A Survey on Trust in Cloud Computing

Kavita Rathi,
Assistant Professor, CSE Department,
Deenbandhu Chhotu Ram University of Science & Technology, Murthal.

Sudesh Kumari,
Student, M.Tech(CSE),
Deenbandhu Chhotu Ram University of Science & Technology, Murthal.

ABSTRACT- Cloud computing has become the burning research topic in the present as it seems to fulfill the current business needs by making the resources of hardware, software, platform and infrastructure available to the consumers as per their requirement and demands whenever and wherever they want. This leads to a lot of implementation challenges that come across, of which the most eminent are trust and security. This paper tries to find out the trust elements which could promote the use of cloud computing among users at large. An attempt is being made to find out the existing trust models and their drawbacks so as to lead to new trust models in the near future to bring more confidence in the use of cloud computing.

KEYWORDS- Trust, Trust Issues, Trust Models, User Behavior Based Trust Models.

I. Introduction
Cloud computing is emerging as an eminent technologies in the field of IT. It provides the scope to avail resources by the enterprise’s own requirements and demands. It follows the “pay-as-you-go” economic model [1] and works on a virtual platform to provide the computing services to the users on demand. New technology always comes out with its own pros and cons, so is the case of cloud computing. The biggest issues that come across in the implementation of cloud computing are found to be security and trust. Distrust of cloud users (CUs) on the cloud service providers and vice versa is a major issue of concern in the adoption of cloud computing at large. Trusted cloud computing is seemingly the primary requirement in adopting cloud computing. Since the cloud service providers (CSPs) exist between the CU and the data centers which provide cloud services, trust among both CUs and CSPs is a critical factor which can never be ignored. This paper focuses on various issues of trust and models of trust for evaluating the trust of users as well as service providers. The first part of the paper focuses on trust definition and its role in implementing cloud computing, followed by the parts presenting trust elements and trust models with their drawbacks.

II. What is Trust?
Trust can be considered as the belief or confidence of the user on the service provider and that of the service provider on the cloud user. Trust is subjective in nature and hence is difficult to define effectively. Every individual have their own thoughts and views regarding trust. Trusted computing is a field of trusted systems where a device is made to behave in a consistent and predictable manner using techniques like cryptography and authentication[2]. Trust can be of several types as per various researchers. As discussed by researchers, Jingwei Huang and David M. Nicol, the various types of trust are, namely, reputation based trust, policy based trust, evidence based trust, service level agreement based trust, societal trust and there could be many other categories like direct, indirect or recommended trust. All these classifications are based on the way the CUs and CSPs define trust. Trust is very important for a cloud computing environment to exist. There are various issues that come across which may lead to distrust among the CUs for availing the services of the cloud service providers (CSPs).

As per the researchers, Yashpal Kadam, Wayne A. Jansen, some of the major issues of trust are stated below:

- **Insider Access:** The data stored on the cloud is not under the control of the CUs and the employees at the CSPs end have the access to that data. This is an issue of distrust for the CUs on the CSPs for sharing their data on the cloud.

- **Composite Service:** Involvement of two or more CSPs for availing a service to the users’ leads to the distrust as any error in data could not be detected as to where the problem occurred.

- **Visibility and Risk Management:** Visibility refers to the transparency that is provided by the CSP who operates vital resources for effective oversight over the security of system and privacy of data. 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. 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 assessment must be detailed and should be done properly in a cloud based implementation.

There are several other issues like everyday changes in the IT world regarding technologies, political boundaries and different rules and regulations across these boundaries and how the policies and rules are implemented along with how the policies are decided for data sharing and resource sharing in a cloud computing environment. All these issues make it important to establish trust among the CUs and the CSPs.

### III. Trust Models in Cloud
Trust evaluation becomes very important in the cloud computing scenarios. Various parameters are
discussed by researchers Ayeesha Kanwal, Rahat Masood, et. al. to evaluate the trustworthiness of the
CSPs by the cloud users. The parameters include integrity of data, ownership and control of data, control of process execution, Quality of service attributes, detection of the entities that could not be
trusted. Trust models are a way of evaluating trust for establishment of trust among the CUs and the
CSPs. A cloud computing environment with management of trust is implemented by three modules:
a trust management module, a SLA management module and a resource management module. The
trust management module is used to evaluate the trustworthiness of a cloud service provider. The
SLA management module is used to make an agreement among the CUs and the CSPs. The resource
management module is used by the CSPs for making the resources available to the CUs as per their
demand as and when required.

