I.J. Wireless and Microwave Technologies, **2017, 4, 14-27**
Published Online July 2017 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2017.04.02

***Available online at** http://www.mecs-press.net/ijwmt*

Trust Models in Cloud Computing: A Review

Ritu[a], Sukhchandan Randhawa[b*], Sushma Jain[c]

[a]*Student, Thapar University, Patiala and 147004, India*
[b]*Lecturer, P.O. Box 32,Thapar University, Patiala and 147004, India*
[c]*Assistant Professor, P.O. Box 32,Thapar University, Patiala and 147004, India*

Abstract

It is common to hear that big or small organizations are moving to cloud computing for its scalability and cost savings. But, how do you decide which cloud provider to trust? Trust is a vital factor, especially for service oriented systems in the area of Information Technology and Security. Several issues have been raised by enterprises and individuals concerning the reliability of the cloud resources. In cloud computing, trust helps the consumer to choose the service of a cloud service provider for storing and processing their sensitive information. In this paper, a methodical literature analysis of trust management and existing trust models is presented to evaluate trust based on various QoS parameters. Key research issues and future research directions in existing literature are also suggested.

Index Terms: Trust model, Cloud Computing, Resource Scheduling, Quality of Service and Reliability.

1. Introduction

Cloud Computing [1] connects huge number of systems in a network: private or public. It gives us highly scalable framework for storing data and applications. After arrival of this kind of computing, the price of computing power, web hosting, data and delivery are reduced remarkably. Cloud computing provides direct cost profits and it has the ability to convert a data centre from an investment-intensive setting to a variable priced setting. The difference that cloud computing has brought in comparison to conventional concepts of grid, distributed and utility computing is to widen horizons across organizational limitations. Cloud computing divides the role of Cloud Service Providers(CSPs) in two categories: the providers which organize the platforms and rent their resources such as memory, Virtual Machines (VMs) and bandwidth etc according to pay-per-use model of pricing and the service providers which lease their cloud resources from various Cloud Service Providers(CSPs) to end users based on their need without considering the location and method of

* Corresponding author. Tel.: 9646011842
E-mail address: sukhchandan@thapar.edu

delivery of these services[2]. A number of computing standard have promised to bring this *Utility Computing* idea and these include Cluster computing, Grid computing and now-a-days *Cloud computing*.

Though, since cloud applications may be important to the core business operations of the clients, it is necessary that the customers have guarantees of service delivery by providers. Service Level Agreements (SLAs) provides this guarantee between the service providers and customers. Service Providers such as Amazon, Dimension data, Google, Salesforce, IBM, iWeb, Microsoft and Sun Microsystems have started to launch new datacentres for hosting applications of cloud computing in different locations around the world to offer redundancy and guarantee reliability in case of site failures.

As the requirements of cloud services are variable in nature, CSPs need to guarantee that they are flexible in delivery of resource services while keeping the users inaccessible from the underlying infrastructure. Latest advancements in microprocessor technology and application software have led to the increasing capability of service hardware to execute applications within VMs in an efficient way. VMs permit both the isolation of cloud applications from device hardware and other VMs. Providers expose applications running within VMs or give access to VMs themselves as a cloud service and allowing clients to install their personal applications. The use of VMs increases additional challenges such as the intelligent resource allocation of physical cloud resources for managing demands for competing resource of the users.

In spite of the quick development of Infrastructure-as-a-Service (IaaS), techniques such as Amazon EC2 1 service, Microsoft Azure 2 service, and services provided by RackSpace 3 and other services, IaaS services continue to be best by vulnerabilities at many levels of software stack, also to leakage of information, to collocated malware infected VM instances. The need for protected cloud storage and cloud computing has been recalled on many occasions. For example, in [3] the author has cited industry decision takers to highlight the fact that security concern is one of the major factors that prevent business entities from deploying their organization's data and computations on cloud. General reasons are lack of knowledge of the state of the data and computing algorithms once it is in the cloud setup, as well as concerns about cloud provider bankruptcy and successive unclearness and recognized procedures of data safety and retrieval.

The reasons for this include both technical, such as the distress of data leakage, data infringement and data modification as well as organizational, such as destroying reputation. In this situation, there is a danger that the economic profit obtained through the fast pace adoption of cloud service technologies will in some cases be rewarded or even over compensated by data losses resulting from unpredicted lack of accessibility as well as theft and destruction of data.

1.1. Architecture of Cloud Computing

This section defines various models of cloud computing related to architecture, business and operation [4][5]. The structural design of cloud computing is described in four layers namely *hardware layer*, *platform layer*, *application layer* and *infrastructure layer*, as shown in Fig. 1[10].

