International Journal For Technological Research In Engineering *ISSN (Online): 2347 - 4718*
International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS - November 2016)

TOWARDS A SECURE AND DEPENDABLE CREDIBILITY-BASED TRUST MANAGEMENT SYSTEM IN CLOUD

S.Nagalakshmi[1], Dr.Rakesh Poonia[2]
[1]Research Scholar, Dr Ambedkar Institute of Technology
[2]Asst. Prof. Dept. of Computer Application, Govt. Engg. College, Bikaner

Abstract: ***An urban development vision for a smart city makes it necessary to integrate multiple Information and Communication Technology (ICT) and Internet of Things (IoT) solutions in a secure fashion to manage a city's assets. Cloud plays an important role in building a smart city to preserve privacy data of the users. Trust administration is a standout amongst most of the difficult issues for the reception and development of distributed computing. A dynamic, dispersed, and non-straightforward administration of cloud presents a testing issue, for example, protection, security, what's more, accessibility. Buyers' protection is not a simple undertaking because of the sensitive data included in the co-operation whilst consumers and the trust administration. Ensuring cloud administrations against their malevolent clients is a troublesome issue. Ensuring the accessibility of the trust administration is another noteworthy test in view of the dynamic way of cloud situations. This paper portrays the configuration and execution of Cloud Armor, a reliability based trust administration structure that gives an arrangement of performance to convey Service as a Trust (TaaS), which involves firstly, unique convention that demonstrates a user security protection and validity of trust inputs, secondly, versatile and powerful believability model that evaluates believability of trust inputs to save cloud service from malevolent clients and analyze a trust dependability of cloud, and lastly, deal with accessibility of distributed usage of certainty maintenance work by availability model. The possibility and advantages of the policies concentrates on utilizing an accumulation of genuine trust criticisms on cloud administrations.***

Keywords: Cloud Computing, Dispersed, Believability, Reliability, Security, Trust.

I. INTRODUCTION

Cloud computing has turned into an unmistakable worldview of processing and IT administration conveyance. The vast productive, dispersed, and nontransparent type of cloud services makes the trust administration in cloud situations a significant challenge [2], [3], [4], [5]. The best origin to estimate the overall truthfulness of cloud services is through customer's feedback. Several analyses identified the value of trust authority and developed resultsto estimate and maintain the faith based on inputs gathered from end users. In practice, it is general that a cloud service encounters malevolent intrusion from its clients. Hence focuses on the upgrading of trust organization in cloud surroundings by introducing few methods to deal with the believability of trust feedbacks.

Some of the key challenges of the trust authority in cloud environment are:

Consumer's Privacy: The dynamic collaboration between cloud providers and consumers may contain sensitive data. There are a few instances of protection ruptures, for example, breaks of sensitive data. Its service responsibility to secure the privacy of the consumer data.

Cloud Services Protection: The cloud services regularly experiences the attacks from its user's. Usually, the cloud services are misled by the attackers by providing ambiguous inputs (i.e. Collusive attack) or by creating a huge number of accounts (i.e. Sybil attack).

Trust Mainframe Service's Availability: A trust management service acts a bridge between the buyers and cloud services for viable trust administration. TMS is a severe problem for availability guaranteeing due to the huge count of users and the highly dynamic quality of the cloud status. Methods that need a considerate of consumers demand and proficiency through similarity measurements or operational availability measurements are not appropriate in cloud nature. TMS ought to be versatile and exceptionally adaptable to be practical in a cloud environment.

The rest of the paper is organized as follows. Section 2 describes the related work. Section 3 shows the problem statement. Section 4 gives outline of proposed system. Section 5 presents the design of the trust management framework respectively. Section 6 reports the models of the system. Finally, Section 7 outlines the implementation of the system and Section 8 provides conclusion.

II. RELATED WORK

Mohamed Nabeel and Elisa Bertino [7] proposed various sparse advantages of distributed computing; various associations have been considering moving their data structure to the cloud. In any case, a basic issue visible to everyone fogs is the way by which to explicitly share information considering fine-grained quality based get to control approaches while in the meantime guaranteeing to group of the information and protecting the security of clients from the cloud. The system that quickly examines the drawbacks of methodologies in light of surely understood cryptographic strategies intending to such issue and after that involves two methodologies that address these disadvantages with various exchanges.

Ivan Damgard, JesperBuus Nielsen, and Daniel Wichs [8] proposed the system that is understood thatall around compassable multiparty be accomplished in the typical model without setup suspicions when the adversary can degenerate a discretionary sum of players. An approach to get around this issue is by hosting a reliable social gathering makes overall setup. The system exhibits work that may rather rely upon physical suppositions, and specifically carefully designed equipment tokens. And also demonstrate that, under normal cryptographic suppositions, such physical setup can be utilized to UC-understand any 2 gathering and multiparty estimation in the nearness of a dynamic and versatile enemy adulterating any count of players

C. Dellarocas [10] proposed a reputation that exhibits a huge impact that cloud service clients have over the trust mainframe system, the ideas of the several cloud consumers can drastically impact the position of a cloud benefit either positively or negatively.

I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad [9] proposed a methodology for consistency administration in cloud surroundings to build up trust between several parties. The methodology is created using a consolidated structure and uses compliant administration approach to establishing trust among the cloud consumers and cloud suppliers.

