Supporting Reputation Based Trust Management for Cloud Services

M.Sathi Ekambareesh,
Assistant Professor, Sir C R R College of Engineering

Abstract- In the growth of cloud computing, managing the trust element is the most difficult problem. Cloud computing has generated major challenges in terms of security and privacy against changes in environments. Trust is one of the most worrying obstacles to the adoption and growth of cloud computing. Although several solutions have been recently proposed for the management of reliable comments in cloud environments, most of the time is taken into account to determine the credibility of trusted comments. In this project, the system proposed a Cloud Armor, a reputation-based trust management framework that provides a set of capabilities to provide Trust as a Service (TaaS). The "Trust as a service" (TaaS) structure to improve trust management in cloud environments. The approaches were validated by the prototype system and experimental results.

Keywords- Cloud computing, Trust, Obstacles, Reputation, Feedbacks

I. INTRODUCTION

The highly dynamic, distributed and non-transparent nature of cloud services makes trust management in cloud environments a significant challenge. According to the Berkeley researchers, trust and security are among the 10 main obstacles to the adoption of cloud computing. In fact, Service Level Agreements alone are not sufficient to establish trust between consumers and cloud providers due to unclear and inconsistent clauses. Consumer feedback is a good source for assessing the overall reliability of cloud services. Several researchers have recognized the importance of trust management and the solutions proposed to assess and manage trust based on comments received from participants. In fact, it is not uncommon for a cloud service to experience malicious behavior (such as collusion or Sybil attacks) by its users. This document focuses on improving trust management in cloud environments by proposing new ways to ensure credibility of trusted comments. In particular, we distinguish the following key aspects of trust management in cloud environments: consumer privacy. The adoption of cloud computing raises privacy issues. Consumers may have dynamic interactions with cloud service providers, which may result in confidential information. There are several cases of privacy violations, such as loss of confidential information (for example, date of birth and address) or behavioral information (for example, who interacted with the consumer, the type of services in the cloud that showed interest, etc.

Undoubtedly, services involving consumer data (for example, interaction stories) should preserve their privacy. Protection of services in the cloud. It is not unusual for a cloud service to experience attacks from its users. Attackers may disadvantage a cloud service by giving more misleading comments (eg, Collusive Attacks) or by creating multiple accounts (eg Sybil Attacks). Indeed, identifying such harmful behaviors poses several challenges. First of all, new users join the cloud environment and old users leave 24 hours a day. This consumer dynamism makes the detection of harmful behaviors (for example, a collusion of feedback) an important challenge. Secondly, users can have different accounts for a particular cloud service, which makes it difficult to detect Sybil attacks. Finally, it is difficult to predict when harmful behavior occurs (ie, occasional strategic VS behavior). Availability of the trust management service. A Trusted Management Service (TMS) provides an interface between users and cloud services for effective trust management. However, ensuring 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 an understanding of users' interests and abilities through similarity measures or measurements of operational availability (eg, uptime to total time) are inappropriate in cloud environments. TMS must be adaptable and highly scalable to be functional in cloud environments.

II. RELATED WORK

Trust is one of the most worrying obstacles to the adoption and growth of cloud computing. Although several solutions have been recently proposed for the management of reliable comments in cloud environments, most of the time it is taken into consideration to determine the credibility of reliable comments. In this project, the system proposed a CloudArmor, a trust-based trust management framework that provides a range of capabilities to provide the Trust as a Service (TaaS). The "Trust as a Service" (TaaS) structure to improve trust management in cloud environments. The approaches have been validated by the prototype system and the experimental results. Here, it has some drawbacks: it is not uncommon for a cloud service to experience malicious behavior on the part of its users, it is not certain that they can trust cloud providers, it is not convincing enough for consumers, SLAs do not They are consistent with each other . providers offer services with similar functionality, customers are not sure they can identify a reliable cloud provider based on their SLA. In this project, the system proposed a Cloud Armor, a trust-based trust management framework that offers a range of capabilities to offer Trust as a Service (TaaS). The "Trust as a service" (TaaS) structure to improve trust management in cloud environments. In particular, the system introduces a model of adaptive credibility that distinguishes between reliable and malicious comments when considering the ability of consumers of cloud services and the consent of most of their

comments. The approaches have been validated by the prototype system and the experimental results. The system proposes a structure that uses service-oriented architecture (SOA) to provide a service of trust. This includes some benefits, not only by preserving consumer privacy, but also by allowing TMS to demonstrate the credibility of a particular consumer's comments, but also has the ability to detect strategic behavior and occasional technical collusion attacks. The workload, always maintaining a desired level of availability. This metric uses particle filtering techniques to accurately predict the availability of each node; Cloud armor uses reliable techniques to identify malicious comments.