- **The Hardware Layer:** The main responsibility of this layer is to manage the physical assets of cloud which includes physical data and application data servers, network routers, connecting switches, power source and cooling systems. Practically, the hardware layer works on data-centres. A datacentre typically comprises of thousands of cloud servers structured in racks and interconnected with each other through network switches, network routers or other connecting material. Some time consuming and complex issues in this layer are the configuration of hardware, fault tolerance, data traffic management, power utilization and managing cooling resource.
- **The Platform Layer:** It is the third layer from bottom; the platform layer consists of application frameworks and operating system files. The purpose of the platform layer is to reduce the trouble of application deployment in VM containers presented in the cloud. For example, Google App Engine (GAE) runs on this layer to provide support for APIs for implementing storage, database and business logic of distinctive web applications.

- **The Application Layer:** This layer resides on top of the architecture and consists of the actual applications of cloud. Different from conventional applications, cloud applications controls the automatic-scaling aspect to achieve increasing performance, availability and lower usage cost of resources provided. The architecture of cloud computing is more flexible than the traditional cloud hosting environments such as dedicated data and application server farms. Every layer is loosely coupled with the layers above and below it, and by doing so it allows each layer to progress separately. The architectural flexibility allows cloud computing to support a broad range of application requirements while minimizing management and maintenance overhead.
- **Infrastructure layer:** Also called as the *virtualization layer*, the cloud infrastructure layer creates large storage space and cloud resources by partitioning the physical cloud resources by using virtualization technique such as Xen and VMware. The infrastructure layer provides many important aspects, such as dynamic resource allocation which are only made available using virtualization technologies.

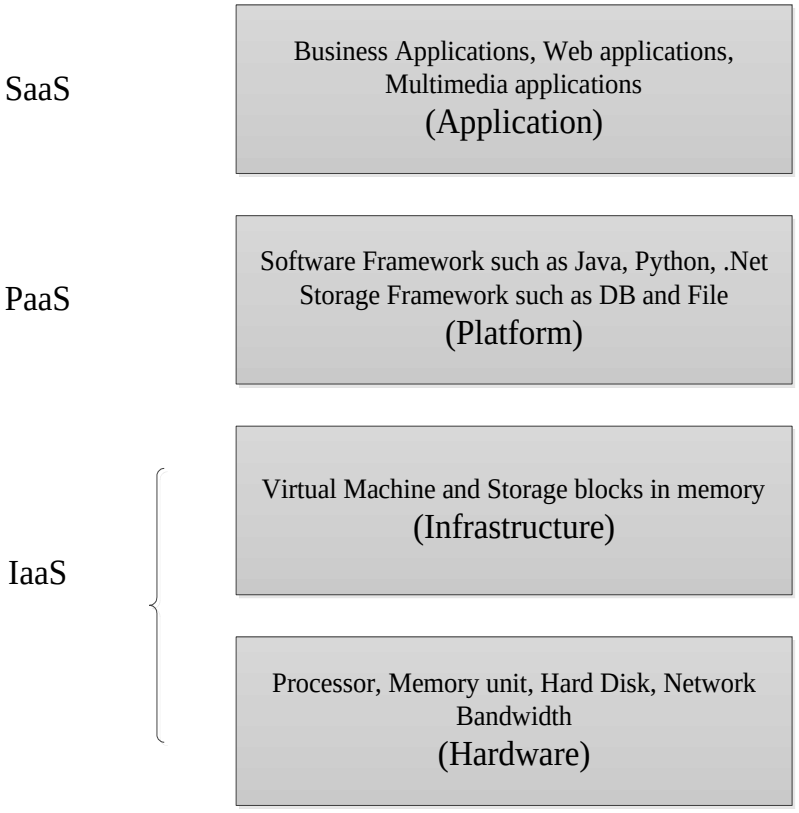

Fig.1. A layered modelling architecture of cloud computing

1.2. Cloud Computing Risks

Although Cloud Computing is the fastest growing technology in computing world, there also exist some risks or cons of cloud computing [1]. Some of these risks are explained below:

- **Security & Privacy:** It is the major concern in cloud computing. Since the management of data and infrastructure in cloud computing is provided by third-party, it is constantly at risk to give the sensitive data and information to such providers. Although the vendors of cloud computing guarantee extra secure password protected accounts and any indication of security violation would result in decrement of number of cloud clients.
- **Lock-In:** It is not easy for the clients to switch from one CSP to the other. It makes the clients dependent upon a particular CSP for a service.
- **Isolation Failure:** This risk consists of the breakdown of isolation mechanism, which separates storage space, memory and routing technique between different tenants.
- **Management Interface**: Public CSP provides interface which is accessible through Internet.
- **Unsafe Deletion of Data:** It is likely that the data which the user has requested for deletion may not get removed. It happens because of two reasons; extra copies of cloud data are stored but not existing and second that the storage disk destroyed also stores user's data from other consumers.

The structure of the paper is as follows: In Section 2, meaning of trust, trust semantics and types of trust are discussed. Section 3 presents the overview existing work related with trust and trust management along with the requirements of trust management. Fuzzy logic based trust model is also discussed along with the types of trust models. This section also presents the existing work in cloud computing and grid computing in terms of trust management. In section 4, the existing gaps in cloud computing are identified. Section 5 presents the need of trust model along with key research issues and future research directions. In Section 6, conclusion is presented.

