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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Trust Management for Reliable Heterogeneous Cloud Service

Shruthi.C, Bhagyashri R Hanji

PG Scholar, Department of Computer Science & Engineering, Global Academy of Technology, Bengaluru, India

Department of Computer Science & Engineering, Global Academy of Technology, Bengaluru, India

ABSTRACT: Cloud computing is another developing computational model. Clouds highlights like fast versatility, pay per use, area freedom, on interest foundation giving capacity and all over system access are drawing in both Cloud purchasers and suppliers. Trust is a standout amongst the most concerned snags for the appropriation and development of distributed computing. Customers' criticism is a decent source to survey general dependability of cloud administrations. In any case, it is not uncommon that a trust administration framework encounters pernicious practices from its clients. Overseeing trust inputs in cloud situations is a difficult issue because of unusual number of cloud administration purchasers and exceptionally dynamic nature of cloud situations. In this paper, we propose the proficient structure to enhance courses on trust administration in cloud situations. We propose a multi-faceted Trust Management (TM) framework design for a distributed computing commercial center. This framework gives intends to distinguish the reliable cloud suppliers as far as various characteristics (e.g., security, execution, consistence) evaluated by numerous sources and foundations of trust data.

KEYWORDS: Cloud computing, trust management, reputation, credibility, credentials, security, privacy, availability

I. Introduction

Trust management is a standout amongst the most difficult issues for the selection and development of distributed computing. The profoundly powerful, conveyed, and non-straightforward nature of cloud administrations presents a few testing issues, for example, protection, security, and accessibility. Protecting purchasers' security is not a simple errand because of the touchy data included in the associations amongst customers and the trust administration. Ensuring cloud administrations against their pernicious clients (e.g., such clients may give deceiving input to hindrance a specific cloud administration) is a troublesome issue. Ensuring the accessibility of the trust administration is another noteworthy test in view of the dynamic way of cloud situations. In this article, we depict the outline and execution of Cloud Armor, a notoriety based trust administration structure that gives an arrangement of functionalities to convey Trust as a Service (TaaS), which incorporates i) a novel convention to demonstrate the validity of trust criticisms and save clients' security, ii) a versatile and hearty believability model for measuring the believability of trust inputs to shield cloud administrations from noxious 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. The plausibility and advantages of our methodology have been accepted by a model and trial examines utilizing an accumulation of certifiable trust criticisms on cloud administrations.

Cloud computing is another rising computational model. Cloud highlights like fast flexibility, pays per use, area autonomy, on interest framework giving capacity and all over system access are pulling in both Cloud customers and suppliers. Trust is a standout amongst the most concerned deterrents for the selection and development of distributed computing. Customers' input is a decent source to survey general dependability of cloud administrations. In any case, it is not strange that a trust administration framework encounters malevolent practices from its clients. Overseeing trust criticisms in cloud situations is a difficult issue because of eccentric number of cloud administration buyers and very dynamic nature of cloud situations. In this paper, we propose the "CloudArmor" system to enhance courses on trust administration in cloud situations. We propose a multi-faceted Trust Management (TM) framework design for a

DOI: 10.15680/IJIRCCE.2016. 0404316

distributed computing commercial center. This framework gives intends to recognize the reliable cloud suppliers regarding distinctive qualities (e.g., security, execution, consistence) evaluated by different sources and foundations of trust data.

Cloud computing innovation is generally developed and most associations need to utilize this innovation in their business forms. Be that as it may, then again, the utilization of this innovation is difficult and numerous associations are worried about putting away their touchy information in their server farms as opposed to putting away them in the distributed storage focuses. In the distributed computing environment, trust, as an answer for improve the security, has pulled in the consideration of specialists. Trust is a standout amongst the most imperative approaches to enhance the dependability of distributed computing assets gave in the cloud environment and has a critical part in the business situations. Believing the client to choose the proper source helps in heterogeneous cloud foundation. In this paper, we show the trust model in view of guidelines of proper. administration quality and pace of execution for cloud assets. Reproduction results demonstrate that the proposed model contrasted and comparable models, notwithstanding considering measures of the nature of administration, chooses the most dependable source in a cloud domain by considering the pace of things.

Trust administration gives a decent approach to enhancing the security. Overseeing trust is major part in cloud situations considering its qualities, for example, dynamic in nature, versatility, asset pooling, on interest self administration. It is another security mode to give security state, unwavering quality, and access control approaches. For appraisal, distinguishing and appropriating vindictive substances taking into account changing and digging the recognized results for security instrument in various frameworks and gathering criticism evaluation. Criticism, suggestion, surveys from the clients is profitable for administration choice in e-market. As of late, a cloud commercial center [2] has been dispatched to bolster shoppers in distinguishing tried and true cloud administration suppliers.

