Jestr

Journal of Engineering Science and Technology Review 10 (2) (2017) 213- 219

Review Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

A Review on Various Trust Models in Cloud Environment

Priya Govindaraj* and N Jaisankar

School of Computer Science and Engineering, VIT University, Vellore, India

Received 24 March 2016; Accepted 12 March 2017

Abstract

Trust plays a crucial role in cloud environment to offer reliable services to the cloud customers. It is the main reason for the popularity of services among the cloud consumers. To achieve this, trust should be established between cloud service provider and cloud consumer. Trust management is widely used in online services, E-commerce and social networks. This review paper focuses on the compilation of the work done by various researchers on trust estimation of service providers and categories of trust models. An attempt is made to identify the various types of trust, quality of service parameters to be considered for trust evaluation and three trust models namely service level agreement (SLA) based trust , recommendation based trust and reputation based trust among various trust models as reported in literature. In this paper, the prime contribution is about various trust mechanisms involving in trust evaluations.

Keywords: Trust, SLA, Reputation, Recommendation

1. Introduction

The development of cloud computing technology in various domains is huge for the last two decades. Even though it has many features but then privacy, security and trust are the most important concern. The cloud consumers don't be aware of their data exactly where it is kept and whether the documents are safe? On what basis the cloud user will trust on cloud providers? Who will be responsible for monitoring, assessing or validating cloud attributes? To answer all the above questions, trust should be adopted in cloud environment. Trust management is introduced by Blaze, M in the year 1996 to overcome the following issues, such as centralized trust, rigidity to support complex trust relationships in large networks and the different forms of policy languages which are used for setting authorization rules and applying security policies [5]. Cloud computing definition is given by "National Institute of Standards and Technology (NIST), it provides three development models SAAS (software as a service), PAAS (platform as a service) IAAS

(Infrastructure as a service) and for deployment models private, public cloud, hybrid and community cloud" [26]. Hassan Takabi et al. have stated that if a user requires any resource first he need to give the request to providers. The request may be handled by different service provider's .In that situation, the trust should be maintained among the cloud provider and customer [17].

Priya G, and N.Jaisankar have examined that the customer gets satisfied not only with service provider assurance but also they are expecting QoS metrics namely reliability, availability, user feedback and customer support [40].

P.D.Manuel et al. stated that the customer wants to use the resources or deploy the resources securely then trust should be addressed and trustworthy domain should exist. In such case, provider and consumer do not have governance on each other. The cloud service customer expects excellent and quality service from the trusted cloud service providers. The provider expects the cloud services should be secured and it let the cloud services should be used by the reliable consumer. The main aim of the trust management in cloud services is to create confidence and faith on providers in the distributed environment [27].

Kai Hwang and Deyi Li have investigated that the customer feedback, QoS, deployment models, reviews, portability and security parameters need to be taken to ensure the trust worthy service provider [22]. Khaled M.Khan and Qutaibh Malluni stated that Customers lose their trust on provider when many of the above stated metrics are not achieved [24]. Buyya, R et al. have defined that customer feedback is an important metric to avoid the major risks in trust [7].

"Cloud Security Alliance, Security Trust and Assurance Registry (CSA STAR)" is an openly accessible database which keeps track of security documents provided by various cloud computing providers and [9]. It is the most governing program for security guarantee in the cloud environment. CSA STAR helps users of cloud services in the following ways:

- Get an apparent view of cloud provider security practices.
- Recognize which providers harmonize the offered infrastructure.
- Maximize long-term savings with vendor clearness.
- Gain knowledge from lessons learned from a group of cloud users.

*E-mail address: gpriya@vit.ac.in

CSA STAR helps the cloud service provider in the following ways:

- To find tools that help set up and manage a vigorous security program.
- To assess their own security level with a corresponding level one certification.
- To edify prospective users on good practices.
- To show increased cloud computing maturity through additional certification.
- To set service provider as a trusted provider to the customers.

Habib, S.M et al. have mentioned that the trust is established in two ways, hosting trust models in centralized storage area and decentralized trust models. In the former method, it needs trusted third party to work on the data. Because user can operate the data apart from the ratings they provide. Since the data is distributed among the entities, it is very difficult to preserve the privacy in the decentralized model [15].

This survey paper is written in the following order, In section 2, this paper confer an overview of trust management which contains the semantics of trust, types of trust and attributes for trust assessment. Section 3 discusses about the various trust models namely SLA Based, Recommendation and Reputation based trust in detail. Section 4, confer the limitation on the existing trust models used in this review paper. Finally, Section 4 contains the conclusion.

