IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. 1 (May – Jun. 2015), PP 66-70
www.iosrjournals.org

Analyzing and Surveying Trust In Cloud Computing Environment

Kavita Rathi[1,] Sudesh Kumari[2.]
Assistant Professor, CSE Department,
Deenbandhu Chhotu Ram University of Science & Technology, Murthal.
Student, M.Tech(CSE),
Deenbandhu Chhotu Ram University of Science & Technology, Murthal.

Abstract: *Cloud computing is the most discussed research area now-a-days which helps to provide elasticity and flexibility in using the computing resources and services to fulfill the requirement of current businesses. Besides many advantages offered by cloud computing, it deals with many obstacles in the path of its growth, that are security issues, data privacy issues and distrust on cloud service providers (CSP). Trust is found to be an essential element for achieving security and confidence in the use of distributed computing. Various issues like data control, ownership, data integrity and security can be considered as important parameters of trust. This paper addresses the existing trust models for trust establishment in cloud services and also tries to find out the shortcomings of these models.*

Keywords- *Trust, Issues of Trust, Trust Models, User Based Trust Models.*

I. Introduction

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources (network, server, storage, application and services) that can rapidly provisioned and released with minimum management effort or service provider interaction[1]-[3]. It comes up with several advantages in distributed computing environments and operates on a virtualized and "pay-as-you-go" economic model [4], it also brings various challenges in its adoption. Trust is found to be one of the major challenges in the adoption of cloud computing as distrust prevents the consumers from its wide use and distrust comes out most because consumers do not have a direct control over their data lying on the cloud. This is the reason why evaluation of trust is critical. Trust has many dimensions, multiple faces and is also multidisciplinary and hence it is very difficult to give a proper definition to it. This paper is organized in the sections as described. The first section presents the theory for the need of trust in the cloud services, followed by the sections focusing on trust issues and existing trust models along with their shortcomings in trust establishment.

II. Need Of Trust

Trust is a social problem, not a purely technical issue [5]. Trust is viewed as a measurable belief that utilizes experience to make trustworthy decisions [6]. The cloud service users (CSU) always have to keep trust on the cloud service providers (CSP) and the CSPs have to keep trust on the CSUs for a healthy establishment of cloud services. In the cloud computing scenarios the CSUs give all their digital resources in the hands of the CSPs and the CSPs hold direct control over almost all the security factors. This is the reason why a CSP has to confer a proper level of trust to the cloud service users. The component of trust is an essential element in the wide use and implementation of cloud services. The relationship of trust is established between the two parties which are stated as trustor and trustee. The trustor is the person or entity who holds confidence, belief, reliability, integrity and ability, etc. of another person or thing which is the object of trust, i.e. the trustee [7]. As per the previous study, following trust characteristics are found:-

- **Trustor and Trustee**[8]

The trust relation is formed by the trustor that is the trusting party and the trustee that is the party which is to be trusted. The development of trust is based on the ability of the trustee to act in the best interest of the trustor and degree of trust that the trustor places on the trustee [8].

- **Susceptible to attack**

Trust is found to be important in the computing environments where there are more possibilities of risk, data losses, vulnerabilities and uncertainty. Due to this reason trust is important in cloud computing environments. A trustor depends on the trustee for not exploiting and misusing his vulnerabilities.

- **Produced actions**[8]

Trust between the trustor and trustee leads to various behavioral changes in the actions of the CSUs. Trust allows the CSUs to take risk and allow their private data to be shared on the cloud. It may also allow the CSUs to continue the use of services of the cloud on a regular basis.

- **Subjective Nature**

Trust is subjective and every individual or enterprise has their own opinions towards the follow up of any technology. Hence there are different requirements of every CSU to judge the trust level of a particular CSP.

III. Trust Issues

There are many aspects of trust in the cloud computing environment based on the CSPs view and the CSUs view. Trust is very important for building relationships between CSUs and CSPs. There are several issues of trust which are categorized by considering following factors:-

- How can trust be defined and evaluated in the cloud computing scenarios.
- How malicious information can be handled in temporary and dynamic cloud relationships.
- How to consider and provide different security levels according to trust degree [6].
- How to manage trust degree change with temporary and dynamic relationships [6].

As per the researchers Ankush Dhiman, Mauli Joshi, Wayne A. Jansen, several trust issues are found, a few are stated below:-

1. Access by Insiders: All the data of the CSUs is stored to the data centers of the CSPs and then the storing and processing of data depends purely on the service providers. The employees of the service providers could see and process the data as they want and there is always high risk of data access by insiders. They could make changes or modifications to the data. Denial of service attack, and creation of 20 account and instance to each account launched a Virtual machine for each and again process continued, to set the resource beyond the limit are some special cases of the malicious insider attack[3]. It is one of the examples of such attacks studied in the Amazon Elastic Compute Cloud (EC2)[3].

