A review on cloud computing security and Privacy

Neha Sehgal , Amninder Kaur

Abstract— For the internet based routing cloud computing is a systematic based architecture. Cloud computing is use to store the data online on the social network sites or e-mail instead of keeping that data on your personal computer. The problem which was faced during cloud computing is data accessed using various resources needs user authentication and access control model for integrated management and control in cloud that environments. The main issue is security and integrity of data in cloud computing. Due to the internal & external attack of security & integrity security checks should be taken. Like one time password which give us security.

Index Terms - Cloud Computing, One time password, Security, Integrity.

I. INTRODUCTION

Cloud Computing is storing of information on web. Cloud computing permit Any human being & organization who can utilize programming that are handle by the outsider. Examples of cloud admin take from online record, Person-to-Person communication, Webmail, Online Business application.

Cloud computing model gain access to data & computer machines from anywhere. Cloud computing introduce a combined pool of machines, information storage a space, system, computer handling power etc. Only purchasing of computers is not enough but you should have also good equipments & programming or programming license. But this is very costly.

1.2 CHARACTERISTICS OF CLOUD COMPUTING

The major quality of cloud computing take on-demand self-service, resource pooling, wide network, fast flexibility & measured services. On-demand self services shows that client can deals with their own resources.Broad network access allows to be offered over the Internet or private systems. A pooled resource tells that client draw from a pool of processing resources. Services can be bigger & also can be smaller. The charges of an client is measured & charged according to that.

Manuscript received June, 2015.

Neha Sehgal*, Computer Science and Engineering, Punjabi University., mohali, india.*

Amninder Kaur*, Computer Science and Engineering, Punjabi University, Mohali, India.*

1.3 TYPES OF CLOUDS

There are four types of clouds

A. Public Cloud – Public cloud is that an open kind of cloud which can be got to be any supporter with a web association and to access the space of cloud.

B. Private Cloud – Private cloud is a secure type of cloud for a particular type of gathering & limits.

C. Community Cloud – Community cloud is that kind of cloud which is imparted among two or more group.

D. Hybrid Cloud – Hybrid cloud is that kind of cloud a blend of no less than two mists, where the mists included are a mixture of open, private, or group [6].

1.4 DEPLOYMENT MODELS

A. Private cloud: Private cloud is that type of cloud which is only used for a single organization, which can be managed internally or by externally. Private cloud need a significant level of engagement. It require organization to re evaluate decision about the existing resources. If it is right than it improves our business but the major problem occurred during this that is security.

B. Public cloud: Public Cloud is that kind of cloud when the access of the services is over the whole network. it is publically used by anyone. There is a little bit difference between private & public cloud architecture.

C. Hybrid cloud: Hybrid network is a composition of of more than two cloud i.e private & public. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

1.5 SPECIFIC SECURITY ISSUES PRETAIN TO FOLLOWING SERVICE MODELS

The cloud computing administration models are:

A. Software as a Service (SAAS):- This is a method for conveying application over the internet. Instead of presenting and caring for programming, one simply get to it through the Internet, freeing yourself from complex programming and equipment administration. SAAS applications are occasionally called Web-based programming, on-interest programming, or encouraged programming. Whatever the name, SAAS applications continue running on a SAAS supplier's servers. The supplier oversees access to the application, including security, openness, and execution.

ISSN: 2278 – 1323

B. Platform as an administration (PAAS):- Platform as an administration (PAAS) is a distributed computing model that conveys applications over the Internet. In a PAAS model, a cloud supplier passes on equipment and programming gadgets ordinarily those needed for application progression to its customers as an organization. A PAAS supplier has the equipment and programming in its own particular framework. As needs be, PAAS frees customers from expecting to acquaint inside equipment and programming with make or run another application. PAAS does not usually supplant a business. Maybe, a business relies on upon PAAS suppliers for key organizations, for instance, Java progression or application encouraging.

C. Infrastructure as a service (IAAS):- Infrastructure as a service (IAAS) is a sort of distributed computing in which an untouchable supplier has host pictured figuring assets over the Internet. Framework as an administration (IAAS) is a sort of distributed computing that gives virtualized preparing assets over the Internet. IAAS is one of three essential classes of distributed computing organizations, i.e. Programming as a Service (SAAS) and Platform as a Service (PAAS). In an IAAS model, a pariah supplier has equipment, programming, servers, stockpiling and other establishment parts for its customers. IAAS suppliers moreover host customers' applications and handle errands including framework support, reinforcement and arranging.

