AN OVERVIEW: TRUST AND REPUTATION IN CLOUD SERVICES

Sarojini.G[1] Vijayakumar.A[2] Selvamani.K[3] George Fernandez.I[4]

[1,2,4]Department of Information Technology, Jerusalem College of Engineering, Chennai 600100, India.
[3]Department of Computer Science and Engineering, Anna University, Chennai 6000025, India.
[1]sarojinigs@gmail.com, [2]kaniporiyalan@yahoo.co.in, [3]selvamani@annauniv.edu,

Abstract-

In the cloud environment, the trust and reputation management are major component for providing virtualized and scalable web services from the service providers to the various cloud users. Many existing systems are not effectively encompasses the trusted and reputed cloud services. The trust can be defined as an act of faith, confidence and certainty based on the application. Also it is expected to behave or deliver the service in a proper way as promised by the service providers. The trust should also provide solution for the specific problem due to some uncertainty and vulnerability caused by the constraints in cloud computing. It correlates the security issues and its solutions in cloud. The trust measures are calculated based on the various parameters of the cloud users and the respective service providers. This recommendation kind of metrics provides an effective way of trusted and reputed cloud services in the cloud environment. Trust and reputation is classified based on behavioral metrics such as subjective/objective, transaction-based/opinion-based, complete/localized information and also rank/threshold. Reputation is the assessment of the tasks which ensures the derived trust based services in cloud. Cloud users basically require the reputed system to guarantee the security in cloud services. Thus the reputation which gains the trusted users might be able to access very cheaper services especially in Infrastructure as a service (Iaas), Platform as a service (Paas) and Software as a service (Saas) with a secure cloud environment. While the cloud is incorporated into a variety of application, the trust and reputation are ensuring basically secure services from the corresponding specified service providers. This kind of cloud services breaks the complications in web services and web applications.

Keywords: Cloud computing, Cloud Service providers, Cloud Users, Trust, Reputation, Security.

I. INTRODUCTION

Cloud computing has recently emerged as a new model for hosting and delivering services over the Internet. Cloud computing is attractive to business owners because it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the petite and increase resources only when there is a rise in service demand. However, despite the fact that cloud computing offers huge opportunities to the software industry, the development of cloud computing technology is currently at its early years, with many issues still to be addressed. Here a survey of trust and reputation in cloud computing is presented by highlighting its key concepts, architectural principles, state-of-the-art implementation as well as research challenges. A better understanding of the design challenges of trust and reputation in cloud computing and identifying major research directions in this increasingly important area are dealt here. Cloud computing is a service delivering mode based on the World Wide Web. It can provide users with scalable services as required through the Internet and it is widely applied in various cloud real-time applications. To utilize computing resources more effectively and safely, people begin to pay close attention to undiscovered security problems in cloud. The features of virtualization, multitenant and openness of cloud computing bring potential security issues to cloud services such as unreliability, insecurity and inconsistency. Security related issues are an important aspect of cloud computing which cannot be ignored. Cloud computing environment is a typical distributed environment; hence the distribution, dynamism, and anonymity of information resources and services are remarkable features of cloud computing environment. Therefore, the traditional centralized access control model has apparently cannot satisfy the security requirements of cloud computing. The implementation of access control in cloud computing environment will face a series of challenges. In cloud computing, researchers are more concerned about the implementation of access control polices through unconventional ways. The

concept of trust management and trust mechanism also ensures a new way of solving security problems in cloud computing environment.

The key barrier in cloud computing is the lack of trust and reputation in clouds by the potential customers. While preventive controls for security and privacy are actively involved in research and focuses their views in cloud accountability and auditability. The complexity as a result of large-scale virtualization and data distribution carried out in current clouds has revealed an vital research agenda for cloud accountability, as has the shift in focus of customer concerns from servers to data. The key issues and challenges are discussed here for achieving a trusted and reputed cloud through the use of detective controls, and present a framework, which addresses trusted and reputed accountability in cloud computing via technical and policy-based approaches. Reputation in general is the assessment of the society about performing a task or service. Cloud users require a reputed system to guarantee the safety of their data, investment and service. Reputation is gained through trust which might be through self experience or through existing user's recommendation. Reputation is based on metrics such as Behavioral, Subjective/objective reputation, transaction-based/opinion-based reputation, complete/localized information and rank/threshold based reputation. Reputation is the opinion of one entity towards another entity based on the above metrics. Trust and Reputation are mutual for both the cloud users and cloud service providers since their status are almost equal.

