ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

Cloud Shield: To Prove Credibility of Cloud Services by Consumer Feedback

AsmaParveen, Sana Fatima, Ruksar Fatima

Abstract— **Trust management is one of the foremost demanding problem for the extension and assumption of cloud computing. The extremely dynamic, distributed, and non-transparent behavior of cloud services establishes difficult problems like privacy, safety, and possibility. Providing security against malicious users is a main issue. Guaranteeing provision of TMS is another important challenge due to the productive activity of cloud environments. Here, we describe structure and implementation of Cloud Shield, a reputation-based trust management that gives collection functionalities to be delivered. Trust as a Service (TaaS), consists of i) a completely unique protocol to prove the quality of trust feedbacks and maintains the privacy of users, ii)to measure the quality of trust feedbacks to secure cloud services from malicious users quality model is developed iii) an availability model to manage decentralized administration.**

Keywords: cloud shield, credibility of cloud,trust as a service, TaaS

I. INTRODUCTION

The highly changing, scattered, and dense nature of cloud services make the trust management in cloud surroundings a major issue. In accordance with the researchers at Berkeley, trust and security are ranked as one of the highest 10 barriers for the assumption of cloud computing. Actually, Service-Level Agreements (SLAs) alone are insufficient to ascertain trust between cloud customers and providers due to its ambiguous and conflicting clauses. Customer's feedback may be a sensible source to assess the comprehensive trustworthiness of cloud services. Many researchers have identified the importance of trust management and proposed solutions to assess and manage trust supported feedbacks collected from cloud users. Actually, it's commonplace that a cloud service may involve in malicious behaviors (e.g., collusion or Sybil attacks) from its cloud users.This focuses on rising of the trust management in cloud environments by proposing novel ways to ensure the quality of trust feedbacks. Particularly we differentiate the following criteria's of the trust management in cloud surroundings:

AsmaParveen*,, Department of Computer Science and Engineering, Khaja Banda Nawaz College Of Engineering, Kalaburagi, Karnataka, India, 9986130446.*

Sana Fatima*,P.G.Student, Department of Computer Science and Engineering, Khaja Banda Nawaz College Of Engineering, Kalaburagi, Karnataka, India, 7829073127.*

Ruksar Fatima, *Department of Computer Science and Engineering, Khaja Banda Nawaz College Of Engineering, Kalaburagi, Karnataka, India, 8884125518.*

- **Consumer's Privacy**:The assumption of cloud computing hike security considerations. The dynamic interactions can be established between the consumers and cloud providers, wherein sensitive data is involved. There are many types of privacy violations such as leak of sensitive data (e.g., DOB and residential address) or behavioral data (e.g., with whom the cloud user interacted).No doubt, the privacy should be maintained for the services which involve consumers' data (e.g., interaction histories).
- **Cloud Services Protection:**It is not uncommon where a cloud service is involved in attacks from its cloud users. Attackers can give a drawback to cloud service by giving several confusing feedbacks (i.e., collusion attacks) or by generating multiple accounts (i.e., Sybil attacks). Actually, there are multiple problems while detecting such malicious behaviors. Initially, the new cloud users need to register the cloud environment and simultaneously old cloud users may leave. An important challenge with this consumer spirit is making the identification of malicious behaviors (e.g., feedback collusion). Next, it becomes very difficult in the detection of the Sybil attacks where users may have numerous accounts for a specified cloud service. Lastly, it is difficult to anticipate when malicious behaviors occur (i.e., strategic VS. occasional behaviors).
- **Trust Management Service's Availability:** For an efficient trust management, trust management service (TMS) introduces an intermediation between cloud users and services. After all we ensure the availability of TMS is a difficult issue due to the incalculable number of cloud users and the highly changing behavior of the cloud surroundings. TMS should be flexible and highly expandable to be operational in cloud environments. In this, we overview the design and the implementation of Cloud Shield (cloud consumer's quality Assessment & trust management of cloud services): a structure for reputation-based trust management in cloud environments. In Cloud Shield, trust is delivered as a service (TaaS) where TMS extents several scattered nodes to manage feedbacks in a decentralized way. Cloud Shield utilizes techniques to distinguish quality feedbacks from malicious users.

II. RELATED WORK

Cloud computing have many economic advantages, with these advantages many organizations are considering to move their information data systems to the cloud.