1.6 CLOUD COMPUTING SECURITY CHALLENGES

A. With same base Business, government, or administrative information n Cloud administration models are required.

B. Data versatility and lawful issues with respect to such government leads as the EU Data Privacy Directive n Lack of norms about how cloud administration suppliers safely reuse disk space and erase existing information

C. Auditing, reporting, and consistence concerns.

D. Loss of perceive ability to key security and operational learning that never again is open to support organization IT security understanding and danger administration.

II. LITERATURE REVIEW

RuWei Huang et.al [1] according to this paper main problem of cloud security is privacy and encryption is only one way which protect the confidential information but it also has some limitations. Authors of this paper try to remove that limitation by designing their privacy preserving cloud storage framework. They design a key derivation algorithm which manages the keys and possible combination of symmetric and asymmetric encryption schemes. They applied bloom filter for cipher text retrieval and also measure the performance with bloom filter.

Sabahi, F. et al [2] proposes that from last few years cloud computing become a major part of technology but on the other side it also have some critical issues such as data stored at remote side should be stored at secure location. Author discuss that it is better to save information on individual system rather than on cloud because that information can be stored at any place. So author discusses reliability, availability and security issues of cloud and also gave some solution to solve some of the few discussed problems.

Jianfeng Yang et. al [3] discussed that cloud computing is fusion of various computing like grid computing, parallel computing and distributed computing etc and objective of cloud computing is to build a system with powerful computing capabilities in low cost. In this paper author discussed various issues like security, privacy, reliability and various model of cloud computing like IAAS, SAAS and PAAS.

Mohamed, E.M. et al [4] proposes that data management in cloud computing may not be fully trustable and due to this new security challenges arises. Author discussed that cloud have single service but different number of clients due to which they have various different demands and cloud use encryption to secure their data. Author of this paper proposed software to improve the data security and apply that software in Amazon EC2 Micro instance.

Du Meng et al [5] discussed security issues, secure data transmission, data management and security etc. author of this paper discussed various strategies and long term direction towards success and also gave some solution to some of the issues.

Chaoqun Yu et. Al [6] discussed various applications of cloud computing and also discussed some important technical issues such as data encryption, access control, integrity authentication etc.

Deyan Chen et. Al [7] discussed that due to advancement in technology all organizations adapting cloud computing but still large organizations would not able to move to cloud. Because cloud still have data security and privacy issues due to large and complexity of data. This paper provide a small review n data security and its issues in cloud computing. Author of this paper also gave some current solutions and describe future work to make reliable cloud computing.

Yun Wang et .al [8] discussed that in previous work there is no criteria of weighting in multi-authority attribute-based encryption in cloud computing. Author of this paper propose a ides of weight into multi authority base encryption scheme. Analyses of this technique show that this e secure and suitable way than existing approaches.

Somani, U. et al [9] discussed that cloud is solution to various problems like resource, distributed computing, scalability etc. But cloud security is still a major issue. In this paper author gave a new concept of digital signature and RSA algorithm for cloud security.

ISSN: 2278 – 1323

III. TECHNIQUE'S USED

The fundamental key to data security is to protect what matters.

Solutions that enable companies to confidently transition to the cloud while still leveraging many of their traditional infra structure and investments offer significant advantages.

Vormetric Data Security solves the enterprise cloud security conundrum by protecting data inside the operating environment while establishing security policies and maintaining control through a centralized management interface. One key differentiator is that Vormetric works with cloud providers and enterprises to protect data regardless of whether it is located in physical, virtual, or cloud environments. This architecture enables enterprises to control access to the data self, even as the virtual machine migrates to the virtual and cloud world.

SSL (Secure Socket Layer) Encryption: Encryption between browser and web server. It usually provides enough security from the workstation to the browser. The use of SSL does not require Cloud service provider for any functionality. It is all in how you have defined your website. It is easy available as it is very inexpensive. All Cloud customers should require encrypted communication. Optical fiber is another tool, since fibers are harder to manipulate than electrical cables.