2. Overview of Trust Management

2.1. Semantics of trust

There are two actors namely trustor and trustee played a vital role in trust management. Trustor builds the trust and trustee manages the trust. In cloud computing environment service customer is being a trustor and service provider is being a trustee. Huang,J. and Nicol D. has proposed the following trust definition "Trust is an intellectual state which contains expectancy in which the trustor expects an exact activity from the trustee, Belief in which the trustor trust the predictable behavior occurs based on the proof of trustees ability, reliability and support and the trustor is keen to acquire the risk for that trust" [18].

Flavio Corradini et al. have stated that trust life cycle contains three activities such as trust establishment, trust update and trust revocation [12]. A. Josang et al. have defined that "Trust is the subjective belief of one entity about another entity within a specific context at a specified time" [4].

2.2. Types of trust

Trust is broadly classified based on trustors expectancy and experience. Based on trustor expectancy further it is divided in terms of performance and belief of trust. Two types of trust based on experience are direct trust and recommended trust which is given in Fig. 1.

Zhu, H Bao and Deng have classified trust into direct and recommended trust. Direct trust is the trust based on own experience with other entity. Trust is established by third party's recommendation when two entities have no direct interactions is called as recommended trust [46]. Jingwei Huang and David M Nicol have proposed two trust types namely trust in performance and trust in belief. "A trust in performance can be denoted by trust_perform (t, e, p, c) which represents the trustor t trusts trustee e concerning e's performance p in circumstance c. If p is made by e in circumstance c then t trusts p in that context. A trust in belief can be represented by trust_b(t,e,b,c) which denotes the trustor t trust the trustee e concerning e' s belief of b in circumstance c. If e trusts b in circumstance c then t also trusts in that circumstance c [21].

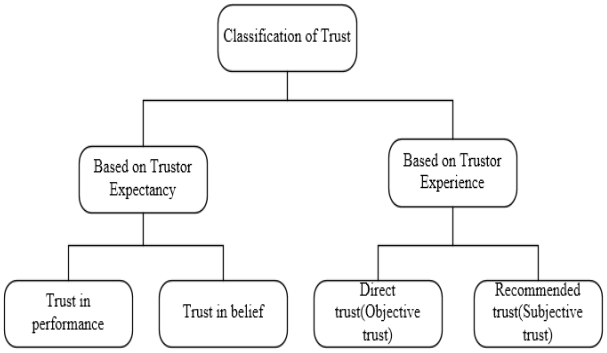

Fig. 1. Classification of trust

2.3. Parameters for Trust Evaluation

Habib, S.M et al. have used multiple capabilities such as accessibility, security and compliance to identify the quality cloud providers [16]. Grandison, T. and Sloman (2000) have defined that the trust is the collection of several parameters namely consistency, trustworthiness, honesty, security, competence, suitability, QOS and return on investments (ROI) [13].Abawajy, J (2011) Stated that trustworthiness mean reliability, capability, security and availability [3].

Table 1. Dimensions used in various layers to assess the Trust Management Issues [36]

Layer	Attributes Used
The Trust Feedbacks Sharing Layer	Credibility ,Privacy Personalization and Integration.
The Trust Assessment Layer	Perspective, Compliance ,Security ,Scalability and Applicability
The Trust Results Distribution Layer	Retort time, Redundancy, Exactness and Confidence

Talal H Noor (2013) has defined set of trust characteristics including authentication, certification, security, confidentiality, and virtualization accountability and consumer availability for analysing various service providers. The author has identified the set of attributes on three layers of the proposed framework to study the trust management issues. A dimension used in each layer is given in table.1 [36].

Wanita Sherchan et al. have identified the basic properties of trust and reputation are subjective, relational, dynamic, propagative, non-transitive, asymmetric, slow, event sensitive, indirect trust and direct trust [39].

Qiang Guo et al. and Abassi and Fatmi have represented that the trust model is built based on the following properties namely asymmetry, reflexivity, context dependence, scalability, partial transitivity, subjective, uncertainty, space based and time based [1, 28]

Sheikh Mahbub Habib et al. have presented various approaches to establish the trust between the customers and the cloud service providers. They categorize these approaches as service level agreements (SLA), audits, measuring and ratings and self-assessment questionnaires. They have identified that there is a lack of a common approach to support the customers in choosing the trustworthy service providers. To overcome these problems trust and reputation models have been used [33].
Habib, S.M et al. have identified various QoS+ parameters to combine trust and reputation in cloud computing which is given in Tab 2. They have stated that trust management system should obtain a mechanism to cumulate multiple attributes regardless of various evaluation procedures used to evaluate the subjective trust parameters i.e. recommendations by other customers or objective trust attributes namely skilled ratings or real time measurements of resistance and response time.[15,16].

