CloudArmor: Supporting Reputation-based Trust Management for Cloud Services

D Deeba[1], Dr. J. Gnana Jayanthi[2]
[1, 2] Department of Computer Science
[1, 2] Rajah Serfoji Govt College

Abstract- *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 consumers' privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against their malicious users (e.g., such users might give misleading feedback to disadvantage a particular cloud service) is a difficult problem. Guaranteeing the availability of the trust management service is another significant challenge because of the dynamic nature of cloud environments. In this article, we describe the design and implementation of CloudArmor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS), which includes i) a novel protocol to prove the credibility of trust feedbacks and preserve users' privacy, ii) an adaptive and robust credibility model for measuring the credibility of trust feedbacks to protect cloud services from malicious users and to compare the trustworthiness of cloud services, and iii) an availability model to manage the availability of the decentralized implementation of the trust management service.*

Keywords- CloudArmor, TaaS, Identity Management Service, Credibility Model, Feedback Cloud Service, Trust management, Reputation.

I. INTRODUCTION

The highly dynamic, distributed, and nontransparent nature of cloud services make the trust management in cloud environments a significant challenge. According to researchers at Berkeley, trust and security is 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. In reality, it is not unusual that a cloud service experiences malicious behaviors (e.g., collusion or Sybil attacks) from its users. This system 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. The adoption of cloud computing raises privacy concerns. Customers 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 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 by creating several accounts. Indeed, the detection of such malicious behaviors' poses several challenges. Firstly, new users join the cloud environment and 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 occur.

II. METHODOLOGIES

A. Detection of service

This layer consists of different users who use cloud services. For example, a new start-up that has limited funding can consume cloud services. Interactions for this layer include: i) service discovery where users are able to discover new cloud services and other services through the Internet, ii) trust and service interactions where users are able to give their feedback or retrieve the trust results of a particular cloud service, and iii) registration where users establish their identity through registering their credentials in IdM before using TMS.

B. Trust Communication

In a typical interaction of the reputation- based TMS, a user either gives feedback regarding the trustworthiness of a particular cloud service or requests the trust assessment of the service 1. From users' feedback, the trust behaviour of a cloud service is actually a collection of invocation history records, represented by a tuple H= (C, S, F, T f), where C is

the user's primary identity, S is the cloud service's identity, and F is a set of Quality of Service (QOS) feedbacks (i.e., the feedback represent several QOS parameters including availability, security, response time, accessibility, price).

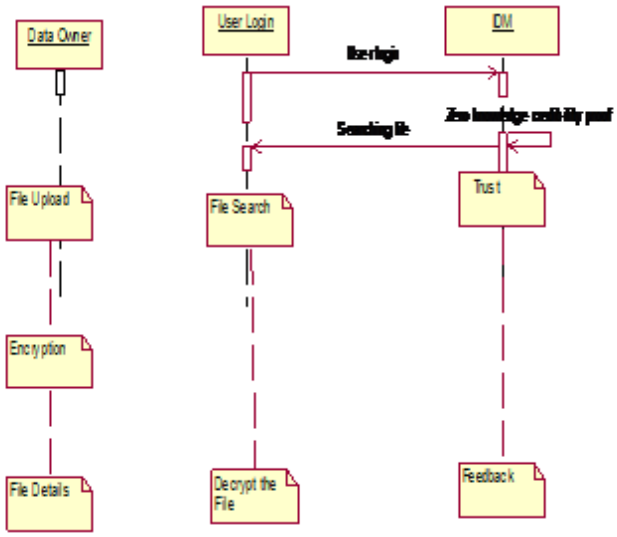

Figure 1: Communication

C. IDM Registration

The system proposes to use the Identity Management Service (IdM) helping TMS in measuring the credibility of a consumer's feedback. However, processing the IdM information can breach the privacy of users. One way to preserve privacy is to use cryptographic encryption techniques. However, there is no efficient way to process encrypted data. Another way is to use anonymization techniques to process the IDM information without breaching the privacy of users. Clearly, there is a trade-off between high anonymity and utility.

