ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

An Authenticated Trust and Reputation System for Hybrid Cloud

Sindhu B S, H M Sanjay

M.Tech Student, Dept of CSE, P.E.S College of Engineering, Mandya, Karnataka, India

Assistant Professor, Dept of CSE, P.E.S College of Engineering, Mandya, Karnataka, India

ABSTRACT: cloud computing acting as essential role in information and communication technology. Establishing trust for resource sharing and collaboration has become an important issue in distributed computing environment .Many cloud service providers offers storage facility based on their needs for its customers and customer has pay for amount based on their usage, thereby reducing the customers' investments over storage systems. still there will be many security concerns like customers data integrity ,security and privacy in cloud storage system. Many numbers of research and various techniques have been developed and deployed for the security issues of cloud data. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage provider to disclose user confidential data on the cloud, authentication as well as trust and reputation calculation and management of cloud service providers (CSPs) is exceptionally basic and scarcely investigated issues for this new paradigm. TO fill the hole, this paper proposes an authenticated trust and reputation system for hybrid cloud services the attribute requirement of cloud service user(CSU) and CSP, the cost, trust, and reputation of the service of CSP the proposed system achieves the following three functions: 1) authenticating CSP to avoid malicious impersonation attacks 2) ascertaining and overseeing trust and reputation regards to the administration of CSP and 3) helping CSU choose desirable CSP Detailed analysis and design as well as further functionality evaluation results are presented to demonstrate the effectiveness of authenticated trust and reputation system for hybrid cloud followed with system security analysis.

KEYWORDS: cloud, authentication, trust, reputation

I. INTRODUCTION

Cloud computing is a new distributed computing paradigm for on-demand and dynamic provisioning of computing resources to potential end-users leveraging virtualization and Internet technologies. It delivers over the Interne infrastructure, platform, and software as subscription-based services. The computing services offered by cloud computing model are commonly referred to as Infrastructures as a Service (Iaas), Platform as a Service (PaaS), and Software as a Service (SaaS) respectively. These servicesare made available in a pay-per-use model to the potential cloud service consumers. Distributed computing is a model to empower advantageous, on-request arrange access for a common pool of configurable processing assets (e.g., servers, systems, storage, applications, and administrations) that could be quickly provisioned and discharged with negligible administration exertion or specialist co-op communication. Cloud computing is highlighted by that clients can flexibly use the framework (e.g., systems, servers, and stockpiles), stages (e.g., working frameworks and middleware administrations), and programming projects (e.g., application programs) offered by cloud suppliers in an on-request way. Not just the working expense and business chances and in addition upkeep costs of specialist organizations can be considerably brought down with Cloud computing, additionally the administration scale is featured by that users can elastically utilize the infrastructure (e.g., networks, servers, and storages), platforms (e.g., operating systems and middleware services), and software's.

The highly dynamic, distributed, and nontransparent nature of cloud services make the trust management in cloud environments a significant challenge. 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) alone are inadequate to establish trust between cloud consumers and providers because of its unclear and inconsistent clauses. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

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.[1]

In particular, we distinguish the following key issues of the trust

Consumers' Privacy : The selection of distributed computing raise protection concerns . Buyers can have dynamic associations with cloud suppliers, which may include touchy data. There are a few instances of protection breaks, for example, holes of delicate data (e.g., date of birth and address) or behavioral data (e.g., with whom the shopper associated, the sort of cloud administrations the purchaser indicated intrigue, and so forth.). Without a doubt, administrations which include purchasers' information (e.g., collaboration histories) ought to protect their security.

Cloud Services Protection: It is not bizarre that a cloud benefit encounters assaults from its clients. Aggressors can hindrance a cloud benefit by giving various deceiving inputs (i.e., arrangement assaults) or by making a few records (i.e., Sybil assaults). In reality, the recognition of such malevolent practices represents a few difficulties. Right off the bat, new clients join the cloud condition and old clients leave all day and all night. This buyer dynamism makes the location of vindictive practices (e.g., input conspiracy) a noteworthy test. Also, clients may have different records for a specific cloud benefit, which makes it hard to identify Sybil assaults. At last, it is hard to anticipate when malevolent practices happen.

Trust Management Service's Availability: A trust management service (TMS gives an interface amongst clients and cloud administrations for powerful trust administration. In any case, ensuring the accessibility of TMS is a troublesome issue because of the flighty number of clients and the profoundly unique nature of the cloud condition. Approaches that require comprehension of clients' interests and capacities through likeness estimations or operational accessibility estimations (i.e., uptime to the aggregate time) are unseemly in cloud situations.

