International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 1 15 – 18

Survey on Various Trust Management Issues in Cloud Environments

Mr. Uday Nalavade
Department of Computer Engineering
RMD Sinhagad Institute of technology, Warje Campus, Pune
udaynalavade55@gmail.com

Prof. Vina M. Lomte
Department of Computer Engineering
RMD Sinhagad Institute of technology, Warje Campus, Pune
vinamlomte@gmail.com

***Abstract*—** Over the past few years, trust management has been one of the hot topics especially in the area of cloud computing. Well-known benefits resulting from cloud computing adoption, several issues have emerged during its evolution: most of them relate to security, privacy and trust management. In particular, its proliferation has placed even more attention to trust management, representing one of the key challenges in the adoption of cloud computing technologies. This paper proposes a survey of existing trust management models addressing collaboration agreements in cloud computing scenarios. Main limitations of current approaches are outlined and possible improvements are traced, as well as a future research path.

Keywords-*Cloud Computing, trust management, reputation, credibility, credentials, security, privacy, availability*

*****

I. INTRODUCTION

Cloud services are accessible through internet portals and indexed on internet search engines like Google, Yahoo, and Baidu. Interactions for this layer are considered as cloud service interaction with users and TMS, and cloud services advertisements wherever suppliers are ready to advertise their services on the net. The Trust Management Service Layer consists of many distributed TMS nodes that are hosted in multiple cloud environments in numerous geographical areas. These TMS nodes expose interfaces in order that users will provide their feedback or inquire the trust ends up in a decentralized method. Interactions for this layer include: i) cloud service interaction with cloud service suppliers, ii) service advertising to advertise the trust as a service to users through the web, iii) cloud service discovery through the web to permit users to assess the trust of recent cloud services and iv) Zero-Knowledge credibility Proof Protocol (ZKC2P) interactions enabling TMS to prove the quality of a selected consumer's feedback.

The Cloud Service client Layer: Finally, this layer consists of various users who use cloud services. As an example, a brand new startup that has restricted funding will consume cloud services (e.g., hosting their services in Amazon S3). Interactions for this layer include: i) service discovery wherever users are ready to discover new cloud services and different services through the web, ii) trust and repair interactions wherever users are ready to provide their feedback or retrieve the trust results of a selected cloud service, and iii) registration wherever users establish their identity through registering their credentials in IdM before utilizing TMS. Our framework additionally exploits an internet travel approach for automatic cloud services discovery, wherever cloud services are mechanically discovered on the web and keep within the cloud services repository. Moreover, our framework contains an Identity Management Service that is accountable for the registration wherever users register their credentials before utilizing TMS and proving the quality of a selected consumer's feedback through ZKC2P.

II. RELATED WORK

According to Hatman: Intra-Cloud Trust Management for Hadoop[2] - S. M. Khan and K. W. Hamlen[1]the authors quoted on Data and computation integrity and security are major concerns for users of cloud computing facilities. Many production-level clouds optimistically assume that all cloud nodes are equally trustworthy when dispatching jobs; jobs are dispatched based on node load, not reputation. This increases their vulnerability to attack, since compromising even one node suffices to corrupt the integrity of many distributed computations. This paper presents and evaluates Hatman: the first full-scale, data-centric, reputation-based trust management system for Hadoop clouds. Hatman dynamically assesses node integrity by comparing job replica outputs for consistency. This yields agreement feedback for a trust manager based on Eigen Trust. Low overhead and high scalability is achieved by formulating both consistency-checking and trust management as secure cloud computations; thus, the cloud's distributed computing power is leveraged to strengthen its security. Experiments demonstrate that with feedback from only 100 jobs, Hatman attains over 90% accuracy when 25% of the Hadoop cloud is malicious.

According to Privacy, Security and Trust in Cloud Computing -S. Pearson, the authors quoted on, Cloud computing refers to the underlying infrastructure for an emerging model of service provision that has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on information technology (IT) budgeting but also affect traditional security, trust and privacy mechanisms. The advantages of cloud computing—its ability to scale rapidly, store data remotely and share services in a dynamic environment—can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers. Some core traditional mechanisms for addressing privacy (such as model contracts) are no longer flexible or dynamic enough, so new approaches need to be developed to fit this new paradigm. In this chapter, we assess how security,

trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed.

