A Survey on Feedback base Trust Evaluation for Cloud Environment

Sandip Machhi
Computer Science and Engineering
Parul University
Vadodara, India
Sandipmachhi23@gmail.com

Prof. G. B. Jethava
Information Technology
Parul University
Vadodara, India
g.jethava@gmail.com

*Abstract***— Cloud computing widely adopted by enterprises and individuals. Cloud computing provide several advantages but still there are many obstacles in cloud. Trust plays major role in commercial cloud environments. In the environment of multi cloud service provider, the assurances are not enough for the cloud users to select the trustworthy cloud service providers. Due to this problem, some cloud users have lack of trust in the services provided by the providers. This paper presents the importance of trust management in cloud environments. It also describes the feedback base trust issues when trust calculation done through feedback of cloud users. It is important to identify the feedback base attacks because less submission of fake feedbacks can also compromise the whole trustworthiness of service provider.**

Keywords- Cloud Computing, Trust Management, Malicious Feedback

I. INTRODUCTION

Cloud Computing has been emerged as new computing way in which two main players. Cloud service providers and cloud end-users. There are several definition propose to define exactly what is cloud computing by different authors. Cloud computing is a relatively new business model in the computing world. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [7]."

The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three "service models" (software, platform and infrastructure), and four "deployment models" (private, community, public and hybrid) that together categorize ways to deliver cloud services [4].

Cloud computing provide several advantages such as rapid elasticity, location independence, device diversity etc. However, there are many open issues which are obstacles in adoption and growth of cloud computing such as security, privacy, vendor-lock in, trust etc [7][11].

Trust Management is widely used in various sectors such as wireless system, e-commerce sector, human sociology etc. In cloud environment, trust evaluation is very important to find the trustworthy of service provider. One major source for trust estimation of service provider is ratings submitted by cloud customers. This paper presents different kinds of attacks when trust calculation done through feedbacks submitted by cloud users [9].

In this paper next section describes that what is trust, requirements of trust in cloud environment and types of trust. Then after distinguishes the different parameters used for trust evaluation and last section describes feedback base trust evaluation attacks, proposed solution by different authors and the summary of attacks and possible occurrences of attack in different stages of trust management.

II. TRUST MANAGEMET

Many years ago, Trust used in social science for constructing human being relationship and now it is important substitute for forming security mechanism in distributed computing environments. Trust management has many security attributes such as reliability, dependability, confidence, honest, belief, truthfulness, security, competence [8].

There are two types of trust 1) Direct trust and 2) Indirect Trust [8]. Direct trust is based on personal experience and Indirect trust state that when any person has no any direct experience then he is rely on others direct trust. This type of trust is known indirect Trust. In cloud environment various service provider is available. Hence, it is very important to identify trustworthy service provider.

Trust is complex relationship among different cloud entity and because trust is more subjective, context dependent, non symmetric and uncertain[3][11] .

There are various ways of evaluation of trust. In e-commerce sector, we can evaluate the trustworthiness by feedback submitted by cloud users. When trust is calculated based on feedback ratings of cloud users there may chance various feedback base attacks. Next section desire the various possible attack on feedback based trust evaluation.

III. CATEGORY OF TRUST MANAGEMENT PARAMETER

We can evaluate trustworthiness based on below classified trust parameters. We may categorize the trust related parameters in three categories [11].

A. Identity Base Trust Parameter

All the security related parameters like Authorization level, User protection level, Data security level, Data Recovery level etc. are involved in identity base trust management parameters.

B. Capability Base Trust Parameter

Capability of cloud resources like RAM, speed of processor, Bandwidth, latency are involved in capability base trust management parameters.

C. Behavior Base Trust Parameter

In behaviour based trust management, need to identify behaviour based parameter like availability, Success Rate, Feedback

A cloud user gives the feedback based on experience of above parameters after completion of transaction or experience of cloud services. When we measure behaviour based trust by cloud consumer feedback, we may get the accurate trust value if all the feedbacks are accurate. In real world, it is not always possible because there may chance of malicious feedback and several attacks possible on feedback base trust evaluation. Next section introduce the possible attacks when trust calculation done through users feedback.

IV. CATEGORY POSSIBLE ATTACKS ON FEEDBACK BASE TRUST EVALUATION

A. Feedback Storage and Evaluation

Trust valuation of a service in existing techniques is mostly centralized, whereas feedback comes from distributed trust participants [9]. Due to centralization may leads to scalability and security issues. Satyjeet and Mahadevan [16] proposed framework for secure application execution based on modified hypervisor that secures the processor architecture. Edna Dias [16] proposed trust model for data security in private cloud environment. Muchahari and Sinha [15] proposed the trust management framework which use of feedback and credibility to calculate trust value. Number of trusted majority feedback can give hint to identify credibility of trusted feedbacks [18].