2. Nesting of Services: This issue includes the use of two or more CSPs. This means that a software as a service provider uses the services of platform as a service provider and platform as a service provider uses another infrastructure as a service provider. In this way, there are multiple levels of hiring and renting the services in a cloud. Liability and performance guarantees are the serious issues that come into account with the composite cloud services [1][3]. An example of such type is LinkUp which is an online storage service which leaded to the loss of access to the significant data of its 20,000 customers [1][3]. It happened because another company named Nirvanix hosted the data for LinkUp and another company named Savvis hosted the application and database for Nirvanix [1][3]. In these situations there is no provider to take responsibility for losses of data and hence this becomes one of the major issues of establishing trust on third party distributers of the cloud services.

3. Degree of Exposure: This issue deals with the level of visibility provided by the CSPs to the CSUs. The detailed network and system, network and storage level monitoring should be implemented for gaining visibility into the security controls and processes employed by the CSP along with their performance over time [3].

4. Risk: Assessing and managing risk in systems using cloud services is again a challenge to be taken. Sometimes consumers are ready to take risk if the control over processes and equipment is towards their end. But in case of cloud services the scenario changes as the control varies. The trust is based on the amount of direct control that any organization is capable of applying on the CSP's with regard to the security employed for the protection of services [3]. Verifying the correct functioning of the system along with the security controls is an important aspect of establishing trust in the cloud services [3]. Risk management and assessment must be detailed and should be done properly in a cloud based implementation.

IV. Trust Models In Cloud

Trust is the most complex relationship among entities, because it is subjective and difficult to be evaluated [9]. Trust models are considered as a methodology that helps to evaluate trust on the CSP's or the third party distributers that are providing the cloud services. Trust models in Cloud computing are very diverse in a way that each model supports different features and evaluates Cloud services on the basis of different parameters and requirements [10].

Figure 1[11] states the various trust models that have been proposed based on the functionality of their evaluation criteria among different levels of services provided by the cloud computing environments.

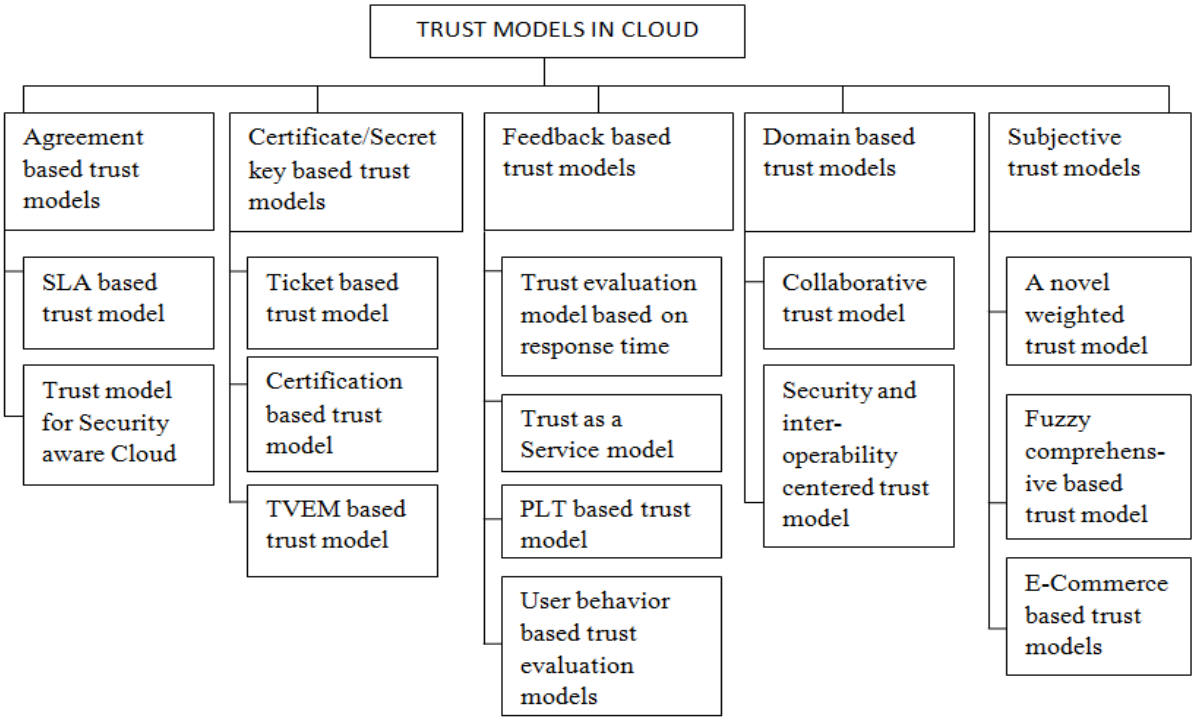

Figure1 [11]. Trust Models in Cloud Computing

Abbreviations used in Figure1 denote the following:-
SLA: Service Level Agreement
TVEM: Trusted Virtual Environment Module
PLT: Prepositional Logic Terms

