IISRC International Conference on Industrial Scientific Research Engineering
International Industrial Scientific Research Corporation
www.worldconferences.org

Trust Management Service: Identifies Collusion Attacks from Detecting Sybil Attacks in the Cloud

KANUPARTHY SIRISHA[1], B. PURUSHOTHAM[2]
[1]PG Scholar, Dept of CSE, Annamacharya Institute of Technology & Science, Tirupathi, AP, India,
E-mail: sireeshab.tech3@gmail.com.
[2]Assistant Professor, Dept of CSE, Annamacharya Institute of Technology & Science, Tirupathi, AP, India,
E-mail: purushbtech2005@gmail.com.

Abstract: Trust administration is a standout amongst the most difficult issues for the appropriation and development of distributed computing. The very rapid, circulated, and non-straightforward nature of cloud administrations presents a few testing issues, for example, protection, security, what's more, accessibility. Safeguarding buyers' protection is not a simple errand because of the touchy data required in the communications amongst purchasers and the trust administration benefit. Securing cloud administrations against their vindictive clients (e.g., such clients might give deluding input to burden a specific cloud administration) is a troublesome issue. Ensuring the accessibility of the trust administration is another critical test as a result of the dynamic way of cloud situations. In this article, we depict the outline and usage of CloudArmor, a notoriety based trust administration system that gives an arrangement of functionalities to convey Trust as a Service (TaaS), which incorporates i) a novel convention to demonstrate the believability of trust inputs and safeguard clients' security, ii) a versatile and hearty validity display for measuring the believability of trust inputs to ensure cloud administrations from vindictive clients and to think about the reliability of cloud administrations, and iii) an accessibility model to deal with the accessibility of the decentralized usage of the trust administration benefit. The plausibility and advantages of our approach have been approved by a model and test contemplates utilizing an accumulation of certifiable trust criticisms on cloud administrations.

Keywords: Cloud Computing, Trust Management, Security, Privacy, Reputation, Availability.

I. INTRODUCTION

The highly dynamic, distributed, and nontransparent nature of cloud services make the trust management in cloud environments a significant challenge [1][2][3][4]. According to researchers at Berkeley [5], trust and security are ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed, Service-Level Agreements (SLAs) alone are in adequate to establish trust between cloud consumers and providers because of its unclear and inconsistent clauses [6]. 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 paper 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.

A. Consumers' Privacy

The adoption of cloud computing raise privacy concerns [11]. 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 [12].

B. 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 [13]. Finally, it is difficult to predict when malicious behaviors occur (i.e., strategic VS. occasional behaviors) [14].

C. 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 [15] or operational availability measurements [16] (i.e., uptime to the total time) are in appropriate in cloud environments. TMS should be adaptive and highly scalable to be functional in
cloud environments.

II. REALTED WORK

Trust management has been one of the hot topics especially in the area of cloud computing [32], [14], [10]. Some of the research efforts use policy-based trust management techniques. For example, Ko et al. [33] propose Trust Cloud framework for accountability and trust in cloud computing. In particular, Trust Cloud consists of five layers including workflow, data, system, policies and laws, and regulations layers to address accountability in the cloud environment from all aspects. All of these layers maintain the cloud accountability life cycle which consists of seven phases including policy planning, sense and trace, logging, safe-keeping of logs, reporting and replaying, auditing, and optimizing and rectifying. Brandic et al. [7] propose a novel approach for compliance management in cloud environments to establish trust between different parties. The approach is developed using a centralized architecture and uses compliant management technique to establish trust between cloud service users and cloud service providers. Unlike previous works that use policy-based trust management techniques, we assess the trustworthiness of a cloud service using reputation based trust management techniques. Reputation represents a high influence that cloud service users have over the trust management system [34], especially that the opinions of the various cloud service users can dramatically influence the reputation of a cloud service either positively or negatively.