Table 2. QoS+ parameters and approaches used [15, 16]

QoS+ parameters	**Approaches to derive the information**
SLA	Standardized SLAs
Compliance	Audit, Standards, Cloud control matrix
Customer support	SLAs, User feedback
Portability	SLAs
Interoperability	
Geographical location	
Performance	Measurement, user feedback
Federated Identity management	SLA
Security	Audits, CSA CAIQ, Certified based attestation mechanism
User feedback	Ratings and Measurements

Raj, G et al. (2014) have identified eight parameter boundaries for trust namely transparency, SLA, policy compliance, security and privacy, portability, performance, authentication, access control and customer support [30].

3. Trust Models

The evaluation process of system trust is called as trust modelling. Jingwei Huang and David M Nicol have proposed several trust methods such as SLA verification based trust, reputation based trust, TAAS (Trust as a service) and cloud transparency trust. In cloud Transparency trust, provider provides self-assessment in either a "Consensus Assessments Initiative Questionnaire (CAIQ) or a cloud controls matrix". The limitation in this model is dishonest provider who can change the data. TAAS model introduces third-party professionals. Cloud trust authority offers a solo end for managing cloud services security from various providers. The limitation exists to form the trust relation among the users and trust brokers [21].

Flavio Corrandini et al. have classified the trust models into three categories. They are policy based, recommendation based and reputation and feedback based trust. They simplify the classification to avoid the complexity in trust models when they belong to different groups. Services provided by different service provider are fully distributed, virtualized and heterogeneous. The existing trust mechanisms such as authentication and authorization are not proper for cloud environment [12]. P.D. Manuel et al. have proposed two trust models namely reputation and transitive trust model. The recommendation from the recommender is highly focused for the trustworthiness in transitive trust model. In reputation trust model, value of the trust is computed from the capability based, identity based and behaviour based trust [27].

Girish Suryanarayana and Richard N.Taylor have categorized trust models into reputation, policy and social network based trust [14]. Talal H Noor et al. have classified the trust management with respect to two perspectives such as service provider and service requester. In service provider perspective, the service provider will assess the trustworthiness of the service requester. In SRP, Service requester will assess the trustworthiness of the provider. The author classifies the trust management into four types, reputation, policy based, recommendation and prediction based trust model [36]. The authors Qing Zhang et al. have presented the trust functions based on the four dimensions objective trust versus subjective, opinion based versus transaction, localized information versus complete information and rank based versus threshold based trust [29].

Kanwal, A et al. have proposed an evaluation metrics for trust models based on security and data control parameters and the QoS attributes. The following criteria have been taken data integrity, QoS attributes, data control and ownership, process performance control, detection of untrusted entities, dynamic confidence update and logging and model complexity [23]. Trust models have been categorized based on Contract, certificate/secret keys and feedback ratings. Having done a detailed review on various categories of trust models proposed by many authors, we classify the trust models into three types SLA based, recommendation and reputation Trust model which are represented by the following Fig. 2.

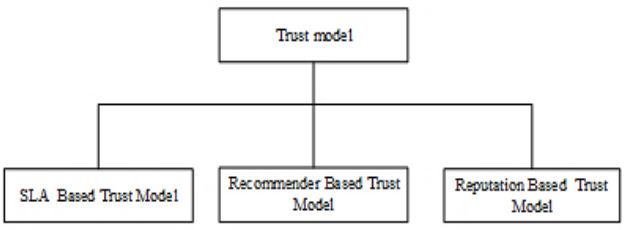

Fig. 2. Classification of Trust Model

3.1. SLA Based Trust Model

Trust models in this category are created on contracts and agreement between the cloud service provider and cloud service customer. The most frequently used contracts are SLAs (service level agreements) and service policy reports. It contains several security documents and QoS parameters to establish the trust between two parties. Jingwei Huang and David M Nicol (2013) have specified SLA verification based trust model based on policy i.e. SLA. In that trust model cloud customer desires to validate and re-examine the trust value after creating the initial trust [21]. M. Alhamad, T. Dillon, and E. Chang have presented the trust model to find the reliable service provider to achieve complicated and

confidential business application. The authors integrated both SLA framework and the trust model to provide a new technique for selecting the trustworthy service provider [25].

Chakraborty, S and Roy, K have proposed a model that uses the SLA based and trust methods to offer a trustworthy design to choose the top cloud service provider among several providers to achieve the functional and non-functional requirements. It has been done in three steps. First, the cloud user identifies and selects a service provider according to their requirements. After this SLA agent has designed the SLA parameters to identify the trusted CSP. Finally, trust management modules calculate the trust rate for a particular cloud provider constructed on the local experience with the service provider, report from the SLA agent and the opinions from external providers.

