www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-2, April 2018
Review Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

A Comparative Analysis of Trust Models in Cloud Computing

U.Kaur[1*], M. Mahajan[2], D. Singh[3]

[1]I.K. Gujral Punjab Technical University, Jalandhar, Punjab, India
[2]Department of Computer Science & Engineering, CGC, Landran, Punjab,India
[3]Department of Computer Science & Engineering, CCET, Punjab, India

Received: 07/Mar/2018, Revised: 20/Mar/2018, Accepted: 15/Apr/2018, Published: 30/Apr/2018

Abstract: Today cloud computing plays a vital role in the industry of internet applications; it covers a vast area of services which are directly or indirectly related to the online data sources. Trust models are playing a very crucial job in cloud computing sector and today trust is the only thing which is the biggest challenge to cloud-based technologies. There are lots of trust models techniques are available in the area of cloud computing to increase the levels of trust in between users and service providers. This survey briefly analyzed the factors and working aspects of cloud-based Trust models and it also compares the factors of different types of Trust models, which are calculating trust values using so many different types of parameters such as data integrity, service availability and data turnaround efficiency.

Keywords: cloud computing, data reliability, trust models, trust management, authentication, cloud security.

I. INTRODUCTION

Cloud computing has already opened the gates of huge possibilities in the area of online services and blob based storage structures. A very good example of successfully implemented cloud-based service is Azure, which is a product of Microsoft and it is extending the existing capabilities of Information Technologies. Cloud computing is an evolving platform which offers dynamic, scalable, shared elastic resources through the internet from remote data centers to the consumers. It acts as a catalyst for the enhancement of business growth. But this technology is still struggling with some issues such as trust, security, privacy which act as the main obstacle to the adoption of cloud computing. Data security is the very crucial aspect of cloud computing because if users lost their trust in cloud-based services it could not be possible to achieve the growth in this sector. To curve this problem it is must use Trust models for the development of trust based cloud computing services.

Cloud consumers usually worried about security and control over the data. A Survey is conducted by the Fujitsu research institute in 2010 on 3000 consumer as in six countries which are Australia, Japan, UK, US, Germany, Singapore [1]. It has been concluded that consumers staying in different countries have different concerns about sharing of data and accessibility of data. In the US 90% of consumers want that permissions must be approved before their data be shared but in Japan, only 77% of Japanese consumers want the facts and strict permissions regarding data privacy [1].

The paper is organized in the following sections such as Role of Trust in covered in section II. Section III covers Trust – Based Models. Section-IV includes comparsion of trust models and Section-V Different approaches of trust models.

II. ROLE OF TRUST

The term trust is an important concept in the paradigm of cloud computing. Cloud Computing provides a virtual platform for the entities which may be classified both as consumer and service providers to interact with each other. As cloud computing provides resources to consumers in three layers such as Infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS). In the IaaS infrastructures such as storage space, servers, networks, and applications are provided to the consumers. Trust factors responsible at this layer are processing speed, bandwidth, fault rate, initiation time[2]. PaaS deals with the deploying the platform for building the applications over the internet whereas in the SaaS software are deployed by the consumers through the browser or any other interface. In the PaaS, SaaS layers trust factors are reliability, integrity and many more. In this entity has the right to access resources in a sharing manner or mode. However, it affects the notion of privacy of the sensitive, confidentiality of information. According to the survey conducted by the Fujitsu, consumers are concerned about the privacy of their data and who has access to the information [1]. On the other side, if users want to use their contents in non-sharable mode, it restricts the concept of the cloud computing which emphasis on flexible, scalable resources. It works as the main problem in the adoption of cloud computing. So, there is an urgent need for a trust model which binds the trust between the two.

The term trust can be defined in various directions such as qualitative and quantitative. In the qualitative direction, trust is defined as it depends on few parameters such as honesty, competence, truthfulness and many more [3]. The main purpose of the trust is to inculcate faith in the entities in the service provider which ultimately particularly influences the development of cloud computing. The computation of trust is calculated depends on the type of the trust model.