The Trust Management permits cloud clients to determine their prerequisites and assessments while getting to the trust score of cloud suppliers. It gives an online front end to the clients for indicating their prerequisites. In light of the necessities, the Trust Management gives the trust score of cloud suppliers. Client can enlist with administrations which has best audits is given by old clients. Client can examination the criticisms of other client and become more acquainted with which administrations is superior to anything all. At that point the client is enlist effectively, the servicer will checked with their confirmation. At that point the client can login to utilizations that administrations and new client likewise give new criticisms about the administration.

II. LITERATURE SURVEY

With virtualization technology, cloud computing offers diverse services (such as virtual computing, virtual storage, virtual bandwidth, etc.) for the public by means of multi-tenancy mode. Although users are enjoying the capabilities of super-computing and mass storage supplied by cloud computing, cloud security still remains as a hot spot problem, which is in essence the trust management between data owners and storage service providers. Yu-Chao Liu et. al [1] proposed a data coloring method based on cloud watermarking to recognize and ensure mutual reputations.

The experimental results show that the robustness of reverse cloud generator can guarantee users0 embedded social reputation identifications. Hence, our work provides a reference solution to the critical problem of cloud security. Mohamed Firdhous et.al[2] the authors look at what trust is and how trust has been applied in distributed computing. Trust models proposed for various distributed system has then been summarized. The trust management systems proposed for cloud computing have been investigated with special emphasis on their capability, applicability in practical heterogonous cloud environment and implementabilty. Finally, the proposed models/systems have been compared with each other based on a selected set of cloud computing parameters in a table.

Mariappan et. al[3] provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. Such leading sessions can be leveraged for detecting the local anomaly instead of global anomaly of App rankings. Furthermore, we investigate three types of evidences, i.e., ranking based evidences, rating based evidences and review based evidences, by modelling Apps' ranking, rating and review behaviours through statistical hypotheses tests. In addition, we propose an optimization based aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the iOS

App Store for a long time period. In the experiments, w e validate the effectiveness of the proposed system, an d show the scalability of the detection algorithm as well as some regularity of ranking fraud activities.

Talal H et. al [4] propose the “Trust as a Service” (TaaS) framework to improve ways on trust management in cloud environments. In particular, we introduce an adaptive credibility model that distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers’ capability and majority consensus of their feedbacks. The approaches have been validated by the prototype system and experimental results. Al Trust management is the major goal in the variety of cloud computing environment. multi-faceted Trust Management (TM) system architecture for a cloud computing marketplace. This system provides means to identify the trustworthy cloud providers in terms of different attributes (e.g., security, performance, compliance) assessed by multiple sources and roots of trust information [5, 8].

Telecommunication industry has been successful in turning the Internet into a mobile service and stimulating the creation of a new set of networked, remote services. Most of these services now run or are supported by cloud computing platforms. Embracing cloud computing solutions is fundamental for the telecommunication industry to remain competitive. However, there are many legal, regulatory, business, market-related and technical challenges that must be considered first. Leonardo et. al[7] listed such challenges and define a set of privacy, security and trust requirements that must be taken into account before cloud computing solutions can be fully integrated and deployed by telecommunication providers.

Reputation attacks to allow consumers to effectively identify trustworthy cloud services. [9]. Hengshu Zhu [10] et. Al optimization based aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the iOS App Store for a long time period. In the experiments, we validate the effectiveness of the proposed system, and show the scalability of the detection algorithm as well as some regularity of ranking fraud activities.

III. PROBLEM STATEMENT

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. Trick users into trusting cloud services that are not trustworthy by creating several accounts and giving misleading trust feedbacks. A Self-promoting attack might have been performed on cloud service sy, which means sx should have been selected instead.

IV. PROPOSED SYSTEM

The Trust Management allows cloud users to specify their requirements and opinions when accessing the trust score of cloud providers. It provides a web-based front end to the users for specifying their requirements. Based on the requirements, the Trust Management provides the trust score of cloud providers. User can register with services which has best reviews is given by old users. User can analysis the feedbacks of other user and get to know which services is better than all. Then the customer is register successfully, the servicer will verified with their proof. Then the customer can login to uses that services and new customer also give new feedbacks about the service.