II. LITERATURE SURVEY

The concept of trust originally derives from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [1]. The standard definition of the cloud environment and its types are given by Mell [2]. [3] Sumeen et al has given a clear reputation based model. [4] [5] has discussed a trust based model for the reduction of uncertainty various ways of trust computation in a conceptual manner. Jameel *et al.* [6] first introduced the term trust management and identified it as a separate component of security services in networks and clarified that trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships. Trust management in cloud is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among themselves. Examples would be in building initial trust bootstrapping [7], coalition operations without predefined trust, and authentication of certificates generated by another party when links are down or ensuring safety before entering a new zone [8]. In addition, trust management has diverse applicability in many decision making situations including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing, and other purposes. Trust management, including trust establishment, trust update, and trust revocation, in cloud environment is also much more challenging than in traditional centralized environments[10] [11] [12]. The trust in the mobile adhoc network is given as a proposed work in the papers [13] [14]. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to changes in topology induced by node mobility or node failure. Further, resource constraints often confine the trust evaluation process only to local information. The dynamic nature and characteristics of cloud services and result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time [8] [9]. Despite a couple of surveys of trust management [15] [16] [17] [18], a comprehensive survey of trust management in cloud does not exist and is the main aim of this paper[19][20][21] The contributions of this paper are: (1) to extensively survey the existing trust management schemes and investigate their general trends; and (2) to extensively survey the existing reputation management schemes and investigate their general trends.

III. OVERVIEW OF TRUST

In the practical world, someone has to be trusted to complete certain process, which implicitly means that the probability that the action performed would be beneficial and with some form of cooperation. Correspondingly, when untrustworthy is dealt, it is the probability that is low enough to stop the action from being performed. Trust is a belief that is predisposed by the individual's opinion about certain critical system features. The concern of trust covers on a range of influential parameters from human's perspectives, which impact the design of systems. Definition of trust in an organizational context by

adding vulnerability associated with risks that one is willing to take as: “The willingness of a party to be vulnerable to the actions of another party based on the expectation that other will perform a particular action important to the person who trusts, irrespective of the ability to monitor or control that other party.”

The degree of trust is defined as an act of trust involves placing yourself at hazard to another’s actions, in a belief, at least partly without clear computability of risk that they will act to your benefit. A mathematical model is developed to compute probability based on past experience to predict future behavior as: Trust is a subjective expectation an agent has about another’s future behaviour that is based on the history of their encounters. Reliability Trust is: “Trust is the subjective probability by which one entity, expects that another individual, performs a given action on which its welfare depends” This description fails to address the situation when it is possible that the damage is too high to choose the most reliable branch. So, the extension of this definition is: “Trust is the extent to which one party is willing to depend on something or some person in a given situation with a feeling of relative security, even though negative consequences are possible.” The area of Internet applications, they classify trust as: Access to a trusted person’s Resources, Provision of Service by the Trustee, Certification of Trustees, Delegation, and Infrastructure Trust. In general, some of these types overlap in the concepts of access control mechanisms (for Access to a Trusted person’s Resources, and Certification of Trustees), trust properties (for Delegation), and context-based trust (for Infrastructure Trust). For example, Certification of Trustees is regarded as a mechanism to earn trust by supplying certified credential. Delegation is widely acknowledged as a trust property where one entity executes (e.g. authorize or inherit) tasks on behalf of others. Finally Infrastructure Trust refers to trust provided by infrastructures or circumstances, where the concept is not rather than context-based trust. All of these are considered properties that have significant impact on trust of a target, but not considered trust classification in our respect.

