International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Survey on Trust Models in Cloud Computing

RamyaGovindaraj[1] Kavitha B R[2], Kumaresan P[3]

[1,2,3]School of Information Technology and Engineering(SITE)
VIT University,Vellore, Tamilnadu, (India)

ABSTRACT

Trust is an important and ever extant factor in cloud computing. At the present, trust is largely based on perception of reputation and regard and scores of self-assessment and the so-called cloud transparency provided by the service providers. This paper provides a survey of existing state-of-the-art trust mechanisms in the cloud computing paradigms for establishing trust, and make observations on their limitations; thereby highlighting areas that future research could be focused on to solve this issue at hand.

Keywords :Cloud Transparency, Data security, Privacy, Trust Mechanisms.

I.INTRODUCTION

Cloud computing has become a frontrunner in the technology sector and is being used far and wide in a multitude of fields. However, there is still a question of the amount of security the service has to offer and the trust that the consumers place on the service and its providers. Traditionally, the basis on which the providers establish trust with the consumers is by the attributes of the service itself and the proof of its ingenuity by the number of consumers it already has. But as consumers we are not, generally, explicitly introduced to the authorities/organizations that monitor, measure, assess, or validate these cloud attributes. As pointed out in [1], “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.”

The problems and issues of trust in cloud computing are constantly being discussed from widelydiverse perspectives [2, 3, 4, 5, 6, 7, 8, 9, 10]. Upon analyzing the different issues raised, a number of models and tools have been proposed by various groups [11, 12, 13]. Each of them contribute to a fractional view of trust in cloud computing, but still lack an overall clarity ofdemonstrating how cloud entities can work together to form a “communal” system, with a solid foundationof trust, serving to simplify the identification ofreliable paths to reliable cloud services. The “NIST Cloud Computing Reference Architecture [14] recognized cloud brokers and auditors as bodiesthat conduct assessment and monitoring of cloud services; however, there are very few works on the chains of trust from cloud users to cloud services and service providers through those very intermediary cloud entities.”

In this paper, we will place emphasis on the theoretical basis for analysis of trust in the cloud. Ourintentionis to review the different state-of-the-art trust mechanisms in clouds and demonstrate the area of trust that each of them covers.

II.MATERIALS AND METHODS

Trust and Security issues are still the most actively researched areas in cloud computing. Trust evaluated by Jingwei H. et al is based on “evidences and subjective logic and is used to evaluate security breaches based on historical data”.As evidenced by an example of an attack, Pearson

S. and Benameur A. in [9] illustrate the present threats posed. They postulate that the existing cloud services pose an integral challenge to data privacy, seeing as how the data in question is present in an unencrypted form at datacenters and warehouses operated and owned, usually, by an organization that is different from the organization of the data owner. Leaking of sensitive data and hence a loss of privacy is an imminent concern for users in the usage of cloud services.For example: “In 2007, criminals targeted the prominent cloud service provider (CSP) Salesforce.com, and succeeded in stealing customer emails and addresses using a phishing attack.”

Huang J. and Nicol D.[24] describe trust as a three-part mental state. “Trust is a mental state comprising: (1) expectancy - the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions); (2) belief - the trustor believes that the expected behavior occurs, based on the evidence of the trustee’s competence, integrity, and goodwill; (3) willingness to take risk - the trustor is willing to take risk for that belief.”

III.STATE OF THE ART TRUST MECHANISMS IN THE CLOUD

3.1. Trust based on SLA (Service level agreement) monitoring and verification

A SLA is a legal document that is signed by both the cloud provider and the cloud user and delineates the quality of service that the service provider guarantees to provide. By monitoring the QoS (Quality of service) and QoE (Quality of Experience), the cloud user can verify that all the services are being provided at the level of quality ensured in the SLA, thus building up trust. [12,13] provide many models and representations that establish trust through the verification of SLA agreements. This “Trust, but verify” tactic has been found to be excellent for improving trust relationships between a cloud provider and a cloud customer. By verifying the trust at frequent intervals, the cloud user helps to improve the cloud provider’s reputation.

One of the problems with this approach is that the SLA provided by the cloud provider seldom focuses on elements such as security, privacy and other “invisible” elements of cloud computing. Usually a majority of cloud users are casual users and they seldom have any significant know-how to fully understand the monitoring of QoS, QoE agreements on their own. Thus, there is a need for a third-party organization that can provide these services for them. The individual users and small organizations that use a public cloud without the ability to monitor these services usually enlist the services of a professional cloud provider, which now provides trust as a service. Trust as a service mechanism is further explained in section 3.2. Private cloud users also contact trust authorities and cloud brokers that perform the monitoring service for them.

