Secured Trust Model in Cloud Computing-A Review

Vani S. Reshmi
Department of Computer Science and Engineering
Basaveshwar Engineering College (Autonomus)
Bagalkot, India

Praveen S. Challagidad
Department of Computer Science and Engineering
Basaveshwar Engineering College (Autonomus)
Bagalkot, India

***Abstract*— Nowadays number of people who outsource their data to the cloud has been increased dramatically. Cloud computing offers cost-effective dynamic, scalable and shared services for enterprises from remote data centre. However, the problem of trusting cloud computing is a highest concern for most enterprises in such a way that trust is extensively in esteem as one of the highest barrier for the acceptance and expansion of cloud computing. So there is a need of trust model which help cloud consumers to find the provider that best satisfies their trust concerns in cloud computing by measuring the trustworthiness of cloud service providers.**

Keywords*— *Cloud Computing; Security; Trust; Trust Evaluation

I. INTRODUCTION

Cloud Computing provides a means by which one can access the applications as utilities, over the Internet. It lets customer to configure, customize, and create applications online. Cloud computing is a new computing paradigm that provides infrastructures, platforms and software as a service in a flexible and on-demand way.

The word Cloud is used to indicate a Network or Internet. That is to say, something that is fetched from remote location is Cloud. It aims to utilize computer resources and to deliver them as services with a high performance at reduced costs.

Cloud Computing directs to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application as in figure 1.

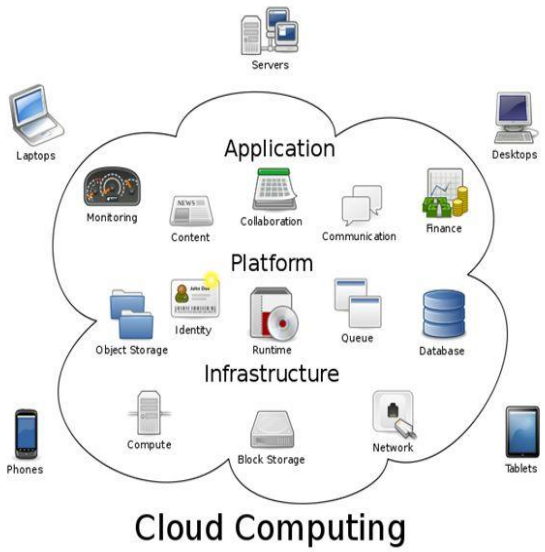

Figure1. Cloud Computing Environment

There are assured services and models working behind the scene making the cloud computing practicable and accessible to end users. Following are the working models for cloud computing:

- Deployment Models
- Service Models

A. Deployment Models

Public cloud: In this deployment model, computing resources are owned, operated and governed by an academic, business, governmental organization, or a group of them. These resources are provided for the public use such as, a single cloud service consumer, an academic, business, governmental organization, or a group of these different cloud service consumers. Transactions in this model are considered business to consumer.

Private cloud: In this deployment model, computing resources are owned, operated and governed by an academic, business, governmental organization, or a group of them. These resources are provided for the same organization e.g. governmental organization, which consists of several consumers. Transactions in this model are considered business to business.

Community cloud: In this deployment model, computing resources are owned, operated and governed by one or many organizations, known as a community of organizations. These resources are provided for a community of organizations to fulfill a certain objective, such as higher performance. Transactions in this model are considered business to business

Hybrid cloud: In this deployment model, computing resources are tied together by different clouds' deployment models, e.g. public and private clouds, by the use of portable mechanisms. These computing resources are provided by two or more of the above deployment models, known as hybrid deployment.

B . Service Modules

Service Models are the suggestion models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

There are numerous other service models all of which can take the form like XaaS, i.e., Anything as a Service. The Infrastructure as a Service (IaaS) is the most basic level of service. Each of the service models makes use of the core service model, i.e., each inherits the security and management mechanism from the underlying model, as shown in the following figure 2:

