INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1951 - 1955
RECEIVED: 10-03-2017. PUBLISHED: 30-03-2017.

March 30, 2017

SERVICE CHECK: EFFECTIVE USER BEHAVIOR ANALYSIS & TRUST MANAGEMENT IDENTIFY BEST CLOUD

[1]S.Logeshwaran, [2]P.Santhosh Kumar, [3]R.Thiruvengadam, [4]Mrs.A.Shobana,

[1,2,3]UG Scholar, Dept Of Information Technology, Sri Balaji Chockalingam Engineering College, Arni,

[4]Assistant Professor of Information Technology, Sri Balaji Chockalingam Engineering College, Arni.

ABSTRACT

Cloud Computing is vast developing technology. DDOS Attack in a Client Server Environment would Collapse the entire system. In the Proposed System, cloud service provides layer provides data sharing resources to the user. A trust management service provides an interface between users and cloud services for effective trust management. Trust management service layer is monitoring the load of every service provider and provides resources to the user based on the previous ratings about the service. We are deploying two algorithms namely, Sybil attack (same user will register by providing same E mail ID), Collusion attacks (Attackers will try to provide Feedbacks continuously within short span of time). In our project, Data owner uploads the file along with the keywords for retrieval. Both are stored separately. Apart from these two attacks. we also implement DDOS attack.The DDOS attack can be implemented in two ways.First, Same user sends the same file request for more times within a time frame. Second, Same user requests different files within a short period of time. Email Alert is send to the Owner in case of any attacks happening.

1. INTRODUCTION

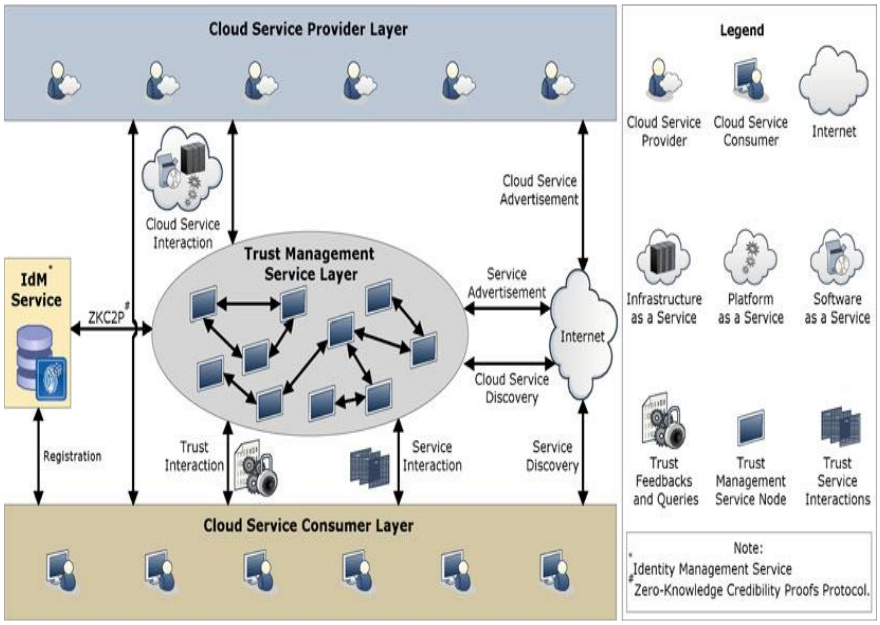
The highly dynamic, distributed, and non-transparent nature of cloud services make the trust management in cloud environments a significant challenge. According to researchers at Berkeley, trust and security are ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed, service-level agreements (SLAs) alone are inadequate to establish trust between cloud consumers and providers because of its unclear and inconsistent clauses. Consumers' feedback is a good source to assess the overall trustworthiness of cloud services. Several researchers have recognized the significance of trust management and proposed solutions to assess and manage trust based on feedbacks collected from participants. In reality, it is not unusual that a cloud service experiences malicious behaviors (e.g., collusion or Sybil attacks) from its users. This paper focuses on improving trust management in cloud environments by proposing novel ways to ensure the credibility of trust feedbacks. In particular, we distinguish the following key issues of the trust management in cloud environments: Consumers' privacy. The adoption of cloud computing raise privacy concerns. Consumers can have dynamic interactions with cloud providers, which may involve sensitive information. There are several cases of privacy breaches such as leaks of sensitive information (e.g., date of birth and 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