Talal h Noor et al [3], explained in their study an outline of the cloud service models and that they surveyed the most techniques and analysis prototypes that with efficiency support trust management of services in cloud environments. They have presented a generic analytical framework that assesses existing trust management analysis prototypes in cloud computing and relevant areas using a set of assessment criteria. Open analysis problems for trust management in cloud environments are mentioned. Trust management and privacy remains considered collectively of the key challenges within the adoption of cloud computing. Many problems associated with general trust assessment mechanisms, distrusted feedback, poor identification of feedback, privacy of participants, and therefore the lack of feedback integration still ought to be addressed. During this article, author and his colleague have presented a comprehensive survey that's, to the most effective of their information, the first to concentrate on the trust management of services in cloud environments. They distinguished the trust management views and classify trust management techniques into four completely different classes. They more planned a generic analytical framework which will be used to compare completely different trust management analysis prototypes supported a group of assessment criteria. They have overviewed and compare thirty representative analysis prototypes on trust management in cloud computing and therefore the relevant analysis areas. On the other hand the present analysis efforts; they additionally inspired additional insight and development of innovative solutions to handle the varied open analysis problems that they need known during this work.

S. Habib, S. Ries, and M. Muhlhauser [4], in this paper, author and his colleague planned a framework to enhance ways that on trust management in cloud environments. Specifically, they introduced a quality model that not only distinguishes between credible trusts feedbacks but also has the flexible to notice the malicious trust feedbacks from attackers. Authors even have given a replication determination model that dynamically decides the optimum replica range of the trust management service in order that the trust management services are continuously maintained at a desired availableness level. The approaches are valid by the example system and experimental results. Specifically, they need distinguished the subsequent key problems with the trust management in cloud environments: Trust strength, availableness of the Trust Management Service, Trust Feedback Assessment and Storage. As future work, they planned to manage more difficult issues like the Sybil attack and also the white washing attack. Performance optimization of the trust management service is another focus of their future analysis work.

ShimpyHarbajanka et al [5], a system planned that implements the trust management system for cloud computing, that assures secure information access through trustworthy cloud service supplier. Here, the trust analysis methodology is planned within which weighted trust issue is calculated considering multiple attributes. The trust issue helps users to spot trustworthy cloud services supplier through that they'll use cloud services. The most purpose of this paper is to introduce a trust management system for cloud computing and to traumatize varied security problems in cloud computing. The trust management system developed can offer authentication, integrity and secure knowledge access. It aims at supporting customers to spot trustworthy services supplier. During this planned work the information management and hosting services are investigated for reliable, sensitive and trustworthy distribution throughout information exchange. The planned work includes information management in cloud servers with security and privacy. It additionally includes the implementation of the 2 servers, 1st offers the services for applications, and secondary server is enforced to consume the first server's services in secured manner. So as to preserve the information in network and storage the crypto logical system is additionally planned. Additionally of that gives a weighted trust analysis for accessing and storing knowledge on the server.

Siani Pearson et al [6],during this paper authors assessed however security, trust and privacy problems occurred within the context of cloud computing and mentioned ways during which they will be addressed . Then they have considered the privacy, security and trust problems related to cloud computing in additional detail, along with connected legal issues, Lack of User Management, Unauthorized Secondary Usage, information Proliferation and Transborder information Flow and lots of additional. During this paper author and his colleague have assessed a number of the key problems concerned, and began the idea of some approaches that they believed are going to make revolution in addressing this case. Auditing is difficult task because of the volatility of the resources used. Current cloud services create an inherent challenge to information privacy. It may be difficult to determine privacy compliance necessities within the cloud. There are laws inserting geographical and different restrictions on the process by third parties of private and sensitive data. These laws place limits on the utilization of cloud services as presently designed.

The work proposes (Kong and Zhai, 2012)[7] a particular mechanism, called Trust-based Recommendation System in service-oriented Cloud computing (TRSC), which evaluates CSP services based on the trust of them. In TRSC, the resulting trust value is obtained combining direct trust and recommendation trust. Direct trust of an user on a cloud service is computed as usual, that is according on the direct interaction. While the recommended trust is evaluated taking into account opinions coming from users, or other authority of the field, who are trusted by the user, considering that this kind of trust is more reliable.

The authors (Noor et al., 2013)[8] developed a platform for a credibility-based trust management of cloud services, called Cloud Armor. The key features of the presented platform are: i) usage of a web crawling approach to automatically discover cloud services; ii) an adaptive and robust credibility model to evaluate credibility of feedbacks; and iii) a trust based recommender to recommend trustworthy cloud services that suit the users needs. Cloud Armor provides an

environment where customers can give feedbacks and request trust assessment for a particular cloud service.