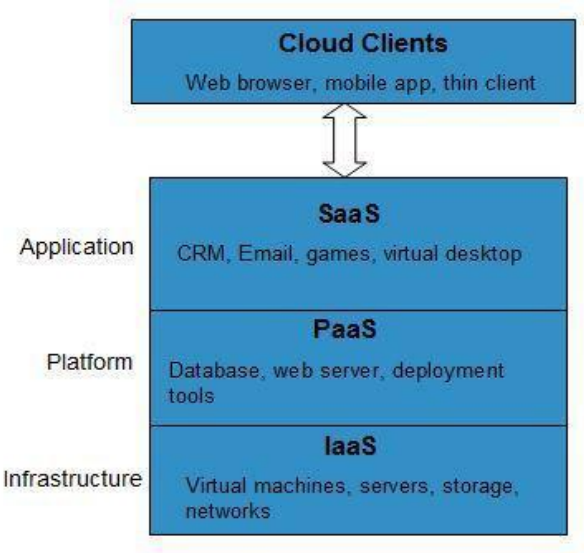

Figure 2. Service Models

Software as a Service: This model demonstrates the application part of the cloud environment and lays above the PaaS to uphold the required remote accessibility. Cloud service providers supply applications for cloud service consumers to access their data remotely that is stored in the underlying cloud infrastructure (e.g., Google Docs & Windows live Mesh). Whereas, the cloud service consumer has no control over this underlying infrastructure such as storage network, or operating systems, they can still control their data.

• Platform as a Service: This model performs the integration part of the cloud environment and lays above the IaaS layer in order to support system integration and virtualization middleware. In PaaS cloud service providers supply software development tools and programming languages (e.g., Google App) for cloud service consumers to develop their own software. On the other hand, cloud service consumers have no control over the underlying cloud infrastructure, but they can control the deployed applications.

• Infrastructure as a Service: This model illustrates the foundation part of the cloud environment. IaaS allows cloud service consumers to rent storage, processing and communication. This is performed through virtual machines that are provided by cloud service providers (e.g., Amazon's Elastic Compute Cloud (EC2) & Simple storage Service S3).

In IaaS, cloud service providers control and manage the underlying cloud environment. On the other hand, cloud service conswners can control their virtual machine such as storage, processing and network.

II. TRUST IN CLOUD COMPUTING

"Trust is renowned as an necessary element of every social transaction but it can be scarcely found in any written contract and is even less likely to be imposed. Trust escapes rational judgment yet everybody seems to be expert in judging trust. Trust is what happens between people or communities, is not easily quant able, takes time and effort to put up and can be easily lost. It's a belief in competence or expertise of other's such that you feel you can rely on others to care for your assets". From technology perspective, trust has always been associated with reliability and Security. The purpose of trusted computing is to crack some of the present security problems through hardware changes to personal computer. Trust is a fundamental empowering factor in association there is uncertainty, interdependence, risk, and fear of opportunism. Trust can be defined as a mental state which consists of expectancy, belief and willingness to take risk. Trust is used for the identification of entity's identity and the confidence on its behaviors. Trust is prejudiced behavior since entity's decision is typically based on its personal experiences. Trust is depicted by trust value. Trust value or trust degree is pre-owned to compute the degree of trust. Trust value a lot relays on special time and special context. Two types of trust are direct trust and indirect trust. Direct trust means trust that is gained by entities' direct interaction. Indirect trust or recommended trust revenue trust that is obtained from credible third party who has direct touch with the designated one. Recommended trust is one of the significant ways to obtain trust degree of unidentified entities.

A. *Featurse of trust*

The main features of Trust are as follows:

* Subjective, uncertainty and fuzzy. Trust pertains to personal mindset or experience and it is not attached to particular boundary.

* Asymmetry. If two entities say A and B have to set trust association, A's estimated trust for B can be diverse from B for A.

* Faithlessness and context-sensitive. Trust will get revolutionized along with particular time and particular context.

* Condition based transitivity. A's trust value for B is not always the same to the recommended trust that is gained from C.

B. *Challenging issues for Trust*

1) Identification: It is very significant that trust management system resourcefully identifies cloud service providers to evaluate their services and cloud service consumers, to refine their feedbacks.

2) Privacy: During interactions in the cloud environment some privacy violations could occur via seep out of the cloud service consumers confidential information or behavioral information.

3) Security: As cloud computing environment has dynamic and distributed nature, it is tricky to recognize from where an molest raised.

4) Dependability: To what extent the cloud service could be dependable and under which conditions.

5) Highly dynamic: Due to the huge no of available cloud services and their consumer's mostly in a highly dynamic manner, new cloud services could launch or others may stop. Cloud consumers may join the cloud, while others may depart from the cloud environment at any time.

6) Scalability: The deployed software by cloud service providers should be able to adapt to changes in work loads by increasing or decreasing the number of its components and by expanding or freeing its computing resources .

7) Integration: Is the ability to integrate various trust management techniques and from different perspectives of participants. Thus, also integrating feedbacks of cloud service consumers.

8) Non-transparent nature: Cloud consumers and providers may initially interact together without any prior experience. Both of which may lack the knowledge of the underneath cloud infrastructure.

9) Distributed environment Since the cloud resources, service providers and consumers are distributed among different locations, feedback collection remain a great challenge.

10) Poor recognition of feedbacks: This could direct to inaccurate trust evaluation consequences.