III. LITERATURE REVIEW

[13] Describe in this paper that we assess how security, trust, and privacy issues occur in the context of cloud computing and discuss ways in which they can be addressed. an on-demand supply mechanism based on a pay-per-use business model. This makes it difficult to comply with data management regulations. [5] Description: We begin this paper with a survey of existing mechanisms to establish trust and discuss its limitations. Therefore, we address these limitations by proposing more stringent mechanisms based on evidence, certification and attribute validation and we will conclude by suggesting a framework for integrating different trust mechanisms to reveal trust chains in the cloud. This system presents an integrated view of trust mechanisms for cloud computing and analyzes the chains of trust that connect the entities of the cloud. Some cloud customers can not make decisions about using a cloud service based solely on informal trust mechanisms. [7] Description: The authors suggest using a trusted network in various data centers to implement a reputation system to establish trust between service providers and data owners. Data coloring and software watermarking techniques collectively protect shared data objects and distributed software modules. These techniques protect multi-path authentication, enable a single session to start in the cloud, and strengthen access control for sensitive data in public and private clouds. Once users move data to the cloud, they can not easily extract their data and programs from one cloud server to run them in another. This leads to a data blocking problem. [12] Describe inconsistent SLA descriptions among cloud service providers, despite other services with similar functionality. Therefore, customers are not sure they can identify a reliable service provider in the cloud based on their SLA. This system provides tools to identify reliable suppliers in the cloud in terms of different attributes evaluated by multiple sources and sources of reliable information; They are not sure they can trust cloud service providers. [9] In this paper, we address these problems by exploiting techniques based on particle filtering. In particular, we develop algorithms to accurately predict the availability of Web services and dynamically maintain a subset of Web services with greater availability ready to merge service compositions. Web services can always be selected from this smaller space, which guarantees good performance in service compositions. Unfortunately, the way to provide real-time availability information for Web services is largely overlooked.

IV. METHODOLOGIES

A. Detection of service

This level is made up of different users who use services in the cloud. For example, a new start with limited funds could consume services in the cloud. Interactions for this level include: i) discovery of services where users can discover new services in the cloud and other services through the Internet, ii) trust interactions and services where users can post comments or retrieve results from trust a particular cloud service and iii) registration in which users establish their identity by registering their IdM credentials before using TMS.

B. Trust Communication In a typical TMS-based reputation interaction, a user provides information about the reliability of a particular service in the cloud or requires the assessment of service trust 1. Depending on the user's response, the reliability of a service in the cloud is actually a collection of history invocation records, represented by a tuple H = (C, S, F, T f), where C is the user's primary identity, S is the identity of the service in the cloud and F it is a set of comments on the quality of the service (QOS) (that is, the comments represent various QOS parameters that include availability, security, response time, accessibility, price).

C. IDM Registration The system proposes to use the Identity Management Service (IdM) that helps TMS measure the credibility of a consumer's comments. However, processing of IdM information may violate user privacy. One way to preserve privacy is to use cryptographic cryptographic techniques. However, there is no effective way to process encrypted data. Another way is to use anonymization techniques to process IDM information without violating user privacy. Clearly, there is a compromise between high anonymity and usefulness.

D. Service announcement and Communication

This level includes several cloud service providers that offer one or more services in the cloud, ie Infrastructure as a service (IaaS), Platform as a service (PaaS) and SaaS (Software as software), publicly on the Web. on models and services projects in the cloud). These services can be accessed in the cloud through Web portals and indexed in Web search engines such as Google, Yahoo and Baidu. Interactions for this level are considered as the interaction of the cloud service with users and TMS.

V. SYSTEM DESIGN

A. The Cloud Service Provider Layer

This level includes several cloud service providers that offer one or more services in the cloud, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), publicly on the Web (more on models and design of services in the cloud). These services can be accessed in the cloud Through web portals and indexed in web search engines like Google, Yahoo and Baidu. Interactions for this level are considered interactions of cloud services with

users and TMS and cloud advertising for providers where they can advertise their services on the Web.

B. The Trust Management Service Layer

This layer consists of several distributed TMS nodes that are hosted in multiple cloud environments in different geographic areas. These TMS nodes expose the interfaces so that users can express their opinion or consult the results of trust in a decentralized way. Interactions for this level include: i) interaction of cloud services with cloud service providers, ii) advertising of the service to publicize trust as a service for users over the Internet, iii) discovery of services in the cloud on the Internet to allow users to assess trust in new cloud services; and iv) Zero Knowledge Credential Test Protocol (ZKC2P) interactions that enable TMS to provide feedback to customers.

C. The Cloud Service Consumer Layer

Finally, this level is made up of different users who use services in the cloud. For example, a new startup with limited funds could use services in the cloud (for example, by hosting its services on Amazon S3).

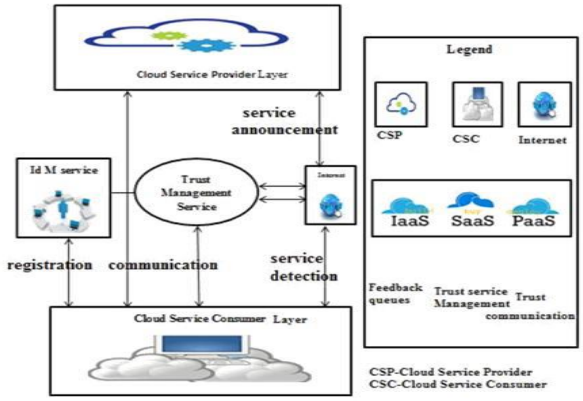

Fig.1: Cloud services.

