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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Survey on Trust and Security Issues in Cloud Computing

Neha Karade[1], Prof. Neha Khare[2]

Research Scholar, Department of Computer Science & Engineering, RGPV University, Takshshila Institute of Engineering & Technology, Jabalpur, M.P India[1]

Assistant Professor, Department of Computer Science &Engineering, RGPV University, Takshshila Institute of Engineering & Technology, Jabalpur, M.P India[2]

ABSTRACT: Cloud computing is the use of computing resources that are shared as services over the internet. Even though its popularity, it faces many hurdle. One of the primary concerns is data security. To overcome this, some security mechanisms are used. Among them cryptography is advantageous because even if the data is accessed without authorization it is not readable. This paper aims to provide a general survey about major cryptographic mechanisms used in cloud is conventional symmetric and asymmetric algorithms, quantum cryptography. Cloud computing is the growing technology. Each organization wants to connect to the cloud computing environment. But some of them resist connecting due to security issues. Various security factors had been raised, some also lead to include third party auditor for solving security issues. Another major factor in concern is the Trust on the cloud service provider's i.e., the level to which an organization can trust the cloud service provider for handling their company's data.

I. INTRODUCTION

Cloud computing is the growing technology. It provides on- demand services to user and also provides access to shared resources. The cloud model is composed of five essential characteristics, three service models and four deployment models. Cloud provides various services such as IaaS, PaaS, and SaaS. It can be deployed at different level i.e. at public, private, hybrid and community cloud. With the technology and services ease new security issues arises. Data on cloud are stored on various physical machines which are unknown from user. Thus their data are at risk. Many security attacks have been developed to acquire knowledge of data. So, some security measures need to be taken to protect user's data. Third party auditing is also done for data protection. The markets are expanding and many vendors are coming up with the similar functionalities. The users are concerned with their data storage location and by whom their data can be accessed. The user cannot easily trust the cloud service provider. Therefore trust management is the important factor which arises in this field.

II. BACKGROUND

In cloud computing, concept of data outsourcing is widely used. Outsourcing means contracts out of a business process to another party. Outsourcing involves transform of data from one organization to another. As users uses cloud computing technology and store their data somewhere on cloud. The vendor who is providing these storage services might not have enough space to store the whole requested space. So, the vendor will contract to other organization to store their data.

So, the user's data is now outsourced to some other firm. Before outsourcing, the whole responsibility of data and employees was with the single organization itself. But with outsourcing took place, single organization was not responsible. This results into security issues. This is one of the most complex issue and required third party auditor to come into play.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Cryptographic cloud was used to enhance the security in the cloud computing environment. It provides strong cryptographic nature as opposed to legal, physical and access control mechanisms. The concept of cryptographic cloud is that the data is control and maintained by the user while security of data is derived from cryptography [10]. To protect data on the cloud several methods have been used. This may be access control method which includes authentication and authorization. But these are generally weak to protect data. Another may be using cryptography and uses encrypt data. It offers better solution for protecting data. Several encryption technique and algorithms has been used.

As data being outsourced, one client data is stores on the same resource where other client's data has been stored. So if one client's data is compromised so there are chances of the other client's data to be compromised. Encryption is one of the security solutions. Although clients still feels insecure as they don't know which other client also has the same measures in place. One solution is to use different encryption keys for each individual client; however it is dependent on the service provider.

III. REVIEW

Several papers were published in the area. The various papers were studied. A paper about cloud computing trust [1] stated that many research has been done on technical aspect but not much work has been done towards trust factor related to consumers. This paper examines the issues surrounding towards the difficulty of the internet users to trust cloud service providers. This has been done by doing consumer feedback survey and then suggestions has been given to cloud service provider.

