Kishor Kumar Reddy, P.R Anisha, K.Srinivasulu Reddy, S.Surender Reddy, IOSR Journal of Computer Engineering (IOSRJCE) ,ISSN: 2278-0661 Volume 2, Issue 1 (July-Aug. 2012), PP 39-46.

[12] http://www.ukessays.com/essays/informationtechnology/implementating-distributed-load-balancing-algorithms-informationtechnology-essay.php

[13] Ali M. Alakeel, A Guide to Dynamic Load Balancing in Distributed Computer Systems, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010.

[14] Zhong Xu, Rong Huang,(2009)"Performance Study of Load Balanacing Algorithms in Distributed Web Server Systems", CS213 Parallel and Distributed Processing Project Report.

[15] P.Warstein, H.Situ and Z.Huang(2010), "Load balancing in a cluster computer" In proceeding of the seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE.

[16] Y. Fang, F. Wang, and J. Ge, "A Task Scheduling Algorithm Based on Load Balancing in Cloud Computing", Web Information Systems and Mining, Lecture Notes in Computer Science, Vol. 6318, 2010, pages 271-277.Zhong

[17] Xu, Rong Huang,(2009)"Performance Study of Load Balanacing Algorithms in Distributed Web Server Systems", CS213 Parallel and Distributed Processing Project Report.