ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services

S.Vaitheki,Dr.V.Ravikumar
Master of engineering student ,'Head of the department'
Department of computer science &engineering, MahaBarathi engineering college
Tamilnadu, India
Vaitheki141@gmail.com

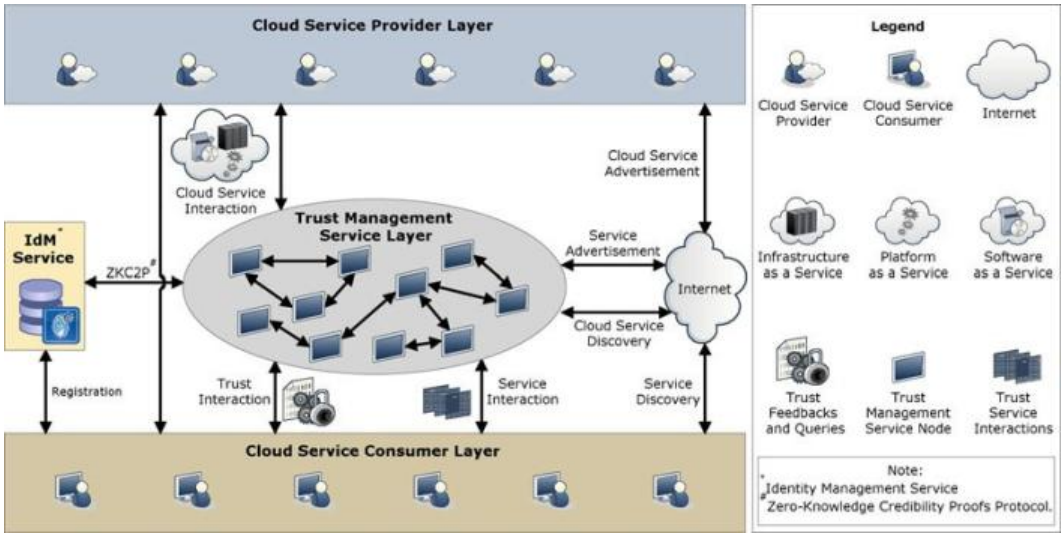
Abstract—Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers' privacy 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. 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.

Index terms - Cloud computing, trust management, reputation, credibility, credentials, security, privacy, availability Terms

I. 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 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 computation per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information to provide data storage or to power large, immersive computergames.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. Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Servic(SaaS). The three service models or layer are completed by an end user layer that encapsulates the



enduserperspective on cloud services.The model is shown infigure below. If a cloud useraccesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider. [4] discussed about a system,the effective incentive scheme is proposed to stimulate the forwarding cooperation of nodes in VANETs. In a coalitional game model, every relevant node cooperates in forwarding messages as required by the routing protocol. This scheme is extended with constrained storage space. A lightweight approach is also proposed to stimulate the cooperation.

II EXISTING SYSTEM

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). Consumers' feedback to assess and manage trust based on feedbacks collected from participants.

DISADVANTAGES OF EXISTING SYSTEM

- 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.
- A Self-promoting attack might have been performed on cloud service sy, which means sx should have been selected instead.
- Disadvantage a cloud service by giving multiple misleading trust feedbacks (i.e., collusion attacks)
- Trick users into trusting cloud services that are not trustworthy by creating several accounts and giving misleading trust feedbacks (i.e., Sybil attacks).

III PROPOSED SYSTEM

- 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.

ADVANTAGES OF PROPOSED SYSTEM

- TrustCloud framework for accountability and trust in cloud computing. In particular, TrustCloud 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.

IVIMPLEMENTATION AND EXPERIMENTAL EVALUATION

In this section, we report the implementation and experimental results in validating the proposed approach. Our implementation and experiments were developed to validate and study the performance of both the credibility model and the availability model

VSYSTEM IMPLEMENTATION

The trust management service's implementation of large research project, named CloudArmor,[2] which offers a platform for reputation-based trust management of cloud services.The platform provides an environment where users can give feedback and request trust assessment for a particular cloud service.

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 actuallya 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 ofQuality 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 0the 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 theIDM information without breaching the privacy of users. Clearly, there is a trade-off between high anonymity and utility.

THE CLOUD SERVICE PROVIDER LAYER

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 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.

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:

i) Cloud service interaction with cloud service providers,

ii) Service advertisement to advertise the trust as a service to users through the Internet,

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

iv) 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 whereusers register their credentials before using TMS and proving the credibility **:**of a particular consumer's feedback through ZKC2

VICONCLUSION

From this Cloud Armor Supporting Reputation-based Trust Management for Cloud Services has been implemented. In cloud computing growth, the management of trust element is most challenging issue. Cloud computing has produce high challenges in security and privacy by the changing of environments. Trust is one of the most concerned obstacles for the adoption and growth of cloud computing. 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

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] Christo Ananth, M.Muthamil Jothi, A.Nancy, V.Manjula, R.Muthu Veni, S.Kavya, "Efficient message forwarding in MANETs", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:6-9

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