The authors have presented a framework which is shown in Fig. 3 that estimates the credibility of a service provider using a quantitative trust model. It contains the following components, cloud service provider, cloud consumer, evaluator, SLA, parameter extractor, trust evaluator, session log archive and policy database. The main module of the structure is trust evaluation engine which calculates the trust on provider. Trust evaluator is a third party who supports the customer to examine SLA and other documents to extract the parameters.

In order to estimate the trust they have identified various pre SLA parameters and post SLA parameters which is removed from SLA or recovered during the sessions. Parameter extractor analyses the SLA and other information and extract SLA parameters which are attained in trust evaluation before authorizing a SLA. These parameters includes CPU capacity, memory size, storage capacity, number of parallel sections, back up occurrence and average time to recovery. Post SLA parameters are evaluated after establishing trust between CSP and cloud consumer.

The authors have identified two post SLA parameters namely total time and average throughput. Policy database stores all the policies which are involved in trust estimation. Session log archive stores the log files of transactions of all sessions between the customer and the provider [8].

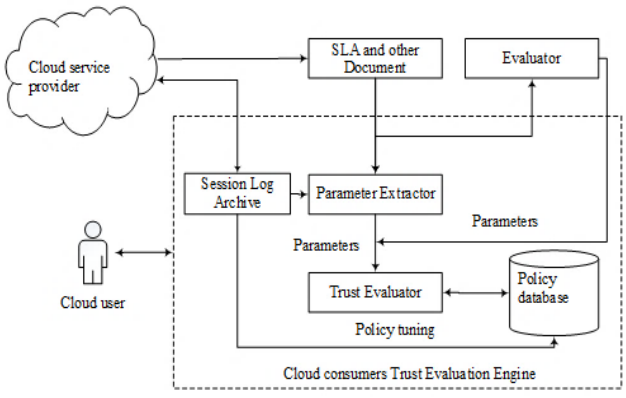

Fig. 3. Framework based on quantitative trust model [8]

D. Marudhadevi et al. have proposed a Trust mining model (TMM) to recognize the trustworthy cloud services. This model supports both cloud provider and service consumer, in which the user can decide to prolong or suspend the services with the service provider. The authors have used rough sets and Bayesian inference to calculate the overall trust value. In fig 4. architecture of the proposed model is given which contains three modules Trust manager, SLA manager and cloud performance monitor. SLA Manager is responsible for negotiating the agreement between service provider and cloud consumer. He communicates to trust manager and updates the trust rate in the contract before the whole agreement scheme is completed.

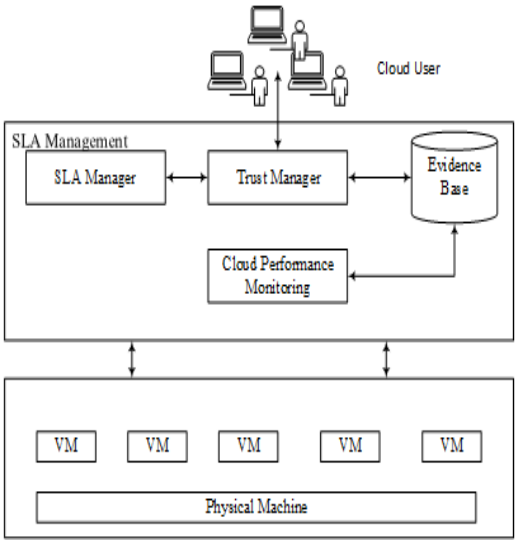

Fig 4. Trust architecture based on SLA [11]

Once the consumer negotiates the services, immediately they started observing the services to compute the trust grade through performance monitor module. Cloud provider monitors the various services, including average task success ratio, rejected number of services, network bandwidth and reliability. The cloud user can give complaints on services if they face any problem on it. All the monitored data, current user feedback and the trust value are saved in evidence base along with the customer's name for future reference [11].

3.2. Recommended Trust Model

Flavio Corradini et al. , Zhu,H Bao and Deng have stated that if two entities, trustor and trustee have no direct interactions then the trust is established through the third party generally third party auditor recommendation which is called as recommended trust. By this way user can trust on services and the providers [12, 46]. Singh,S. and Chand,D have proposed a trust assessment mechanism which evaluates the finishing trust value based on three metrics namely customer's self-trust, third party trust and friends trust on service providers [34].

Dehua Kong and Yuqing Zhai have proposed recommendation based trust scheme in service oriented computing (TRSC). They designed the structure of TRSC in which the cloud service is evaluated by combining both direct and recommendation trust. In Fig.5 web portals is the medium where cloud providers register their services and cloud users also register their requirements and get the recommendation results.

