Sonanchal Singh et al. 2019, 7:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

A Survey on Cloud Model Services and Unreliable Node Detection Techniques

M. Tech. Scholar Sonanchal Singh Asst. Prof. Sumit sharma
Dept. Computer Science and Engineering
Vaishanavi Institute of Technology and Science
Bhopal, MP, India

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 paper gives a brief review of trust based cloud model where different techniques of this model were explained. Here related work adopt by other researchers were detailed. This paper gives an evaluation parameter list for the comparison of method as well.

Keywords: Cloud Computing, Fuzzy logic, Trust Computing, Resource Management.

I. INTRODUCTION

Cloud computing provides internet based services on a utility basis to the business process. The tenants share a pool of resources that are dispersedly owned and managed. Hence security is a major concern in the cloud environment.

The consumers will loss the control of data in the cloud environment and hence a proper trust mechanism is necessary to ensure data security and privacy [1]. As the cloud computing is composed of different local systems and includes the members from multiple environments, therefore the security in cloud is complicate. In one side, the security mechanism should provide guarantees secure enough to the user, on the other side, the security mechanism should not be too complex to put the users into an inconvenient situation.

The openness and flexibility of the computer and popular commercial operating systems have been important factors supporting their widespread adoption. However, that very same openness and flexibility have been proved to be a double edged sword, because it brings complexity, reduces trust degree and threat against security. So there should be a balance between the security and the convenience [2]. While downloading files from the Spyware, Trojans etc. while the user works with the user interface in order to access the web services. The data in the infected computer is no longer safe. Thus even after taking all the safety measures such as installing antivirus software also, there exist the risk of our sensitive data getting hacked when we use the web-service of cloud computing [3].

An effective trust management system helps cloud service providers and consumers reap the benefits brought about by cloud computing technologies. Despite the benefits of trust management, several issues related to general trust assessment mechanisms, distrusted feedbacks, poor IDentification of feedbacks, privacy of participants and the lack of feedbacks integration still need to be addressed.

Traditional trust management approaches such as the use of Service Level Agreement (SLA) are inadequate for complex cloud environments. The vague clauses and unclear technical specifications of SLAs can lead cloud service consumers to be unable to identify trustworthy cloud services [4].

© 2019 Sonanchal Singh et al. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

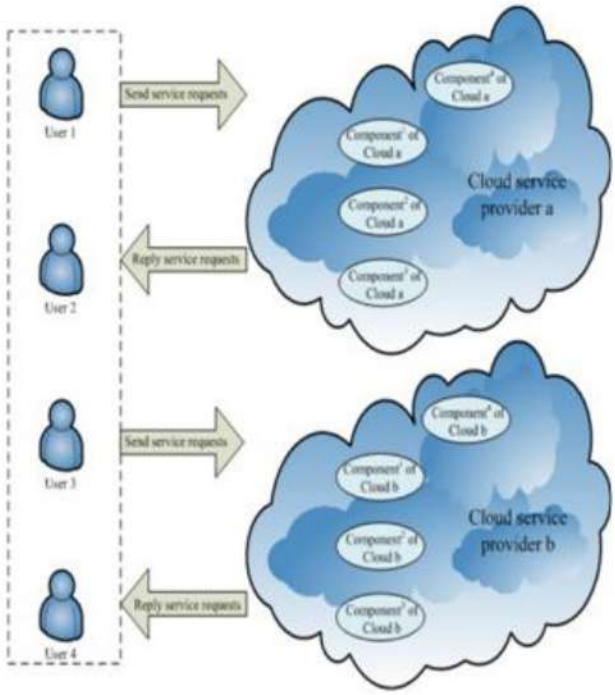

Figure 1: Architecture of Cloud Computing.

II. CLOUD COMPUTING SERVICES

1. Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface [5]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider [6]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

3. Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components.