The primary focus of this trust type lies in content or information provisions in direct interactions between two parties. A trusted person is a provider who has an authority over content or information, and a trustee is a consumer, either another service in a workflow or end user. This trust type is generally found in data workflows, where the service providers are regarded as information provisions. Before providing or granting accesses to the information, trust relationship is determined in a way that a decision can be made. The degree of trust usually relates to a set of accesses and permissions granted. For instance, a certificate as an identity proof of a consumer can be used to determine a trust level specific to information and access rights. We differentiate between Resource Access Trust and Content (RATC) or Information Provision Trust (IPT), despite falling in the same category.

There is extensive research to describe Resource Access Trust where the resource is owned by, or under the authority of, the trustor. This is widely known as access control. Trusting a trustee to provide a particular content or information and assign relative access rights are fully decided by a trustor. Policy is widely used for the declaration of conditions and rules associating with rights and permissions. However, neither access rights nor permissions are regarded in Content or Information Provision Trust. After receiving content or information, the authority is simultaneously transferred to the consumer. Policy-based trust using policies to establish trust, focused on managing and interchanging credentials and enforcing access policies. Policy-based trust works are generally assumes that trust is established easily by obtaining a sufficient amount of credentials pertaining to a specific party, and applying the policies to provide that party certain access rights. The recursive problem of trusting the credentials is frequently solved by using a trusted party to serve as an authority for issuing and verifying credentials.

Reputation-based trust using reputation to establish trust, where historical interactions or performance for an entity are combined to assess its future behaviour. Research in reputation that is based trust uses the history of an entity’s actions/behavior to compute trust, and may use referral-based trust (information from others) in the absence of (or in addition to) personal knowledge. In the latter case, work is being done to calculate trust over social networks (a graph where vertices are public and edges denote a relation among public), or across paths of trust (where two parties may not have direct trust information about one another, and must rely on a third

party). Recommendations are trust decisions made by other users, and combining these decisions to form a new one, often personalized, is another commonly addressed problem. Generalized models of trust there is a wealth of research on modeling and defining trust, its prerequisites, conditions, components, and consequences.

The Trust models are highly useful for analyzing human and agenized trust decisions and for operational computable models of trust. The modeling of trust related works describes values or factors that play a role in computing trust, and leans more towards psychology and sociology for a decomposition of what trust comprises. The modeling research ranges from basic access control polices (which specify who to trust to access data or resources) to analyses of competence, values, risk, significance, utility, etc. These subcomponents underlying trust help our understanding of the more delicate and multifaceted aspects of composing, finding, and using trust in a computational setting.

Trust in information resources trust is an increasingly common subject in web related research regarding whether web resources and web sites are reliable. Moreover, trust on the web has its own array of varying uses and meanings, including capturing ratings from users about the superiority of information and services they have used, how web site design influences trust on content and content giver, broadcasting trust over links, etc. With the advent of the semantic web, new work in trust is harnessing both the likely gained from device understanding, and addressing the problems of reliance on the content available in the web so that agents in the semantic web can eventually make trust decisions autonomously. Provenance of information is the key to support trust decisions, as is automated detection of opinions as distinct from objective information.

IV. OVERVIEW OF REPUTATION

Reputation is public knowledge and represents the collective opinion of members of a group and it is based on the cumulative trust opinion of a group of agents. Since trust is highly skewed, this cumulated result may not be of equal use to all agents. Reputation is derived using the beliefs such as competence in which reputation as a subject is able to produce the expected result and play a positive role in the agent's plan; dependence belief: the agent's belief that it is necessary to rely on the subject to achieve its goal(s); disposition belief: the belief that a subject is not only capable of performing a given task but is also currently available to perform that task; motivation belief: the belief that a subject is motivated to cooperate with the agent and that this inspiration is expected to prevail in the face of conflicting motives; persistence belief: the belief that a subject will trail through on its obligation; self-confidence belief: the belief that the subject is confident to do the given task; enthusiasm belief: the belief that the subject is willing to perform the given task.