2. Trust in Cloud

Trust comprises of three factors; Expectancy, belief and willingness to take risks. Trust in cloud computing is a measure of reputation of the specific CSP which has some set of resources for users. Trust in cloud plays a vital role to make the cloud business grow and the provider can get more profit. To make the provider trustable, some criteria are needed to help the user in selecting a CSP.

2.1. Trust Semantics

Trust is frequently used in the literature of Trust in cloud, often as a common term for "privacy" and "security" [6]. What is the meaning of the term "trust"? It is a multifaceted social phenomenon. Based on social science trust, the following definition is followed:

It is a state of mind comprising:

Expectancy: It is when the trustor expects a particular behaviour from the trustee party such as providing legal content or efficiently performing cooperative procedures.

Belief : The trustor considers that the behaviour he has expected would occur based on the information evidence of capability of the trustee, reliability and helpfulness.

Willingness of taking risk: For that belief the trustor is prepared to take risk.

It is essential to note that the trustor cannot control the expected behaviour of trustee; the trustor's faith in those predictable actions of trustee is dependent on the ability of trustee, capability and integrity.

The truthfulness of the trustee gives the trustor an assurance with reference to the expectedness of the trustee's behaviour. In cloud computing two kinds of trust have been identified, based on the expectancy of trustor: the *trust in performance* tells about performance of the trustee, but the *trust in belief* is trust comprised of trustee's belief. The performance trustee could be what the trustee claim or the successfulness trustee's actions. *Trust in belief* is transitive in nature; *trust in performance* is not; though, *trust in performance* is

broadcasted through *trust in belief* [7,8]. From the above definition, the trustor's state of belief depends upon the evidence related to the trustee's capability, truthfulness and concern. This leads to rational structures of interpretation from *belief in proof* to *belief in expectancy*. This is the basic idea behind trust in cloud computing.

2.2. Types of Trust

The trust in cloud computing is divided into various categories namely *Reputation Based Trust, SLA verification based trust, Policy-based trust, Evidence-based trust* and *Societal trust.*

In *Reputation Based Trust***,** the reputation of an entity is the collected estimation of public's trust towards that entity. Generally, many entities in a community trust an entity that has high reputation; an entity, which is required to build trust decision on a trustee, uses the reputation to compute or approximate the trust level of the trustee. The reputation of cloud affects the selection process of cloud services; therefore, CSPs try to construct and preserve higher reputation. Reputation is classically represented by a broad score reflecting the overall outlook, or a small number of scores on numerous foremost aspects of performance. In *SLA verification based trust,* after establishing the preliminary trust and accessing a cloud service, the cloud user is required to validate and re-examine the trust value. SLA is a lawful agreement between the two communicating parties: user and provider. Therefore, monitoring the QoS parameters and verification of SLA document are essential source of trust management for cloud computing. A third CSP party is required to provide these types of services.

In *Policy-based trust*, it is required to construct a "formal". In a related area, Public Key Infrastructure (PKI) is an extensively used technology that utilizes "formal" trust methodologies to support key certification, digital signature and validation. It also supports data attribute certification and validation. In this, the trust in a Certification Authority (CA) is dependent on the CA's confirmation with definite certificate policies. It is taken w.r.t to delivering and retaining public key certificates which are validated. Certificate policies play a main role in PKI trust.

In *Evidence-based trust,* a belief of trustor in the predictable behavior of trustee is based on the proof about attributes of adaptness, helpfulness and honesty. With respect to that expectation evidence-based trust is expressed as follows:

$$believe(c, attrb1(sb, av1)) \wedge ... \wedge believe(c, attrbn(sb, avn)) \rightarrow trust\_ * (c, sb, x, ct)$$

which states that if a cloud user *c* believes a subject *sb* has attribute *attrb*1 with value a*v*1, ..., attribute *attrbn* with value a*vn*, then *u* trusts (it is either *trust in belief* or *other one*) *sb* w.r.t *x*, the performance of *sb* or information is believed by *sb*, in a particular context *ct*.

Societal trust consists of any individual and a company. In cloud also, each entity must be trusted. In Information security service sector, trust plays a vital role between the supplier and the client to help the business grow.

3. State of Art

In this section, trust management and its techniques are discussed. Trust models in grid and cloud are discussed. Fuzzy logic and trust models based on fuzzy are also presented.