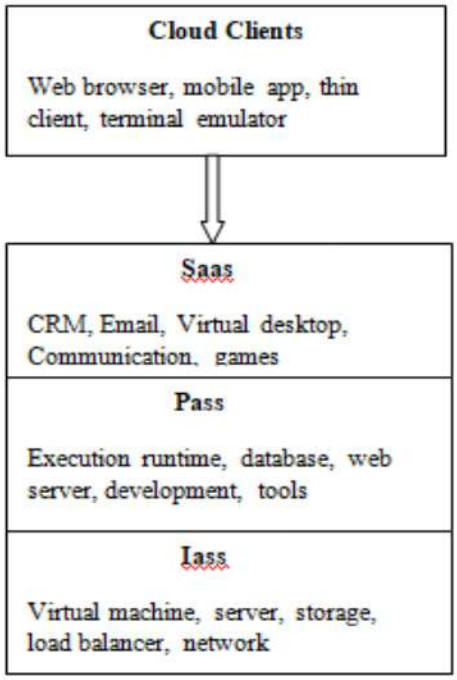

Figure 2: Cloud computing Services.

III. LITERATURE SURVEY

Chen et al. [6] has focused on analysis of confidentiality and data sensitivity & security problems in cloud architecture and environment covering all the stages of life cycle of data. In this study, the authors elaborated privacy protection, data security, data segregation, cloud security and cloud computing.

They have analyzed these issues and also provided a solution for resolving these issues. These issues are primarily at SPI (SaaS, PaaS, IaaS) level and the major challenge is data sharing. After the analysis of data security and privacy the comprehensive solution is to meet the need of identification and isolation of data is primary task ate design level of cloud based applications.

In [7] paper proposes a new trust model and related algorithm to decrease trust management overhead and improve malicious node detection ability based

on domain partition. Partitioning nodes into domains is helpful for decreasing the overhead of trust management in terms of trust storage and computation. Domain and cross-domain sliding-windows are proposed and utilized to store the most recent trust values. Then, an algorithm is designed to compute domain and cross-domain trust values for nodes, and a filter procedure is adopted to remove malicious trust evaluations and malicious nodes from a domain.

Azad et al. [78] proposed machine to machine reputation system to evaluate the trustworthiness of machines in IoT. Only reputation social trust metric is considered in this study. The participants sign a trust value to the machine based on their experiences and interactions with the machine. Then, they send trust values' cryptograms to the bulletin board. Utilizing secure multi-party computation methods, the reputation requester calculates the global reputation of machine by utilizing the reported cryptograms in the bulletin board.

Rafey et al. [9] to enhance cooperation between trusted nodes and adjust the trust scores dynamically based on the node behavior. In this model, node transaction attributes (e.g., node computation power, confidence, context importance, and feedback), and node social attributes (e.g., friendship, centrality, and relationship) are considered. In the trust computation phase, each node computes the overall trust values of other nodes based on its own direct interactions and recommendations from other nodes. Also, their model integrates the social relationships and context of interactions in the trust computation. The trust accuracy in this model can be affected by recommendations from dishonest nodes that assign higher trust values to their group of allies.

Chen et al. [10] for effective service composition and resistance against trust-related attacks. In their model, they consider both QoS trust metrics including energy status and quality reputation and social trust metrics based on social similarities. However, this study doesn't consider the contextual and dynamic nature of trust.

Cloud computing [11] provide us a podium to use a wide range of services that are based on the internet to deal with our industry procedures & various services of Information technology. But besides its all advantages it also increase the threat for security when a TTP (Trusted Third Party) is involved. By involving a TTP (Trusted Third Party) there is still a chance of heterogeneity of Users which effects security on a cloud. In this research, the authors propose a TTP (Trusted Third Party) independent approach for IDM (Identity Management) with the capability of using unique data on unreliable Data Protection Techniques for Building Trust in Cloud Computing. Using predicate data over the encoded data and using multi organization calculation and computing and active bundle scheme are the approaches used here. In this scheme the bundle has self-reliability checking procedure, it include PII, protection mechanism, privacy policies and virtual machine for policy enforcement of these policies. The resolution lets the use of IDM solicitation on unreliable clouds. Cloud computing is very effective security service that is based on conceptual technology. Data retrieval and safety of the security of data is the main issue in cloud architecture and environment.