In [1]Authors described herein Service Level Agreement normally cloud service providers give surety with technical and functional description. But users are not sure to select a cloud provider only with service level agreement. They propose here a multi-faceted Trust Management system for cloud computing to identify a truthful cloud provider. They do this with the help of various attribute value with many sources and base of trust information. Main objective of this system is to give brief representation of trust management system for cloud computing. By this architecture the multi-faceted nature is proposed with multiple attributes. Based on cloud consumer's opinion cloud providers are rated. Later cloud users feedbacks and technical measurements are combined to assure the cloud providers trustworthiness. **In [2]**Authors describedit is surely understood that all around composable multiparty calculation can't, by and large, be accomplished in the standard model without setup presumptions when the foe can degenerate a subjective number of players. One approach to get around this issue is by hosting a trusted third get-together produce some worldwide setup, for example, a Common reference string (CRS) or an Public key Infrastructure (PKI). The late work of Katz demonstrates that we may rather depend on physical suppositions, and specifically carefully designed equipment tokens. In this paper, we consider a comparable yet entirely weaker physical presumption. We accept that a player (Alice) can mostly disengage another player (Bob) for a brief part of the calculation and keep Bob from conveying more than some set number of bits with nature. For instance, confinement may be accomplished by requesting that Bob put his usefulness on a sealed equipment token and accepting that Alice can keep this token from imparting to the outside world. On the other hand, Alice may cooperate with Bob specifically however in an extraordinary once who she oversees and where there are no high-data transfer capacity correspondence channels to the outside world. We demonstrate that, under standard cryptographic presumptions, such physical setup can be utilized to UC-understand any two gathering and multiparty calculation within the sight of a dynamic and versatile enemy undermining any number of players. We additionally consider an option situation, in which there are some trusted outsiders however no single such gathering is trusted by the majority of the players. This trade off permits us as far as possible the utilization of the physical set-up and consequently may be favored practically speaking.**In[3]**Authors focushere trust as a service architecture's design and implementation is analyzed. It helps to identify the difference between trustworthy and malicious feedbacks by the reliability model. The characteristics of Taasare :

a) A reliability model: A model that takes the majority union of feedbacks also with distinguishing the reliable and malicious feedbacks.
b) Shared trust feedback estimate and storage: For eliminating the disadvantages of centralized model the TM service gives trust feedback and storage estimate.

There were many techniques presented for managing the feedbacks from all its members. The problem of reliable trust feedback was avoided here. The management systems sometimes observe malicious behavior of users. But user's behavior changes based on their experience.

In [4]Authors define here sharing storage and computing resources along with on demand system which depends on pay as you go business model the cloud computing reduces cost of its service model. These characteristics affect information technology costs with an impact on security and trust strategies. Some merits of cloud computing like scaling, sharing of resources and remote data storage becomes its limitations by keeping data confidentiality with its customers. How security and privacy problems arise in cloud computing and the ways in which they can be resolved are proposed here ,**In[5]**Authors focusedon benefits proposed by cloud computing helps cloud providers and consumers with the trust management system. But the problems of trust management, decentralized feedbacks, low identification feedback and protection of users are still to be resolved. For cloud environment the service level agreement approaches are inappropriate. The fuzzy technical specification of SLA may allow consumers for selecting trustful cloud services. This is the first strategy which focuses on the trust management of cloud services.

In[6]Authors describedas of late more consideration is paid towards information concealing, this paper goes for giving classification and trustworthiness towards both the information and additionally picture. Reversible information concealing (RDH) in encoded pictures gives amazing property that the first cover can be loss lessly recouped. All the past strategies for implanting information by reversibly abandoning room after encryption may subject to a few mistakes on the information and also picture extraction. In this paper I propose a novel technique by holding room before encryption with a customary RDH calculation, and therefore it is simple for the information hider to reversibly insert information in the encoded pictures. The proposed strategy can accomplish genuine reversibility, which is information extraction and picture recuperation are free from any blunder. Tests demonstrate that this novel strategy can install more than 10 times ale payloads (i.e) effectiveness for the same picture quality as the past strategies.

III. EXISTING SYSTEM

In accordance with the researchers at Berkeley, trust and security are ranked as one of the highest 10 barriers for the assumption of cloud computing. Actually, Service-Level Agreements (SLAs) alone are insufficient to ascertain trust between cloud customers and providers due to its ambiguous and conflicting clauses. Customer's feedback may be a sensible source to assess the comprehensive trustworthiness of cloud services. Many researchers have identified the importance of trust management and proposed solutions to assess and manage trust supported feedbacks collected from cloud users.

Disadvantages of Existing System:
1.Ensuring the supply of Trust Management Service could be a tough downside as a result of the unpredictable variety of users and also the extremely dynamic behavior of the cloud services in cloud environment. A Self-promoting attack may need to be operated on cloud service system.