11) Weak Service Level Agreement: Traditional Service Level Agreements could not cover all features for complex cloud environment. The ambiguous statements and indistinct technological specifications of SLAs usually prevent cloud service consumers from easily identifying trustworthy and suitable cloud services.

C. Trust Evaluation Attributes

A Trust that is used to measure the truthfulness of cloud services based on the following attributes:

1) Data Integrity: It is a wide term that includes data security, privacy and accuracy.

2) Security: Cloud service providers should protect their consumer's personal information and ensure them, that their data are safely addressed.

3) Privacy: Refers to the degree of sensitive information reveal of cloud service consumers during their interactions with the cloud service providers.

4) Credibility: Measures the quality of service supplied by cloud service providers to cloud service consumers.

5) Tumarround efficiency: This includes the actual turnarround time and the promised turnarround time. The actual turnarround time, is the time taken from the start of a cloud consumer application for a task and the delivery of this task. Whereas, the promised turnarround time, is the duration of the task completion expected by the cloud service provider.

6) Availability: Refers to the degree of availability and accessibility of cloud service provider resources, components or services.

7) Reliability: Is the ability of a cloud service provider to perform the agreed upon functions under the specified conditions and duration. It is also referred as the success rate.

8) Adaptability: This imposes the availability of data storage and processing in a redundant manner to overcome single point of failure times. This requires the installation of a backup software .

9) Service level agreement: SLA should clearly specify technical and functional descriptions required from a cloud service provider. Complying to this agreement would increase cloud service provider trustworthiness.

10) User feedback: Refers to the cloud consumer opinion on the service being offered by the cloud service provider. A protocol that distinguishes honest feedbacks from misleading ones was proposed in. Accordingly, cloud services should be evaluated independently and weights could be given to each of the above mentioned attributes.

D. Need of Trust in Cloud Computing

- By means of cloud computing the security boundary is compromised in view of the fact that the data is processed on machines that are owned and controlled by someone else.
- The contractors or sub-contractors may also process the classified data autonomously of the trusted vendors, there by increasing the risk of unlawful use, resale or outflow of sensitive data.
- So Trust is a critical aspect of cloud computing.
- Where the problem of trusting cloud computing is a highest concern.

Therefore trust is widely regarded as one of the most important obstacles for the adoption and growth of cloud computing.

III. LITERATURE SURVEY

In [1], the author shot to explore the consequence of trust adoption by proposing a model for trust evaluation on the bases of Expectancy Disconfirmation Theory model and Bayesian network. This model has four main components firstly the Expectation which defines customer's anticipation about service & its performance, then comes perceived performance which indicates customer's experience after using service then disconfirmation is another component which indicates difference between expectation and performance.

In [2], The author propose a dynamic trust evaluation method to deal with cloud user's behavior, via Entropy Method to reflect the essential regular pattern of user's behavior evidence, making the evaluate way become a dynamic model , weaken the subjectivity of simply using AHP , moreover , still need AHP to make the result fit people's subjective experience , so puts forward a integrate

algorithm that combine Entropy Method and AHP , in this way , the final evaluate value will keep the balance between objective and subjective and provide quantitative analysis foundation for security control. In this paper, author has proposed an users trust evaluate model based on integrate algorithm, The main factors trust rules and implement detail have been introduce, this model considered the balance between objective and subjective, it has higher diction ratio and lower positive ratio, moreover, the model dynamically combine the historical UB with the new one, it makes the evaluate process based on users habit. In this paper, author only evaluate user's behavior, when cloud user have some abnormal behavior, and take timely measure to protect cloud security.

In [3], The author presents a trust management model based on multi-agent and trust evaluation. It adopts the centralized distribution management mode and sets up multiple third-party agents in the cloud; furthermore, it can manage the users and cloud services by the collaboration of the agents effectively. By using multiple third-party agents, it can reduce the single-agent's pressure of computation, storage and the users' waiting time. The experiment shows that the trust management model is effective. This paper proposes a cloud trust model based on multiagent, using centralized distribution management mode to manage users and cloud services. It uses direct trust-value, indirect trust-value and comprehensive trust-value to make the trust evaluation of users and service providers. The experiment shows that using multi-agent can reduce the pressure of storage and it can also reduce the user's waiting time when there are large numbers of notes. The trust management model is effective.

In [4], based on Quality of service and speed of accomplishing or implementing the cloud resources are used to build a trust model. Author presented a trust model to select the best source. The proposed model, in addition to enchanting account criteria of quality of service such as processor speed, response time, bandwidth, cost and so on is consider the speed of implementation of works. The proposed model (trust Model Turnaround Trust) has improved performance.