Interactions for this level include: i) discovery of services where users can discover new services in the cloud and other services through the Internet; and iii) registration in which users establish their identity by registering their IdM credentials before using TMS. Our framework also uses a web-crawling approach to automatic discovery of cloud services, where cloud services are automatically detected on the Internet and stored in a repository of cloud services. In addition, our framework contains an identity management service, which is responsible for registering where users register their credentials before using TMS and demonstrating the credibility of a particular consumer's comments through ZKC2P. A service provider that includes storage services or client software available through a private (private cloud) or public (cloud) network. In general, it means that storage and software are available for processing on the Internet.

VI. CONCLUSION

From this Cloud Armor, reputation-based trust management has been implemented for cloud services. In the growth of cloud computing, managing the trust element is the most difficult problem. Cloud computing has generated big challenges in terms of security and privacy when changing the environment. Trust is one of the most worrying obstacles to the adoption and growth of cloud computing. Although several solutions have been proposed recently for the management of reliable comments in cloud environments, most of the time is taken into account to determine the credibility of trusted comments. Furthermore, in the future, we will also improve the performance and security of the cloud.

VII. BIBOLOGRAPHY

[1]. 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]. Sampathirao Raju and Marlapalli Krishna "Critique of Web Recommendation System for Time Series Datasets", International Journal for Research on Electronics and Computer Science (IJRECS), Vol.04, Issue.18, pp: 1623-1629, Nov-2014.

[4]. Anguluri Manoja, and Marlapalli Krishna. "An Efficient Strategy towards Recognition of Privacy Information", International Journal of Reviews on Recent Electronics and Computer Science, 2(11), pp: 3630-3634, Nov-2014.

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

[6]. Manda Pradeep Chandra, Marlapalli Krishna and Prathipati Ratna Kumar. "Better Message Transmission Solution in Steganography", International Journal for Research on Electronics and Computer Science, pp:5500-5504, Vol.07, Issue.2, Nov-2016.

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

[8]. Dr. M. Krishna. "The VLIW Architecture for Real-Time Depth Detection in Image Processing", International Journal of Computer Science & Mechatronics, pp: 1-9, Vol.2.Issue.VI, Dec-2016.

[9]. Dr. M. Krishna. "An Efficient Multi Dimensional view for vehicles by Patch memory management in image processing", International Journal of Computer Science & Mechatronics, PP:1-10, Vol.1.Issue.V, Dec-2016.

[10]. Venkata Ramana N., Nagesh P., Lanka S., Karri R.R. (2019), "Big Data Analytics and IoT Gadgets for Tech Savvy Cities". In: Omar S., Haji Suhaili W., Phon-Amnuaisuk S. (eds) Computational Intelligence in Information Systems. CIIS 2018. Advances in Intelligent Systems and Computing, vol 888. pp 131-144, Springer Nature. DOI: 10.1007/978-3-030-03302-6_12.

[11]. Soni Lanka., Madhavi M. R., Abusahmin, B.S., Puvvada, N., Lakshminarayana, V., (2017), "Predictive data mining techniques for management of high dimensional big-data". Journal of Industrial Pollution Control vol 33, pp 1430-1436.

[12]. Sheikh Mahbub Habib , Sebastian Ries y, Max M• uhlh• auser, Towards a Trust Management System for Cloud Computing.

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

[14]. S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud Trust Management for Hadoop," in Proc. CLOUD'12, 2012.

[15]. Krishna M., Chaitanya D. K., Soni L., Bandlamudi S.B.P.R., Karri., R.R.: (2019), "Independent and Distributed Access to Encrypted Cloud Databases". In: Omar S., Haji Suhaili W., Phon-Amnuaisuk S. (eds) Computational Intelligence in Information Systems. CIIS 2018. Advances in Intelligent

Systems and Computing, vol 888. pp 107-116, Springer Nature. DOI: 10.1007/978-3-030-03302-6_10

[16]. Dr. Marlapalli Krishna, V Devi Satya Sri, Bandlamudi S B P Rani and G. Satyanarayana. "Edge Based Reliable Digital Watermarking Scheme for Authorized Ownership" International Journal of Pure and Applied Mathematics pp: 1291-1299, Vol-119, Issue-7, 2018.

[17]. Dr. Marlapalli Krishna, Bandlamudi S B P Rani, V Devi Satya Sri and Dr. Rama Rao Karri. "Filter Based Jpeg Compression for Noisy Images" Journal of Advanced Research in Dynamical and Control Systems, pp: 1233-1248, Vol-9, Issue-18, 2017.