International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 5 Issue 3|| March 2016 || PP.17-23

Trust based Mechanism for Secure Cloud Computing Environment: A Survey

Manisha Sinha[1], Dr. Sanjay Silakari[2] and Dr. Rajeev Pandey[3]
[1]*(M.E. Student, Dept. of CSE, UIT-RGPV, India)*
[2]*(Head of Department, Dept. of CSE, UIT-RGPV, India)*
[3]*(Assistant Professor, Dept. of CSE, UIT-RGPV, India)*

ABSTRACT *:* *Ubiquitous computing has revolutionized interaction of humans and machines. Cloud computing has been mainly used for storing data and various computational purposes. It has changed the face of using the internet. But, as we know every technology has its pros and cons. Securing cloud environment is the most challenging issue for the researchers and developers. Main aspects which cloud security should cover are authentication, authorization, data protection etc. Establishing trust between cloud service providers (CSP) is the biggest challenge, when someone is discussing about cloud security. Trust is a critical factor which mainly depends on perception of reputation and self-assessment done by both user and CSP. The trust model can act as security strength evaluator and ranking service for cloud application and services. For establishing trust relationship between two parties, mutual trust mechanism is reliable, as it does verification from both sides. There are various trust models which mainly focuses on securing one party i.e., they validate either user or service node. In this survey paper, the study of various trust models and their various parameters are discussed.*

KEYWORDS -Mutual *trust, cloud security, secure environment, Cloud Service Node (CSP), and reliability*

I. INTRODUCTION

Over the past few years, cloud computing has interrupted nearly each and every part of IT. Sales, marketing, finance and support all of these applications are reengineered to take advantage of cloud's instant access no download and as we go attributes. Cloud computing is an emerging technology, which is a new pattern of business computing. It can dynamically provide on demand computing services over the internet. Today, most of the organizations all over the world are making use of cloud services. It has been mainly used for huge amount of data storage and computational purposes.

It has become very important paradigm for IT service delivery. As a technology, cloud computing has achieved its goal of being elastic, robust, flexible, economical and readily available. For start-up organizations, which have limited funding, cloud computing provide high-end computing facilities to access various technologies. Cloud computing services leverage the technology that uses the internet and remote server to maintain data and applications. It allows the users to use the applications without actually installing them.

The NIST (National Institute of Standards & Technology) defines the cloud computing as: [1]

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provide interaction."

According to [2]"A cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers."

It provides resource pooling, elasticity, scalability, on-demand services and many other new technologies for performing task with fewer burdens. One of the biggest advantages of storing data in cloud is unlimited access to the data, irrespective of time and place. The figure 1 shows a typical cloud computing environment comprises of user's computer and various networking devices.

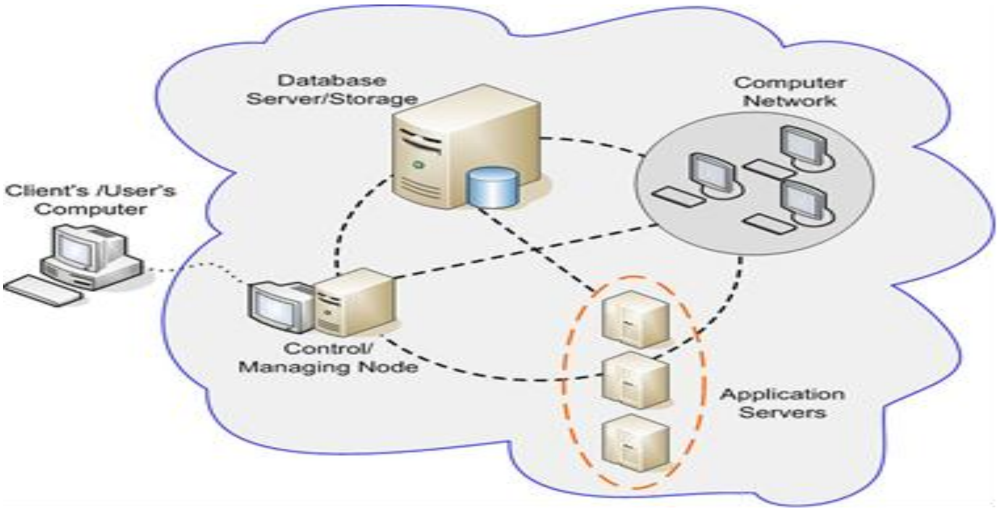

Figure 1: A typical cloud environment. [4]