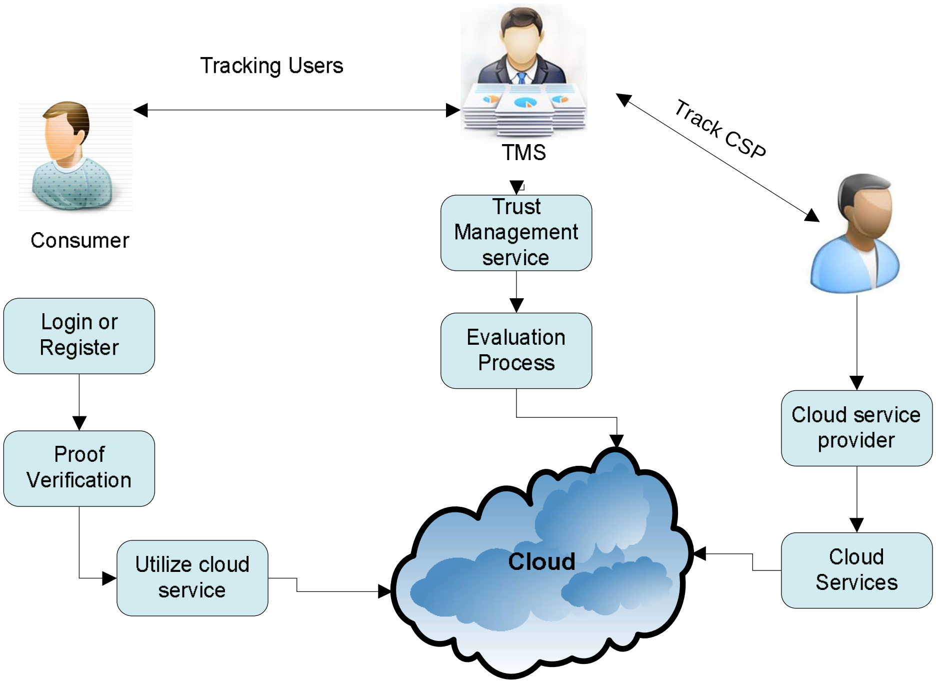


Figure 1: Architecture of Proposed System

Trust Management Service

Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers’ privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against their malicious users (e.g., such users might give misleading feedback to disadvantage a particular cloud service) is a difficult problem. Guaranteeing the availability of the trust management service is another significant challenge because of the dynamic nature of cloud environments.

Cloud Services

1. Cloud Service Providers (CSPs)

CSP can be a person, enterprise, or entity responsible for building a service available to interested parties. Cloud service providers host and manages the underlying infrastructure and offer cloud services (eg. Software as a Service, Platform as a Service and Infrastructure as a Service) to cloud service user, cloud service broker and cloud reseller.

2. Cloud Service User (CSUs)

CSU is a person or enterprise that maintains a business relationship with, and uses service from cloud providers.
Business organizations, government authorities, educational institutions and individuals belonging to the category of service user, may use cloud services to meet their business, national, educational, and personal needs (without offering any services to others).

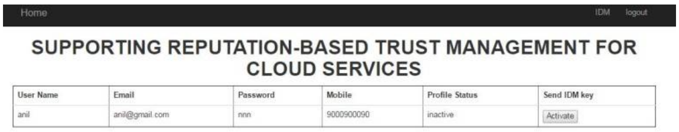
3. Cloud Service Broker (CSB)

CSB is an entity that manages the usage, performance and delivery of cloud services, and negotiates relationships between CSPs and CSUs. Two types of brokers are introduced in cloud market. First, there are brokers that concentrate on negotiating relationships between CSPs and CSUs without managing and owning the cloud infrastructure. Second, there are brokers that add some extra service on top of CSPs to enhance and secure the cloud environment for the CSUs.

4. Trust Engine (TE)

TE is the trust engine contained in a cloud broker. It is a core part of the model that performs the trustworthiness Calculation for CSPs and CSUs.

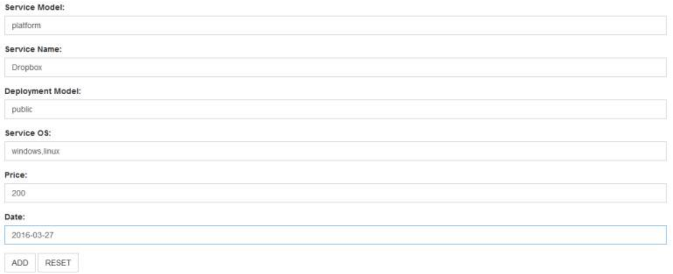
V. RESULTS



SUPPORTING REPUTATION-BASED TRUST MANAGEMENT FOR CLOUD SERVICES

User Name	Email	Password	Mobile	Profile Status	Send IDM key
anil	anil@gmail.com	nnn	9000900090	inactive	Activate

Figure 2: Activating User account by IDM after registering to cloud. IDM is responsible for managing identity if user.