B. Accuracy of Trust Result

Identification of the credible feedbacks from multiple submitted feedbacks is most challenging issue due to dynamical nature of cloud environment [9]. Accuracy of Trust closely relate with Robustness of Trust Evaluation. We may get the accurate trust result accuracy by reducing different possible attacks.

C. Collusion Attacks

This attack occurs when multiple users group together to give fake feedbacks to increase or decrease the trust result of service provider. This behaviour is called as collusive malicious feedback behaviour [17]. Three types of collusion attacks can be possible.

a) Self-Promoting Attack

Whole group Enter all positive feedback to promoting Cloud service provider.

b) Slandering Attack

Whole group enter all negative feedback for Cloud service provider.

c) Occasional Feedback Collusion

Collusion attacks in cloud services occur sporadically. Time is crusial parameter to identify occasional collusion attack [17]

Irissappane, S. Jiang and J. Zhang [19] proposed clustering approach which separate the malicious feedbacks from submitted feedbacks. S. Liu, J. Zhang, C. Miao and A. C. Kot [20] proposed clustering Method to improve the effectiveness of trust system. In this method cluster form based on ratings differences of all the ratings. Trust value is gained by aggregating credible weighted ratings. To detect Occasional Feedback

Collusion, we can calculate the occasional variation in submitted all feedbacks within the all feedback behaviour.

D. Sybil Attacks

Such Attack happen when malicious users give multiple fake feedback using different identity (i.e. Producing number of fake ratings using small amount of different product purchasing in very short time.) to increase or decrease the trust result [17].

Individual unfair feedbacks give unfairly without collaborating with others. Such feedbacks are given for several reasons such as lack of expertise, dishonesty or irresponsibility of the user etc. Attacker can apply different identities to conceal their negative previous trust record. Three types of Sybil attacks can be possible.

a) Self-Promoting Attack

User enter positive feedback to promoting Cloud service provider. This attack also known as ballot-stuffing attack [6].

b) A Slandering Attack

User enter negative feedback to promoting Cloud service provider. This attack also know as bad-mouthing attack [6].

c) Occasional Sybil Attacks

Malicious users can increase or decrease trust result by creating many accounts and submit fake feedbacks in very short period of time [17].

We may mitigate the Sybil attack by strong identity authentication using previously stored identity records. It can detect by calculation of occasional variation in submitted all identities within all identity behaviour [17].

E. Intoxication Attacks

In this attack, a member behaves as expected for specific period of time to obtain a high reputation and start to misbehave after gaining high reputation. Intoxication makes it difficult for the system to find such misbehaving members because of their high reputation.

This attack is also known as on-off attack. A member firstly gives good behaviour and with the increase of some more time user gives bad ratings. Such members are difficult to identify because member has maintain good reputation previously. In P2P network system, this attack known as dynamic personality of peers.

To resolve this attack, mostly used techniques is forgetting factor [21]. Although, malicious users many times used the forgetting factor. Sun and Liu proposed [21] Forgetting factor that when trust result lower than threshold more farseeing forgetting factor used otherwise short forgetting factor.

F. Discrimination Attacks

This attack happen when some service provider provides good services in some geographically regions and in some regions provides bad services to user. These ensured contradictory feedbacks among such regions and it may ensure as collusive attack. We have not found any solution for such attack [13].

G. Newcomer Attacks

A member can create newcomer attack if it can easily register as with new identity although member has already registered with service provider and produce some bad behaviour previously. This attack is also known as re-entry attack. Ultimately it converted in Sybil attack [13]. We can reduce newcomer attack comparing the credential recodes using different parameters such as location, unique id etc.

V. OCCURANCE OF ATTACKS IN TRUST MANAGEMENT

In this section we summaries different phases of occurrence of some attacks in trust management system. Newcomer attack and Sybil attack mostly occur in login phase. Discrimination attack and Intoxication attack can occur in transaction phase and collusion and Sybil attack can occur in trust evaluation phase. Although, trust result accuracy is based on quality of assessment from all feedbacks.

CONCLUSION

Cloud computing provide many advantages but still there are many obstacles in cloud based on usage of cloud. A most challenging issue that required to give focus in cloud computing is security and trust management, due to dynamic nature of cloud environment, which are important component of cloud security. When trust result evaluated by feedbacks of cloud user then there may possibility of malicious feedback submission. It is important to identify the feedback base attacks because less submission of fake feedbacks can also compromise the whole trustworthiness of service provider. In future, we need to find the other possible attacks on feedback collection, feedback evaluation and solution for how to prevent and detect those attacks effectively by strong trust model.

ACKNOWLEDGMENT

Special thanks to IJCSET and Parul University.