2.Giving disadvantage to a cloud service by providing several dishonorable trust feedbacks (i.e., collusion attacks)
3. Conspiracy on users into checking the trust of services provided by the cloud are not authentic by making multiple accounts and producing ambiguous trust feedbacks (i.e., Sybil attacks).

IV. PROPOSED SYSYTEM

Feedbacks from cloud users is assumed to be a better source to determine the overall authenticity of services of cloud. Here, we are introducing novel methods that help in determining reputation based attacks and allowing users to efficiently determine authenticity of cloud services. We propose a quality model that not only determines ambiguous trust feedbacks from collusion attacks but also detects Sybil attacks no matter whether is it produced in a sort span of time or taking larger delay(i.e., strategic or occasional attacks respectively). We also establish an availability model that preserved the TMS at a specified level.

Advantages Of Proposed System:

1) Trust Cloud structure for liability and trust in cloud computing. Especially Trust Cloud consists of 5 layers which also includes workflow,
2) Develop a multi-faceted Trust Management (TM) system design structure for cloud computing to assist the cloud service users to determine authenticity of cloud service providers.

V. SYSTEM ARCHITECTURE

The Cloud Shield structure relies on the service oriented architecture (SOA), that brings trust as a service. SOA and internet services are foremost important technologies for cloud computing in perception that services (e.g., infrastructures, platforms, and software) are exposed in clouds as services. Above all, the TMS spans multiple scattered nodes which expose interactions so that cloud users will give their feedbacks or examine trust results. Figure below shows the structure, which consists of 3 totally different layers, specifically the Cloud Service Provider Layer, the Trust Management Service Layer, and the Cloud Service Consumer Layer.

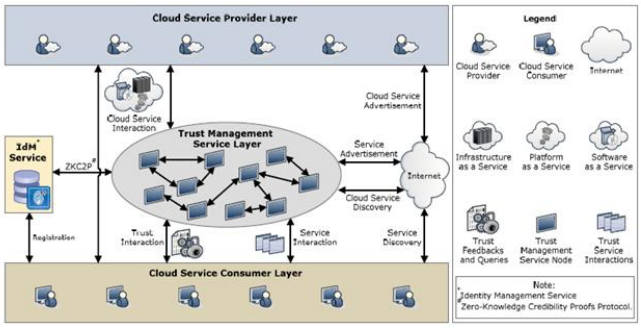

Fig:Architecture of Cloud Shield Trust Management framework.

.

The Cloud Service Provider Layer: This layer consists of various cloud service providers, which offers 1 or multiple cloud services, i.e., IaaS (Infrastructure as aService), PaaS (Platform as a Service), and SaaS (Softwareas a Service), openly on the Internet. These cloud services are available through internet portals and indexed on internet search engines like Google, Yahoo, and Baidu. For this, interactions are considered as cloud service interaction with cloud users and TMS, and cloud services advertisements where providers which are ready to explore their services on the internet.

The Trust Management Service Layer: This layer includes multiple scattered TMS nodes that are hosted in several cloud surroundings in numerous geographical areas. These TMS nodes disclose interfaces in order that users offer their feedback or examine the trust results in a decentralized way. Interactions consists of: i)cloud service interaction with cloud service providers, ii)service advertisement to explore the trust as a operation to users through the web, iii) cloud service discovery through the web to allow cloud users to determine 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: Lastly, this layer includes various cloud users who access services provided by cloud. As an instance, a new startup has restricted funding can utilize services of cloud (e.g., posting their services in Amazon S3). For this interactions are: i) service discovery here cloud users are capable of discovering new cloud services and alternative services through the web, ii) trust and service interactions here cloud users are capable to send their feedback or derive the trust results of a precise cloud service, and iii) registration where users produces their identification by registering their privileges in IdM before utilizing the service of TMS. This structure also depicts a Web crawling method for automatic cloud services analysis, in which cloud services are automatically, gets analyzed on the web and stored in a cloud services database. Furthermore, the structure includes an Identity Management Service (see Figure 1) which is answerable for the registration where cloud users register their privileges before using services of TMS and proving the quality of a appropriate customers feedback through ZKC2P.

VI. METHODOLOGY

The following steps are used to perform encryption and decryption on a file.

1. For a specified algorithm generate a key for a given array of bytes.
2. Generate a cipher text for a specified algorithm.
3. For encryption and decryption initialize the cipher text.