1.1 Security Measures in Cloud Computing

There are various challenges of cloud computing such as compliance concerns, security and privacy, lack of standards and continuously evolving cloud environment. But among these, most challenging issue in cloud is privacy and security. Security must be an integral but separately configurable part of the cloud. Today, there are various fake cloud service providers, who used to cheat the users or customers by making fake websites. When any user registers with them by login and proving their important credential details, these organizations use the information for their own profit. The most basic example is the fake messages coming from bank websites which are actually send by intruders to the customer. A user should never share his/her important details till he do not get satisfied by the terms and conditions and service level agreement of the cloud service provider.

Irrespective of traditional technologies, cloud has various extra-ordinary features, such as in cloud; resources are heterogeneous, totally virtualized and completely distributed which are belonging to cloud providers.So, in cloud, security concerns are mainly related to risk areas such as lack of control, external data storage, multi-tenancy, integration with internal security. [11] Moving sensitive and critical data to the public cloud environment is of great concern. A cloud service node must ensure that the customers will have excellent security and privacy controls over their applications, data and various services. [12]

Downtime, data loss and password weakness are some of the problems in cloud which we generally do not experience in traditional IT solutions so frequently as compared to cloud environment. The security is often a major of concern for companies who have already adopted cloud services. While dealing with cloud at business or corporate level, the sensitive data i.e., confidential and expensive data is transmitted over the network. Managing such important data at ground level is very much difficult and costly. Generally cloud computing have following security areas, which are mainly concerned: [19]

(1) Physical Security

Cloud service providers have to physically secure the IT hardware; such as routers, servers etc. against unauthorized access, theft, interference, fires, floods etc. and must ensure for essential supplies such as electricity; are sufficiently present without any disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally designed, specified, maintained, constructed, monitored and managed) data centres.

(2) Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, Para- and post-employment activities such as training programs, security screening potential recruits, security awareness, proactive security monitoring and supervision, service level agreements, disciplinary procedures and contractual obligations embedded in employment contracts codes of conduct, policies etc.

(3) Availability:

Cloud providers must ensure that customers can rely on them for accessing their data and applications; at least in part. Failures at any point not only within the cloud service providers' domains but also outside of it. This may disrupt the communications chains between users and applications.

(4) Application security:

Cloud providers ensure that applications available as a service via the cloud are secure by designing, implementing, specifying, testing and maintaining appropriate application security measures in the cloud environment. Consequently, customers are also required to assure themselves that cloud applications are efficiently secured for their specific purposes, including their compliance obligations.

(5) Privacy:

Providers must ensure that all critical data; like credit card number, bank account details etc. are secure in cloud and only authorized users have access to these confidential data. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud. The key security design principles apply to all the detailed security design recommendations. This unified security approach includes the following design principles:

- Assume attackers are authenticated and authorized.
- Do not trust client information initially.
- Use established strong cryptographic techniques.
- Automate security operations.
- Limit routing and audit extensively.
- Implement effective governance, risk management and compliance.

According to cloud security alliance as with any security area the organizations should adopt a risk-based approach to moving to the cloud and selecting security options. They should have good idea of their comfort level for transitioning to the cloud and which deployment models and locations fit their security and risk requirements. The security of cloud mainly depends on the type of cloud i.e., public, private, community or hybrid; being used by any organization. Public cloud is the most vulnerable among all types. As the name suggests, public cloud is easily approachable by anyone. In fact, vulnerable users, like intruders, hackers can easily check the components and they can misuse it. Here, most of the time, authentication of user is not required. As no verification id done from the side of cloud service provider, they remain unaware about the vulnerable elements present in the cloud environment. The private cloud is more secure than the public cloud as it is used by any particular organization. There is need of authentication for being authorized user of the private cloud. But, private cloud has threat from its own authorized users. It means, there can be some user who can use the important and private information of the organization of his own need own greed. And he/she can pass this information to third party, which can be highly vulnerable to the corresponding organization.