Service Model:
platform

Service Name:
Dropbox

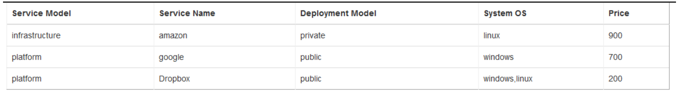
Deployment Model:
public

Service OS:
windows,linux

Price:
200

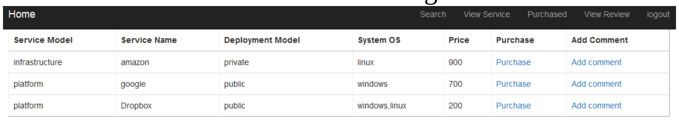
Date:
2016-03-27

Figure 3: Service added by the Service Provider.



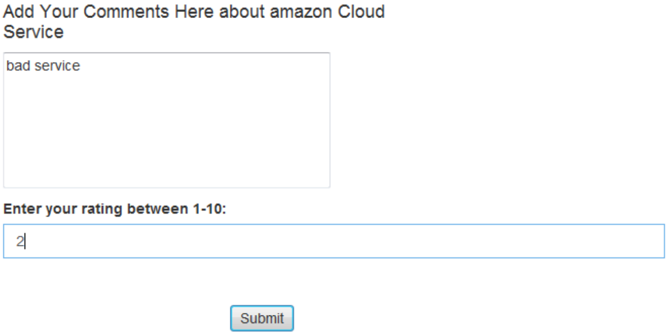
Service Model	Service Name	Deployment Model	System OS	Price
infrastructure	amazon	private	linux	900
platform	google	public	windows	700
platform	Dropbox	public	windows,linux	200

Figure 4: Added Services to Cloud by the cloud service provider. Service provider can add any kind of services for the data consumers usage.



Service Model	Service Name	Deployment Model	System OS	Price	Purchase	Add Comment
infrastructure	amazon	private	linux	900	Purchase	Add comment
platform	google	public	windows	700	Purchase	Add comment
platform	Dropbox	public	windows,linux	200	Purchase	Add comment

Figure 5: Search and View Services by Cloud service Consumer. Consumer can add comments and purchase their interest of cloud services



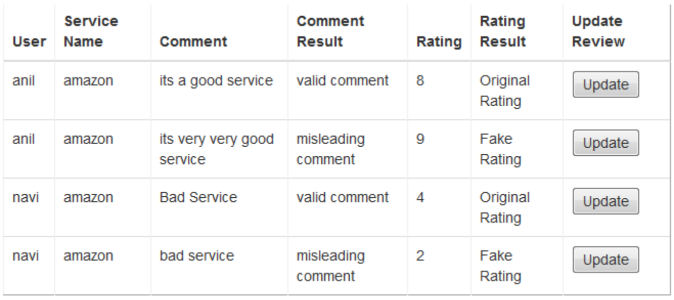
Add Your Comments Here about amazon Cloud Service

bad service

Enter your rating between 1-10:

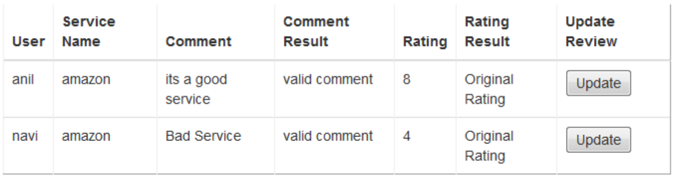
2

Figure 6: Comments AND rating given by the consumer.



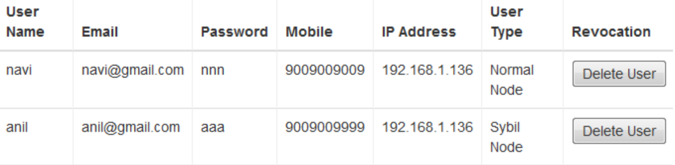
User	Service Name	Comment	Comment Result	Rating	Rating Result	Update Review
anil	amazon	its a good service	valid comment	8	Original Rating	Update
anil	amazon	its very very good service	misleading comment	9	Fake Rating	Update
navi	amazon	Bad Service	valid comment	4	Original Rating	Update
navi	amazon	bad service	misleading comment	2	Fake Rating	Update

Figure 7: Collusion Attack Detection from the Trust Manager. Multiple Misleading comments given by the consumer to the same services is treated as misleading comments. Then those comments are removed by the TM. Only valid comments are given for the services.



