# Effective Handling of Reputation-Based Trust Management in Cloud Environment

**Sonali Jivan Nikam**[1], **Dr. S. N. Kini**[2]

[1]Department Computer Engineering, Jayawantrao Sawant College of Engineering,
Hadapsar Pune-28, Savitribai Phule Pune University, Pune, India

[2]Professor Computer Engineering, Jayawantrao Sawant College of Engineering,
Hadapsar Pune-28, Savitribai Phule Pune University, Pune, India

**Abstract:** ***Trust management is a standout amongst the most difficult issue for the tackling and development of cloud computing. Many challenging issues such as privacy, security, and availability occur by highly dynamic, distributed, and non-transparent nature of cloud services. Saving consumers' privacy is not an easy task due to the confidential information invo lved in the interactions between customers and the trust management service. Protecting cloud services against their malicious clients (e.g., such clients may give misleading feedback to inconvenience a specific cloud service) is a complicated issue. Due to the dynamic nature of cloud environments, assuring the availability of the trust management service is a challenging issue. In this article, we elaborate the design as well as implementation of Cloud Armor, a reputation-based trust management system which provides an arrangement of functionalities to deliver Trust as a Service (TaaS), including i) a novel convention to demonstrate the credibility of trust inputs as well as save clients' security, ii) Not only a versatile but also robust credibility model for measuring the credibility of trust feedbacks to keep cloud services from malicious clients and to analyze the dependability of cloud services, and iii) an availability model to deal with the accessibility of the decentralized usage of the trust management service. The achievability and advantages of our methodology have been tried by a model and test studies utilizing a collection of true trust feedbacks on cloud services.***

**Keywords:** Cloud computing, trust management, reputation, credibility, credentials, security, privacy, availability

## 1. Introduction

Consumers' feedback is a best source to assess the overall trustworthiness of cloud services. Different researchers have known the significance of trust management as well as proposed solutions to assess as well as based on feedbacks manage trust collected from participants. The focus of this paper is totally on improving trust management in cloud environments by presenting novel ways. It is so to ensure the credibility of trust feedbacks. In particular, we differentiate the following key issues of the trust management in cloud environments. The adoption of cloud computing increases privacy concerns. Customers can have dynamic interactions with cloud providers. The interaction may involve sensitive information. There are different cases of privacy breaches first is leaks of sensitive information e.g., date of birth as well as address or behavioral information e.g., with whom the consumer interacted, the kind of cloud services the consumer showed interest etc. Undoubtedly, services which involve consumers' data e.g., interaction histories should preserve their privacy. It is not unusual that a cloud service experiences attacks from its users. Attackers can disadvantage a cloud service by giving multiple misleading feedbacks or they creating several accounts. Indeed, the detection of such malicious behaviors' poses various challenges. Firstly, new users join the cloud environment as well as old users leave around the clock. This consumer dynamism makes the detection of malicious behaviors a significant challenge. Secondly, users may contain multiple accounts for a particular cloud service, which makes it difficult to detect Sybil attacks. Finally, it is difficult to guess when malicious behaviors will going to occur.

## 2. Related Work

S. Habib, S. Ries, and M. Muhlhauser, 2011 -This paper proposed a data coloring method based on cloud watermarking to recognize and ensure mutual reputations. The experimental results describes that the robustness of reverse cloud generator can guarantee users embedded social reputation identifications in good sense. Hence, our work provides a reference solution to the critical problem of cloud security.[1]

P. Mell and T. Grance 2011 - The authors not only look at what trust is but also how trust has been applied in distributed computing. Trust models proposed for different distributed system has then been elaborated. The trust management systems proposed for cloud computing. It has been investigated with special emphasis on their capability, applicability in practical heterogonous cloud environment as well as implementabilty. Eventually, the proposed models/systems have been compared with each other based on a selected set of cloud computing parameters in a table.[2]
L. Yao and Q. Z. Sheng 2011- Propose the "Trust as a Service" (TaaS) framework to improvise the ways on trust management in cloud environments. We propose an adaptive credibility model that distinguishes between credible trust feedbacks as well as malicious feedbacks by considering cloud service consumers' capability and majority consensus of their feedbacks. The approaches have been validated by the prototype system as well as experimental results. Al Trust management is the major goal in the variety of cloud computing environment. multi-faceted Trust Management (TM) system architecture for a cloud computing marketplace. This system provides means to identify the trustworthy cloud

providers in terms of different attributes (e.g., security, performance, compliance) assessed by multiple sources and roots of trust information [3]