The figure 2 various risks and threats which affects the cloud security. These are business risk, legal risk, operations risk and technical risks. Technical risks comprises of malware threats which are one of the biggest threat for the cloud, application vulnerabilities, network threats etc.

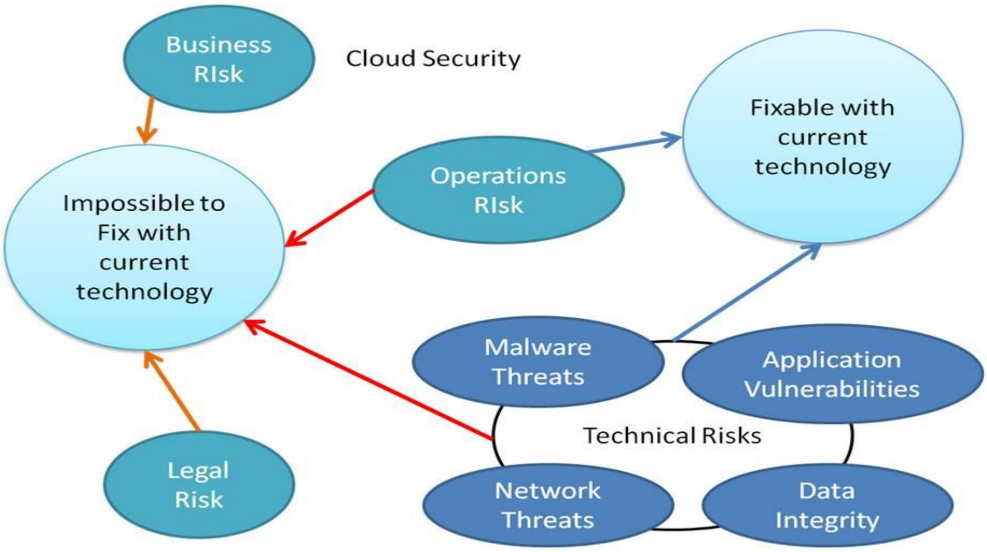

Figure: 2 Cloud Security Risks [19]

Various cloud security attributes are federal policies, configurable security policy management, logical security policies, programmable infrastructure, on-demand elastic service and adaptive trust zones.

1.2 Trust Mechanism for Cloud Computing

Although, cloud computing has so many advantages, but still it restricts clients or users to move to cloud. One the most common and crucial reason is lack of trust between users and cloud service providers. So, for establishing a secure environment for cloud, trust is very much important. Before we learn trust from cloud computing point of view, firstly try to understand, what trust actually means.

Trust can be defined as [13, 14] a subjective mutual measurable relationship between two parties which are willing to act securely reliably and dependably, in a given situation for a context of time.As addressed in [10] "the growing importance of cloud computing makes it increasingly imperative that we grapple with the meaning of trust in the cloud and how the customer, provider, and society in general establish that trust."

Based on the concepts of trust developed in social sciences [15, 16] "Trust is a mental state comprising:

Expectancy - the trustor expects a specific behaviour from the trustee (such as providing valid information or effectively performing cooperative actions);

Belief - the trustor believes that the expected behaviour occurs, based on the evidence of the trustee's competence, integrity, and goodwill;

Willingness to take risk - the trustor is willing to take risk for that belief."

The trust mechanism can provide an efficient way for improving the security of cloud computing. It can be adapted as a solution for the problem of security of the system.