3.1. Trust and Trust Management

Firdous *et al.* [9] and Han *et al.* [11] have studied that the status and trust have originated from society which studies the pattern of human behaviour. Zaobin *et al.* [12] have explained the relationship among various entities of social network in trust management system. Trust is analysed by researchers in various fields such as human psychology, sociology and business economics. McKnight and Chervany [13] have elaborated that trust is a mental outlook which focuses on the effects of trusting and not trusting someone. Trust is a social

relationship between people in the society. Paoli *et al.* [14] and Akhoondi *et al.* [15] have explained that the social outline of trust is commonly used in multi user systems and social networking. Economic experts recognize trust with regard to usefulness. Huang *et al.* [16] and Mui [17] have explained that the scientists in Information Technology (IT) have utilized the advantages of all these research works, as they offer critical vision of human mind. The computing technology researchers have studied trust in various fields such as public distributed systems (e-commerce), open, peer to peer networking , cloud computing, semantic web technology, cloud computing, web services and mobile networks. Though there has been various studies done on trust; it has also increased the complexity of trust in several areas of computing. The thought behind this is that there is no common description of trust in cloud computing such as beliefs, outlook, possibilities, expected behaviour, honest quotient and so on.

McKnight and Chervany [13] have recognized 16 aspects of trust which are classified in Table 1 as follows:

Table 1. Aspects of Trust

Class	Aspects of trust
Proficiency	Capable, Skilled, Dynamic
Expectedness	Predictable
Generosity	First-Class (Or Moral), Caring, Responsive
Reliability	Truthful, Plausible, Consistent, Loyal
Other	Direct, Cautious, Shared Understanding, Personally Smart.

De Oliveira and Maziero have categorized relationships of trust into social networks, hierarchical trust and social groups. Zhang *et al.* [18], have divided trust into categories: Rank-based vs. Threshold-based, Complete information vs. Local information, Transaction-based vs. Opinion-based and Subjective trust vs. Objective trust.

3.1.1 Trust Management Requirement

The prerequisite of an efficient trust management system are presented as follows:

a) Accuracy of Information

Chong *et al.* [19] have explained that precision of facts and information is known as accuracy of trust which means that the computation of trust is accurate at estimation time. There is no power over the correctness of the trust value provided by the trust management system. So much of information is needed to evaluate the value of trust in a network system. This set of information could be misleading or false in nature to make us trust the service provider. Correct calculation of trust is important because it has enhanced the relationship between service provider and its consumers. It has also helped to improve the business of e-commerce websites in which trust is the crucial factor. Also, the incorrect information has led to false business conclusions which results in low quality verdict and outcomes. Trust has been improvised by sharing the experience of users about the quality of service offered by different providers. That is why the user needs the guarantee of the information correctness to trust that particular provider. The issue in providing accurate trust to users is that the data of trust is excessively common. It does not indicate the required trust information by the user but it gives a single value as a trust value. Transactions have taken as applicable when computing trust value related to a new transaction. For instance, a service provider may be excellent in one service but not so good in other service. Hence the earlier transaction is taken as one of the parameter in evaluating trust. Trust computation needs much information such as trust value of different services providers. E-commerce also has faced the problem of consistency of trust evaluation system. False and biased ratings may affect trust evaluation. The purpose of false rating is to increase or decrease a supplier's reputation. False feedbacks may affect the reliability of the trust system and level of trust of a service provider. Most vulnerable system to false ratings is e-commerce where anybody can temper with ratings.

For instance, the cause of bad quality of trust level could even be a small amount of false information. Hence the overall reputation of the provider will get affected and trust system becomes unreliable. As it is impracticable to anticipate all ranking providers to supply genuine ratings in an open atmosphere such as e-Commerce, it is essential to have an approach that is proficient to identify false ratings to defend the integrity of the trust system. Hence a process is needed which can identify and check the false ratings to build an efficient trust evaluation technique. As the quality of such trust evaluation system is relied on the accuracy of ratings gathered as input, thus efficient security against inequitable ratings is fundamental requirement of trust computation system.

b) Information Security

Security is protection of data in online transactions and is considered as a basic factor in e-commerce as it led to some new security threats. The acceptance of security systems is required for trust management. When security loophole occurs then the trust management system must act in quick manner to lessen the level of threat, operational effects and the day to day business. The system must be competent enough to support mixture of response ratings from large number of users. To support high service availability, the cloud trust management service, all previously recorded data managed become available for evaluations of trust. It also bears the utilization of diverse trust evaluation functions by distinct clients over similar rating taken from an entirely distributed ecommerce users.

Additionally as the communication about diverse services raises, the request for trust information may increase and boost its complication of the system to acquire data. The trust maintenance system must have the ability to vary dynamically in several distinct ways which could have an effect on the value of trust of multiple users with no communication details. The websites which involves online transaction also relies on trust models that support integrity, availability, reliability and secrecy of the data and information.

The user cannot do a transaction of some product without revealing their personal details, address to ship the product, bill details and priority of the item. The service users might be not interested in providing these details if they have trust issues with the provider. Online shopping websites are required to make sure that their trust system is safe and reliable to users and it can work well in dealing with sensitive information also. Efficient prevention procedures should be considered and flawlessly incorporated with the plan of trust administration systems.

3.2. Trust Management Framework and Trust Model

The framework of trust management system should be able to facilitate the CSPs to allow the users to calculate and decide values related to potential transactions. The techniques which can provide accurate value for trustworthiness is needed for trust administration system. It combines the fundamental safety procedures and trust assessment components which can filter ratings.