3.2 Trust as a service

As seen in Section 3.1, third-party professionals that can monitor and verify SLA agreements for ensuring QoS play a very important role in establishing trust between the cloud provider and cloud user through verification. These parties can play a crucial role in providing trust in other aspects of cloud services as well.

RSA, in following with its philosophy of "Trust = Visibility + Control" [23], announced the CTA (Cloud Trust Authority) which provides TAAS (Trust as a Service). It provisions a single point for managing security across multiple cloud platforms. The CTA initially provided the "identity service", that enabled a single sign-on mechanism across multiple cloud platform and the "compliance profiling service". that allows a user to compare the security mechanisms of multiple providers against a common standard. CTA could thus play a crucial role in trust management.

CTA has its demerits too. The cloud customer must judge the assertions made about the cloud services in the CTA and even more crucially, the cloud customer must judge the usefulness of the CTA as an intermediate agent.

3.3 Trust based on Reputation

Trust and reputation may seem as if they are the same thing, but they are different. Trust is fundamentally established between two people while the reputation of a person depends upon the opinion of a community towards that person. Trust and reputation are connected in the manner that a person with a good reputation usually tends to be trustworthy. Thus building up a reputation is one way in which cloud providers can establish a trust relationship with the customers.

A customer might user reputation as an initial method to establish trust on a cloud provider. The reputation of a cloud service provider represents the view of a community towards that provider and is thus useful in choosing one particular cloud provider when many options are available for the customer [25]. But after the initial selection reputation does not seem to be of much use in building up more trust. As a user grows familiar with the services offered and the SLA agreements, they will turn to monitoring and SLA verification to maintain their trust with the provider.

Trust based on reputation is used widely in P2P (Peer to Peer) networks and in e-commerce. When a customer is deciding which cloud service to enlist, reputation will play a big role in their decision. Thus, trust based on reputation is an important trust mechanism [11,13].

3.4 Transparency Mechanisms

An established basis for cloud providers in gaining trust is through transparency and accountability. In business, person with honesty and integrity is usually trusted, and the same concept applies for cloud computing too. The CSA (Cloud Service Alliance) launched the "Security, Trust and Assurance Registry (STAR)" program with an aim to improve transparency in the cloud. Through the "Consensus Assessments Initial Questionnaire (CAIQ)" or a "Cloud Control Matrix", cloud providers can publish a self-assessment of their security mechanisms. The STAR program can help filter out the untrustworthy cloud providers, with whom the user's data cannot be regarded as safe. The users would typically want a third-party professional organisation to verify the security self-assessments made by the cloud providers.

3.5Formal certification, audit, and standards

Due to the fact that self-assessments may be fabricated due to dishonesty on the part of cloud service providers, some postulate that formal certificationor approval from a reliableautonomous authority is necessary for a good cloud market; others argue that this “would stifle industry innovation”.This is said even though certifications and external audits have been used. although for a more general purpose but notspecific to clouds,for far longer. Anofficialprocedure for valuation of cloud service providers and the service providedby both them and independent third parties, acceptable to both cloud providers and users, does not yet exist.

IV.RESULTS AND DISCUSSION

We have surveyed the existing trust mechanisms in the cloud domain and have discussed how each of them address a specific aspect of trust. Each of them fall short in completely solving the problem of a lack of trust in the cloud computing paradigms. Combining all of the mechanisms to amass the services or aspect covered by each of them separately will help us curb most of the trust issues.

A repute-based trust mechanism that effectively echoes the view of the public of a service or the service provider should be in place. Once they establish a market based on trust, they need to maintain this reputation. Here’s where the user’s continuous involvement is a must, the user must validate and evaluate that trust periodically based on many parameters. QoS and QoE parameters and the verification of SLA can help users. Thus we can ensure all or most of the trust issues are handled by the same mechanism.

In order to let users see how the cloud service providers work, cloud transparency mechanisms are in place. But one major issue is that most of the information provided in these transparent mechanisms come from the service providers themselves and hence are not always reliable. One possible solution to the problems posed in the above mechanism is formal accreditation and audit. The mechanisms of formal accreditation and audit in the cloud do not exist yet and are still in discussion.