Policy based trust:

PKI is widely used technology that support digital signature, attribute certification and validation as well as key certification and validation. The trust ideas used in PKI can apply formal trust mechanism in cloud.PKI issue and maintain valid public key certificates which is based on certification authority's conformance with certain certificate policies. These certificate policies play an important and central role in PKI trust. [17]

Evidence-based trust:

To use evidence as the attribute in calculating trust, there are two things; one is the trustor's expectation on the trustee. In cloud computing environment, these aspects include performance, security and privacy. And the second one is the trustee's expectation on trustor. This includes capability, consistency and intension of the trustor.By creating trust zones or logical groups of workloads a better and more efficient security can be delivered. Adaptive trust zones in cloud environment provide good security measures for cloud.

1.3 Mutual Trust- A More Reliable Mechanism

Many cloud providers do not expose their infrastructure to customers. And normally, there is not any strict rules regarding verification for reliable and trusted users. The mutual trust mechanism of customer and cloud service provider involves two evaluations. One is trust evaluation of customer's behaviour and the other is trust evaluation of cloud service providers.

- It allows the users to handover their sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., insertion, deletion, updating and block level modification,
- It ensures that authorized users or customers, (i.e., those who have the right to access the owner's file) that they can retrieve the latest version of the outsourced data,
- It enables indirect mutual trust between the users and the various cloud service nodes, and
- It allows the owner to grant or revoke access to the outsourced data.

Trust model of customer's behaviour**:** This is done by collecting commonly used parameters in cloud interactions, such as application vulnerability, resource utilization rate, user's access frequency. [10]

The figure 3 shows about the user's trust model, which defines how user is verified by authentication and declaration. Then cloud service node verifies the user by doing several verifications, and after doing this procedure, it gives the conformation to the user for using the services.

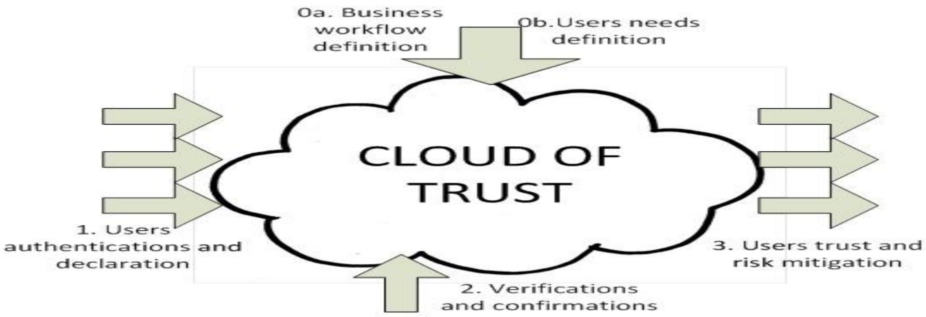
0a. Business workflow definition
0b.Users needs definition
CLOUD OF TRUST
1. Users authentications and declaration
2. Verifications and confirmations
3. Users trust and risk mitigation

Figure 3: User's Trust Model [19]

Trust model of cloud service providers:Cloud users tend to nodes with high credibility, just like ants always select the path having high level of pheromone concentration. [10]
Mutual Trust:It is the confidence that both customers and cloud service nodes show to each other for future interactions. While calculating mutual trust of any cloud computing environment, there are various parameters which one should know, direct trust, trust pheromone, heuristic pheromone, mutual trust threshold.

Cloud users always use to choose the service nodes which have high credibility for using resources or services, and ants always choose the path to their destination which has high level of pheromone concentration. The trust degree of any node must be high then only user will select it for using services. Trust degree means how reliable is a particular node or any user or customer.Ant colony optimization (ACO) is a problem solving method and can be easily combined with other methods, so it is feasible to apply ACO in mutual trust mechanism for cloud computing environment.

II. LITERATURE REVIEW

2.1 Mutual Trust Based Access Control Model

In cloud computing there are various on demand services like virtualization and some others are offered to the user. But in these services there are various can be occurs an issue which mentioned is called as access control issues. In [10] a mutual trust based model is presented. This uses an access control mechanism with trust management to provide an access control over the cloud data. In this technique user's behavior and credibility of the services is used to manage the build a trust management for the access control. To solve such problems a trust based control management is used, in that a trust management is used to restrict unauthorized access in the given system. In trust management techniques different trust levels for the user is assigned to access the data. In that different access at the different level is provided. The two-sided verification of user and cloud service provider provide a secure environment.