Some research efforts also consider the reputation based trust management techniques. For instance, Habib et al. [6] propose a multi-faceted Trust Management (TM) system architecture for cloud computing to help the cloud service users to identify trustworthy cloud service providers. In particular, the architecture models uncertainty of trust information collected from multiple sources using a set of Quality of Service (QoS) attributes such as security, latency, availability, and customer support. The architecture combines two different trust management techniques including reputation and recommendation where operators (e.g., AND, OR, NOT, FUSION, CONSENSUS, and DISCOUNTING) are used. Hwang et al. [4] propose a security aware cloud architecture that assesses the trust for both cloud service providers and cloud service users. To assess the trustworthiness of cloud service providers, the authors propose the trust negotiation approach and the data coloring (integration) using fuzzy logic techniques. To assess the trustworthiness of cloud service users, they develop the Distributed-Hash-Table (DHT)-based trust overlay networks among several data centers to deploy a reputation-based trust management technique. Unlike previous works which do not consider the problem of unpredictable reputation attacks against cloud services, we present a credibility model that not only detects the misleading trust feedbacks from collusion and Sybil attacks, but also has the ability to adaptively adjust the trust results for cloud services that have been affected by malicious behaviors.

III. ZERO-KNOWLEDGE CREDIBILITY PROOF PROTOCOL (ZKC2P)

There is a strong relation between trust and identification as emphasized in [20], 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. However, there is no efficient way to process encrypted data [11]. 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 [21]). Thus, we propose a Zero-Knowledge Credibility Proof Protocol (ZKC2P) 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.

A. Identity Management Service (IdM)

Since trust and identification are closely related, as highlighted by David and Jaquet in [20], 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 = (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.

B. Trust Management Service (TMS)

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 service1. 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, Tf), 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).

C. Assumptions and Attacks

We assume 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 [22]) or to decrease the trust result of cloud services (i.e., a slandering attack [23]). 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 [13], [22] 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., white washing attacks.)

IV. 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 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.

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).

V. 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: 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.

VI. SYSTEM ARCHITECTURE

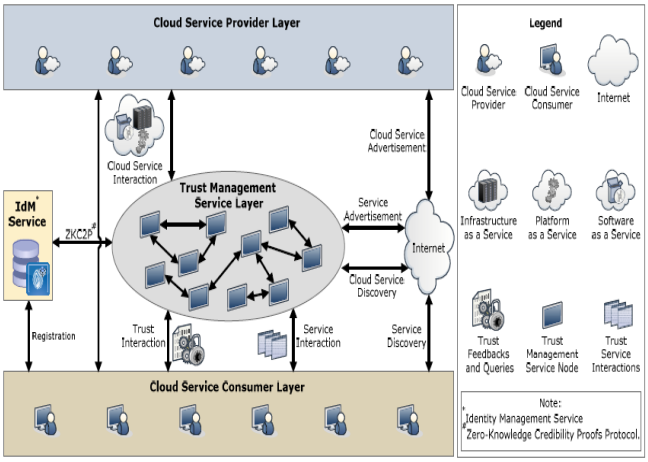

Fig.1. System Architecture.

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 can be found.

The Trust Management Service Layer: This layer consists of several distributed TMS nodes which are hosted in multiple cloud environments in different geographical areas as shown in Fig.1. 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 prove the credibility of a particular consumer's feedback.

The Cloud Service Consumer Layer: Finally, 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: 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. 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.

VII. MODULES

- Availability Model
- Credibility Model
- Trust Management Service's Availability
- Cloud Services Protection

A. Modules Description

Availability Model: High availability is an important requirement to the trust management service. Thus, we propose to spread several distributed nodes to manage feedbacks given by users in a decentralized way. Load balancing techniques are exploited to share the workload, thereby always maintaining a desired availability level. The number of TMS nodes is determined through an operational power metric. Replication techniques are exploited to minimize the impact of crashing TMS instances. The number of replicas for each node is determined through a replication determination metric that we introduce. This metric exploits particle filtering techniques to precisely predict the availability of each node.

Credibility Model: The credibility of feedbacks plays an important role in the trust management service's performance. Therefore, we propose several metrics for the feedback collusion detection including the Feedback Density and Occasional Feedback Collusion. These metrics distinguish misleading feedbacks from malicious users. It also has the ability to detect strategic and occasional behaviors of collusion attacks (i.e., attackers who intend to manipulate the trust results by giving multiple trust feedbacks to a certain cloud service in a long or short period of time). In addition, we propose several metrics for the Sybil attacks detection including the Multi-Identity Recognition and Occasional Sybil Attacks. These metrics allow TMS to identify misleading feedbacks from Sybil attacks.

