Cloud Armor: A Trusty Supporting Reputation-based Management for Cloud Services

Reddypally Srishylam[1] and Mohammad Umar[2]
[1] Asst. Professor, CVR College of Engg/CSE Dept, Hyderabad, India
Email: srisailamreddypally@gmail.com
[2] Asst. Professor, CVR College of Engg/CSE Dept, Hyderabad, India
Email: umarmohd25@gmail.com

***Abstract*: Trust controlling may be a standout among the primary tough matter for the effort and development of cloud computing. The very dynamic, scattered, and non-transparent nature of cloud facilities ends up in several difficult problems like privacy, security, and handiness. Saving consumers' privacy isn't a simple task attributable to the direction concerned within the communications between customers and also the trust controlling service. Protective cloud services against their spiteful shoppers (e.g., such shoppers could provide dishonorable feedback to inconvenience a selected cloud service) may be a sophisticated issue. Attributable to the dynamic nature of cloud environments, reassuring the provision of the trust management service may be a problematic issue. during this article, we incline to describe the planning and application of Cloud Armor, a reputation-based trust management system that provides a conference of functionalities to deliver Trust as a Service (TaaS), which joins i) a completely unique convention to demonstrate the quality of trust inputs and save clients' security, ii) a flexible and sturdy quality model for measurement the quality of trust feedbacks to stay cloud services from malicious shoppers and to investigate the Irresponsibleness of cloud services, associated iii) an handiness model to manage the accessibility of the suburbanized usage of the trust management service. The possibility and assistances of our methodology are tried by a model and take a look at studies utilizing a set of true trust feedbacks on cloud services.**

***Index terms*: Cloud computing, trust controlling, repute, authority, security, secrecy.**

I. INTRODUCTION

Cloud computing [6] refers to pool of services that square measure offered to a client on pay per use basis. It helps IT firms to specialize in their business or strategic comes instead of technical aspects. It elevates the necessity of shopping for pricey servers. Users needn't to hassle concerning installation and package maintenance. in the main 3 service model square measure offered by cloud that square measure Infrastructure as a service (IaaS), Platform as a Service (PaaS) and package as a service (SaaS). At SaaS level applications square measure hosted by suppliers on network, these services square measure utilized by customers over web on demand basis. an online browser is employed to access totally different software's from the cloud suppliers. A user needn't to put in package on his machine, solely Associate in Nursing instance of package is required. For instance Google Apps, SQL Azure. In PaaS model as name implies it provides platform to create numerous applications. numerous facilities offered by PaaS to deploy applications embrace application planning, development, testing and hosting [10]. Suppliers offer servers and network for application preparation while not shopping for actual hardware and package. The downfall of PaaS is movable-ness drawback. Users got to pay high price if he desires to migrate from one supplier to a different. Iaas is model during which solely hardware is employed by services for his or her operation. Users needn't to buy pricey servers; they'll rent server and network house, memory, cupboard space etc. This reduces hardware maintenance at native level. a number of IaaS vendors square measure Amazon straightforward Storage Service (S3) for information backup, Amazon Elastic Cloud Computing (EC2), Go Grid, VMW square measure etc.

A. Cloud Security:

As companies are placing more information on cloud, threats are increasing about the safety of environment. Security and data protection are one of serious concern in cloud development and adoption. Restricted manipulation on data can cause miscellaneous security problems which include data outflow, unprotected interface, resource sharing, data availability and inner attacks [9]. As all aware cloud is increasingly accepted, but still people have certain confusion in their mind that their data might not be secure at other end. Security in cloud computing is one of big matter because equipment used to deliver services does not own by users. The consumers have no authority, nor any knowledge of, what is happening with their data. Service Provider Layer have various security concerns some of them are Data transmission, Privacy, People and Identity, Audit and Compliance, integrity and Binding problems. Security difficulties faced by Virtual Machine Layer are VM Escape, VM Sprawl, Insecure VM migration, Malicious VM Creation, Cloud legal and Regularity complains Identity and Access management. Data Centre are vulnerable to different type of attack at Physical and Network level.