3.2.1 Trust Model Definition

Foster *et al.* [20] have explained that the trust model is defined as the scale of trust among two parties on each other. The idea of trust was taken from the relationship between customer and CSP. Such relation has some scope defined which is security threats. When the service provider monitors the actions of cloud system, the user or the clients generate ratings. There are two outlooks to define a trust model in computing world:

Customer's outlook - what security does the service provider have?
Provider's outlook – what type of customer does it have?

The clients must be informed about the security faults and vulnerabilities that exists in the system or that

have the possibilities. Trust model is nothing but some set of protocols which are to be followed by the service provider and their users or customers. Users also have the facility to provide some rules to overpower the activities on cloud according to their choices. The syntax of the protocol must be in understandable and standard form. It must be able to interpret the instructions every time the user made a request. The continuous mentoring of the activities happening in the cloud helps the users or clients and provider to have the information about the threats breaching the security of the cloud network. The rating provided by the clients does not add much to the trust management system. It is better to make list of expectations from the cloud user's activities so that the provider will know about his expectations form the user. Also it tells about how the provider can manage the cloud instances. If there is an increase in the count of cloud instances within same time phase every year then the provider will allocate the resources automatically thereby increasing satisfaction.

3.3 Types of Trust Models

Trust models are classified based on trust management as shown in Table 2.

Table 2. Types of Trust management based on flow of control

Type of Management	Main Policy
Centralized trust management	After one transaction completion the client report rating to the trusted party.
Decentralized trust management	A peer to peer system is present.
Distributed trust management	Data is shared among different brokers

Another category of trust models is based on flow of a transaction as shown in Table 3.

Table 3. Types of Trust management based on flow of transaction

Type of Management	Management Strategy
Static trust management	Rules are defined by trust administration system
Dynamic trust management	Profiles are as a trust model engine which define trust

Static trust model have a predefined design and flow of the process of transaction. The model worked according to the design defined at the starting. A dynamic model works with future activities and unidentified process flow. The static model works according to system manner but dynamic model adjusts with different parameters and progress based on the previous cached data stored in a data store.

3.4 Trust Models in Grid computing

Manuel *et al.* [21] have introduced a trust model which computes the resources of grid and cloud by cloud broker. In heterogeneous atmosphere the cloud broker selects the suitable resources on the basis of individual users. This model was executed with Kerberos authentication and PERMIS authorization to improve the broker's belief. This trust model has estimated the value of trust based on identity based trust and behavioural trust. The introduced method took parameters for both grid and cloud entities.

Varalakshmil *et al.* [22] have reported a trust model which is based on a reputation of a cloud provider. This model has used intermediate entities and brokers. This design depends on several brokers in every sphere. The entities are linked with various brokers. The entities are shared among different brokers, with each entities linked with two or more brokers. This increases the problem of redundant data managed at broker. This has also enhanced the network passage at broker's site and side by side handles client's requests. The issues related

with the maintenance of brokers were resolved using this model.

3.5 Trust Models in Cloud environment

Abawajy [23] has presented a distributed standard that has enabled client and provider communication via trust based model. This method has efficiently controlled false ratings. It has diluted the effects of wrong ratings consequences and giving accurate and quality assessment of cloud services. Zhang *et al.* [22] have proposed a model which works on neutral factors of trusted environment. This model is consistent and trustworthy as it has used the TCCP model which has moved from third party trust to trusted platform of IaaS.

Hwang *et al.* [25] have proposed a new approach to integrate virtual clusters, data centers, and trusted data accessibility according to reputed systems. A peer to peer cloud system was introduced for security of clouds and data storage area at scope of system. It has protected an entity objects at document accessibility level. Some computing technology organization such as Amazon, Google, and IBM employ protective solutions to give safety to service models in cloud i.e. IaaS, PaaS, and SaaS. Zhang [26] have suggested that trusted computing motivates clients to use sharable resources and application services provided by the provider. Trust is the main factor in choosing a cloud provider from the list to use the services. When the customer wants a service, he first checks if the provider meets all the requirements. Then he checks two things. First, the present capabilities of the provider and second is the past credentials of the provider. Past credentials describe the past reputation of provider and records of services provided by the provider. It consists of different factors such as reliability, availability, and turnaround time and data integrity. Present capabilities illustrate about the services offered at present. It includes factors like speed of processor, average throughput, hard disk capacity, RAM size, network bandwidth, latency of the given resource

Pearson [27] has elaborated the theoretical background and provided a basic view of how cloud computing not only impacted IT budgeting but also affected conventional mechanisms. In this chapter, the author has explained different issues related to security, trust and privacy in a cloud. Zissis and Lekkas [28] have proposed the solutions based upon cryptography, specifically Public Key Infrastructure (PKI) operating in coordination with LDAP and SSO, to make sure that the system authentication, integrity and data confidentiality of storage and communications. The generic design ethics of a cloud environment were identified in this paper which originated from the necessity to control important vulnerabilities and threats. Firdous *et al.* [29] have suggested a complete survey on the trust management systems which is implemented on distributed computing systems with a special focus cloud computing.