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1951 - 1955
RECEIVED: 10-03-2017. PUBLISHED: 30-03-2017.
March 30, 2017

privacy. Cloud services protection. It is not unusual that a cloud service experiences attacks from its users. Attackers can disadvantage a cloud service by giving multiple misleading feedbacks (i.e., collusion attacks) or by creating several accounts (i.e., Sybil attacks). Indeed, the detection of such malicious behaviors poses several challenges. First, new users join the cloud environment and old users leave around the clock. This consumer dynamism makes the detection of malicious behaviors (e.g., feedback collusion) a significant challenge. Second, users may have multiple accounts for a particular cloud service, which makes it difficult to detect Sybil attacks. Finally, it is difficult to predict when malicious behaviors occur (i.e., strategic vs. occasional behaviors). Trust management service's (TMS) availability.

2. RELATED WORK

Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumer's privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service.Cloud computing provides cost-efficient opportunities for enterprises by offering a variety of dynamic, scalable, and shared services. Usually, cloud providers provide assurances by specifying technical and functional descriptions in Service Level Agreements (SLAs) for the services they offer. 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.



INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1951 - 1955
RECEIVED: 10-03-2017. PUBLISHED: 30-03-2017.
March 30, 2017

3. TECHNICAL RIDE

USER REGISTRATION

In this module user registration is handled. The user detail like username, password, user personal details and cloud server with service provider details. The details are saved into Server. After Registration user can login and access the cloud server.

MAIN CLOUD SERVER

In this module main cloud server is deployed. Within this all access are maintained and monitored. Main server all details about service provider and user's information. If any New Request is comes from the user means server will collect all request and process that request. Based on the Request it will redirect it to that particular service providers and it verifies the attacks.

CLOUD SERVICE PROVIDERS

Cloud service providers are the providers who gives the cloud services like iaas, saas, paas. Service providers are given the services based on the amount, hardware configuration and also software services.

DETECTION OF COLLUSION ATTACKS

In this module server will detects the collision attacks happened. Collusion attack means there is same Attackers will try to provide Feedbacks continuously within short span of time. If it is happened means server will blocks that user and also removes the feedback information.

DETECTION OF SYBIL ATTACKS

In this module server will detects the Sybil attacks happened. Sybil attacks means there is same user will register by providing same E mail ID, mobile number with different usernames. Server will checks that same mail, mobile number repeated at the time registration means it blocks that user doesn't allowed that user.

RATING ANALYSIS OF BEST SERVICE PROVIDERS

Based on the feedback provided by the users about the services providers we will rank the best providers. Server will check the feedback at the time of given either it may be positive or Negative Feedback. Depends on Positive Feedback it ranks.

4. FUNCTIONAL RIDE

Particle Filtering based Algorithm

The sequential importance sampling (SIS) algorithm is a Monte Carlo (MC) method that forms the basis for most sequential MC filters developed over the past decades. This sequential MC (SMC) approach is known variously as bootstrap filtering, the condensation algorithm, particle filtering, interacting particle approximations, and survival of the fittest. It is a technique for implementing a recursive Bayesian filter by MC simulations. The key idea is to represent the required posterior density function by a set of random samples with associated weights and to compute estimates based on these samples and weights. As the number of samples becomes very large, this MC characterization becomes an equivalent representation to the usual functional description of the posterior pdf, and the SIS filter approaches the optimal Bayesian estimate.

CONCLUSION

Given the highly dynamic, distributed, and non-transparent nature of cloud services, managing and establishing trust between cloud service users and cloud services remains a significant challenge. However, malicious users may collaborate together to (i.e., collusion attacks, Sybil attacks) In this paper, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services. Identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks. We also develop an availability model that maintains the trust management service at a desired level.

FUTURE ENHANCEMENT

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.

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] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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,