There are various trust models that can be seen in the diagram stated above. Out of these this paper focuses on the study of user behavior based trust models as basically when we think of trust it is only about the consumer trusting the CSP but it is equally important to judge the user for its trustworthiness for using the cloud services. In cloud computing, due to users directly use and operate the software and operating system, so the impact and destruction for the software and hardware cloud resources are worse than the current internet users who use it to share resources [12]. This makes it important to check the user for its reliability to provide access to the use of cloud resources and also keep track of the fact that the feedback comes out from correct and authenticated group of CSUs. Trust is found to be two way which deals with trust from both the CSUs on CSPs and vice versa.
Some of the reasons that lead to distrust in the use of cloud services are:-

- Risk of data leaks.
- Security risks of stored data location.
- Risk of data to be investigated.
- Interruptions in cloud services.
- Risk of data damage.
- Risk of collapse of the CSP.

These reasons focus on the trust of the CSU on the CSP. Though the consumers trust the CSPs for their work, it does not ensure the safety of data as the consumer may also be malicious. It is very important to detect such kind of CSUs and not allow them to use the cloud services. They could make fake identifications and be in the cloud and put some malicious data to the cloud which could lead to the blockage of various cloud services to other CSUs. The possible reasons leading to user behavior mistrust are [14]:-

- Destructive behavior by individuals towards their business counterparts or commercial competitors or some persons.
- Damage to the cloud resources consisting of software services, platform services, infrastructure and hardware services by the errors caused by users or in configurations.
- Detection of malicious code or software in the cloud.

- Errors in the authentication and identification of users.

Whatever is the reason of mistrust in CSU, there must be proper monitoring by the CSP on the behavior of CSUs so that it could be ensured that the cloud services are only used by the trustworthy users. Cloud computing model brings some new security threats such as resource sharing, fate sharing, and data lock in [13]. These risks are sources of concern for users and prevent them from using cloud computing [13]. Due to these kinds of risks, the CSPs have to keep concern for the CSUs to provide them with a trustworthy cloud environment. Several researchers have given many elements of trust that are useful in identifying the CSUs' trust in the use of cloud services. As formulated in [13]-[16], following trust elements of CSUs are compiled as given below:-

- **Location of stored data:** In the cloud environments, data can be stored anywhere and the CSUs are not aware of the physical location of data which is a concern of trust.

- **Data to be investigated:** The data is shared and stored at different locations hence it becomes very difficult to convince the CSUs against any unnecessary action to be taken on their data by anyone.

- **Sharing of data:** How the data is distributed over the cloud and how it is protected is a major concern for the CSUs.

- **Availability of Services:** The cloud services must be available to the CSUs whenever they want and they must be available round the clock.

- **Long-term Viability:** CSUs want their data to be available and viable to them for long and hence they want that the CSP must not go down and nothing wrong should happen to their data. Ideally, cloud computing provider should never go broke or get acquired by a larger company. But user must be assured about the data will remain available even after such an event [13]."

- **Compliance regulation and audit:** Compliance includes correspondence of the appearance of the constitute specifications, standards and Law [6]. These laws, rules and regulations for security and privacy differ from location to location [6]. Each country, state, local bodies have their own rules and regulation. So the compliance is one of the most important issues in cloud computing [6].

- **Back up of data and Recovery:** A CSP must have the techniques to recover data losses in case of any disaster or any other circumstance that may lead to loss of data.

- **Access privileges to the Users:** CSPs must have a proper mechanism to assign the access privileges to different kinds of users in the cloud data center and access control of data must be civilized and authenticated.

- **Governance:** The cloud resources are spread and shared all over the globe and hence it is very important to decide the protocols and governing body of the CSPs is working independent of the political conditions of a particular country.

- **Transparency:** The CSP should display the relevant information about its policies and conditions for using the cloud services and these should be transparent to the CSUs through a proper design of its web interface and graphics. Also the CSPs must communicate with the CSUs through video conferencing or other communication media while assigning the resources to a CSU. The transparent way of customer dealing by a CSP will help the CSP to gain more user confidence and trust.

These are some of the major trust elements that are useful for the CSUs to evaluate trust of the CSPs. The CSPs that provide more information about all these elements are found to be trustworthy and their services are considered to be used by more CSUs. Only the trust of the CSP is not enough but the trust of the CSU is equally important for a healthy cloud computing environment. From [12] and [14] the basic principles for evaluation of user trust are found to be as stated below:-

- **Effect of Expired User:** The user that is not using the cloud for a long time and is very old is not considered for evaluating trust of the user behavior.