Huang and Nicol [30] has suggested that trust in cloud computing relies on the reputation of the provider and self-estimation of their services. Trust is reputation based which is an aggregate opinion of a community, SLA verification based trust which focuses on visible elements, Trust as a Service, which includes Cloud Trust Authority (CTA) to provide a single point for organizing security of cloud services from different CSPs, Policy based and Evidence-based trust.

3.5.1 Fuzzy Logic based Trust Model in Cloud

Sun et *al.* [31] have introduced a subjective trust management architecture based on fuzzy set theory TMFC which is based on in-depth research on previous studies. Gu *et al.* [32] have proposed VMs based trust model for cloud computing considering two aspects. The timeliness strategy is used to ensure the response time and idle time of servers is also minimized. The trust values for each CSPs are calculated using fuzzy theory to get successful response. Xia *et al.* [33] have introduced a trust model with multiple trust decision factors based on fuzzy set theory. The fuzzy AHP theory is used which is based on entropy weight mechanism. Wagng *et al.* [34] have suggested that the existing approaches which are based on probability and fuzzy set theory didn't give enough importance to uncertainty. To eliminate this problem, the authors have proposed a quantifiable subjective trust evaluation approach. This approach has used projected value and hyper-entropy of the particular cloud to compute the reputation of trust objects.

3.5.2 Barriers in the existing work

Trust is essential in case of decentralized data sites and the cloud resources are shared among large number of hosts, which is specifically a fact in cloud computing environment. The main issue with cloud computing nowadays is the security requirement. The biggest and necessary concern of cloud users is that "if the data they have shared is also being shared with someone else on the same resource?" Controlling and possession is also difficult issue. The clients don't use a system when he has no power over the properties provided by them. CSPs must provide control over the data to clients.

The two levelled variable trust relation is formed between the provider and the client when the enterprises stores or deliver their data to the resources provider. The enterprise trust on the provider and the user's of that enterprise also trust the CSP. The services which are based on clouds are so common nowadays. Threats on security and privacy of user's data are quite a big distress. Some problems may occur such as legal issues, standard SLA's because the CSP is a self-regulating firm. Security became the main concern for protecting the cloud services from service failures and refining trust in cloud. CSP has to deliver different services to distinct consumers which lead to safety issues in virtual cloud atmosphere.

In virtual environment, some of the privacy issues are identification management, data loss due to sharing of resources, usage control, virtualization hardware safety, user's content protection and malware attacks. The cloud user's mind-set is that a cloud is not much safe than local system. If good level of transparency is provided by the cloud resource provider then it would result in secure cloud system. The data located on cloud is not actually presented at single location but located across all over the virtual layer of cloud network. The problems related to transparency are physical locality of the data and protection profiles of the data processing sites. Set up assurance between the provider and the consumer entity is very important. The reputation of cloud provider is becoming the obstacle for the user to employ cloud services. It is difficult for the CSPs to make their own reputation because the Software as a Service (SaaS) mechanism is new to everyone. When there is less clarity for user about why their private information is being asked for, or who is going to process their data? , this lack of command and lack of observance of the cloud supplier result in doubt or distrust.

There exist a security concern about the data is protected or not. Consequently the cloud users may hesitate from utilizing the services available by CSPs. They worry about their sensitive information being shared all over the network without their consent. Some fake provider's uses customer's data and make profit out of it without getting noticed by the users. A lot of risk is involved in sharing the data on different cloud storage locations, especially the private content or confidential information. But the problem is the lack of standard provided by trust models available in cloud infrastructure.

4. **Need of Trust Model in Cloud Environment**

There are several cloud trust models introduced by various researchers and organizations with their best parameters and efficiency. Security becomes most important criteria for the clients to choose one of the available cloud resources. When the user wants to choose a specific service, then he/she needs some ranking application to evaluate the quality of cloud service. A standard which assess the reliability of cloud resources is the requirement of cloud clients to choose a service.

There is need of trust management framework which must be able to discover the mechanism for providing safety in a cloud atmosphere to be evaluated and ranked. So a tool is required which helps us to rely on the services of a cloud is the essential demand of the cloud computing network. Model must contain factors to wrap all the security features. The complexity of cloud computing makes us consider both the physical security parameters and architectural configurations. The subjective characteristic of trust is appropriate for acquiring the complexity of cloud. The following are the characteristics which must be considered while proposing a trust model:

- To model a less complex and reliable trust model for cloud computing environment.
- Enables cloud users to select the best available resources in a heterogeneous cloud computing infrastructure.
- Encourages the customers to use shared resources and services delivered by the cloud provider.