Trust model acts as an interface between the user/consumer and resource provider. Clients set up an agreement between consumer and provider. Trust model helps to choose the best reliable service provider. It also helps to set up an SLA agreement between the consumer and cloud service provider. There exist several trust models such as identity-based, reputation-based, behavior and capability based on a cloud computing each with varying characteristics. The value of trust can be computed by the depending on the trust model.

III. TRUST-BASED MODELS

- **FIFO Model**: It comes under the categorization of the non-trusted model. In this model, list of potential cloud resources for a particular user QoS requirement is identified and a job is allocated to the first cloud resource [4].

  Advantages:
  (i) Simple, efficient and easy to implement.
  (ii) No complex algorithm.

  Disadvantages:
  (i) It is a non-trusted model.
- **QoS Trust Model:** It falls under the category of trusted models by PaulManuel. Quality of Service (QoS) is based on the attributes such as availability, reliability, data integrity and turn around efficiency. It works according to following equation [3], in which Cloud resource with the highest value is selected for the job[4].

  QT= w1*AV+w2*RE + w3*DI +w4*TE Equ (3)

- **Combined Trust Model**: [4] In this architecture of trust models – three models named as Capability, Identity and Behavior - based Trust. In this framework, a job is proposed to the cloud resource selected. The decision is based on the three attributes.

- **SLA Based Trust Model**: In these model two inputs such as service level agreements criteria and experiences of users are used to test the level of trustworthiness for resources used in the cloud. The main characteristics of this model are that it can be implemented for different domains of cloud services and based on those domain users are able to obtain particular trust value of the same type of services [5].

- **Trust model for a file Exchange:** In Canedo, E. D., de Sousa Junior Et. al proposed a trust model for a file exchange in a secure and reliable manner. This trust model focuses on computational problems in an area related to security, trust, and reputation to ensure exchange of files on private cloud [6].

- **Interaction based Trust model:** Ahmad et al. propose a trust model based an interaction between the cloud provider and user [7]. This model works in three turns the first turn consists of satisfaction level of the user for previous experience of a cloud provider. In the second turn, the user must have concerns about cloud computing issues such as SLA, cloud advantages and disadvantages related to securities at different levels. Second turn emphasis on implementation of different securities cloud provider can be assumed to be reliable. At the third turn, a user can trust on the reliable cloud provider.

- **Trust Evaluation Model:** Xiaonian Wu et al. proposes a trust evaluation model based on D-S evidence theory and sliding windows for the evaluation of the credibility of the entities and detect the malicious entities[8]. In this architecture of trust model first-hand evidence is interaction among entities and sliding window is used to evaluate the timeliness of interaction evidence. Trust is calculated on the basis of D-S theory with help of interaction devices.

- **Turnaround trust Model:** In this trust model cloud resources will be selected according to the two factors such as trust and run-speed. Further, trust is a composition of availability, reliability and data integrity and turnaround efficiency. It works according to the following equations, which are used to calculate the values [9].

  Trust value of resource = w1*AV + W2*RE +W3*DI +W4* TE (Eq. 3.1)

  Run-speed value = $CPU_{JOB}/CPU_{RESOURCE}$(Eq. 3.2)

  Turnaround trust = w1*TRUST +w2 *run-speed (Eq. 3.3)

- **Behavior-Based Trust Model:** In these types of models system follows the user behavior transactions history to judge the behavior and privacy of grid entities, it is also helpful to protect cloud resources and cloud-based application. This model dynamically judges the security levels of the cloud-based services and due to this mechanism, the service provider can

easily detect the user behaviors so they can easily fulfill the security-related requirements [4].

- **TVEM Based Trust Model:** Trusted Virtual Environment Module (TVEM) is trust- based module software which provides trust- based services to a virtual environment of cloud-based services [10]. This module is a protection module and plays a vital role in the trust for a virtual environment which can be situated at any remote location and the virtual machine environment has the migration based possibilities to other platforms. The only downside point of TVEM is it cannot be implemented in hardware, we can only implement this trust-based module in a software. The reason behind this is TVEM is a software, which is working based on the phenomena of Trust base data module and cryptographic confidentiality module.