The core components of TRSC are trust computing, information and cloud service management. Information management is responsible for managing the trust association between the cloud user and the ratings about the service provided by the cloud consumers. Finally, they all stored in trust and recommendation repository. Cloud service management observers the registered services and categorize into diverse groups based on their types. They are kept in CS repository. Based on the cloud consumer's

requirement, trust computing provides the cloud services trust values. When a cloud service user requests for a service, the system will recommend them services. After that user can rate the services otherwise default value is given by the system. Users can directly report the trust ratings with other users also [10].

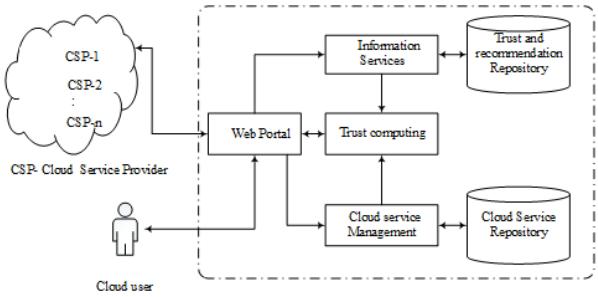

Fig 5. Architecture of TRSC [10]

Rizvi, S et al. have presented an objective trust model i.e. feedback system for the third party auditor in fig 6. where three cloud actors namely cloud service user, cloud service provider(CSP) and third party auditor are involved. CSPs are ranked based on the trust values evaluated by the model. The final trust value for each CSP is calculated by third party auditor by using third party assessment results and the feedback received from cloud service customer. When a CSP wants to register their services and the information about the services in the cloud market, first it sends a request to the third party auditor. Then third party auditor will evaluate the CSP by using the Cloud Security Alliance (CSA) security recommendations.

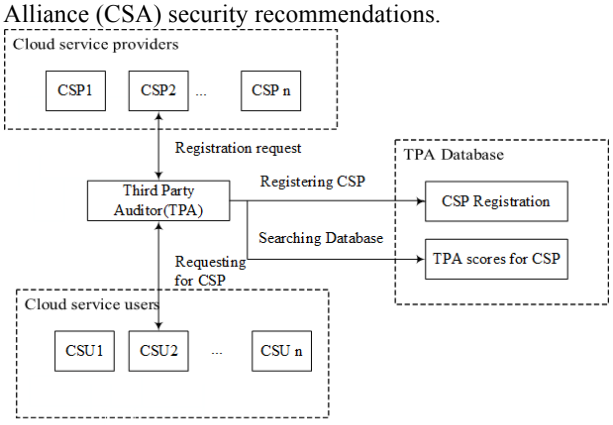

Fig. 6. Feedback system for the third party Auditor [31]

After the evaluation has done, the score for each service offered by the CSP is stored in database. That auditing score is rated from 1 to 10 where 1 represents lowest and 10 represent highest score [31].

Hui Fang et al. have proposed a distrust structure for recommender systems which deals with personal and impersonal features of trust and distrust. They identified the following personal characteristics such as compassion, capability, truthfulness and probabilities which are shown based on user's previous ratings whereas impersonal aspects are designed based on user liveliness in the network. They have been developed two logistical regression models by using those factors to calculate the user trust and distrust values [19]. Xiaoqi Li, Michael R et al. have designed the model which integrates the recommender system and D-S evidence theory to establish the trust in Grid P2P environment [43].

3.3. Reputation based trust Model

In this classification, trust models are based on reputation and feedback. In this model, it collects the feedbacks and an opinion of customers to measure the trust on the cloud resources provided by the provider. Trust model collects the feedback based on various QoS and security parameters offered by CSP. It will be useful for the customers to choose the service provider who guarantee the QoS to its users.

Jingwei Huang and David M Nicol have stated that "Reputation of an entity is the collective opinion of a community towards an entity". It is the value showing the overall belief. CSP with high reputation will be the most trusted among the community [21].

Abawajy, J have presented an honesty ranking factor that states an attitude on how reliable is a service provider of used information. It is hard to find out an inactive rates and malicious rates. They improve a mechanism to know the credibility of opinions and filter out opinions that are untruth. The author has implemented a feedback filtering algorithm to identify and filter out the dishonest feedbacks by computing the trustworthiness of feedback ratings using their own experience and a threshold value [3]. Borowski, J.F et al. have developed a system which collaborate a reputation trust mechanisms with agent-based safety system to safeguard against wicked failure ratings. Reputation based trust is calculated based on the interaction between the agents. Agents relay the intervallic status requests to the peers in their region. As soon as the peer received the query they have to reply with their present status. If the reply is not acknowledged then the agent is faulty. Each interaction result is either 0 or 1. The overall Reputation based trust rating is calculated by an average of many interactions [6].