It stated that if security is not handled properly, the entire area of cloud computing would fail since cloud computing mainly involves managing personal sensitive information in a public network. Consumer feedback survey has been done on the basis of following objectives i.e. is there a consumer lack of trust with cloud service provider or is there a way for cloud service providers to earn consumers trust.[1]

A Reputation Management system was made for cloud and sensor networks integration [2] and it stated that trust is very important factor while using cloud services. User data may be at risk as it is stored somewhere on the cloud which the user is not aware of. This paper proposed how to calculate and mange the trust and reputation regarding the service of cloud service provider and it also helps cloud users to choose from different cloud providers available. It considers various parameters required to calculate trust. [2]

A paper [3] stated that the mutual trust and protection is necessary while using cloud services. The paper defines that the customers should force the cloud service provider to provide them authentication to their data. It is based on reverse access control model. The cloud service provider ensures the policy that client should not violate with respect to security of the cloud environment. Here cloud architecture for mutual protection and vector matrix were proposed. [3]

A paper [4] stated that trust can be quantified based on few concepts of trust mechanism. They proposed a synthesize trust degree evaluating model by using direct trust degree, indirect trust degree, trust weight, trust attenuation and specifically quantified the evaluation parameters. This paper focused on more evaluation of the external behaviour rather than that of internal evaluation for the trust value. The use of different trust domain was fixed.

The paper uses different trust degree which can be stated that the level of trust between the entities that can be quantified and quantitative value can be discrete and continuous according to the situation. Direct trust degree can be stated as the level of confidence of an entity on another under the direct contact drawn from historical records in a given context. Indirect trust degree can be defined as the trust between entities formed through a third party recommendation which is essentially an indirect reputation. So overall trust degree can be defines as the weighted sum of direct and indirect trust. [4]

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Paper [5] mainly discusses on the user view on trust and evaluates it. Different strategies were proposed for calculating user view for trust. The paper reveals that user does not have full control over their data which make them mistrust the cloud services. The user has fear of their data loss, data misused and many other risks. [5]

A trusted computing platform [6] stated that the cloud computing is supported with the trust. The trust factor plays very important role. Cloud computing is based on this trust
Module. The author discusses authentication, data access and protection of data in cloud. This paper proposed an integrated

Trusted computing platform into cloud computing system. It focuses mainly on confidentiality, dynamic services, trust among the cloud service provider and user and dynamically building trust domains. [6]

A paper on flexible data access control [7] stated that storing data on cloud releases burden from user to maintain it. But due to distrust on cloud service providers and for the sake of security of data users do not easily access cloud services instead they store their data in an encrypted form. This data was not easily accessible by all the other applications. Some application do need to access data for example- eHealthService. Therefore trust plays important role in data sharing. In this paper, a scheme was proposed to control data access in cloud computing and evaluate trust by using Attribute-based encryption and Proxy re-encryption technique. [7]

A paper [8] stated that the most challenging issue for the growth of cloud computing was the trust management. Data privacy and security was an important aspect. Because of dynamic nature of cloud environment trust management was very challenging. The Cloud Armor was implemented in this paper. It is a trust based reputation model for providing trust based service. [8]

A paper on workflow applications in cloud computing [9] stated that workflow technique has been used in cloud computing to make effective services. There are workflow scheduling algorithms which focuses on execution time and cost of cloud services. But it is not free from threats and attacks so a trust service oriented model was required. This paper proposed a trust service-oriented workflow scheduling algorithm. This algorithm works to calculate trust metric and provides policies to enable users to select from different services available according to requirements. [9]

A table is made providing various such research work done with the methods proposed with its advantages and disadvantages. Analyzing this table we can conclude that trust factor is very important for using cloud computing services through any vendor.