- **Collaborative Trust Model:** In this paper, they are using approach based cloud computing to elaborate the dynamic context and definition of risk signal [11]. This approach provides a collaborative trust model which provides firewall based on cloud services environment, it has three advantages: First, they are adopting for the different policies for the different level of domains. Secondly, this model captures the transaction context and the historical entity based data to detect the entity influences and the trust measurement values dynamically. Thirdly, this model fully compatible with the firewalls, it also does not challenge/break the local control policies of firewalls.

IV. COMPARISON OF TRUST MODELS

The following table discusses the trust model concepts, their pros, and limitations.

Table 1: Comparison of trust model approaches

S No.	Trust Model Approaches	Concepts	Pros	Limitations
1	Trust Model by Ahmad.[7] Cloud Provider's and cloud User	Based on three turns- first turn, second and third turn. The first turn considers the previous experience of cloud users. In the Second turn, user has aware of cloud computing concepts such as SLA, Advantages, and disadvantages.	Transparency between the entities (Users and providers).	It does not check malicious feedback by a user.
2	Trust Model for File Exchange.[6]	Trust is evaluated on the basis of node storage space, link, and processing, operating system.	Selection of reliable node for an exchange of files.	_____
3	QoS based trust model.[4]	Calculation of Trust value based on parameters reliability, data integrity and turn-around efficiency.	Best resource provider is selected.	Dependency on user requests.
4	QoS trust model for IAAS[2].	Model is proposed on parameters such as initiation time, processing time, bandwidth, fault rate, price [2].	(i) It is cost effective. (ii) Increased value of QoS.	Non-quantifiable Characteristics are compared.
5	Trust model Using firewall [12].	Model is built on the concept of firewall which enhances security in different domains such as inter and intradomain trust relationships. Calculation of trust depends on the context and entity's history behavior.	Robust, Secure, Performance is better. It has multiple advantages different security policies are framed. Transaction, context, historical.	An absence of transaction topic in the computation of trust value[12,13].

IV. DIFFERENT APPROACHES OF TRUST MODELS

V.

The following table analyzes the performance of various trust models and the different approaches of trust models in terms of parameters such as availability, reliability, data integrity, turn-around efficiency, complexity, efficiency, accuracy and its application domain.

Table 2: Comparison of trust models based on parameters

TRUST MODELS	Availability	Reliability	Data Integrity	Turn-around Efficiency	Complexity	Efficiency	Accuracy
FIFO Model	Low	Low	Low	Low	Low	Low	Low
QoS Trust Model	High	High	High	High	High	High	High
TVEM Based Model	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Turn-around Trust Model	High	High	High	High	High	High	High
Collaborative Trust Model	Medium	Medium	Medium	Medium	High	High	Medium
Behavior-Based Model	Medium	Medium	Medium	Medium	Medium	Medium	Medium
SLA Based Trust Model	Low	Low	Low	Low	Low	Low	Low
Trust Evaluation Model	High	High	High	High	High	High	High

CONCLUSION

The term trust which acts as a catalyst in the growth of cloud computing has been analyzed in various existing trust models. In this paper, a survey on trust models based on various techniques has been provided. The trust model has been compared from different perspectives such as concepts, advantages, and disadvantages. Furthermore, some trust models have been compared in terms of parameters such availability, reliability, turn-around efficiency, data integrity, complexity, efficiency. This review may help the reviewers and service providers to select a best suited Trust model for their services to gain trust-based transactions in between users and service providers.

ACKNOWLEDGMENT

Authors are highly thankful to the department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

REFERENCES

[1] M. Sato, *"Personal data in the cloud: A global Survey of Consumer attitudes"*, Fujitsu Limited, Japan, 2010.

[2] M. K. Goyal, A. Aggarwal, "*QoS based trust management model for Cloud IaaS*." In the proceedings of the 2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC), India, pp. 843-847, 2012 .

[3] P. D. Manuel, M. I. Barr, S. T. Selvi, *"A novel trust management system for cloud computing - IaaS providers*", JCMCC-Journal of Combinatorial Mathematics and Combinatorial Computing, Vol. 79, Issue.3, 2011.

[4] P. Manuel, *"A trust model of cloud computing based on Quality of Service"*, Annals of Operations Research, Vol.233, Issue.1, pp. 281-292, 2015.