For the evaluation of trust among the CUs and the CSPs, many trust evaluation models come across
as stated below:

- **Agreement Based Trust Models**[4]: These models include the various trust models in which
  the trust between the CUs and CSPs is evaluated by various agreements regarding the
  services to be provided by the CSPs to the users. They comprise of the mutual agreements
  between both the parties, namely, the CUs and the CSPs.

- **Certificate/ Key Based Trust Models**[4]: In these models, secret keys are shared between
  the CUs and CSPs for ensuring the confidentiality and integrity of data. These keys are issued
  by the certificate authority or a trusted third party.

- **Feedback based Trust Models**[4]: These models focus on the feedback by the users which
  should also be trustworthy to evaluate the trustworthiness of a CSP. The feedback is based on
  various security parameters and quality of service attributes provided by the CSPs.

- **Domain based Trust Models**[4]: These models are generally used in the grid computing
  environments and are of less concern with their inter and intra domain relationship issues in
  cloud computing environments.

- **Subjective Trust Models**[4]: These models provide a subjective and theoretical approach
towards evaluation of trust among CUs and the CSPs. They are focused on the fuzzy set
theory and probability theory techniques for trust evaluation.

As discussed above, various trust models exist for evaluation of trust of the CSPs by the CUs but
there is very less work done for evaluation of CUs trust by the CSPs. The cloud user must also be
trustworthy for a healthy and reflective cloud computing environment. The models that deal with the
evaluation of trustworthiness of the CU are categorized as user behavior based trust models which
can be stated under the broader category of feedback based models[4].
IV. User Behavior Based Trust Models

Most of the trust models in practice in today’s cloud computing scenario focus on the trust evaluation of the CSP by the CU but for the proliferation of the cloud computing technology to survive for long, it is equally important to keep focus on the fact that the correct user is using the services of the cloud and it will do no harm to the cloud resources by its malicious and unpredictable activities. To evaluate the trustworthiness of the users some of the researchers have given their models so as to judge the behavior of the users and allow them to continue with the services of the cloud or not. These models are categorized under the user behavior based trust models.

The possible reasons leading to user behavior mistrust are [6]:-

- 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.

These reasons lead to the cause of evaluating the trust of the users that are using the cloud services so that it could be ensured that the sharing of data and resources on the cloud is of no harm as the cloud is always used by a trustworthy user along with a trustworthy CSP.

User behavior trust can be sub categorized into four types of sub-trust, namely, security behavior sub-trust, contract behavior sub-trust, expense behavior sub-trust and identity re-authentication sub-trust[5].

Cloud computing model brings some new security threats such as resource sharing, fate sharing, and data lock in [7]. These risks are sources of concern for users and prevent them from using cloud
computing [7]. Due to these kinds of risks, the CSPs have to keep concern for the CUs to provide them with a trustworthy cloud environment. Several researchers have given many elements of trust that are useful in identifying the CUs’ trust in the use of cloud services.

From the contributions by the researchers in [7], [8], [9], [10], following trust elements of CUs are stated as below:-

- **Location of stored data**: In the cloud environments, data can be stored anywhere and the CUs 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 CUs 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 CUs.

- **Long-term Viability**: CUs 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 [7]."

- **Compliance regulation and audit**: Compliance includes correspondence of the appearance of the constitute specifications, standards and Law [11]. These laws, rules and regulations for security and privacy differ from location to location [11]. Each country, state, local bodies have their own rules and regulation. So the compliance is one of the most important issues in cloud computing [11].

- **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 CUs through a proper design of its web interface and graphics. Also the CSPs must communicate with the
CUs through video conferencing or other communication media while assigning the resources to a CU. The transparent way of customer dealing by a CSP will help the CSP to gain more user confidence and trust.

The drawbacks of the existing models are found that they hardly focus on the user authentication and those which deal with the user behavior approach lack transparency as their element to establish trust among the CUs.

V. Conclusion and Future Work

This paper focuses on the various trust issues along with the trust elements and trust models that exist for the evaluation of trust among the CUs and the CSPs. It is found from the study that most of the models lack transparency as their element for establishment of trust. User behavior study is based on the way how the user act in using the cloud services and it is found to be eminent for the evaluation of the trustworthiness of the CU and it is found to be equally important for the cloud computing to be used at large by the organizations, individuals, enterprises or educational institutions. There is lot to be done regarding the evaluation of user trust by the CSP in the cloud computing environment in the near future.

REFERENCES