Table 1

S. no	Methods		Pros	Cons
1	An architecture for mutual protection in cloud computing was proposed and based on concept of mutual trust.	2010	It deals with authentication and authorization based on Concept of mutuality.	It is not yet implemented and the profile and vector method used was not accepted by any international Standard.
2	The trust degree evaluation method was proposed for trust calculation	2010	Trust degree was calculated using various trust factors such as direct trust and indirect trust	Not other attributes were considered.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

3	An integrated trusted computing platform was Introduced.	2010	In this trusted computing technology was extended	It was hardware and platform based.
4	A multi-faceted trust management system architecture was proposed for cloud computing. This system provides means to identify the trustworthy cloud providers in terms of different attributes.	2011	Trust weight was calculated to determine the trusted cloud service provider.	Generally SLA was considered as a whole contract between user and cloud service provider. But users were not satisfied with it
5	A trust service scheduling was proposed. This algorithm works to calculate trust metric and provides policies to enable users to select from different services available.	2014	The results show the approach was effective and feasible and user can select workflow services from various cloud services.	It was difficult to deal with dynamic changes in cloud computing environment.
6	The design and implementation of cloud Armor was done. It was a trust based reputation model for providing trust as a service.	2015	Several techniques have been displayed detecting attacks.	Not much accurate results were obtained.
7	Security and trust was provided to user using consumer	2015	Trust management was introduced.	It considers only user feedback. Other parameters were not considered.
8	A scheme was proposed to control data access and evaluate trust by using attribute based encryption and proxy Techniques.	2016	A framework was made for securing cloud computing by applying different algorithm. The cloud services can be secured automatically as the cryptographic keys were generated based on trust model.	Cryptographically stored data sometimes creates problem as some other common application might need to access the Data.

IV. CONCLUSION

The study suggested that trust is very crucial factor in the development of cloud computing technology. Many trust and reputation models were proposed and were analyzed in this paper. A table was prepared with the researches done in this field with the methods proposed with its pros and cons. This shows future development in the field of trust management system in cloud computing.

REFERENCES

[1] Albert S. Horvath III and Rajeev Agrawal, "Trust in Cloud Computing" Proceedings of the IEEE Southeast Con - Fort Lauderdale, Florida, April 9 - 12, 2015.
[2] Chunsheng Zhu and Hasen Nicanfar, "A Trust and Reputation Management System forCloud and Sensor Networks Integration", pp.557- 562, IEEE ICC-Ad-hoc and Sensor Networking Symposium,2014.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

[3] Aiiad Albeshri1 and William Caelli,"Mutual Protection in a Cloud Computing Environment", pp.641-646,12th IEEE International Conference on High Performance Computing and Communications, Brisbane, Australia,2010.
[4] Ma Li and Zhang yongmei, "A Synthesize Trust Degree Evaluation Method in Distributed System",pp.5186-5190, Proceedings of the 8thWorld Congress on Intelligent Control and Automation, Jinan, China, July 6-9 2010.
[5] Tian Li-Qin and LIN Chuang, "Evaluation of User Behavior Trust in Cloud Computing",volume-7,pp.v7-567-v7-572, 2010 International Conference on Computer Application and System Modeling, Beijing East, China, ICCASM 2010.
[6] Zhidong Shen, Li Li, Fei Yan and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform",pp.942-945, International Conference on Intelligent Computation Technology and Automation, Wuhan, China, 2010.
[7] Zheng Yan, Xueyun Li, Mingjun Wang and Athanasios V. Vasilakos, "Flexible Data Access Control based on Trust and Reputation in Cloud Computing", IEEE Transactions on Cloud Computing, 2015.
[8] Talal H. Noor, Quan Z. Sheng, Lina Yao, Schahram Dustdar and Anne H.H. Ngu, "CloudArmor: Supporting Reputation-based Trust Management for Cloud Services", IEEE Transactions on Parallel and Distributed Systems, 2015.
[9] WenAn Tan, Yong Sun, Ling Xia Li, GuangZhen Lu, and Tong Wang, "A Trust Service-Oriented Scheduling Model for Workflow Applications in Cloud Computing",pp.868 -878, IEEE SYSTEMS JOURNAL, VOL. 8, NO. 3, SEPTEMBER 2014.
[10] Akansha Deshmukh, HArneet Kaur Janda and Sayalee Bhusari, "Security on cloud using Cryptography", vol.5, issue 3, IJARCSSE, March 2015.