Secure Clouds Through Reputation-Based Cloud Service Trust Management

NEELAM SAISRI
M.Tech Student, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Dr. V. SANGEETHA
Associate Professor, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Dr. M.SAMBASIVUDU
Associate Professor, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Abstract: **Inadequate mechanisms for managing user trust in cloud services are a major roadblock to the broad adoption of this technology. Difficulties with privacy, security, and availability are inevitable in the cloud because of the service's intrinsic malleability, dispersion, and lack of transparency. Due to the sensitive nature of the information shared between customers and the trust management service, confidentiality must be maintained at all times. It's difficult to prevent malicious individuals from disrupting cloud services (for example, by providing false or misleading feedback to make a cloud service seem bad). Due to the dynamic nature of cloud infrastructure, it may be challenging to guarantee the constant availability of the trust management service in a cloud environment. We discuss the design and implementation of Cloud Armor, a reputation-based trust management framework that offers a collection of functions to provide Trust as a Service, with the goals of protecting cloud services from malicious users and comparing the trustworthiness of various cloud services. A unique protocol to verify the credibility of trust feedbacks while protecting users' anonymity; and (ii) an adaptive and resilient credibility model for gauging the veracity of trust feedbacks. Our approach's benefits and viability have been demonstrated through prototype development and experimentation with real-world trust feedback on cloud services.**

Keywords: **Cloud Computing; Trust Management; Malicious Feedback;**

I. INTRODUCTION:

The identification of malicious actions might be difficult in a cloud environment due to the nature of the environment. To begin, there is a constant influx of new users into the cloud environment, while an outflow of previous users occurs around the clock. Due to the ever-changing nature of consumers, identifying harmful activities such as feedback collusion may be an extremely difficult task. Second, users may have many accounts for the same cloud service, which makes it harder to identify Sybil assaults since they are more difficult to differentiate between. In conclusion, it is impossible to anticipate when harmful activities may take place (i.e., strategic versus occasional behaviors). A Word on the Availability of the Trust Management Service: An interface between users and cloud services that facilitates efficient trust management is provided by a trust management service, abbreviated TMS. Yet, because of the unpredictability of the number of users and the very fluid nature of the cloud environment, ensuring the availability of TMS is a challenging challenge to solve. In cloud systems, strategies that demand an awareness of the interests and skills of users via similarity metrics or operational availability measurements (i.e., uptime to total time) are not applicable. In order for TMS to perform well in cloud settings, it has to be very scalable and adaptable. The perception of reputation and the self-assessment of cloud service providers are major factors that influence levels of trust in cloud computing at the current time [1]. Trust is an essential component of cloud computing. At the beginning of this work, we provide an overview of the many known methods for building trust and comment on the constraints imposed by these methods. After addressing those shortcomings, we offer more stringent processes based on evidence, attribute certification, and validation, and we finish by recommending a framework for integrating everything together. The writers made reference to Users of cloud computing services have substantial worries over the integrity of their data and computations, as well as their security. When it comes to work distribution, many production-level clouds make the optimistic assumption that all cloud nodes are equally trustworthy. Instead of taking reputation into account, job distribution is dependent on node load [2]. This makes them more susceptible to attack since the integrity of numerous distributed calculations may be compromised even if only one node is compromised. The first full-scale, data-centric, reputation-based trust management solution for Hadoop clouds is presented and evaluated in this study. Hatman performs a dynamic analysis of the node's integrity by comparing the outputs of task replicas to ensure consistency. As a result, EigenTrust-based agreement feedback is generated for a trust manager. By framing both consistency

checking and trust management as secure cloud computations, it is possible to achieve low overhead while simultaneously achieving great scalability [3][4]. As a result, the cloud's distributed computing power is used in order to increase the cloud's security. Tests show that with input from just 100 tasks, Hatman can achieve an accuracy of over 93% even when 26% of the Hadoop cloud contains malicious data.

II. PROBLEM STATEMENT:

Feedback from customers is an important factor to consider when determining the overall credibility of cloud services. Numerous scholars have acknowledged the relevance of trust management and have developed strategies to measure and maintain trust based on the feedback obtained from participants [5]. Because of the unpredictability of the number of users and the very fluid nature of the cloud environment, ensuring the availability of the TMS is a challenging challenge to solve. Cloud service sy may have been the target of a self-promoting assault; hence, the selection of sx should have been made instead. Provide various trust feedbacks that aren't accurate, which will put a cloud service at a disadvantage (i.e., collusion attacks). By generating many identities and providing trust feedback that is not accurate, consumers might be duped into trusting cloud services that are not trustworthy (i.e., Sybil attacks).