II. RELATED WORK

Privacy-Preserving Fine-Grained Access Control in Public Clouds.With many economical benefits of cloud computing, many organizations have been considering moving their information systems to the cloud. However, an important problem in public clouds is how to selectively share data based on fine-grained attribute based access control policies while at the same time assuring confidentiality of the data and preserving the privacy of users from the cloud. In this article, we briefly discuss the drawbacks of approaches based on well known cryptographic techniques in addressing such problem and then present two approaches that address these drawbacks with different trade-offs[2]

Universally Compassable Multiparty Computation with Partially Isolated Parties. It is well known that universally compassable multiparty computation cannot, in general, be achieved in the standard model without setup assumptions when the adversary can corrupt an arbitrary number of players. One way to get around this problem is by having a trusted third party generate some global setup such as a common reference string (CRS) or a public key infrastructure (PKI). The recent work of Katz shows that we may instead rely on physical assumptions, and in particular tamper-proof hardware tokens. In this paper, we consider a similar but strictly weaker physical assumption. We assume that a player (Alice) can partially isolate another player (Bob) for a brief portion of the computation and prevent Bob from communicating more than some limited number of bits with the environment. For example, isolation might be achieved by asking Bob to put his functionality on a tamper-proof hardware token and assuming that Alice can prevent this token from communicating to the outside world. Alternatively, Alice may interact with Bob directly but in a special which she administers and where there are no high-bandwidth communication channels to the outside world. We show that, under standard cryptographic assumptions, such physical setup can be used to UC-realize any two party and multiparty computation in the presence of an active and adaptive adversary corrupting any number of players. We also consider an alternative scenario, in which there are some trusted third parties but no single such party is trusted by all of the players. This compromise allows us to signicantly limit the use of the physical set-up and hence might be preferred in practice. [3]

Efficient and Secure Dynamic Auditing Protocol for Integrity Verification. In Cloud Storage information homeowners host their information on cloud servers and users (data consumers) will access the information from cloud servers. As a result of the information outsourcing, however, this new paradigm of knowledge hosting service additionally introduces new security challenges, which requires associate freelance auditing service to ascertain the information integrity within the cloud. Some existing remote integrity checking strategies can solely serve for static archive information and, thus, can't be applied to the auditing service since the information within the cloud are often dynamically updated.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Thus, economical and secure dynamic auditing protocol is desired to convert information homeowners that the information area unit properly holds on in the cloud. Economical and privacy-preserving auditing protocol was proposed to provide data integrity. Then, this scheme extends the auditing protocol to support the information dynamic operations, that is economical and incontrovertibly secure in the random oracle model. Also auditing protocol supports batch auditing for each multiple homeowners and multiple clouds, without exploitation any sure organizer. The analysis and simulation results show that projected auditing protocols area unit secure and efficient, particularly it scale back the computation value of the auditor.[4]

III. PROPOSED ALGORITHM

In an authenticated trust and reputation system for hybrid cloud services consists of following modules

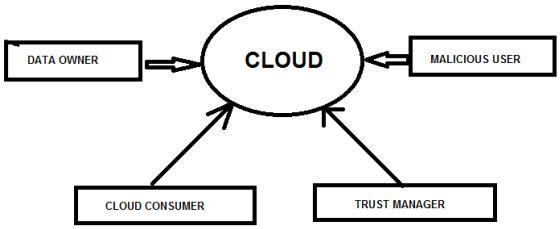

Fig: 1 Block Diagram

Data owner: In this module, initially the data owner has to get register to the cloud server (CS1,CS2,CS3,CS4) . Data owner will login to the corresponding cloud server he got registered. Data owner encrypt will upload file to the cloud server (CS1, CS2, CS3, CS4) Data owner verifies the file he uploaded either it is safe or not. Data owner can view, how many file has been uploaded to the corresponding cloud servers(CS1,CS2,CS3,CS4) Data owner will send file to trust manager to store the data owner file to the corresponding cloud servers (CS1,CS2,CS3,CS4)

Cloud server: The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud consumer. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

Trust manager: Trust manager provides login authorization for both data owner and the end user. Trust manager can view all the cloud status .Trust manager can view the feed backs given by end user and lists all positive and negative feed backs. Trust manager lists no of users in cloud services(IAAS,PAAS,SAAS).Trust manager can view the attackers in cloud servers(CS1,CS2,CS3,CS4) and the no of time attacked.

Cloud consumer: Cloud consumer first has to register to the cloud server (CS1, CS2, CS3, CS4) which particular cloud he has to use. Cloud consumer has to login to the cloud he got registered. Cloud consumer feedback about the data (positive or negative feedback)

Attacker : Attacker will view registered users and cloud files.

Collusion Attacks : to mislead feedbacks about the cloud **.**

Sybil Attacks : When user uses more transaction per day (Exceeds the limit which is assigned by the Trust Manager).