Algorithm1: The keys in this algorithm are calculated in the following manner:

1) Select at random any 2 prime numbers such as p and q.
2) Compute n = pq.
3) Compute (n) = (p − 1)(q − 1) = n − (p + q − 1),
4) Select an integer e where 1 < e < (n) and gcd(e, (n)) = 1; i.e., e is coprime.
5) Calculate d as $d \equiv e^{-1} \pmod{(n)}$;
6) $d \cdot e \equiv 1 \pmod{(n)}$
7) e is released as the public key exponent.
8) d is kept as the private key exponent.
9) The public key includes mod n and the public (encryption) exponent e. The private key includes mod n and the private (decryption) exponent d, and should be kept secret. p, q, and (n) should also be kept secret as they are used to find the value of d.

The algorithm includes4 steps: key generation, key distribution, encryption and decryption. The algorithm includes a *public key* and a *private key*.

Key distribution: In key distribution mechanism the users has to send their public key as (n, e) in order to send their encrypted messages. But private key is not distributed. If Alice is sending message to Bob, then, Alice should generate a cipher text using his public key, where as Bob can decrypt the message using her private key, hence Alice's public kley is known to all.

Encryption: Consider a message M that is to be transmitted between 2 users Alice and Bob. Firstly we need to calculate the integer value of M as m and find gcd (*m*, *n*) =1. Then generate the cipher text c for the given message m by using the corresponding users public key.

Decryption: The user Alice can regenerate m from c by applying their respective private key as exponent of d. For *m*, she can regenerate the original message *M* by reversing the padding scheme.

Key generation: The keys in this algorithm are calculated in the following manner:Select at random any 2 prime numbers such as p and q.

Algorithm 2:Trust Results & Credibility Weights Caching

Count |Vc(c; s)|Cache /*TMS instance counts the total number of new trust feedbacks given by a particular consumer*/
if|Vc(c; s)|Cache >= eCache(c) then /*TMS determines whether a recalculation is required for credibility factors related to the consumer*/
Compute ȷ(c); Compute B(c)
Compute M_{id} (c); Compute Cr(c; s)
end if
Count |V(s)| Cache /*TMS instance counts the total number of new trust feedbacks given to a particular cloud service*/
if |V(s)| Cache >= eCache(s) then /*TMS determines whether a recalculation is required for credibility factors related to the cloud service including the trust result*/
Compute D(s); Compute Cr(c; s)
Compute T r(s)
end if

Mid= Multi-identity Recognition
D(s) = Feedback Density
Cr =credibility aggregated weights
Tr(s) = Trust Results.

We propose to cache the trust results and the credibility weights based on the number of new trust feedbacks to avoid unnecessary trust result computations. The caching process is controlled by two thresholds: one for users' eCache(c) and one for cloud services eCache(s). If the TMS instance receives a trust assessment request from a user, it should use the trust result in the cache as much as possible, instead of computing the trust result from scratch. The TMS instance updates the cache based on the number of new trust feedbacks (i.e., since the last update) given by a particular consumer |Vc(c, s)| Cache and the number of new trust feedbacks given to a particular cloud service |V(s)| Cache.

VII. CONCLUSION

The extremely dynamic, distributed, and non-transparent behavior of cloud services establishes difficult problems like privacy, safety, and possibility, managing and establishing trust between cloud service users and cloud services major challenge, Guaranteeing provision of TMS is another important challenge due to the productive activity of cloud environments. Cloud service users' feedback may be a sensible source to assess the overall trustworthiness of cloud services. Yet, malicious customers could collaborate together to i) disadvantage a cloud service by sending several misleading trust feedbacks (i.e., collusion attacks) or ii) Force the data users into having trust in cloud services that are not trustworthy by creating multiple accounts and sending misleading trust feedbacks (i.e., Sybil attacks). In this, we have introduced novel techniques that help in the detection of reputation based attacks and allowing the customers to effectively distinguish trustworthy cloud services. In particular, we present a quality model that not only distinguishes misleading trust status from collusion attacks but also identify Sybil attacks no matter whether these attacks takes place in a shorter or longer period of time (i.e., strategic or occasional attacks respectively). The trust management service can be maintained at a desired level by developing an availability model. Feedbacks from cloud users are assumed to be a better source to determine the overall authenticity of services of cloud.

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 inClouds," 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.

AsmaParveen,*,M.tech(ph.d),Head of The Department,Department of Computer Science and Engineering, Khaja Banda Nawaz College Of Engineering, Kalaburagi, Karnataka, India, 9986130446*

Sana Fatima,*P.G.Student, Department of Computer Science and Engineering, Khaja Banda Nawaz College Of Engineering, Kalaburagi, Karnataka, India, 7829073127*

RuksarFatima,*ph.d,Vice-Principal,Department of Computer Science and Engineering, Khaja Banda Nawaz College Of Engineering, Kalaburagi, Karnataka, India, 8884125518*