2.2Secure model using various trust level

In [18] a trust model based measurement technique is used which provides an enhanced functionality to deal with such problems which can be occurs in access control in cloud computing. In that a trust model is used to provide various trust levels to the user to access cloud data. In this method, various security measures in cloud computing is provided to get access to that data. An evaluation of the various parameters which consists security concerns in cloud services is presented. Different parameter consist different value, sub-parameters and functions. On the basis of these parameters and these functions various trust levels are assigned to the user to provide better access for that data.

2.3 Centralized access control model

In [11] a centralized access control mechanism is presented. In that multi parameter and multifactor user based authentication system is presented, which defines various access levels for the different users. An admin have all the access control to the data. In this way, it provides an enhanced framework to provide access control in cloud storage. In that system authentication of the user is a multi-step process, once user gets authenticated then user can access the data file which he owns. In that way user can access only the file which he/she owns. That protects data from unauthorized access.

2.4 ACO based access control mechanism

In [5] an ant colony system (ACS) based access and control mechanism technique to resolve the security issues in cloud computing. In existing techniques a K-mean clustering technique is used to provide authentication but this technique belongs to lazy learning family and required an enhancement to get better performance for the system. Ant colony based system is an widely used technique which used to provide better results for the authentication and access control issues in the cloud computing. But ant colony system is also dependent on the parameters. Thus a technique is required to provide some better performance for the access control in cloud scenario.

2.5 Various trust management models

In [6] a review over the various techniques which used to various security issues in cloud computing is presented. there are techniques like provable data possession, proof of retrievability, HAIL, Plutus, Sirius, attribute based encryption etc. are used to provide access control in cloud computing. But a mutual trust between cloud service provider and the data owner is the biggest issue in these techniques. Thus a mutual trust based access control model is presented, which considers mutual relation between the cloud service provider and cloud service consumer, to provide better access control for the data.

2.6 Indirect mutual trust based technique

In [7] a dynamic data and indirect mutual trust based technique is presented. In that technique owner's data stored at cloud server and dynamic updating for that data is provided to the user. It also provides latest outsourced data to the user. It enables indirect mutual trust between the owner and the cloud service provider (CSP). It provide grant or revoke access to the data. Thus, this technique provides an enhanced functionality to provide access control for the user. In that technique digital signature based technique is used to provide access control for the user.

2.7 Various attacks and vulnerabilities in cloud environment

In [8] a review over the attacks, vulnerabilities which occurs in the process of cloud computing is presented. In cloud computing various on-demand services are provided. That reduce users cost and infrastructure overhead to perform tasks. But there are several attacks to get any unauthorized access to these services are performed by the various intruders or unauthorized users. In cloud virtual machines are provided to the user to access various cloud services and provide a cost effective way to access these services. But vulnerability in this virtual machine can generate various threats to the services like issue of the privacy and security of the user's data. Thus to reduce these threats techniques are required to provide better access to the user.

2.8 Mutual trust oriented security model

In [9] a mutual trust oriented security model for the access control in the cloud computing is provided. In cloud computing various on-demand services are provided to the user. But there are various issues related to these services are also presented. Like issues related to the security of the data are also there thus access control system is used to provide controlled access to the user and also reduce the risks of unauthorized access. In traditional access control system some issues occurred thus new mutual trust based access control system is presented. In existing systems there is no trust for the users is taken to provide access control. But in trust based model a trust level is used to provide better access control for the user.The comparison table gives the detail information about various access mechanism, their advantages and disadvantages.