Reputation is also the global perception of a node's trustworthiness in a network. Reputation-based cooperation stimulation mechanisms make use of the status assessment of the nodes derived from the individual-level trust models to decide which of them to penalize. However, it is vital to point out here that it is only possible to evaluate the reputation of a node in a centralized personalized-level trust model. In distributed personnel-level trust models, although demonstrations from spectator nodes are sorted by an agent node to form an estimate of the reputation of a subject node for interaction decision making, the result may only be an guess of the total perception of a subject node's trustworthiness in a network. On the other hand, in the system-level trust model prose, the term reputation-based cooperation stimulation mechanism is commonly used. The location of a given member of a community within a social network can be used to infer some properties about degree of expertise, i.e., reputation. Experts who are well-known and highly regarded by most other members of the community tend to be with no trouble to identify as highly connected nodes in the social network graph of their community. This relation information could be a basis for a reputation mechanism used by users' assistant agents instead of having to option to overt ratings issued by each user.

Reputation is "overall quality or character as seen or judged in general as". The Reputation slab is responsible for maintaining the reputation of a node. This duty encompasses many tasks. This block manages reputation representation, updates reputation based upon the new observations made by the "Watchdog", integrates the reputation information based on other available information, ages the reputation, and creates an output metric of trust. Reputation systems are widely

used in diverse domains. E-commerce systems, such as *eBay, Yahoo* auctions and Internet-based systems such as Keynote, maintain reputation metrics at a centralized trusted person. Additionally, they use a well defined number for representing reputation. As a result, these systems use several arguable heuristics for the major steps of reputation updates and integration. In fact, much closer to our context are standing systems such as those planned for ad-hoc networks, CONFIDANT and CORE, and PEER-to-PEER networks. These systems are dispersed and also maintain a numerical representation of the reputation by borrowing tools from the realms of game theory.

Reputation systems try to counter selfish routing misbehavior of nodes by forcing nodes to oblige with each other. Recently reputation systems were projected in the domain of ad-hoc networks, which formulate the problem in the territory of Bayesian analytics than game theory. These systems can counter any arbitrary misbehavior of nodes. A transaction occurs whenever two nodes make an exchange of information or participate in a collaborative process. With each exchange, the nodes generate ratings indicating the “Cooperativeness” of their partner node. The first approach, based on binary ratings, will be familiar to many readers. The second approach is based on interval ratings and appeals to the Dirichlet Process, which is gaining popularity in the statistics and machine learning literature. Another way of learning about other nodes in the network is to make use of the experiences of other nodes in the neighborhood. Different nodes have different reputations for other nodes because they may have developed the reputation based on a disjoint set of events. Reputation is used to establish trust, where past interactions or performance for a unit are combined to evaluate its prospect of behavior. Research in reputation-based trust uses the history of an entity’s actions/behaviour to evaluate trust, and may use referral based trust (information from others) in the absence of (or in addition to) first-hand knowledge. In the latter case, work is being done to compute trust over social networks (a graph where vertices are people and edges denote a social relationship between people), or across paths of trust (where two parties may not have first hand trust data about each other, and must rely on a third party). Recommendations are trust decisions made by other cloud users, and adding these decisions to synthesize a new one, often personalized, is another commonly addressed problem.

V. CONCLUSION

Trust may be better seen as a motivating idea underlying many problems and contexts rather than as a precise idea to be studied under a uniform framework. Trust research in the semantic web poses new challenges that can be better met by building on the different but noteworthy body of work in modeling trust in computer science. Another potentially productive research direction is to use social associations in evaluating trust among collaborators in a group setting by employing the concept of social networks. Examples of social networks are strong social relationships including co-workers or relations, membership in the same squad, and loose social relationships including school alumni or friends with common interests or members in partnership activities. Social trust may include friendship, honesty, privacy, and social reputation or recommendation based which is either from direct or indirect interactions for sociable purposes. An important and interesting research direction is to construct a composite trust metric based on social trust and other trust components that are representing quality-of-service (QoS) to successfully perform tasks to meet both performance and trust requirements.

REFERENCES

[1] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, “A survey of trust and reputation management systems in wireless communications,” Proc.IEEE, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.