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 (i.e., uptime to the total time) are inappropriate in cloud environments. TMS should be adaptive and highly scalable to be functional in cloud environments.

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 (i.e., strategic VS. occasional behaviors).

VIII. CONCLUSION & FUTURE WORK

The highly progressive, disseminated, and nontransparent nature of cloud administrations, overseeing and building up trust between cloud benefit clients and cloud administrations remains a huge test. Cloud benefit clients' input is a decent source to survey the generally speaking dependability of cloud administrations. Be that as it may, malignant clients may team up to i) weakness a cloud benefit by giving numerous deceptive trust criticisms (i.e., arrangement assaults) or ii) trap clients into trusting cloud benefits that are not reliable by making a few records and giving deluding trust criticisms (i.e., Sybil assaults). In this paper, we have displayed novel systems that assistance in identifying reputation based assaults and permitting clients to viably distinguish reliable cloud administrations. Specifically, we present a believability model that not just recognizes deluding trust inputs from conspiracy assaults additionally identifies Sybil assaults regardless of these assaults occur in a long or brief timeframe (i.e., vital or incidental assaults individually). We likewise build up an accessibility demonstrate that keeps up the trust administration benefit at a sought level. We have gathered countless trust criticisms given on true cloud administrations (i.e., more than 10,000 records) to assess our proposed strategies. The test comes about exhibit the pertinence of our approach and demonstrate the ability of identifying such pernicious practices. There are a couple of headings for our future work. We plan to join distinctive trust administration methods for example, notoriety and proposal to build the trust comes about exactness. Execution enhancement of the trust administration is another concentration.

IX. REFERENCES

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

[2] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks, 2013, pp. 3–42.

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

[4] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.

[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
[6] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Proc. of TrustCom'11, 2011.
[7] 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.
[8] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, "A Trust Management Framework for Service-Oriented Environments," in Proc. of WWW'09, 2009.
[9] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation Attacks Detection for Effective Trust Assessment of Cloud Services," in Proc. of TrustCom'13, 2013.
[10] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising From Cloud Computing," in Proc. CloudCom'10, 2010.
[11] E. Friedman, P. Resnick, and R. Sami, Algorithmic Game Theory. New York, USA: Cambridge University Press, 2007, ch. Manipulation-Resistant Reputation Systems, pp. 677–697.
[12] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.
[13] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in Proc. of AINA'10, 2010.
[14] Y. Wei and M. B. Blake, "Service-oriented Computing and Cloud Computing: Challenges and Opportunities," Internet Computing, IEEE, vol. 14, no. 6, pp. 72–75, 2010.
[15] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Sep 2011, accessed: 05/06/2012, Available at: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-
145 cloud-definition. pdf.
[16] O. David and C. Jaquet, "Trust and Identification in the Light of Virtual Persons," pp. 1–103, Jun 2009, accessed 10/3/2011, Available at: http:// www.fidis.net /resources/ deliverables /identity of- identity/.
[17] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-preserving Data Publishing: A Survey of Recent Developments," ACM Computing Surveys, vol. 42, no. 4, pp. 1–53, 2010.
[18] A. Birolini, Reliability Engineering: Theory and Practice. Springer, 2010.
[19] T. H. Noor and Q. Z. Sheng, "Trust as a Service: A Framework for Trust Management in Cloud Environments," in Proc. of WISE'11, 2011.
[20] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in Proc. SERVICES'11, 2011.

Author's Profile:

Kanuparthy Sirisha did her bachelor of Technology in Computer Science & Engineering at JB Womens Engineering College, Tirupathi and doing Master of Technology in Computer Science at AITS, Karakambadi, Tirupati, Chittoor, and Andhra Pradesh, India.

Mr. B.Purushotham, did his bachelor of Technology in Computer Science& Engineering at JNT University, Hyderabad, and had done Master of Technology in Computer Science & Engineering at SV University, Tirupati, Chittoor, Andhra Pradesh, India.