In [5], author presents a fuzzy mathematic based model for trust evaluation in cloud environment and considered the interactions between the cloud entities that is the number of successful transaction and the number of failed transactions are counted for calculating trust. Simulation results show that the proposed model has some identification and containment capability in synergies unethical, promotes interaction between entities, and improves the performance of the entire cloud environment.

In [6], author tackle problems related to trust in cloud computing by making a novel trust model stranded on a certification scheme for security of the cloud. A multiple signatures process as well as dynamic delegation is used to build the model. This approach ropes autonomic cloud computing systems in the management of dynamic content in security certificates, establishing a trustworthy cloud environment. And focused on security certification and presented an overview of a certification scheme and process underneath the requirements. Author also provided a novel chain of trust grounded on certification scheme and an example showing certification process in a actual scenario.

In [7], author argues the advantages and the disadvantages of users satisfaction. In Three turns a trust model has been projected between the cloud provider and the customer. At first turn author considers the users previous experience about the service provided by cloud provider, at second turn user must have information about what are the Advantages and Dis-Advantages of using the cloud and what are all the SLA s associated with it and what level of security it is providing. Now at third turn owner/ user is in the position that he says he trusts or relies on cloud.. It also verified that after going through such turns both cloud providers and users can be transparent to each others. Such transparency can develop a trust on cloud providers and their environments.

In [8], authors present a trust model which helps the Customer to evaluate trust of particular cloud service and also helps in selecting trustworthy resource. Author integrates SLA framework with his own model to comeup with a new and novel solution for selection of cloud providers. The trustworthy resources of cloud will be agreed on mainly by considering two inputs those are the experience of user and the SLA criteria's.

Table I. Table of Comparison for different methods used to build a trust in cloud environment

Sl No	Method	Advantages	Dis-Advantages
1	Expectancy Disconfirmation Theory (EDT) and Bayes' Theorem	Reveals the need of trust in cloud technology adoption by simulation results using EDT model and Bayes' Theorem	More parameters needs to be considered to sustain trust in cloud environment
2	Entropy Method and AHP	dynamic trust evaluate method can effectively distinguish user's abnormal behavior	only evaluate users behavior , when cloud user have some abnormal behavior , we have to take timely measure to protect cloud security
3	Cloud trust management based on multi-agent	Multi-agent can reduce the pressure of storage and it can also reduce the user's waiting time. The trust management model is effective.	Credibility of third party
4	Turnaround_Trust trust model	Better performance	More Complexity
5	Fuzzy based trust model	recognition and inhibition capability in synergies cheating, makes better performance of the entire cloud environment	------
6	Certification-Based Trust Model	Guarantees and establishes trust in an autonomic computing scenario.	Only some browsers will sustain the certificates issued by Enterprise root CA
7	PKI based trust model	Full control of security properties of PKI. On demand certificate revocation issuing.	Uneven load or single point of failure.

8	SLA-Based Trust Model	This model can worn for different domains of cloud services and based on that, domain users can get a more specific trust value of the same concept of services.	Disobedience s of SLA

IV. CONCLUSION

In modern years, cloud computing has become exciting and fast growing area of research and development. But today the problem of trusting cloud computing is a foremost concern for most cloud customer's in such a way that trust is broadly considered as one of the highest barrier for the growth and adoption of cloud computing. In order to evaluate trust management systems, trust model needs to be developed. Here, in this work discussion is made on some general concepts of cloud computing and issues of Trust in cloud computing with a survey of existing models for Trust in cloud computing.

REFERENCES

[1] Akinwale et.al "Trust: A Requirement for Cloud Technology Adoption"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 8, 2015
[2] LI Jun-Jian et.al "User's Behavior Trust Evaluate Algorithm Based On Cloud Model" Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control, 2015
[3] Xiaolan Xie et.al "Trust Management Model of Cloud Computing Based on Multi-agent" International Conference on Network and Information Systems for Computers, 2015
[4] Atoosa Gholami et al. " A Trust Model Based on Quality of Service in Cloud Computing Environment" International Journal of Database Theory and Application Vol.8, No.5, 2015
[5] Ali. Mohsenzadeh "Trust Model to Enhance Security of Cloud Computing" Journal of mathematics and computer science 2015
[6] Marco Anisetti et al. "A Certification-Based Trust Model for Autonomic Cloud Computing Systems" IEEE International Conference on Cloud and Autonomic Computing, 2014
[7] Ms. Heena Kharche et al. "Building Trust In Cloud Using Public Key Infrastructure" International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012
[8] Mohammed Alhamad et al. "SLA-Based Trust Model for Cloud Computing" International Conference on Network-Based Information Systems, 2010