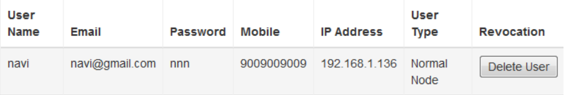
User	Service Name	Comment	Comment Result	Rating	Rating Result	Update Review
anil	amazon	its a good service	valid comment	8	Original Rating	Update
navi	amazon	Bad Service	valid comment	4	Original Rating	Update

Figure 8: After deleting misleading comments by the trust manager.



User Name	Email	Password	Mobile	IP Address	User Type	Revocation
navi	navi@gmail.com	nnn	9009009009	192.168.1.136	Normal Node	Delete User
anil	anil@gmail.com	aaa	9009009999	192.168.1.136	Sybil Node	Delete User

Figure 9: Detection of Sybil attack in cloud. User registered to cloud in the same session with multiple identities is treated as Sybil node. For detection of Sybil attack is done by tracking users IP address



User Name	Email	Password	Mobile	IP Address	User Type	Revocation
navi	navi@gmail.com	nnn	9009009009	192.168.1.136	Normal Node	Delete User

Figure 10: After deletion of Sybil node from the cloud.

VI. CONCLUSION

In this Paper described the design and implementation of Cloud Protector, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS), which includes i) a novel protocol to prove the credibility of trust feedbacks and preserve users' privacy, by finding trust worthiness of users feedback and ratings to protect cloud services from malicious behavior (collusion) and to compare the trustworthiness of cloud services, and ii) an availability model to manage the availability of the decentralized implementation of the trust management service. The feasibility and benefits of our approach have been validated by a prototype and experimental studies using a collection of real-world trust feedbacks on cloud services.

REFERENCES

[1] Yu-Chao Liu, Yu-Tao Ma, Hai-Su Zhang, De-Yi Li and Gui-Sheng Chen, "A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking", International Journal of Automation and Computing, pp 280-285, 2011.

[2] Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan, "Trust Management in Cloud Computing: A Critical Review", International Journal on Advances in ICT for Emerging Regions, pp 24-36, 2011.

[3] Mariappan.R, Deivanai.A, B.Hema and Thamizharasi.V, "Investgation of Ranking Rating and Review Using Statistical Hypotheses Tests", International Journal of Engineering Sciences & Research Technology, Volume 4, 2015.

[4] Talal H. Noor and Quan Z. Sheng, “Trust as a Service: A Framework for Trust Management in Cloud Environments”, Springer, pp. 314–321, 2011.

[5] Habib, S.M, Ries. S. and Muhlhauser. M, “Towards a Trust Management System for Cloud Computing”, Trust, Security and Privacy in Computing and Communications, pp 933 – 939, 2011.

[6] Talal H. Noor, Quan Z. Sheng, Member, IEEE, Lina Yao, Schahram Dustdar, Senior Member, IEEE, and Anne H.H. Ngu, “CloudArmor: Supporting Reputation-based Trust Management for Cloud Services”, IEEE Transactions on Parallel and Distributed Systems, 2015.

[7] Leonardo A. Martucci, Albin Zuccatoy, Ben Smeetsxz, Sheikh M. Habib, Thomas Johansson and Nahid Shahmehri, “Privacy, Security and Trust in Cloud Computing The Perspective of the Telecommunication Industry”, Third International Symposium on Multidisciplinary Emerging Networks and Systems, 2012.

[8] Sheikh Mahbub Habib, Sebastian Ries, Max M and uhlha user, “Towards a Trust Management System for Cloud Computing”, International Conference on Trust, Security and Privacy in Computing and Communications, PP 933 – 939, 2011.

[9] Talal H. Noor, Quan Z. Sheng, and Abdullah Alfazi, “Reputation Attacks Detection for Effective Trust Assessment Among Cloud Services”, International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[10] Hengshu Zhu, Hui Xiong, Senior Member, Yong Ge, and Enhong Chen, “Discovery of Ranking Fraud for Mobile Apps”, Transactions On Knowledge And Data Engineering, 2015.