VPN (Virtual Private Network): VPNs are most commonly used for home based or mobile applications. When users connect to the internet from home or any public place like airport, hotel etc., then he will be signed into his VPN and get secure communication. Many Cloud providers offer VPNs to cover the area from the work station in user facility to user connection to the internet and across the internet.

IPSec (Internet Protocol Security): IPSec is a prominent appearance of VPN, usually used between facilities where there is a large amount of traffic. In the case of Cloud, Cloud service provider will define and usually facilitate the IPSec device to install user network where it connects to the internet and to facilitate high speed encryption and decryption without keeping workload on servers.

A proper use of encryption can give good protection against eaves dropping. Traffic analysis is harder, but on the other hand, not only that many need protection against this kind of threat. A proper use of encryption can give good protection against active attacks. In order to protect against man-in-the middle attacks, one should observe if there are any delayed response times, in order to detect if there is any "Middle Man".

IV. CONCLUSION

Approach	Advantages	Dis-advantages
One-time password	**This is short-lived OTP values, which are desirable for enhanced security.**	Strong authentication systems address is the limitations of static passwords by incorporating an additional security credential,
SSL (Secure Socket Layer) Encryption	This is very secure & very inexpensive. You can also use optical fiber.	Fibers are harder to manipulate than electrical cables.
VPN (Virtual Private Network)	it allows remote users to securely access the enterprise's systems	This is most commonly used for home based or mobile applications.
IPSec (Internet Protocol Security)	Thanks to the flexibility of the Internet Protocol, IP sec has become a popular international standard, making it easier to maintain, and it is more secure as well.	Disadvantages of IPSec is CPU Overhead Compatibility Issues

REFERENCES

[1]. RuWei Huang *"Research on Privacy-Preserving Cloud Storage Framework Supporting Cipher text Retrieval",* published in International Conference on Network Computing and Information Security (NCIS), volume 1, pp 93-97, IEEE 14-15 May2011.

[2]. Sabahi, F. "*Cloud computing security threats and responses*" published in IEEE 3ed International Conference on Communication Software and Networks (ICCSN), pp 245-249, 27-29May 2011.

[3]. Jianfeng Yang ; "*Cloud Computing Research and Security Issues*" published in International Conference on Computational Intelligence and Software Engineering (CiSE), pp 1-3, 10-12 Dec. 2010.

[4]. Mohamed, E.M. ; Abdelkader, H.S. ; El-Etriby, S. "*Enhanced data security model for cloud computing*" published in 8th International Conference on Informatics and Systems (INFOS), pp 12-17, IEEE 14-16 May 2012.

[5]. Du Meng Data security in cloud computing published in 8th International Conference on Computer Science & Education (ICCSE), pp 810-813, IEEE 26-28 April 2013.

[6]. Chaoqun Yu ; Lin Yang ; Yuan Liu ; Xiangyang Luo Research on data security issues of cloud computing published in International Conference on Cyberspace Technology (CCT 2014), pp 1-6, IEEE 8-10 Nov. 2014.

ISSN: 2278 – 1323

[7]. Deyan Chen ; Hong Zhao "*Data Security and Privacy Protection Issues in Cloud Computing*" published in International Conference on Computer Science and Electronics Engineering (ICCSEE), volume 1, pp 647-651, IEEE 23-25 March 2012.

[8]. Yun Wang ; Dalei Zhang ; Hong Zhong "Multi-authority based weighted attribute encryption scheme in cloud computing" published in 10th International Conference on *Natural Computation (ICNC)*, pp 1033-1038, IEEE 21aug 2104.

[9]. Padilha, R. ; Pedone, F. "Confidentiality in the Cloud" published in International Conference on *Security and Privacy*, Issue 1, volume 13, pp 57-60, feb,2015.

[10]. Somani, U. ; Lakhani, K. ; Mundra, M. "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing" published in 1st International Conference on *Parallel Distributed and Grid Computing (PDGC)*, pp 211-216, oct,2010,

Neha Sehgal M. Tech (Computer Science and Engineering) Punjabi University, P.U.R.C.I.T.M, Mohali, India.

Amninder Kaur (Computer Science and Engineering) Punjabi University, P.U.R.C.I.T.M, Mohali, India.

ISSN: 2278 – 1323