Table 1: Compression table for different techniques used to provide access control in cloud computing

S.no	Technique	Advantages	Disadvantages
1	Role based access control mechanism	Different role for the various user to access cloud data is assigned	Still trust and reliability is required.
2	Dynamic data and indirect trust based system	A flexible dynamic mutual trust based technique is provided. Updated outsourced data is provided	Proper management for the security is missing
3	Mutual trust based Access control system	A mutual trust among the different users are provided which is missing in existing techniques	Functionality for the trust management is required.
4	ACO (Ant colony optimization) based access control mechanism	Ant colony optimization based technique is used to provide access control to access cloud services.	ACO having inherent defects like depends on the parameters and not able to provide a global solution for the problems

III. CONCLUSION

In cloud computing a huge amount of data can be shared over the web among different users or cloud clients. Thus, the security and privacy of the data is the biggest concern in cloud computing. An access control mechanism is required to restrict unauthorized access to the data. In this paper, survey of various trust based model in cloud computing were studied and analysed. Hence the security of cloud computing environment can be enhanced using trust models. A new framework to provide more reliable and secure access control for the user's data can be used for the future work.

REFERENCES

[1] P. Melland T. Grance, “The NIST definition of cloud computing (draft),” NIST special publication, vol. 800, no. 145, pp. 7-11, 2011.

[2] Buyya R., Yeo, C S., Venugopal , S., Broberg, J., &Brandic, I. Cloud computing and emerging IT platforms: Vision hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 2009. 25(6), 599-616.

[3] Li W, Ping L: Trust model to enhance Security and interoperability of Cloud environment. In Proceedings of the 1st International conference on Cloud Computing. Beijing, China: Springer Berlin Heidelberg; 2009:69–79.

[4] Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.

[5] Bhatt Akshaykumar1, Mohammed HussainBohra “A Secured Cloud Computing Mechanism for Enhancing Mutual Trust Access Control” IJAERD, 2015.

[6] Anup R. Nimje, V.T. Gaikwad, H.N. datir “A Review of Various Trust Management Models for Cloud Computing Storage Systems” IJECS, February 2014, 3(2) pp. 3924-3928

[7] AyadBarsoum and Anwar Hasan “Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems” IEEE, 2013.

[8] ChiragModi, Dhiren Patel, BhaveshBorisaniya, Avi Patel, MuttukrishnanRajarajan “A survey on security issues and solutions at different layers of Cloud computing” Springers, 2013.

[9] Abdul FahadRahman, Neethu V M, Ranjith T K, Radhika K, Ranjith Ashok, Nicy K S” MACINTOS: Mutual Access Control in Trust Oriented Security Model in Cloud Computing” IJCIT, 2015.

[10] LIN Guoyuan, WANG Danrul, BIE Yuyul, LEI Min “MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing” china communication, 2014.

[11] Sultan Ullah, ZhengXuefeng and Zhou Feng “TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing” IJSIA, 2013.

[12] Al-Sakib Khan Pathan1 • Mohssen M. Z. E. Mohammed “Building Customer Trust in Cloud Computing with an ICT-Enabled Global Regulatory Body” wireless perscommun, 2015.

[13] Viriyasitavat, W., & Martin, A. Formal trust specification in service workflows. IEEE/ IFIP 8th international conference on embedded and ubiquitous computing (EUC), 11–13 December, 2010, pp. 703–710.

[14] Viriyasitavat, W., & Martin, A. (2012). A survey of trust in workflows and relevant contexts. IEEE Communications Surveys & Tutorials, 14(3), 911–940.

[15] Blomqvist K: The many faces of trust. Scand J Manage 1997,13(3):271–286.

[16] Mayer R, Davis J, Schoorman F: An integrative model of organizational trust: Past, present, and future. Acad Manage Rev 1995,20(3):709–734.

[17] Huang J, Nicol D: Implicit trust, certificate policies aand formal semantics of PKI. Information Trust Institute, University of Illinois at Urbana-Champaign. 2009.

[18] RizwanaShaikh, Dr. M. Sasikumar “Trust Model for Measuring Security Strength of Cloud Computing Service” science direct, 2015.

[19] https://en.wikipedia.org/wiki/Cloud_computing.