IV. TYPES OF TRUST MODELS

The trust in cloud computing is divided into various categories namely Reputation Based Trust, SLA verification based trust, Policy-based trust, Evidence-based trust and Societal trust [11, 12].

Reputation Based Trust: the reputation of an entity is the collected estimation of public's trust towards that entity. Generally, many entities in a community trust an entity that has high reputation; an entity, which is required to build trust decision on a trustee, uses the reputation to compute or approximate the trust level of the trustee. The reputation of cloud affects the selection process of cloud services; therefore, CSPs try to construct and preserve higher reputation. Reputation is classically represented by a broad score reflecting the overall outlook, or a small number of scores on numerous foremost aspects of performance.

SLA: verification based trust, after establishing the preliminary trust and accessing a cloud service, the cloud user is required to validate and re-examine the trust value. SLA is a lawful agreement between the two communicating parties: user and provider. Therefore, monitoring the QoS parameters and verification of SLA document are essential source of trust management for cloud computing. In CSP party is required to provide these types of services.

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

Evidence-based trust:, A belief of trustor in the predictable behavior of trustee is based on the proof about attributes of adeptness, helpfulness and honesty. With respect to that expectation evidence-based trust is expressed as follows: believe(c, attrb1(sb, av1))∧... ∧ believe(c, attrbn(sb, avn)) → trust_ * (c, sb, x, ct) which states that if a cloud user c believes a subject sb has attribute attrb1 with value av1, ..., attribute attrbn with value avn, then u trusts (it is either trust in belief or other one) sb w.r.t x, the performance of sb or information is believed by sb, in a particular context ct.

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

Evaluation Parameter

As various techniques evolve different steps of working for classifying user query into appropriate category. So it is highly required that proposed techniques or existing work need to be compare on same experimental environment.

$$\text{Precision} = \frac{\text{True\_Positive}}{\text{True\_Positive} + \text{False\_Positive}}$$

$$\text{Recall} = \frac{\text{True\_Positive}}{\text{True\_Positive} + \text{False\_Negative}}$$

$$F\_Score = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

$$Accuracy = \frac{Correct\_Classification}{Correct\_Classification + Incorrect\_Classification}$$

In above true positive value is obtain by the system when the specified node is real and system also says that the node is real. While in case of false positive value it is obtain by the system when the specified that node is malicious and system also says that the user is real. Similarly in case of True negative value it is obtain by the system when the algorithm specified that node is real and system says that the node is malicious.

V. CONCLUSIONS

In this survey, paper 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, paper 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]. 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).

[2]. 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).

[3]. 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).

[4]. 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).

[5]. 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).

[6]. Satish Kumar and Anita Ganpati, "Multi-Authentication for Cloud Security: A Framework," International Journal of Computer Science & Engineering Technology (IJCSET),Vol. 5, Issue 4, pp. 295-303, Apr. 2014.

[7]. V. Sulochana and R. Parimelazhagan, "A Puzzle Based Authentication Scheme for Cloud Computing," International Journal of Computer Trends and Technology (IJCTT), Vol. 6, Issue 4, pp. 210-213, Dec. 2013.

[8]. 70. Azad M.A., Bag S., Hao F., Salah K. M2m-rep: Reputation system for machines in the internet of things. Comput. Secur. 2018;79:1–16. doi: 10.1016/j.cose.2018.07.014.

[9]. 80. Rafey S.E.A., Abdel-Hamid A., El-Nasr M.A. CBSTM-IoT: Context-based social trust model for the Internet of Things; Proceedings of the 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT); Cairo, Egypt. 11–13 April 2016; pp. 1–8.

[10]. Chen Z., Ling R., Huang C.M., Zhu X. A scheme of access service recommendation for the Social Internet of Things. Int. J. Commun. Syst. 2016;29:694–706. doi: 10.1002/dac.2930.

[11]. J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005.

[12]. V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[13]. Peiyun Zhang, Senior Member, IEEE, Yang Kong, And Mengchu Zhou. "A Domain Partition-Based Trust Model For Unreliable Clouds". IEEE Transactions On Information Forensics And Security, VOL. 13, NO. 9, SEPTEMBER 2018.