4.1 Key Research issues to be considered in a Trust model

Following are few research questions which need to be addressed in order to implement a robust trust model in cloud computing:

- How accurately can a trust model compute the information gathered from multiple heterogeneous information sources?
- How to bring consensus by modeling multiple attributes of cloud computing?
- How to use accurately, the trust values in a given context which has been computed in a different context?
- How trust model improves the cloud resource utilization?

4.2 Future Research Directions

- In future, this work can be widened to employ in multiple domain cloud atmosphere.
- A non-centralized model can be introduced that would work for homogeneous set of CSPs.
- Some other security features can be employed to prevent the system from different attacks using separate techniques. There are some other parameters which can be considered in a trust model in future for optimizing the rules such as price comparison, allocation rate, probability of selection and security.

5. Conclusion and Future Scope

Now days, security is the main threat in any computing paradigm. Cloud computing is also one of the emerging computing paradigms, as organizations are progressively switching their data to the cloud platform.

To assure the quality of service in terms of security, a new term i.e. “Trust” is proposed. Various trust models have been proposed in the existing work. Trust model in cloud computing is the most in-demand mechanism to provide security in cloud computing. The objective of this review is to introduce the user various techniques which help to select the most reliable and trusted cloud service provider. The trust value of homogeneous resources, available on cloud, is calculated on the basis of QoS parameters using decision system. There are some questions which must be addressed which must be answered before designing any new trust model.

References

[1] Cloud Computing Tutorial, [Online], Available: http://www.tutorialspoint.com/cloud_computing/cloud_computing_tutorial.pdf

[2] R. N. Calheiros, R. Ranjan, A. Beloglazov, C.A. De Rose, and R. Buyya., “ CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms,” *Software: Practice and Experience*, pp.23-50, 2011.

[3] R. Buyya, C.S. Yeo, S. Venugopal , J. Broberg, I. Brandic., “ Cloud computing and emerging IT platforms: Vision, hype,and reality for delivering computing as the 5th utility,” *Future Generation Computer Systems*; pp. 599–616, 2009.

[4] Q. Zhang, L. Cheng, and R. Boutaba., "Cloud computing: state-of-the-art and research challenges," *In Journal of internet services and applications*, pp.7-18, 2010.
[5] Tanvir Ahmed, "Cloud Computing a Solution for Globalization", International Journal of Education and Management Engineering(IJEME), Vol.6, No.4, pp.30-38, 2016.
[6] J. Huang and D.M. Nicol., "Trust mechanisms for cloud computing," .*Journal of Cloud Computing*, pp.1-14, 2013.
[7] D. Nicol, J. Huang., "A formal-semantiics-based calculus of trust," In Internet Computer Sytems IEEE, pp. 38–46, 2010.
[8] J. Huang, M.S. Fox., "An ontology of trust: formal semantics and transitivity," *In proceedings of the ICEC*, New York, NY, USA, pp. 259–270, 2006.
[9] M. Firdhous, O. Ghazali, and S. Hassan., "Trust management in cloud computing: a critical review," *The International Journal on Advances in ICT for Emerging Regions, 2012'*
[10] Manpreet kaur, Hardeep Singh,"A Review of Cloud Computing Security Issues", International Journal of Education and Management Engineering(IJEME), Vol.5, No.5, pp.32-41, 2015.
[11] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A Survey of Trust and Reputation Management in Cloud Systems in Wireless Communications", IEEE, vol. 98, pp. 1755-1772, 2010.
[12] Z. Gan, J. He, and Q. Ding, "Trust relationship modelling in e-commerce-based social network," *In International conference on computational intelligence and security*, Beijing, China., pp. 206-210, 2009.
[13] D. McKnight and N. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," in proceedings of *34th Hawaii International Conference on System Sciences*, Island of Maui, HI, USA, 2001.
[14] D. Paoli, Stefano and Gangdharan, G.R. and Kerr, Aphra and D'Andrea, Vincenzo and Serrano, Martin and Botvich, Dmitri, "Toward trust as result: An interdisciplinary approach," *In Proceedings of ALPIS, Sprouts: Working Papers on Information Systems*, vol. 10, no. 8, pp. 1-6, 2010.
[15] J. Habibi, M. Akhoondi, and M. Sayyadi, "Towards a Novel model for inferriing trust in heterogeneous systems of social networks," *In proceedings of 2nd Asia International Conference on Modelling & Simulation.*, Kuala Lumpur, Malaysia,. pp. 52-58, 2008.
[16] G. Zhu, H. Huang, and S. Jin, "Revisiting trust and reputation in multi-agent systems," *In proceedings of Inter-national Colloquium on Computing, Communication, Control, and Management (ISECSM)*, Guangzhou, Chiina, pp. 424-429, 2008.
[17] L. Mui, "A Computational models of trust and reputation:: agents, evolutionary games,, and social networks.," Boston, USA, PhD Thesis 2002.
[18] Q. Zhang, T. Yu, and K. Irwin, "A Classification Scheme for Trust Functions in Reputation-Based Trust Management," *In International Workshop on Trust, Security, and Reputation on the Semantic Web*, Hiroshima, Japan, 2004.
[19] S.K. Chong, J. Abawajy, M. Ahmad, and I.R.A. Hamid., "Enhancing Trust Management in Cloud Environment," *Procedia-Social and Behavioral Sciences*, pp.314-321, 2014.
[20] I. Foster, Y. Zhao, I. Raicu, and S. Lu., "Cloud computing and grid computing 360-degree
[21] P.D. Manuel, S.T Selvi, and M.E Barr., "Trust management system for grid and cloud resources," *In proceedings of First International Conference on Advanced Computing, ICAC*, pp. 176-181, IEEE, 2009.
[22] P. Varalakshmi, S.T. Selvi, A.J Ashraf, and K. Karthick., "B-tree based trust model for resource selection in grid," *In proceedings of International Conference on Signal Processing, Communications and Networking, ICSCN'07,* pp. 222-227, 2007.
[23] J. Abawajy., "Establishing trust in hybrid cloud computing environments," *In proceedings of 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* IEEE, pp. 118-125, 2011.
[24] W. Han-Zhang and H. Liu-Sheng., October., "An improved trusted cloud computing platform model based on DAA and privacy CA scheme," *In proceedings of International Conference on computer Application and System Modeling (ICCASM),* IEEE, Vol. 13, pp.13-33, 2010.