V.FUTURE SCOPE

From our studies of the various state-of-the-art trust mechanisms used in the cloud computing paradigm, it is obvious that most or all of the mechanisms deal with one particular aspect of trust. By making sure one aspect is secured and failing to pay heed to the other (sometimes more pressing) issues is often not the best tactic to use. Since we know we are dealing with a sensitive issue such as data privacy and security, the future discussions and mechanisms can be focused on addressing multiple aspects of trust. It may be pertinent for cloud services and cloud service providers, in the future, to additionally focus on building trust, reputation and high regard among their existing customer base; perhaps by introducing newer characteristics aimed at bettering customer relationships and customer satisfaction thereby ensuring loyalty.

VI. CONCLUSION

Trust is an ever important aspect of cloud computing. We have presented the current research and practices of trust mechanisms in the paper. It is obvious that each of them deal with a specific aspect of trust and deals with addressing that aspect alone. Future studies could be aimed at addressing more than one aspect of trust and thereby being more efficient in solving the enigma of trust in the cloud computing paradigm. Cloud transparency mechanisms also aid in providing clarity of the process to any cloud user thereby increasing accountability and responsibility of the cloud service providers.

REFERENCES

[1] Michael B: In clouds shall we trust? IEEE Security and Privacy 2009.

[2] Everett C: Cloud computing: A question of trust. Computer Fraud Security 2009.

[3] Garrison G, Kim S, Wakefield RL: Success factors for deploying cloud computing. Commun ACM 2012.

[4] Ghosh A, Arce I: Guest editors' introduction: In cloud computing we trust - but should we? Secur Privacy, IEEE 2010.

[5] Habib S, Hauke S, Ries S, Muhlhauser M: Trust as a facilitator in cloud computing: a survey. J Cloud ComputAdvSystAppl 2012.

[6] Khan K, Malluhi Q: Establishing trust in cloud computing. IT Prof 2010.

[7] Michael B, Dinolt G: Establishing trust in cloud computing. IANewsletter 2010.

[8] Park J, Spetka E, Rasheed H, Ratazzi P, Han K: Near-real-time cloud auditing for rapid response. In 26th International conference on advanced information networking and applications workshops (WAINA). Washington, DC, USA: IEEE Computer Society; 2012.

[9] Pearson S: Toward accountability in the cloud. Internet Comput IEEE 2011.

[10] Takabi H, Joshi J, Ahn G: Security and privacy challenges in cloud computing environments. Secur Privacy IEEE 2010.

[11] Abawajy J: Establishing trust in hybrid cloud computing environments. In Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications,. Washington, DC, USA: IEEE Computer Society; 2011.

[12] Haq IU, Alnemr R, Paschke A, Schikuta E, Boley H, Meinel C: Distributed trust management for validating sla choreographies. In Grids and service-oriented architectures for service level agreements.

[13] Dimitrakos T, Moona R, Patel D, McKnight D (Eds): Trust model for optimized cloud services. Berlin Heidelberg: Springer; 2012.

[14] NIST: NIST cloud computing standards roadmap, NIST CCSRWG-092. Gaithersburg, MD,USA: NIST; 2011.

[15] Blomqvist K: The many faces of trust. Scand J Manage 1997.

[16] Mayer R, Davis J, Schoorman F: An integrative model of organizational trust: Past, present, and future.

[17] Huang J, Nicol D: A formal-semantics-based calculus of trust. IEEE 2010

[18] Shaoham Y: Temporal logics in AI: Semantical and ontological considerations, 1987.

[19] Huang J, Fox MS: An ontology of trust: formal semantics and transitivity. In Proceedings of the ICEC'06,. New York, NY, USA.

[20] Hwang K, Kulkareni S, Hu Y: Cloud security with virtualized defense and reputation-based trust mangement. InDependable, Autonomic and Secure Computing, 2009. DASC '09. Washington, DC, USA

[21] CSA: STAR (security, trust and assurance registry) program. Cloud Security Alliance 2011.

[22] RSA: RSA establishes cloud trust authority to accelerate cloud adoption. RSA 2011.

[23] EMC: Proof, not promises: Creating the trusted cloud. EMC 2011.

[24] Huang J, Nicol D: Trust mechanisms for cloud computing, Journal of Cloud Computing: Advances, Systems and Applications: Advances, Systems and Applications, 2013.

[25] Priya .G, Jaisankar N ," A Reputation Based Trustworthy System For Cloud Environment" in International Journal of pharmacy and Technology,Vol 8,No 3 ,pp No:16702-16708,September 2016.