K. Ren, C. Wang, and Q. Wang 2012 - This paper listed such challenges and define a set of privacy, security and trust requirements that must be taken into account before cloud computing solutions can be fully integrated and deployed by telecommunication providers. Reputation attacks to allow consumers to effectively identify trustworthy cloud services. [4]

C. Dellarocas2003 -It provides a holistic view of ranking fraud as well as proposes a ranking fraud detection system for mobile Apps. Specifically, we first propose to correctly locate the ranking fraud by mining the active periods which is called leading sessions, of mobile Apps. These leading sessions can be leveraged for detecting the local anomaly instead of global anomaly of App rankings. Furthermore, we investigate three types of evidences, i.e., one is ranking based evidences second one is rating based evidences and third one is review based evidences, by modelling Apps' ranking, rating and review behaviours through statistical hypotheses tests. Additing to this, we propose an optimization based aggregation method to integrate all the evidences for fraud detection. [5]

R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, L. Qianhui, and L. B. Sung 2011 - The optimization which is based on aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the iOS App Store for a long time period. In the experiments, we validate the effectiveness of the proposed system, then show the scalability of the detection algorithm as well as some regularity of ranking fraud activities.[6]

## 3. Proposed Work

Given the highly dynamic, distributed, and nontransparent nature of cloud services, managing and establishing trust between cloud service users and cloud services remains a significant challenge. User's feedback of Cloud service is a decent source to assess the whole trustworthiness of cloud services. However, malicious users may collaborate together to i) disadvantage a cloud service by adding number of misleading trust feedbacks (i.e., collusion attacks) or ii) trick users into trusting cloud services that are not trustworthy by creating different accounts as well as adding misleading trust feedbacks (i.e., Sybil attacks). In this paper, the novel techniques is introduced that gives a help in detecting reputation based attacks, also allowing users to effectively identify trustworthy cloud services. In particular, credibility model is also introduced that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks happens in a long or short period of time (i.e., strategic or occasional attacks respectively). An availability model is also developed which maintains the trust management service at a desired level. We have collected a large number of consumer's trust feedbacks given on real-world cloud services to evaluate our proposed techniques. The experimental results demonstrate the applicability of our approach and show the capability of detecting such malicious behaviors. There are a few directions for our future work. 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.

## 4. Architectural View

The architecture diagram of the system shown below helps us to understand the system.

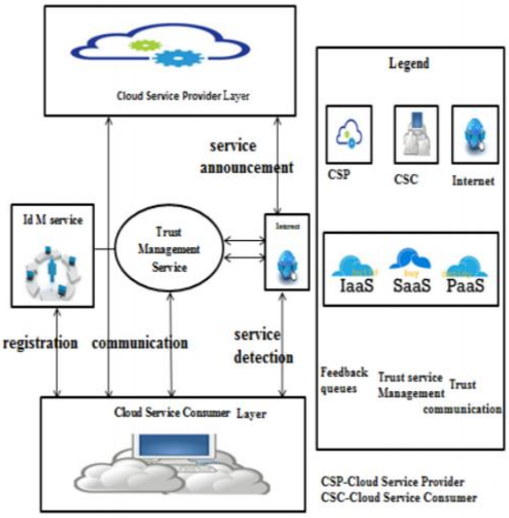

**Figure 1:** System Architecture

- User's feedback of Cloud service is a decent source to assess the whole trustworthiness of cloud services In this paper, the novel techniques is introduced that gives a help in detecting reputation based attacks, also allowing users to effectively identify trustworthy cloud services
- The credibility model is also introduced that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks happens in a long or short period of time (i.e., strategic or occasional attacks respectively).
- We also develop an availability model that maintains the trust management service at a desired level. We also develop an availability model that maintains the trust management service at a desired level.