[25] K. Hwang, S. Kulkareni, and Y. Hu. ,"Cloud security with virtualized defense and reputation-based trust management," *In proceedings of Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC'09,* IEEE, pp. 717-722, 2009.
[26] Q. Zhang, L. Cheng, and R. Boutaba., "Cloud computing: state-of-the-art and research challenges," *The Journal of Internet Services and Applications*, pp. 7-18, 2010.
[27] S. Pearson., "Privacy, security and trust in cloud computing," *In* proceedings *of Privacy and Security for Cloud Computing,* Springer London. pp. 3-42, 2012.
[28] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues," *In Future Generation computer systems, pp.* 583-592, 2012.
[29] M. Firdhous, O. Ghazali, and S. Hassan., "Trust management in cloud computing: a critical review," *In the International Journal on Advances in ICT for Emerging Regions.2012*
[30] J. Huang and D.M. Nicol., "Trust mechanisms for cloud computing," .*Journal of Cloud Computing: Advances, Systems and Applications*, pp. 1-14, 2013.
[31] X. Sun, G. Chang and F. Li, "A trust management model to enhance security of cloud computing environments," *In proceedings of Second International Conference on Networking and Distributed Computing (ICNDC) IEEE,* pp. 244-248, 2011.
[32] L. Gu, C. Wang, Y. Zhang, J. Zhong, and Z. Ni., "Trust Model in Cloud Computing Environment Based on Fuzzy Theory," *International Journal of Computers Communications & Control*, pp. 570-583, 2014.
[33] H. Xia, Z. Jia, and E.H. Sha., "Research of trust model based on fuzzy theory in mobile ad hoc networks." *Information Security, IET*, pp. 88-103, 2014.
[34] S. Wang, L. Zhang, N. Ma, and S. Wang., "An evaluation approach of subjective trust based on cloud model," *In proceedings of International Conference on Computer Science and Software Engineering,* IEEE, pp.1062-1068, 2008.

Authors' Profiles

Ritu received the B.E. degree in computer technology from Maharshi Dayanand University, Rohtak, India in 2012 and the M.E. in Information Security in Computer Science from Thapar University, Patiala, India in 2016. She is currently working as Software Developer in TCS. Her research interests are focused on Cloud Computing and Information Security in different domains

Sukhchandan received M.E. degree in Computer Science and Engineering from Thapar University, Patiala, India in 2012. She received B.E. degree in Computer Science and Engineering from Chitkara Institute of Engineering and Technology, Rajpura, Punjab, India in 2010. She had done Diploma in Information Technology from Thapar Polytechnic, Patiala, India in 2007. She is pursuing PhD in Wireless Sensor Networks.

Her research interests are focused on Wireless Sensor Networks, power efficiency, data aggregation and load balancing algorithm in Wireless Sensor Networks. She has joined Thapar University as Lecturer in 2012.

Sushma Jain received the B.E. degree in computer technology from S.A.T.I., Vidisha, India in 1993 and the Ph.D. degree in Computer Science from Thapar University, Patiala, India in 2012.

She worked as a Lecturer with the S.A.T.I., Vidisha from 1996 to 2001. She joined Thapar University in Feb. 2001 and is currently working as an Assistant Professor at the Computer Science & Engineering Department in Thapar University Patiala, India. Her research interests are focused on Wireless Sensor Networks, in particular development of data aggregation and load balancing algorithm and scheduling of resources. She is member of ACM and has number of publications in very highly reputed SCI indexed journals.

How to cite this paper: Ritu, Sukhchandan Randhawa, Sushma Jain,"Trust Models in Cloud Computing: A Review", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.4, pp.14-27, 2017.DOI: 10.5815/ijwmt.2017.04.02