B. Overview of Trust is a social problem:

There are lots of definitions of trust. Basically trust refers to confidence or belief of one entity on other. One cannot build trust in a day. It is normally based upon provider's position in market. As users are putting their resources on provider's datacenters so there is major concern about the trustworthiness of providers and services. Two parties are

DOI:10.32377/cvrjst1217

involved in any trusted relationship: one is trusting party (i.etrustor) and other party to be trusted (i.e trustee) [1-5], [7]. Various risks are involved: location security risk, data disclosure problem, data misplacement issue, data investigation concern. In cloud environment hostile user can add malicious code and take CPU space, resources and time. To model attractive cloud computing, trust should be introduced and there should be some trustworthy regions where users can deploy their applications and use resources safely.

II. Related Work

Trust is one amongst the foremost involved problems for the acceptance and growth of cloud computing. Though many solutions are expected recently in managing trust feedbacks in cloud environments, the way to confirm the believability of trust feedbacks is generally neglected. During this project the system projected a Cloud Armor, a reputation-based trust management outline that gives a collection of functionalities to deliver Trust as a Service (TaaS). "Trust as a Service" (TaaS) framework to enhance ways in which on trust management in cloud environments. The approaches are valid by the epitome system and experimental results. Here, it provides some drawbacks are, it's common that a cloud service involvements malicious behaviors from its users, it's undecided whether or not they will trust the cloud suppliers, It not convincing enough for the customers, SLAs don't seem to be consistent among the cloud suppliers albeit they provide services with similar practicality, Customers don't seem to be certain whether or not they will establish a trustworthy cloud supplier solely supported its SLA. During this project the system projected a Cloud Armor, a reputation-based trust management framework that gives a collection of functionalities to deliver Trust as a Service (TaaS). "Trust [11], [12] as a Service" (TaaS) framework to enhance ways in which on trust management in cloud environments. specifically, the system introduce associate degree adaptation believability model that distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers' capability and majority agreement of their feedbacks. The approaches are valid by the epitome system and experimental results. The system proposes a framework mistreatment the Service orientating design (SOA) to deliver trust as a service. Here it includes some edges are, It not solely preserves the consumers' privacy, however conjointly permits the TMS to prove the believability of a selected consumer's feedback, It conjointly has the flexibility to discover strategic and occasional behaviors of collusion attacks, Load equalization techniques are exploited to share the employment, thereby invariably maintaining a desired accessibility level, This metric exploits particle filtering techniques to exactly predict the provision of every node, Cloud Armor exploits techniques to spot credible feedbacks from malicious ones.

III. Proposed System

A. Trust Management

Long back, Trust applied in scientific correction for constructing individual association and currently it's necessary additional for forming security device in distributed computing atmospheres. Trust management has several security qualities like dependableness, irresponsibleness, self-assurance, honest, belief, honesties, security, ability [8]. There are 2 variations of trust 1) trust and 2) Indirect Trust [8]. Trust is predicated on personal expertise and indirect trust state that once anyone has no any direct knowledge then he's have faith in others trust. This kind of trust is implicit indirect Trust. In cloud setting varied service supplier is obtainable. Hence, it's vital to spot trustworthy service dealer. Trust is advanced relationship among totally different cloud unit and since trust is additional particular, context dependent, non-rhombohedra and inexact. There are varied ways that of analysis of trust. In e-commerce sector, we will measure the trait by feedback submitted by cloud users. Once trust is calculated supported feedback scores of cloud users there could probability varied feedback base attacks. Next section need the assorted attainable attack on reaction primarily based trust evaluation.

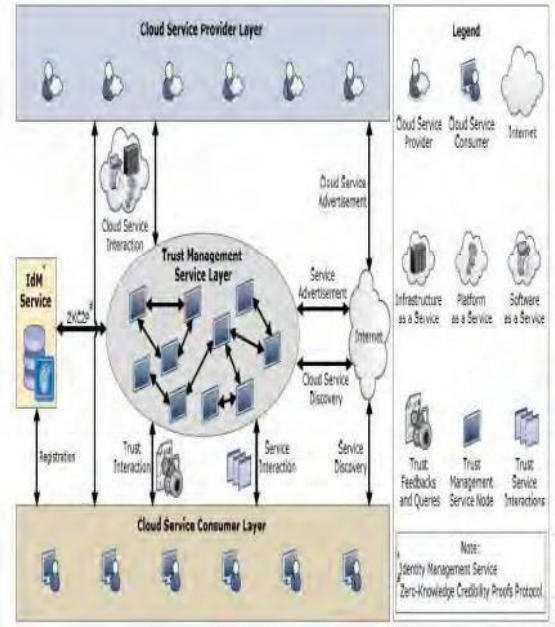

Figure 1. System architecture

B. Implementation

i. User Registration:

Users are the important entities in our scheme. Initially the user wants to register their credentials in the corresponding system. These credentials are including some personal information about users like, name, date of birth, address, contact number etc... This personal information is stored in Identity Management Services. This acts like a database in this manner. After this registration only, the user can use all the services provide from cloud. But this information is

DOI:10.32377/cvrjst1217

stored very securely. We need to protect the user's privacy from unauthorized activities.

ii. Upload Services:

Cloud service provider is responsible for provide useful services to the user. Their services are classified into three categories. These are, Infrastructure As a service, Platform As a Service, Software As a Service. Under these three categories, the CSP upload the services for users. These details are stored in Identity management Service. Services detail information shown in Figure 3.

iii. Send Feedback:

After uploading the services, the user can use these services from the cloud. To use these services, the user needs to store their credentials in IDM services. Then the user can share their opinion to the cloud regarding to the services, shown in Figure 4. This feedback also stored in the identity management Services. This IDM service sore the user details and product details as shown in the Figure 2, according to their feedback service.

iv. Feedback Collusion Detection:

Trust Management Service is the one, which use all the details stored in the IDM for check the user's credibility. Users have a limit to send the feedback for a service. There is a threshold value for that. If they cross the limit, we can identify if they are trying to increase/decrease the service rate. Suppose they cross the limit, the trust management service separate them from the users list. This process is called as feedback collusion detection.

v. Sybil Attack Detection:

Some users are very brilliant. Because they know, if we cross the limit, we would catch. So they use the different accounts for increase/decrease the service rate. In our system, their credentials also stored in identity management service this record are viewed by trust management service. Our TMS service cross checking the user's credentials. Some credential of user's are cannot to change like date of birth, mobile number, mail id. Using that similarity, the TMS can found the unauthorized users. This is called as Sybil attack detection.

Figure 2. Product details

Figure 3. Services page

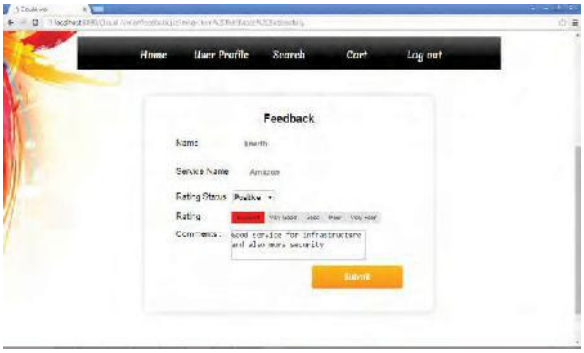

Figure 4. Feedback

IV. Conclusions

Cloud computing source many consecrations but still there are a unit many difficulties in cloud supported practice of cloud. A most tough issue that required to surrender focus in cloud computing is security and trust controlling, due to dynamic nature of cloud atmosphere, that area unit very important part of cloud security. Once trust result appraised by responses of cloud user then there may chance of malicious feedback submission. It is significant to identify the feedback base attacks as a outcomes of less submission of fake feedbacks might negotiation the entire trait of service provider. In future, we'd wish to hunt down the other gettable attacks on feedback collection, feedback analysis and account the thanks to forestall and notice those attacks efficiently by strong trust model.

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.

DOI:10.32377/cvrjst1217

[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] 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.

[6] 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.

[7] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Proc. of TrustCom'11, 2011.

[8] K. Hoffman, D. Zage, and C. NitaRotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, vol. 42, no. 1, pp. 1– 31, 2009.

[9] Lina Yao Quan Z. Sheng Zakaria Maamar, Achieving High Availability of Web Services Based on A Particle Filtering Approach, 2012

[10] 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.

[11] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Proc. of TrustCom'11, 2011.

[12] Sheikh Mahbub Habib , Sebastian Ries y, Max M• uhlh• auser, Towards a Trust Management System for Cloud Computing.

DOI:10.32377/cvrjst1217