III. PROPOSED METHODOLOGIES:

The feedback provided by consumers of cloud services is a valuable source that may be used to evaluate the overall reliability of cloud services. We have introduced unique strategies that aid in identifying reputation-based attacks and enable consumers to successfully select trustworthy cloud services. Our techniques are offered as a contribution to the field of computer security. We provide a credibility model that not only detects false trust feedback resulting from collusion assaults but also recognises Sybil attacks, regardless of whether or not these attacks take place over an extended or a condensed period of time (i.e., strategic or occasional attacksorthy cloud services. Our techniques are offered as a contribution to the field of computer security [6]. We provide a credibility model that not only detects false trust feedback resulting from collusion assaults but also recognises Sybil attacks, regardless of whether or not these attacks take place over an extended or a condensed period of time (i.e., strategic or occasional attacks). In addition, we are working on developing an availability model to ensure that the trust management service remains operational at the required level. In addition, we are working on developing an availability model to ensure that the trust management service remains operational at the required level. a methodology for establishing responsibility and trust in cloud computing called TrustCloud. Specifically, TrustCloud is composed of five levels, which include workflow, create a plan for a complex Trust Management (TM) system architecture for cloud computing, with the goal of assisting consumers in locating reputable cloud service providers.

IV. ENHANCED SYSTEM:

The trust management service is dependent on a high level of availability. Decentralized management of user input necessitates the deployment of several distributed nodes. Using load-balancing strategies to distribute the burden ensures a constant degree of availability. An operational power measure is used to calculate the number of TMS nodes. Using replication strategies, the effect of TMS instance failures is mitigated. We offer a replication determination measure for determining the number of copies for each node. This measure uses particle filtering methods to estimate the availability of each node with precision. The performance of the trust management service is significantly impacted by the veracity of feedback. We thus offer many criteria for the identification of feedback collusion, including feedback density and occasional feedback collusion. These analytics differentiate between deceptive feedback and malevolent users. In addition, it can identify strategic and occasional collusion attack activities (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 suggest a number of measures for the identification of Sybil assaults, such as multi-identity recognition and occasional Sybil attacks. These parameters enable TMS to recognise deceptive Sybil attack responses. For efficient trust management, a trust management service (TMS) offers an interface between users and cloud services. Due to the unpredictability of the number of users and the extremely dynamic nature of the cloud environment, however, it is impossible to ensure the availability of TMS. In cloud systems, approaches that require an awareness of users' interests and skills through similarity metrics or operational availability measurements (i.e., uptime to total time) are inapplicable. To perform in cloud contexts, a TMS should be very adaptable and scalable. It is fairly uncommon for consumers to launch assaults against cloud services. Several deceptive responses (i.e., collusion attacks) or the creation of many accounts may be used by attackers to disadvantage a cloud service (i.e., Sybil attacks). Moreover, the identification of such harmful conduct presents a number of difficulties. Initially, new users join the cloud environment, and old ones depart

continuously. This consumer dynamic makes it very difficult to identify fraudulent conduct (such as feedback collusion). Second, users may have several accounts for a single cloud service, making it difficult to identify Sybil assaults. Finally, anticipating the occurrence of malevolent action (i.e., strategic versus occasional behaviors) is impossible.

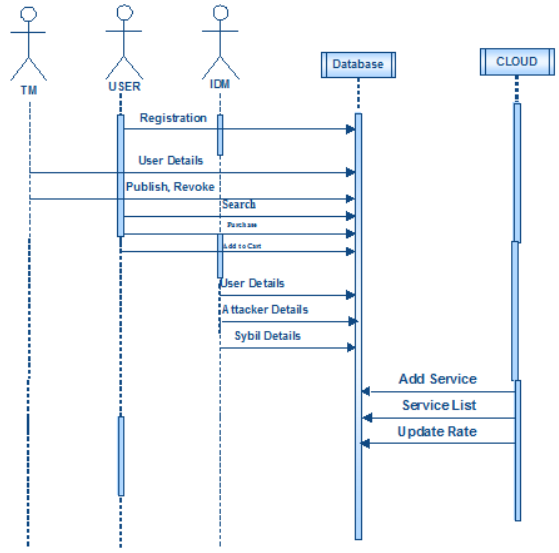

Fig 1: Sequence of System

V. CONCLUSIONS:

We have introduced unique strategies that aid in the detection of reputation-based assaults and enable consumers to properly select trustworthy cloud services. These techniques were developed by us. In particular, we provide a credibility model that not only recognizes deceptive trust feedbacks resulting from collusion assaults but also recognises Sybil attacks, irrespective of the length of time during which they are carried out (i.e., strategic or occasional attackseptive trust feedbacks resulting from collusion assaults but also recognises Sybil attacks, irrespective of the length of time during which they are carried out (i.e., strategic or occasional attacks). In addition, we are working on developing an availability model that will allow the trust management service to remain operational at a certain level. To test the efficacy of our proposed methodologies, we gathered a large number of customer trust feedbacks from actual cloud services (i.e., over 10,000 records). The results of the experiments indicate the applicability of our methodology and show that it is capable of identifying such malevolent activities. There are a few different paths that our work in the future may take. We want to integrate a variety of trust management strategies, such as reputation and recommendation, with the goal of improving the accuracy of trust outcomes. Another primary emphasis of our ongoing and future research efforts is the performance optimization of the trust management service.

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] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust Management of Services in Cloud Environments: Obstacles and Solutions," *ACM Computing Surveys*, vol. 46, no. 1, pp. 12:1–12:30, 2013.