J.H. Abawajy and A.M. Goscinski have defined that "Reputation is a measure that is derived from direct or indirect knowledge of previous communications of peers and is used to access the level of trust a peer puts into another". Existing trust models used in distributed and grid computing have taken all the feedback about a service given by the customers. There may be some malicious users who can give negative feedback about a service purposely and this may lead to a wrong opinion about a service among the customers. Existing mechanisms simply use feedback values and calculates the trustworthiness of a service instead of checking whether the feedback given by the customer is reliable, unbiased and trustworthy. The current trust models used in cloud computing identify the malicious users and fake feedbacks [20].

P.D. Manuel et al. (2011) have proposed the cloud trust management model in which trust value is assessed from the following major components such as trust estimator based on identity, capability and behaviour. They have calculated the final trust value based on trust value found in all three components such as T_{ib}(IBTE), T_{cb} (CBTE) and T_{bb} (BBTE) [27].

Shangguang Wang et al. have proposed a light weight reputation measurement approach in Fig. 7 to discover the instability of feedback scores for services. It contains two phases such as trust vector and reputation calculation. In trust vector first adopts a classical model to find the insecurity of feedback scores. In the reputation calculation stage, the reputation score for the cloud service is calculated by using fuzzy logic and finally, the reputation values are deposited in reputation storage [32].

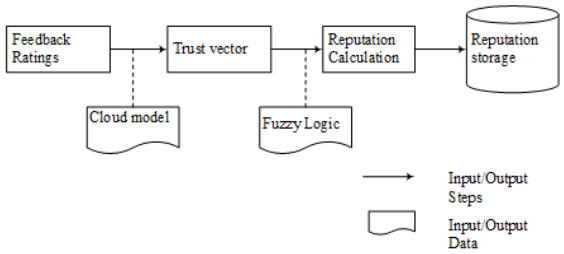

Fig. 7. Reputation measurement approach [32].

Talal H Noor and Quan Z Sheng have proposed TAAS framework where they have introduced adaptive reliability model that differentiate credible feedback by considering customer competency and agreement of their opinion ratings [35].

Talal H Noor et al. have reported the methods to detect the fake ratings from mischievous users and provide enhancement on trust group . They have been introduced the following techniques , Credibility proof protocol to preserve the privacy of the cloud service users, Feedback density is used to handle the feedback agreement issue by recognizing reliable trust opinions and Multi Identity Recognition identifies forged trust opinions from wicked users who use various identities to use trust results[37].

Talal H Noor et al. have designed and implemented a Cloud Armor, trust management framework based on reputation which is used to deliver the trust as a service. This framework contains the following modules. A new protocol is used to demonstrate the reliability of trust feedbacks and reserve user's privacy. A reliability and adaptive model is used to calculate the trustworthiness of feedbacks which keep the services from wicked users and identifies the honesty cloud services. Finally, they designed a model to accomplish the accessibility of the trust management services [38].

Vijayakumar, V et al. have discussed an approach for choosing the grid services based on trust and reputation to implement the jobs [41]. Xiaonian Wu et al. have implemented a trust assessment framework to find the malicious entities using Dempster Shafer theory. In their model, direct interactions are taken as first hand evidences and recommendation trust values are considered as second hand evidences. Finally the cumulative of recommended trust values forms the reputation of entities [42].

Zaki Malik and athman Bouguettaya have introduced RATE Web, a framework for establishing the trust in service oriented environment. It consists of a cooperative model in which web services distribute their experiences of the service providers with their customers through feedbacks. Service provider's reputation is calculated by aggregating the different ratings. They have used the following reputation evaluation metrics namely rater credibility, majority rating, past rating history, personal experiences for credibility evaluation, personal experiences for reputation assessment and temporal sensitivity [45].

4. Discussions

There are certain limitations have found in the trust models which are reviewed in this paper. In SLA based model, safety and privacy is not taken into an account and users are not able to assess on their own. They need the help of third party either broker or cloud trust authority. In recommended trust model, lack of a standardization process i.e. selection of which criteria provided by service provider are suitable to be evaluated and recommended is complex and the third party auditor is efficiently certified by whom is always not clear. In reputation and feedback trust model, reputation is more convenient on selecting the services at the beginning stage but later stage it is not satisfactory. The complication is high because huge amount of customers have to rate a services. To overcome these issues, we may combine reputation and recommended trust models to improve the efficiency.

