CLOUD ARMOR: SUPPORTING REPUTATION BASED-TRUST MANAGEMENT FOR CLOUD SERVICES

G. JAYASUDHA, M.Sc., M.Phil., B.Ed.,
T.JEEVA.,MCA.,(M.Phil).,
DEPARTMENT OF COMPUTER APPLICATIONS
KAILASH WOMENS COLLAGE
NANGAVALLI.

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 Cloud Armor, 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. The feasibility and benefits of our approach have been validated by a prototype and experimental studies using a collection of real-world trust feedbacks on cloud services.

INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services.

These services typically provide access to advanced software applications and high-end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

BENEFITS OF CLOUD ARMOR

Advantages

Trust Cloud framework for accountability and trust in cloud computing. In particular, Trust Cloud consists of five layers including workflow,

Propose a multi-faceted Trust Management (TM) system architecture for cloud computing to help the cloud service users to identify trustworthy cloud service providers.

CREDIBILITY PROOF PROTOCOL

Since there is a strong relation between trust and identification as emphasized in, we

Cloud service users' feedback is a good source to assess the overall trustworthiness of cloud services. In this paper, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services.

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 also develop an availability model that maintains the trust management service at a desired level.

propose to use the Identity Management Service to help 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. Full anonymization means better privacy, while full utility results in no privacy protection (e.g., using a de-identification anonymization technique can still leak sensitive information through linking attacks).

Thus, we propose a Zero-Knowledge Credibility Proof Protocol to allow TMS to process IdM's information (i.e., credentials) using the Multi-Identity Recognition factor (see details in Section 4.2). 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.

Identity Management Service

Since trust and identification are closely related, as highlighted by David and Jaquet in, we believe that 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 ¼ ðC; Ca; T iÞ 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 T i represents the user's registration time in TMS.

Trust Management Service

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 behavior 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). Each trust feedback in F is represented in numerical form with the range of [0, 1], where 0, 1, and 0.5 means negative, positive, and neutral feedback respectively. T f is the timestamps when the trust feedbacks are given. Whenever a user c requests a trust assessment for cloud service s, TMS calculates the trust result, denoted as T rðsÞ, from the collected trust feedbacks as follows:

$$\mathcal{T}_r(s)=\frac{\sum_{c=1}^{|\mathcal{V}(s)|}\mathcal{F}(c,s)*\mathcal{C}_r(c,s,t_0,t)}{|\mathcal{V}(s)|}*(\chi*\mathcal{C}_t(s,t_0,t)),\quad(1)$$

where VðsÞ denotes the trust feedbacks given to cloud service s and jVðsÞj represents the total number of trust feedbacks. Fðc; sÞ are trust feedbacks from the c th user weighted by the credibility aggregated weights Crðc; s; t0; Tþ to allow TMS to dilute the influence of those misleading feedbacks from attacks. Fðc; sÞ is held in the invocation history record h and updated in the corresponding TMS. Ctðs; t0; tÞ is the rate of trust result changes in a period of time that allows TMS to adjust trust results for cloud services that have been affected by malicious behaviors. x is the normalized weight factor for the rate of changes of trust results which increase the adaptability of the model. More details on how to calculate Crðc; s; t0; tÞ and Ctðs; t0; tÞ.

Assumptions and Attack Models

That TMS is handled by a trusted third party. We also assume that TMS communications are secure because securing communications is not the focus of this paper. Attacks such as Man-In-The-Middle (MITM) is therefore beyond the scope of this work. We consider the following types of attacks:

Collusion attacks

Also known as collusive malicious feedback behaviors, such attacks occur when several vicious users collaborate together to give numerous misleading feedbacks to increase the trust result of cloud services (i.e., a self-promoting attack) or to decrease the trust result of cloud services (i.e., a slandering attack). This type of malicious behavior can occur in a non-collusive way where a particular malicious user gives multiple misleading feedbacks to conduct a self-promoting attack or a slandering attack.

Sybil attacks

Such an attack arises when malicious users exploit multiple identities to give numerous misleading feedbacks (e.g., producing a large number of transactions by creating multiple virtual machines for a short period of time to leave fake feedbacks) for a self-promoting or slandering attack. It is interesting to note that attackers can also use multiple identities to disguise their negative historical trust records (i.e., whitewashing attacks).

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 behavior 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).

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 toprocess encrypted data. Another way is to use anonymization techniques to process theIDM information without breaching the privacy of users. Clearly, there is a trade-off between high anonymity and utility.

The cloud service provider layer

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). These cloud servicesare 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.

The trust management service layer

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. Interactions for this layer include:

Cloud service interaction with cloud service providers, Service advertisement to advertise the trust as a service to users through the Internet

Cloud service discovery through the Internet to allow users to assess the trust of new cloud services, and

Zero-Knowledge Credibility Proof Protocol (ZKC2P) interactions enabling TMS to customers feedback.

The cloud service consumer layer

This layer consists of different users who use cloud services. For example, a new startup that has limited funding can consume cloud services (e.g., hosting their services in Amazon S3). Interactions for this layer include:

Service discovery where users are able to discover new cloud services and other services through the Internet, Trust and service interactions where users are able to give their feedback or retrieve the trust results of a particular cloud service, and Registration where users establish their identity through registering their credentials in IdM before using TMS. Our framework also exploits a Web crawling approach for automatic cloud services discovery, where cloud services are automatically discovered on the Internet and stored in a cloud services repository. Moreover, our framework contains an Identity Management Service, which is responsible for the registration where users register their credentials before using TMS and proving the credibility of a particular consumer’s feedback through ZKC2P.

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, 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.

REFERENCES

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

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

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

14, 2013.