[5] M. Alhamad, T. Dillon, "*SLA-Based Trust Model for Cloud Computing*", In the proceedings of the 13th International Conference on Network-Based Information Systems, Japan , pp. 321-324, 2010.

[6] E. D. Canedo, R. T. Junior, "*File Exchange in a Private Cloud supported by a Trust Model*" , In the proceedings of the 2012 International conference on Cyber-Enabled Distributed Computing and Knowledge Discovery , China, pp. 89-96, 2012.

[7] S.Ahmad, B. Ahmad, S. M. Saqib, R. M. Khattak, "*Trust model: Cloud's provider and cloud's user*", International Journal of Advanced Science and Technology, Vol.44, pp. 69-80, 2012.

[8] X. Wu, R. Zhang, B. Zeng, S. Zhou, *"A trust evaluation model for cloud computing*", Procedia Computer Science, Vol.17, pp.1170-1177, 2013.

[9] A. Gholami, M. G. Arani, "*A trust model based on quality of service in cloud computing environment*", International Journal of Database Theory and Application, Vol. 8, Issue.5, pp.161-170, 2015.

[10] F. J. Krautheim, D. S. Phatak, A. T. Sherman, "*Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Computing*", In the proceedings of the International Conference on Trust and Trustworthy Computing, Germany, pp. 211–227,2010.

[11] Z. Yang, L. Qiao, "*A collaborative trust model of firewall-through based on Cloud Computing*", In the proceedings of the 2010 14th international conference on Computer supported cooperative work in design , China ,pp. 329-334, 2010.

[12] S. Ries, J. Kangasharju, " *A Classification of Trust System*", In the proceedings of the OTM_Confederated International Conferences " On the Move to Meaningful Internet systems", France, pp. 894-903, 2006.

[13] A. Gholami, M. G. Arani, "*A trust model for resource selection in cloud computing environment*", In the proceedings of the 2nd In Knowledge-Based Engineering and Innovation (KBEI), Iran, pp. 144-151, 2015.

[14] F. Messina, G. Pappalardo, "*A trust-based approach for a competitive cloud/grid computing scenario"*, In the proceedings of the 6th International Symposium on Intelligent Distributed Computing, Italy, pp. 129-138, 2013.

[15] Z. Chen, W. Yao, "*Security and trust model for data disaster-recovery service on the cloud*", In In the proceedings of the International Conference on Trustworthy Computing and Services, China, pp. 140-147,2012.

[16] A. Chandrasekar, K. Chandrasekar, " *QoS Monitoring and Dynamic Trust Establishment in the Cloud*", In the proceedings of the International Conference on Grid and Pervasive Computing, China, pp. 289-301, 2012.

[17] R. K. Ko, P. Jagadpramana, "*Towards achieving accountability, auditability and trust in cloud computing*", In the proceedings of the International Conference on Advances in Computing and Communications , India pp. 432-444 , 2011.

[18] D. J. Kim, D. L. Ferrin, H. R. Rao, "A *trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents*", Decision Support Systems, Vol. 44, Issue. 2, pp. 544-564, 2008.

About the Authors

Usvir kaur, pusing Ph.D degree from IKGPTU, Jalandhar. She has received M.Tech degree from Punjabi University, Patiala in 2010. She has done her B.Tech degree from GNDEC,Ludhiana. Her research interests are cloud computing, network security and web mining. She has published numerous papers in international, national journals.

Dr. Manish Mahajan has completed his Ph.D degree of Computer Science & Engineering in 2016. He has completed his M.Tech from B.B.S.E.C, Fgs. He has completed his B.Tech in information technology in 2004 from M.M.E.C, Mullana. His research fields are image processing, information security and steganography. He has published various research papers in international , national journals. He has membership of various professional societies such as IAENG, ICST,CSI and many other.

Dr. Dheerendra Singh currently working as a associate professor at Chandigarh college of Engineering & Technology. His research interests are Cloud Computing, Web Engineering, S/w Engineering, Operating Systems, Data structures & Programming, C++ Language. He has published numerous papers in international , national journals.