IV. SIMULATION RESULTS

An authenticated trust and reputation system for hybrid cloud services we login with data owner and cloud consumer used the cloud for there usage and give the feedback of that particular cloud .and in figure2 shows if any attacked the file we can recover by click on recover link. Figure3 show that reputation of cloud based on number of user used that particular cloud .figure4 list all the users who login as different cloud services

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

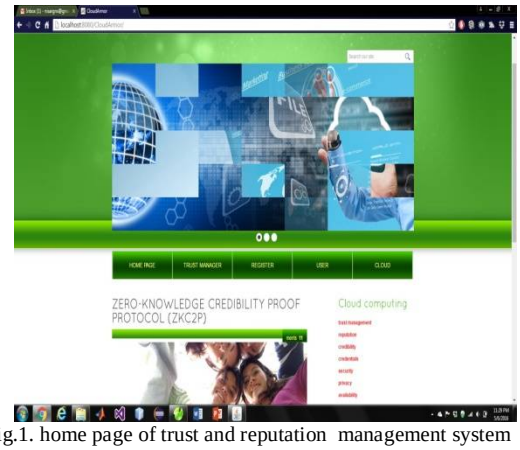

Fig.1. home page of trust and reputation management system

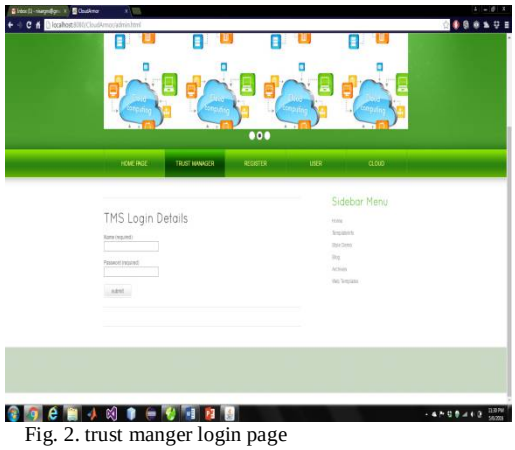

Fig. 2. trust manger login page

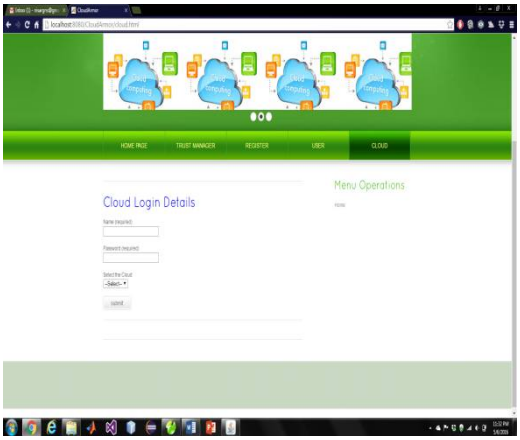

Fig. 3. cloud login page

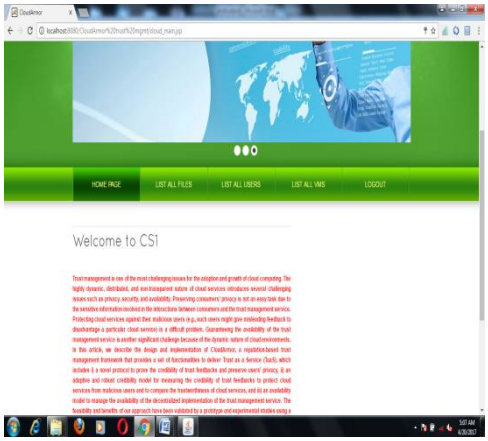

Fig 4. cloud server home page

V. CONCLUSION AND FUTURE WORK

Given the exceptionally powerful, circulated, and non transparent nature of cloud administrations, overseeing and building up trust between cloud benefit clients and cloud administrations remains a critical test. Cloud administration clients' criticism is a decent source to survey the general reliability of cloud administrations. Notwithstanding, vindictive clients may work together to i) inconvenience a cloud benefit by giving numerous deceptive trust inputs (i.e., agreement assaults) or ii) trap clients into trusting cloud benefits that are not reliable by making a few records and giving misdirecting trust criticisms (i.e., Sybil assaults). In this paper, we have displayed novel procedures that assistance in distinguishing notoriety based assaults and enabling clients to adequately recognize dependable cloud administrations. Specifically, we present a believability model that not just distinguishes deceiving trust criticisms from arrangement assaults additionally identifies Sybil assaults regardless of these assaults happen in a long or brief timeframe (i.e., key or periodic assaults individually). We likewise build up an accessibility model that keeps up the trust administration benefit at a coveted level.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

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.

BIOGRAPHY

Sindhu B S is a final year student of Master of Technology (M.Tech) Pursuing in Computer Engineering, P.E.S college of Engineering, Mandya, Karnataka, India. he received Bachelor of Engineering (BE) from Bahubali college of engineering , shravanabelagola, Karnataka, India. Her research interests are cloud computing , Android application, Big data etc.

H M Sanjay Assistant Professor in the Computer Science Department, P.E.S College of Engineering, Mandya. He received Master of Science(MS) degree from university of Bedfordshire . His research interest are cloud networks and data analytics, etc.