REFERENCES

[1] Sheikh Mahbub Habib, Sebastian Ries, Max Muhlhauser, Towards a Trust Management System for Cloud Computing, IEEE Trust, Security and Privacy in computing and Communications(TrustCom), Pages 933-939, 2013

[2] B.Kezia Rani, Dr.B.Padmaja Rani, Dr. A. Vinaya Babu, Cloud Computing and Inter-Clouds-Types, Topologies and Research Issues, ELSEVIER, Volume 50,Pages 24-29, 2015

[3] Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries and Max Muhlhauser, Trust as a Facilitator in Cloud Computing: A survey, Journal of Cloud Computing,1:19,2012

[4] Rajkumar Buyya, Christian Vecchiola, Thamarai Selvi, Mastering in Cloud Computing, Morgan Kaufmann, May 2013

[5] Maricela-Georgiana Avram, Advantages and challenges of adopting cloud computing from an enterprise perspective, ELSEVIER, Volume 12, Pages 529-534, 2014

[6] Soon-Keow Chong, Jemal Abawajy, Masitah Ahmad, Isredza Rahmi, Enhancing Trust Management in Cloud Environment, ELSEVIER, Volume 129, Pages 314-321, 2014

[7] Dawei Sun, Guran Chang, Lina Sun, Xingwei Wang, Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments, ELSEVIER, Volume 15, Pages 2852-2856, 2011

[8] Khald M. Khan and Qutalbah Malluhi, Establishing Trust in cloud computing, Qatar University, IEEE IT professional, Volume 12(5), 2010

[9] Talal H. Noor and Quan Z. Sheng, Trust as Service: A framework for Trust Management in Cloud Environments, Springer, Volume 6997, Pages 314-321,2011

[10] Rizwanna Shaikh, Dr. M. Sashikumar, Trust Model for Measuring Security Strength of Cloud Computing Service, ELSEVIER, Volume 45, Pages 380-389, 2015

[11] Paul Manuel, Thamarai Selvi Somasundaram, A Novel Trust management System for Cloud Computing – IaaS Providers, ResearchGate Journal of Combinatorial Mathematics and Combinatorial Computing, 79:3-22, 2011

[12] Soon-Keow Chong, Jemal Abawajy, Isredza Rahmi A. Hamid, Masitah Ahmad, A Multilevel Trust Management Framework for Service Oriented Environment, Elsevier, 129:396-405, 2013

[13] Dongxia Wang, Tim Mullerr, Yang Liu and Jie Zhang, Towards Robust and Effective Trust Management for Security: A Survey, ACM, 2014

[14] Satyajeet N Srujan Kotikela, Mahadevan Gomathisankaran, CTrust: A framework for Secure and Trustworthy application execution in Cloud Computing, International Conference on Cyber Security", 2012

[15] Manoj Kumar Muchahari, Smriti Kumar Sinha, A New Trust Management Architecture for Cloud Computing Environments, IEEE International Symposium on Cloud and Services Computing (ISCOS0), 2012

[16] Edna Dias, de Sousa, R T, de Carvalho , R.R., de Oliveira Albuquerque R., Trust Model for Private Cloud, IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic(CyberSec), 2012

[17] Talal H. Noor, Quan Z. Sheng, Lina Yao, Schahram Dustdar, Anne H.H. Ngu, CloudArmor: Supporting Reputation-based Trust Management for Cloud Services, IEEE Transactions on parallel and Distributed Systems, 2014

[18] L. Xiong and L. Liu, Peertrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communications, IEEE Transactions on Knowledge and Data Engineering, volume 16, no. 7, pp. 843-857, 2004

[19] A. A. Irissappane, S. Jiang, and J. Zhang, A Biclustering-based approach to filter dishonest advisors in multi-criteria e-marketplace, In Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems, pages 1385-1386, 2014

[20] S. Liu, J. Zhang, C. Miao, Y. L. Theng, and A. C. Kot, An integrated clustering-based approach to improve the robustness of reputation systems, In Proceeding s of the 10th [21] International Conference on Autonomous Agents and Multi agent System, Volume 3, pages 1151-1152, 2011

[21] Y. L. Sun, Z. Han, W.Yu and K. R. Liu, A trust evaluation framework in distributed networks: Vulnerability analysis and defence against attacks, In Proceeding s of the 25th International Conference on Computer Communication, IEEE, pages 1-13, 2006

[22] L. Xiong and L. Liu, Peertrust: Supporting Reputation-based trust for peerr-to-peer electronic communities, 16(7):843-857,2004

[23] Rizwana Shaikh, M. Sasikumar, Trust Framework for Calculating Security Strength of Cloud Service, IEEE International Conference on Communication, Information & Computing Technology, 2012

[24] Whitby, a. Josang A. & Indulska, J., Filtering out malicious ratings in Bayesian reputation system. In proceeding 7th Int. workshop on Trust in Agent Societies.

[25] Lin Guoyuan, Wang Danru, Bie Yuyu, LEI Min, MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing

[26] Josang, A. and Quattroiocchi, Advanced features in Bayesian reputation systems, Trust, Privacy and Secuirty in Digital Business, Vol. 5695, Heidelberg: Springer, pp. 105-114,2009

[27] Child, I.: The Psychological Meaning of Aesthestic Judgments. Visual Arts Research 9(2(18)),51-59 (1983)