5. Conclusion

In this review, we have discussed an overview of trust management which includes the highlights on semantics of trust, types of trust and attributes used for evaluating trust. Further, we identify the various trust models classified by many researchers and we mainly focused on three trust models namely SLA based, Reputation based and recommendation based trust model. Customers are worried about their data and seeking high confidence level even though a service or provider has a higher trust value. The lack of efficient and reliable trust evaluation system is still a major concern. To improve the efficacy of trust results we can combine reputation and recommender based trust mechanisms in future. New mechanisms may be designed to assess the trusty service provider using fuzzy sets and rough sets.

References

[1] Abassi, R; El Fatmi, S.G, Towards a generic trust management model, in 19th International Conference on Telecommunications, Jounieh pp.1-6 (2012) .

[2] Abawajy, Determining Service Trustworthiness in Intercloud Computing Environments in pervasive Systems, Algorithms, and Networks , 10th International Symposium , pp.784-788(2009).

[3] Abawajy, Establishing Trust in Hybrid Cloud Computing Environment, in 10th International Conference on Trust, Security and Privacy in Computing and Communications), IEEE,pp.118-125. (2011).

[4] A.Josang, R., Ismail and C.Boyd (2007), A survey of trust and reputation systems for online service provision, Decision Support Systems., 4 (2), pp. 618-644. (2007)

[5] Blaze, M., Feigenbaum, J and Lacy Decentralized trust management, IEEE Symposium on Security and Privacy, Oakland, pp.164-173(1996).

[6] Borowski, J.F, Hopkinson, K.M, Humphries, J.W, Borghetti, B.J, Reputation-Based Trust for a Cooperative Agent-Based Backup Protection Scheme, IEEE Transactions on Smart Grid ,2(2), pp.287-301(2011).

[7] Buyya, R.Chee Shin Yeo. and Venugopal, S ,Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities in 10th IEEE International Conference on High Performance Computing and Communication. , pp.5-13 (2008).

[8] Chakraborty, S and Roy, K ,An SLA-based Framework for Estimating Trustworthiness of a Cloud in IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications ,pp.937- 942 (2012).

[9] https://cloudsecurityalliance.org/star/

[10]Dehua Kong and Yuqing Zhai, Trust Based Recommendation System in Service-oriented Cloud Computing in Cloud and Service Computing International Conference ,Shanghai,pp.176-179(2012).

[11]D.Marudhadevi,V.Neelaya Dhatchayani and V.S Shankar Sriram,A ,Trust evaluation model for cloud Computing using Service level Agreement ,Security in Computer Systems and Networks, The Computer Journal,58(10),pp.2225-2232 (2014).

[12]Flavio Corradini, Francesco De Angelis, Fabrizio Ippoliti and Fausto Marcantoni, A Survey of Trust management models for cloud computing in 5th International Conference on Cloud Computing and Services Science, Lisbon, Portugal ,pp.155-162 (2015).

[13]Grandison, T. and Sloman, M,A survey of trust in Internet Applications in Communications Surveys and Tutorials, IEEE ,3(4),pp.2-16(2000).

[14]Girish Suryanarayana and Richard N. Taylor, A Survey of Trust Management and Resource Discovery Technologies in Peer-to-Peer Applications in Institute for software Research(ISR) Technical Report , UCI-ISR-04-6(2004) .

[15]Habib, S.M, Ries, S. and Muhlhauser.M, Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation in 7th International Conference on Ubiquitous Intelligence and Computing and Autonomic and Trusted Computing ,pp.410-415(2010).

[16]Habib, S.M., Ries, S. and Muhlhauser, M, Towards a Trust Management System for Cloud Computing', in International Conference on Trust, Security and Privacy in Computing and Communications, pp.933-939 (2011).

[17]Hassan Takabi, James B.D. Joshi and Gail-JoonAhn, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy ,8(6),pp.24-31 (2010).

[18]Huang,J. and Nicol D ,A Formal-Semantics-Based Calculus of Trust in Internet Computing, IEEE ,14(5), pp.38-46(2010).

[19]Hui Fang, Guibing Guo, Jie Zhang, Multi-faceted trust and distrust prediction for recommender systems, Decision Support Systems ,71,pp.37-47(2015).

[20]J. H. Abawajy and A. M. Goscinski, A reputation based grid information Systems in International Conference Computational Science, pp.1015-1022 (2006)

[21]Jingwei Huang and David M Nicol, Trust mechanisms for cloud computing, Journal of Cloud computing, 2(1), pp.2-9(2013).

[22]Kai Hwang and Deyi Li,Trusted Cloud Computing with Secure Resources and Data Coloring, Internet Computing,14(5),pp.14-22 (2010).

