International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Trust as a Service: A Framework for Trust Management in Cloud Environments

[1,] D.Deeba, [2,] Dr.J.Gnana Jayamani
Dept. of Computer Science
Rajah Serfoji Government Arts 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, 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.

Key word: Cloud computing, trust management, reputation, credibility, credentials, security, privacy, availability.

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 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.

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 project focuses on improving trust management in cloud environments by proposing novel ways to ensure the credibility of trust feedbacks. In particular, it distinguishes 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 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. Firstly, 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. Secondly, 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.

• **Trust Management Service's Availability.** A trust management service (TMS) provides an interface between users and cloud services for effective trust management. However, guaranteeing the availability of TMS is a difficult problem due to the unpredictable number of users and the highly dynamic nature of the cloud environment. Approaches that require understanding of users' interests and capabilities through similarity measurements or operational availability measurements are inappropriate in cloud environments. TMS should be adaptive and highly scalable to be functional in cloud environments.

2. EXISTING SYSTEM

The highly dynamic, distributed, and nontransparent nature of cloud services make the trust management in cloud environments a significant challenge . 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 .

3. PROPOSED SYSTEM

In this paper, the design and the implementation of CloudArmor (CLOud consUmers creDibility Assessment & tRust manageMent of clOud seRvices):a framework for reputation-based trust management in cloud environments is proposed. In CloudArmor, trust is delivered as a service (TaaS) where TMS spans several distributed nodes to manage feedbacks in a decentralized way. CloudArmor exploits techniques to identify credible feedbacks from malicious ones. In a nutshell, the salient features of CloudArmor are:

Zero-Knowledge Credibility Proof Protocol (ZKC2P). Introduce ZKC2P that not only preserves the consumers' privacy, but also enables the TMS to prove the credibility of a particular consumer's feedback. Propose that the Identity Management Service (IdM) can help TMS in measuring the credibility of trust feedbacks without breaching consumers' privacy. Anonymization techniques are exploited to protect users from privacy breaches in users' identity or interactions.

A Credibility Model. The credibility of feedbacks plays an important role in the trust management service's performance. Therefore, propose several metrics for the feedback collusion detection including the Feedback Density and Occasional Feedback Collusion. These metrics distinguish misleading feedbacks from malicious users.

Advantages of Proposed System

- TMS will prove the users' feedback credibility without knowing the users' credentials
- TMS processes credentials without including the sensitive information
- Anonymized information is used via consistent hashing
- Detects Sybil attacks no matter these attacks take place in a long or short period of time (i.e., strategic or occasional attacks respectively)

4. MODULE DESCRIPTION

4.1 Cloud Service Provider

A cloud provider is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals. Cloud providers are sometimes referred to as cloud service providers or CSPs.In this project IaaS is utilized from the cloud server.The user need to create an account in the cloud server.The user needs to upload the created website to the cloud.The database is connected using the connection string.In this an e-commerce website is hosted in the cloud.The user can access the service by giving the URL.

4.2 Identity Management Service (IdM)

IdM can facilitate TMS in the detection of Sybil attacks against cloud services without breaching the privacy of users. When users attempt to use TMS for the first time, TMS requires them to register their credentials at the trust identity registry in IdM to establish their identities. The trust identity registry stores an identity record represented by a tuple $I = (C, Ca, Ti)$ for each user. C is the user's primary identity (e.g., user name). Ca represents a set of credentials' attributes (e.g., passwords, postal address, and IP address) and Ti represents the user's registration time in TMS.

4.3 Trust Management Service

4.3.1 Zero-Knowledge Credibility Proof Protocol (ZKC2P)

A Zero-Knowledge Credibility Proof Protocol (ZKC2P) to allow TMS to process IdM's information (i.e., credentials) using the Multi-Identity Recognition factor. In other words, TMS will prove the users' feedback credibility without knowing the users' credentials. TMS processes credentials without including the sensitive information. Instead, anonymized information is used via consistent hashing (e.g., sha-256). The anonymization process covers all the credentials' attributes except the Timestamps attribute.

4.3.2 Feedback Collusion Detection

Malicious users may give numerous fake feedbacks to manipulate trust results for cloud services (i.e., Selfpromoting and Slandering attacks).Introduce the concept of feedback density to support the determination of credible trust feedbacks. Specifically, consider the total number of users who give trust feedbacks to a particular cloud service as the feedback mass, the total number of trust feedbacks given to the cloud service as the feedback volume. The feedback volume is influenced by the feedback volume

collusion factor which is controlled by a specified volume collusion threshold. This factor regulates the multiple trust feedbacks extent that could collude the overall trusted feedback volume.

5. 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. 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, novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services is presented. In particular, this project 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). Also develop an availability model that maintains the trust management service at a desired level. The experimental results demonstrate the applicability of this approach and show the capability of detecting such malicious behaviors.

REFERENCES

[1]Siani Pearson and Azzedine Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing , 2010

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

[3] Kai Hwang Deyi Li, Trusted Cloud Computing with Secure Resources and Data Coloring, Sept.-Oct. 2010

[4] Sheikh Mahbub Habib , Sebastian Ries , Towards a Trust Management System for Cloud Computing

[5] Lina Yao Quan Z. Sheng Zakaria Maamar, Achieving High Availability of Web Services Based on A Particle Filtering Approach, 2012

AUTHORS

[1] D.Deeba

Msc, Mphil (computer science)

Rajah Serfoji Government Arts College

[2] Dr.J.Gnana Jayamani M.C.A., M.Phil., Ph.D., (Asst.Proff)
Rajah Serfoji Government Arts College