- **Evaluation of trust based on records:** The recent records of behavior of user in using cloud services are considered to be more fruitful as compared to the older records. If the user is accessing its own domain and has a behavior which is predictable is considered less useful and important in evaluating the trust of user. On the other hand, if the user has a unpredictable and unusual access to cloud resources, this record makes more influence in evaluating the user trust.

- **Repetitive access to cloud resources by user:** If the user accesses the cloud resources less frequently then it is difficult to evaluate its behavior, while more user access gives more significant results to predict its behavior whether user is trustworthy or not.

- **Actions based on analysis:** There must be proper strategies to punish the non-trustful behaviors. On analyzing the behavior of users whether found to be trustful the a trust value assigned is higher and user is found to be trustworthy to continue with the cloud services and if the trust value is found lower than some standard value defined then the user has to be discontinued from the cloud services and also must be blocked for future.

The models in [13],[14],[15],[16] are found to be missing transparency as a trust element and also they are basically theory based which do not provide some parameters to calculate the trust values for the user trust evaluation. The model in [14] is policy based and evaluates the user behavior based on the login of the users and its response become slower when registered users increase in number. Another limitation is found to be the fact that if user access is less and not repetitive then the result shown is not representative and stable.

V. Conclusion And Future Work

This paper gives an overview of the various trust issues and trust models. The main focus is on the users' trust based models which describe the importance of trustworthy users as well as trustworthy CSPs for a healthy cloud computing environment. The main trust elements are found as data backup and recovery, storage location of data, availability of services and transparency. Most of the models are found to be ignoring transparency and regular updates to users regarding any changes towards CSPs' end as elements of user trust. Most models that exist, focus on the trustworthiness of the cloud service providers and less work is done towards the evaluation of checking out the trustworthiness of the user who is using the cloud services. Lot of research is possible in this direction in future.

References

[1]. Ankush Dhiman, Mauli Joshi, "Analysis of Performance for Data Center under for Private Cloud through Cloud Computing", International Journal of Engineering and Computer Science(IIECS) issn:2319-7242, vol.3 Issue 6, Page. 6422-6431, June 2014.

[2]. Hong Cai, Ning Wang, Ming Jun Zhou, "A Transparent Approach of Enabling SaaS Multi-tenancy in the Cloud", IEEE 6th World Congress on Services, 2010.

[3]. Wayne A. Jansen, NIST, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences, 2011.

[4]. Michael Armbrust, Armando Fox, et al., "A view of Cloud Computing", Communications of the ACM, vol. 53, April 2010.

[5]. Kai Hwang, Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, 2010.

[6]. Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", Advanced in Control Engineering and Information Science, Procedia Engineering 15, page. 2852-2856, 2011.

[7]. Yashashree Bendale, Seema Shah, "Feasibility of User Level Trust in Cloud Computing", UACEE International Journal of Computer Science and its Applications, vol.2 : issue2[ISSN 2250-3765].

[8]. Felix Meixner, Ricardo Buettner, "Trust as an Integral Part for Success of Cloud Computing", ICIW 2012: The Seventh International Conference on Internet and Web Applications and Services, 2012.

[9]. Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Modeling and Evaluation of Trust in Cloud Computing Environments", 3rd International Conference on Advanced Computer Control (ICACC), 2011.

[10]. Xiaoyong Li, Junping Du, "Adaptive and Attribute based Trust model for service-level agreement guarantee in cloud computing", IET Information Security, 2012.

[11]. Ayesha Kanwal, Rahat Masood, Um E Ghazia, Muhammad Awais Shibli and Abdul Ghafoor Abbasi, "Assessment Criteria for Trust Models in Cloud Computing", IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 2013.

[12]. Tian Li-qin, LIN Chuang, Ni Yang, "Evaluation of User Behavior Trust in Cloud Computing", 2010 International Conference on Computer Application and System Modeling (ICCASM 2010).

[13]. Ahmad Rashidi and Naser Movahhedinia, "A model for User Trust in Cloud Computing", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol. 2, No.2, April 2012.

[14]. Yashashree Bendale, Seema Shah, "User Level Trust Evaluation in Cloud Computing", International Journal of Computer Applications, Vol. 69-No.24, May 2013.

[15]. Shakeel Ahmad, Basir Ahmad, Sheikh Muhammad Saqib and Rashid Muhammad Khattak, "Trust Model: Cloud's Provider and Cloud's User", International Journal of Advanced Science and Technology, Vol. 44, July 2012.

[16]. EY Building trust in the Cloud, Insights on governance, risk and compliance, June 2014.