Aim of the authors (Rizvi et al., 2014) [9] is to propose objective trust model, since it involves thirdparty auditors to develop unbiased trust between CSP and users. In this way, customers have a baseline to assess services and CSPs. In this case, third-party auditor assigns score for each CSP, basing on predetermined criteria significant to trust. More precisely, when a CSP is willing to enter the cloud market, it applies to be scored by the third-party auditor. The evaluation can be done using different set of criteria, such as those proposed by CSA (Cloud Security Alliance, 2013). However, when scoring a CSP, the customer feedback is taken into account too. For each criteria identified and evaluated by the third-party auditor, the obtained score will be integrated with feedback coming from end users. Like other recommendation based systems, the approach used in this case is similar to ones adopted by the e-commerce trust models.

Huang and Nicol, 2013 [10] found that even if some work in literature discusses about this two groups in a separate way, we prefer to refer to them as a whole class. Because of their similarity, in this way the aim is avoiding ambiguity. The reputation of an entity is the aggregated opinion of a community towards that entity. Thus, an entity with high reputation is the one trusted by various entities in the community. In this way, an entity that needs to retrieve trust opinion on a trustee, may use the reputation to evaluate the trust level of that subject. The reputation of a CSP helps end users (especially individual users) in choosing a cloud service from many options without particular requirements. A similar approach is defined as ”social trust”. As already said, this group includes trust models that collect feedback and opinions from other users, evaluating the trust on services and providers. Trust model collects and manages the feedback regarding different QoS and security parameters offered by CSPs. Based on this information, users will prefer the CSP that guarantees all the necessary QoS and security attributes for its customers.

The authors (Pawar et al., 2012) [11]propose an uncertainty model, which calculates trust values based on different parameters, namely (i) SLA monitoring compliance, (ii) service provider ratings, and (iii) service provider behavior. More in detail, the SLA monitoring defines the opinion about a CSP from the established SLAs about its services. Each of them are provided with a single SLA that includes several common indicators, such as CPU, memory, disk space usage, number of virtual machines. For each indicator of an SLA, a monitor evaluating the compliance/noncompliance of the indicator is provided. Then, CSP ratings are determined with the computation of all ratings, based on consensus and conjunction ratings. To calculate trust values, the model take into account features like belief, disbelief, uncertainty, and base rate.

The work presents (Marudhadevi et al., 2014)[12]a trust mining model (TMM) to identify trusted cloud services while negotiating an SLA. The challenge for the user is to monitor the services provided from the CSP and check if they meet the conditions mentioned in the agreement. To perform this, the user needs further information such as prior data or knowledge about what is happening on the CSP side, which can help him to better realize the effective QoS. The trust model evaluates the trust degree on the prior data obtained about the service at the time of the SLA. Then, this information is divided into multiple common at tributes like the number of service denials, average response time, task success ratio and number of complaints registered by the users. Usually, attributes used to formulate any trust model can be either objective or subjective, while this work uses both types of values. In this way, advantages introduced with this approach are both for CSPs and end users. From one side, the CSP can monitor the performance and improve its services to establish better trust relations with the users. And from the other side, the customer can perceive as secure working with the CSP.