[23]Kanwal, A., Masood, R., Ghazia, U.E., Shibli, M.A and Abbasi, A.G, Assessment Criteria for Trust Models in Cloud Computing in Green Computing and Communications .Beijing pp.254-261(2013).

[24]Khaled M. Khan and Qutaibah Malluhi, Establishing Trust in Cloud Computing in IT Professional, 12(5), pp. 20-27 (2010).

[25]M.Alhamad, T. Dillon, and E. Chang, SLA-based Trust Model for Cloud Computing in International Conference on IEEE Network-Based Information Systems ,pp. 321-324 (2010).

[26] http://www.nist.gov/itl/cloud/

[27]P.D. Manuel, Mostafa Ibrahim Abd-El Barr and S. Thamarai Selvi , A Novel Trust Management System for Cloud Computing IaaS Providers, Journal of Combinatorial Mathematics and Combinatorial Computing ,79,pp.3-22 (2011).

[28]Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, Modelling and evaluation of trust in cloud computing environments in International Conference on Advanced Computer Control ,pp.112-116(2011).

[29]Qing Zhang, Ting Yu and Keith Irwin, A classification scheme for Trust functions in Reputation based trust in International Semantic Web Conference, (2004)

[30]Raj, G., Sarfaraz, M. and Singh, D, Survey on trust establishment in cloud computing in International Conference on The Next Generation Information Technology Summit, pp.215-220(2014).

[31]Rizvi, S., Jungwoo Ryoo, Yuhong Liu, Zazworsky, D. and Cappeta, A, A centralized trust model approach for cloud computing in Wireless and Optical Communication Conference, pp.1-6.(2014).

[32]Shangguang Wang, Lei Sun, Qibo Sun, Jie Wei and Fangchun Yang, Reputation measurement of cloud services based on unstable feedback ratings in International Journal of web and Grid services,11(4),pp.362-376(2015).

[33]Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries and Max Muhlhauser, Trust as a Facilitator in cloud computing: A Survey, Journal of Cloud Computing: Advances, Systems and Applications, 1(19), pp.1-18(2012).

[34]Singh, S. and Chand, D, Trust evaluation in cloud based on friends and third party's recommendations, Recent Advances (RAECS) in Engineering and Computational Sciences,pp.1-6(2014).

[35]Talal H Noor and Quan Z Sheng, Trust as a service: A framework for trust management in cloud environments in Web Information System Engineering, pp.314-321(2011).

[36]Talal H Noor, Quan Z Sheng, Sherali Zea dally and Jian Yu, Trust management of services in cloud environments: Obstacles and solutions in Journal of ACM Computing Surveys, 46(1), pp.1-35(2013 a).

[37]Talal H Noor, Quan Z Sheng, Abdullah Alfazi, Jeriel Law and Anne HH Ngu, Identifying fake feedback for effective trust management in cloud environments in Service-Oriented Computing, pp.47-58(2013 b).

[38]Talal.H.Noor, Sheng, Q.Yao, L.,Dustdar, S. and Ngu, A.H.H, CloudArmor: Supporting Reputation-based Trust Management for Cloud Services, IEEE Transactions on Parallel and Distributed Systems,99(2014).

[39]Wanita Sherchan ,Surya Nepal and Cecile Paris ,A survey of trust in social networks in Journal of ACM Computing Survey ,45(4),pp.1-33(2013).

[40] Priya G,N Jaisankar , A Reputation based Trustworthy System for Cloud Environment in International Journal of Pharmacy and Technology,2(3),pp.16702-16708(2016).

[41] Vijayakumar, V., Wahida Banu, R. S. D. and Abawajy, J. H ,An Efficient Approach based on Trust and Reputation for Secured Selection of grid Resources, International Journal of Parallel, Emergent and Distributed Systems,27(1), pp.1-17 (2012).

[42] Xiaonian Wu, Runlian Zhang, Bing Zeng and Shengyuan Zhou(2013)'A Trust Evaluation Model for Cloud Computing', in Procedia Computer Science,Vol 173,pp.1170-1177.

[43] Xiaoqi Li,Michael R and Jiangchuan Fan and Mingyn Chen ,A grid and P2P Trust model Based on recommendation Evidence Reasoning, Journal of Computer Research and development ,42(5) ,pp.797-803(2005).

[44] Yinghong Lou and Wenlin Wang, The Research of Trusted Technology under Cloud Environment in Information Science and Cloud Computing Companion ,pp.231-235(2013).

[45] Zaki Malik and Athman Bouguettaya, RATEWeb: Reputation Assessment for trust establishment among web services Web Engineering, International Conference (2011).

[46] Zhu, H Bao and Deng, Computing of Trust in Distributed Networks in International Association for Cryptologic Research (2003).