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

[3] Sumin Jiao, Zhixiao Yang, Bin Zhang, “A Reputation Computation Model for Trusted Networks Considering Uncertainties based on Cloud Theory “Computer Research and Development (ICCRD), 3rd International Conference on vol. 1.,pp. 473–476, 2011.

[4] Feng Li & Jie Wu, ‘Uncertainty modeling and reduction in MANETs’, IEEE Transactions on Mobile Computing, vol 9, no. 7, pp.1035-1048, 2010.

[5] Marsh S P. Formalising "Trust as a Computational Concept". Ph. D dissertation. University of Stirling, Scotland 1994.

[6] Jameel H, Hung L X, Kalim U, "A Trust Model for Ubiquitous Systems Based on Vectors of Trust Values". In Proc. of the 7th IEEE International Symposium On Multimedia. Washington: IEEE Computer Society Press., pp. 674-679, 2005.

[7] Sun Y, Yu W, Han Z, Liu KJR. "Information Theoretic Framework of Trust Modeling and Evaluation for ad-hoc Networks". IEEE Journal on Selected Areas in Communications, Selected Areas in Communications, vol 249,no 2: pp.305-319, 2006.

[8] Wei Wang, Guosun Zeng. "Trusted Dynamic Level Scheduling Based on Bayes Trust Model". Science in China Series F-Information Sciences, vol 50 no3 pp.456-469,2007.

[9] Chen Jincui, Jiang Liqun. "Role-Based Access Control Model of Cloud Computing". Energy Procedia, vol 13: pp.1056 - 1061, 2011.

[10] S. Wang, L. Zhang, N. Ma, and S. Wang, "An evaluation approach of subjective trust based on cloud model," in Computer Science and Software Engineering, 2008 International Conference on, vol. 3, pp. 1062–1068, 2008.

[11] Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision Decision support systems, vol. 43, no. 2, pp. 618–644, 2007.

[12] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 10th International Conference on, pp. 933– 939, 2011.

[13] H. Kim, H. Lee, W. Kim, and Y. Kim, "A trust evaluation model for QoS guarantee in cloud systems," International Journal of Grid and Distributed Computing, vol. 3, no. 1, pp. 1-8, 2010.

[14] Rizwana A. R. Shaikh, M. Sasikumar, 2012 "Trust Model for a Cloud Computing Applications and Services," Computational Intelligence & Computing Research (ICCIC), IEEE International Conference on, pp. 1-4, Dec. 2012.

[15] M. Kuehnhausen, V. S. Frost, and G. J. Minden, "Framework for assessing the trustworthiness of cloud resources," in Proc. IEEE Int. Multi-Discipl. Conf. Cognit. Methods Situation Awareness Decision Support, pp. 142–145, Mar. 2012,.

[16] Das and M. M. Islam, "SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems," IEEE Trans. Depend. Secure Computing, vol. 9, no. 2, pp. 261–274,Mar./Apr. 2012 .

[17] Xiaoyong Li, Junping Du , "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing "International Institution of Engineering and Technology on vol. 1.,pp. 39–50, 2012.

[18] Lin Guoyuan, Wang Danru, BieYuyu, Lei Min , "MTBAC: A Mutual Trust Based Access Control in Cloud Computing," China Communications, pp. 154–162, 2014.

[19] Guoyuan Lin, Yuyu Bie, Min Le, "ACO-BT M: A Behavior Trust Model in Cloud Computing Environment," International Journal of Computational Intelligence Systems, pp. 1-11, 2013.

[20] Guoyuan Lin, Yuyu Bie, Min Lei. "Trust Based Access Control Policy in Multi-Domain of Cloud Computing". Journal of Computers., vol 8 no 5 1357-1365, 2013.

[21] Y. Sun and Y. Liu, "Security of online reputation systems: The evolution of attacks and defenses," IEEE Signal Process. Mag., vol. 29, no. 2, pp. 87–97, Mar. 2012.

[22] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surv. Tuts., vol. 13, no. 4,pp. 562–583, Fourth Quarter 2011.