**Table 1:** Survey Table

| *Paper* | *Technique* | *Advantages* | *Disadvantage* |
|---|---|---|---|
| Privacy and Security for Cloud Computing | memory management algorithms | transparency in the cloud implementation | regulatory issues |
| Trust mechanisms for cloud computing | formal trust mechanisms | gives self-assessments | Unimproved mathematical formal framework |
| Reputation attacks detection for effective trust assessment of cloud services | trust management techniques based on feedback | Framework gives accountability and trust in cloud computing | The detection of reputation attacks involves several issues including i) Consumers Dynamism ii) Multiplicity of Identities |
| Trust management of services in cloud environments: Obstacles and solutions | scalability and availability techniques are used for trust management systems | Compare different trust management research prototypes based on a set of assessment criteria. | challenging issues such as privacy |
| CloudArmor: A platform for credibility-based trust management of cloud services | visualization techniques such as the creation of the hardware platform and the operating | effectively evaluates the trust of cloud service provider | problem of unpredictable reputation attacks against cloud services |
| Hatman: Intra-cloud trust management for Hadoop | policy-based trust management techniques | highly dynamic, distributed, and nontransparent nature of cloud services | difficult issue for the tackling and development of cloud computing |
| An Analysis of Security Challenges in Cloud Computing | various techniques like phishing, exploitation of software and fraud | analyzed almost every security threat found across both the cloud models | security issues are concerned |
| Towards a trust management system for cloud computing | evaluation methods followed to evaluate the attributes | efficiently differentiate between a good and a poor quality | performance issues |

## 5. Conclusion

As of this Cloud Armor Supporting Reputation-based Trust Management for Cloud Services has been applied. Now cloud computing development, the controlling of trust component is supreme perplexing problem. Cloud computing has yield great challenge in security and privacy by the varying of environment. Trust is precise disturbed problems used for the acceptance and advance of cloud computing. Though several resolutions have been projected presently in managing trust feedbacks in cloud environments but in what way to regulate the trustworthiness of trust feedbacks is typically unnoticed. Moreover in future, we also increase the performance of cloud as well as the security.

## References

[1] S. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in Proc. 10th Int. Conf. Trust, Security Privacy Comput. Commun., 2011, pp. 933–939.

[2] P. Mell and T. Grance. (2011, Sep.). The NIST definition of cloud computing [Online]. Available: http://csrc.nist.gov/ publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[3] L. Yao and Q. Z. Sheng, "Particle filtering based availability prediction for web services," in Proc. 9th Int. Conf. Service-Oriented Comput., 2011, pp. 566–573.

[4] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[5] C. Dellarocas, "The digitization of word of mouth: Promise and challenges of online feedback mechanisms," Manage. Sci., vol. 49, no. 10, pp. 1407–1424, 2003

[6] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, L. Qianhui, and L. B. Sung, "TrustCloud: A framework for accountability and trust in cloud computing," in Proc. IEEE World Congr. Services, 2011, pp. 584–588.

[7] 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.

[8] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," J. Cloud Comput., vol. 2, no. 1, pp. 1–14, 2013.

[9] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[10] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[11] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, "Compliant cloud computing (C3): Architecture and language support for user-driven compliance management in clouds," in Proc. 3rd Int. Conf. Cloud Comput., 2010, pp. 244–251.

[12] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, "A trust management framework for service-oriented environments," in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 891–900.

[13] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation attacks detection for effective trust assessment of cloud services," in Proc. 12th Int. Conf. Trust, Security Privacy Comput. Commun., 2013, pp. 469–476.

[14] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in Proc. 2nd Int. Conf. Cloud Comput., 2010, pp. 693–702.

[15] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving digital identity management for cloud computing," IEEE Data Eng. Bull, vol. 32, no. 1, pp. 21–27, Mar. 2009.

[16] E. Friedman, P. Resnick, and R. Sami, "Manipulation-resistant reputation systems," in Algorithmic Game Theory. New York, USA: Cambridge Univ. Press, 2007, pp. 677–697.

[17] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[18] F. Skopik, D. Schall, and S. Dustdar, "Start trusting strangers? bootstrapping and prediction of trust," in Proc. 10th Int. Conf. Web Inf. Syst. Eng., 2009, pp. 275–289.

[19] H. Guo, J. Huai, Y. Li, and T. Deng, "KAF: Kalman filter based adaptive maintenance for dependability of composite services," in Proc. 20th Int. Conf. Adv. Inf. Syst. Eng., 2008, pp. 328–342.

[20] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," in Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl., 2010, pp. 27–33.

[21] Y. Wei and M. B. Blake, "Service-oriented computing and cloud computing: Challenges and opportunities," IEEE Internet Comput., vol. 14, no. 6, pp. 72–75, Nov./Dec. 2010.

[22] P. Mell and T. Grance. (2011, Sep.). The NIST definition of cloud computing [Online]. Available: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[23] O. David and C. Jaquet. (2009, Jun.). Trust and identification in the light of virtual persons pp. 1–103 [Online]. Available: http://www.fidis.net/resources/deliverables/identity-of-identity/

[24] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-preserving data publishing: A survey of recent developments," ACM Comput. Surv., vol. 42, no. 4, pp. 1–53, 2010.