Sr. No.	Paper Title / Year	Technique	Advantages	Research Gap
1	Intra-Cloud Trust Management for Hadoop S. M. Khan and K. W. Hamlen	dynamically assesses node integrity by comparing job replica outputs for consistency This yields agreement feedback for a trust manager based on Eigen Trust. Low overhead and high scalability	the cloud's distributed computing power is leveraged to strengthen its security	This increases their vulnerability to attack, since compromising even one node suffices to corrupt the integrity of many distributed computations.
2	CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services Talal h Noor	outline of the cloud service models and that they surveyed the most techniques and analysis prototypes that with efficiency support trust management of services in cloud environments.	information management and hosting services are investigated for reliable, sensitive and trustworthy distribution throughout information exchange	The planned work includes information management in cloud servers with security and privacy.
3	S. Habib, S. Ries, and M. Muhlhauser	replication determination model that dynamically decides the optimum replica range of the trust management service	replication determination model that dynamically decides the optimum replica range of the trust management service	Not handle more difficult issues like the Sybil attack and also the whitewashing attack. Performance optimization of the trust management service is another focus
4	Security Issues and Trust Management in Cloud is Computing Shimpy Harbajanka	trust analysis methodology is planned within which weighted trust issue is calculated considering multiple attributes	information management and hosting services are investigated for reliable, sensitive and trustworthy distribution throughout information exchange	More useful when focused on weighted trust analysis for accessing and storing knowledge on the server.
5	Privacy, security and trust in cloud computing, S. Pearson	System focused on the key problems concerned, and began the idea of some approaches that they believed are going to make revolution in addressing this case	considered the privacy, security and trust problems related to cloud computing in additional detail, along with connected legal issues	Need to find solution for laws inserting geographical and different restrictions on the process by third parties of private and sensitive data.
6	Trust based recommendation system in service-oriented cloud computing, Kong, D. and Zhai, Y. (2012).	Trust-based Recommendation System in service-oriented Cloud computing (TRSC), which evaluates CSP services based on the trust of them.	trust is evaluated taking into account opinions coming from users, or other authority of the field, who are trusted by the user, considering that this kind of trust is more reliable	Generally direct trust of an user on a cloud service is computed as usual, that is according on the direct interaction. Need to consider as a future scope
7	A trust evaluation model for cloud computing using service level agreement, Marudhadevi, D., Dhatchayani, V. N., and Sriram, V. S. (2014).	trust mining model (TMM) to identify trusted cloud services while negotiating an SLA.	Usually, attributes used to formulate any trust model can be either objective or subjective, while this work uses both types of values	In this system the challenge for the user is to monitor the services provided from the CSP and check if they meet the conditions mentioned in the agreement

III. CONCLUSION

In this paper, we propose a system to enhance the cloud based trust and reputation. User's feedback is a good source to know the level of trustworthiness which may be later used to achieve high level of trust by developing the loose ends. However, malicious users are always the issue and so are in this case, but the framework works at its best to detect malicious users. The integration of credibility model to that of availability module enhances the robustness against Sybil attacks making the system more secure.

IV. FUTURE SCOPE

We plan to combine different trust management techniques such as reputation and recommendation to increase the trust results accuracy. Performance optimization of the trust management service is another focus of our future research work.

REFERENCES

[1] S. M. Khan and K. W. Hamlen, "Hatman: Intra-cloud trust management for Hadoop," in Proc. 5th Int. Conf. Cloud Comput., 2012, pp. 494–501.

[2] Hatman,"Hatman: Intra-cloud Trust Management for Hadoop,"Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, 2012

[3] T. H. Noor, Q. Z. Sheng, A. H. Ngu, SchahramDustdar and Lina Yao, "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services,"

[4] S. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in Proc 10th IntConf Trust, Security Privacy Computer Communication 2011, pp. 933–939

[5] ShimpyHarbajanka et al,"Security Issues and Trust Management in Cloud Computing",WIR '16, March 21-22, 2016, Indore, India © 2016 ACM. ISBN 978-1-4503-4278

[6] S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks. New York, NY, USA: Springer, 2013, pp. 3–42.

[7] Kong, D. and Zhai, Y. (2012). Trust based recommendation system in service-oriented cloud computing. In Proceedings of the 2012 International Conference on Cloud and Service Computing, pages 176–179. IEEE Computer Society

[8] Noor, T. H., Sheng, Q. Z., Ngu, A. H., Alfazi, A., and Law, J. (2013). Cloud armor: a platform for credibilitybased trust management of cloud services. In Proceedings of the 22nd ACM international conference on Conference on information & knowledge management, pages 2509–2512. ACM

[9] Rizvi, S., Ryoo, J., Liu, Y., Zazworsky, D., and Cappeta, A. (2014). A centralized trust model approach for cloud computing. In Wireless and Optical Communication Conference (WOCC), 2014 23rd, pages 1–6. IEEE.

[10] Huang, J. and Nicol, D. M. (2013). Trust mechanisms for cloud computing. Journal of Cloud Computing, 2(1):1–14

[11] Pawar, P. S., Rajarajan, M., Nair, S. K., and Zisman, A. (2012). Trust model for optimized cloud services. In Trust Management VI, pages 97–112. Springer

[12]]Marudhadevi, D., Dhatchayani, V. N., and Sriram, V. S. (2014). A trust evaluation model for cloud computing using service level agreement. The Computer Journal, page bxu129.