D. Service announcement and Communication

This layer consists of different cloud service providers who offer one or several cloud services, i.e., IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service), publicly on the Web (more details about cloud services models and designs can be found). These cloud services are accessible through Web portals and indexed on Web search engines such as Google, Yahoo, and Baidu. Interactions for this layer are considered as cloud service interaction with users and TMS.

III. RESULT AND DISCUSSION

- **Cloud Service Provider**

This layer consists of different cloud service providers who offer one or several cloud services, i.e., IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service), publicly on the Web (more details about cloud services models and designs can be found in. These cloud services are accessible through Web portals and indexed on Web search engines such as Google, Yahoo, and Baidu. Interactions for this layer are considered as cloud service interaction with users and TMS, and cloud services advertisements where providers are able to advertise their services on the Web.

- **Cloud Service Consumer**

This layer consists of different users who use cloud services. For example, a new start-up that has limited funding can consume cloud services (e.g., hosting their services in Amazon S3). Interactions for this layer include: i) service discovery where users are able to discover new cloud services and other services through the Internet, ii) trust and service interactions where users are able to give their feedback or retrieve the trust results of a particular cloud service, and iii) registration where users establish their identity through registering their credentials in before using TMS.

- **Identity Management Service (IdM)**

We propose to use the Identity Management Service (IdM) helping TMS in measuring the credibility of a consumer's feedback. However, processing the IdM information can breach the privacy of users. One way to preserve privacy is to use cryptographic encryption techniques

- **Trust Management Service**

This layer consists of several distributed TMS nodes which are hosted in multiple cloud environments in different geographical areas. These TMS nodes expose interfaces so that users can give their feedback or inquire the trust results in a decentralized way.

- **Feedback Collusion Detection**

Malicious users may give numerous fake feedbacks to manipulate trust results for cloud services (i.e., self promoting and Slandering attacks). Some researchers suggest that the number of trusted feedbacks can help users to overcome such manipulation where the number of trusted

feedbacks gives the evaluator a hint in determining the feedback credibility. However, the number of feedbacks is not enough in determining the credibility of trust feedbacks

IV. CONCLUSION

Cloud service users' feedback is a good source to assess the overall trustworthiness of cloud services. However, malicious users may collaborate together to i) disadvantage a Cloud service by giving multiple misleading trust feedbacks (i.e., collusion attacks) or ii) trick users into trusting cloud services that are not trustworthy by creating several accounts and giving misleading trust feedbacks (i.e., 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. In particular, we introduce a credibility model that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks take place 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 have collected a large number of consumer's trust feedbacks given on real-world cloud services (i.e., over 10,000 records) 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.

V. FUTURE WORK

Although several solutions have been proposed recently in managing trust feedbacks in cloud environments, how to determine the credibility of trust feedbacks is mostly neglected. Additionally in future, also enhance the performance of cloud as well as the security. In the future, will deal with more challenging problems such as the Sybil attack and the Whitewashing attack. Performance optimization of the trust management service is another focus of our futureless search work.

REFERENCES

[1] A. Birolini, Reliability Engineering: Theory and Practice. Springer2010.

[2] C. Dellarocas, "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms," Management Science, vol. 49, no. 10, pp. 1407–1424, 2003.

[3] 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, 2009.

[4] 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. of CLOUD'10, 2010.

[5] Jingwei Huang and David M Nicol, Trust mechanisms for cloud computing, April 2013

[6] J. Huang and D. M. Nicol, "Trust Mechanisms for Cloud Computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.

AUTHORS

First Author- D Deeba, B.Sc., M.SC., Rajah Serfoji Govt College (Autonomous), djdeeba02@gmail.com

Second Author- Dr.J.Gnana Jayanthi MCA, M.Phil., Ph.D., Rajah Serfoji Govt College, (Autonomous) Assistant Professor of Computer Science.