Kan Yang and XiaohuaJia [5] proposed the system in distributed computing, data mortgage holders have their data on cloud servers and information shoppers will get to the data from cloud servers. As a delayed consequence of the information outsourcing, regardless, this new perspective of learning encouraging advantage moreover exhibits new security issues, which needs relating independent investigating administration to decide the data respectability within the cloud. A current remote respectability verifying the systems can exclusively serve for static file and, along these lines, can't be connected to the reviewing benefit subsequent to the data inside of the cloud are regularly powerfully upgraded. Subsequently, temperate and secure component reviewing convention is craved to change over data mortgage holders that the data range unit legitimately hangs on in the cloud. Functional and security ensuring assessing tradition were proposed to give data respectability.

III. PROBLEM STATEMENT

The Problem Statement of the framework address the issues of ensuring the accessibility Trust Management Service is a troublesome issue because of the uncountable sum of consumers and the type of cloud status is highly dynamic. Another issue is caused by the malicious consumer which can mislead the cloud services reliable by collusion attack and by Sybil attack. The cloud service can also be damaged by other attacks such as self-promoting and slandering attack.

IV. PROPOSED SYSTEM

The Proposed framework helps the consumer and cloud service provider to overcome the issues using simple techniques. The feedback of the cloud service consumers is a positive origin to measure the truthfulness of whole cloud service. Some of the novels approach that supports in identifying the reliability-based intrusions and permitting consumers to adequately recognize authenticate cloud services. The false trust feedbacks are identified from Collusive attacks using credibility model and also detects the Sybil attack. The trust administration service at the desired level is maintained using availability model.

V. THE TRUST MAINFRAME SERVICE FRAMEWORK

The Trust Mainframe Service structure is resolved as a Web utility known as Cloud Armor, constructed to develop a user-friendly cloud environment for both cloud consumer and for cloud suppliers. This structure is established on the service-oriented architecture (SOA), which convey service as a trust (TaaS). The trust management architecture spreads various scattered nodes that establish compound so that clients can give their comments or can check the trust outcomes. Fig 1states the architecture, It consists of 3 unique layers, specially the "Cloud Service Supplier Layer, the Trust Mainframe Service Layer, and the Cloud Service user Layer".

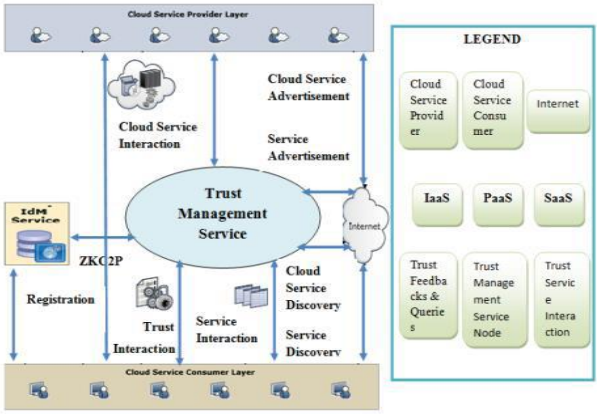

Fig 1 Trust Management Framework

The Cloud Service Supplier Layer: It offers one or more cloud services such as IaaS, PaaS, and SaaS openly on the web. These cloud assistance are available through the internet and tabulated on the web platform. Considered the Collaborations of this layer as cloud service communication with clients and trust mainframe service, and cloud services publicity where suppliers are able to promote their services on the web.

The Trust Mainframe Service Layer: The different nodes are disposed of in the various cloud environments. These nodes act as an interface for the user to share their feedbacks and investigate about the trust outcomes in a dispersed way. It also includes some of the interactions such as cloud service interaction, service promotion, cloud service discoveries and ZKC2P enables TMS to prove user's feedback credibility.

The Cloud Service User Layer: It includes various consumers who use cloud services. This layer includes some of the interactions such as service discovery, trust, and services interaction where users can view the trust result and can give their feedback about a specific cloud service and

registration where users need to register with IdM before using trust administration service.

The Structure of the Trust Mainframe Service represents the performance of the "web crawling" technique for automated cloud service discovery in the online and saved in the cloud service repository. One more benefit of the framework is it contains IdM service in which the user needs to register before using Trust Management Service.

The Cloud Service User Layer: It includes various consumers who use cloud services. This layer includes some of the interactions such as service discovery, trust, and services interaction where users can view the trust result and can give their feedback about a specific cloud service and registration where users need to register with IdM before using trust administration service.

The Structure of the Trust Mainframe Service represents the performance of the "web crawling" technique for automated cloud service discovery in the online and saved in the cloud service repository. One more benefit of the framework is it contains IdM service in which the user needs to register before using Trust Management Service.

VI. SYSTEM MODELS

The system construction and the implementation of cloud reliability-based trust administration system ("Cloud Armor-Cloud consumer's credibility Assessment & trust management of cloud services"). A structure for integrity-based trust management in a cloud administration environment the trust is expressed as a service (TaaS) where TMS traverses several dispersed nodes to control criticisms in a decentralized way.

Cloud Armor exploits strategies to distinguish trustworthy comments from mischievous ones. The notable components of Cloud Armor are:

Zero-Knowledge Credibility Proof Protocol (ZKC2P): The ZKC2P protocol protects the customer's confidentiality and also empowers the TMS to demonstrate the trustworthy of a specific clients input. The Identity management service (IdM) is introduced to support the TMS in assessing the integrity of trust inputs rupturing customer's protection. Anonymization methods are misused to shield consumers from protection ruptures in user's personal identity or connections.

A Credibility Model: The reliability of inputs plays an imperative part in the trust administration service's performance. Several measurements for the criticism collision detection including the "Feedback Density" and "Occasional Feedback Collusion". These measurements recognize ambiguous comment from the nasty consumers. It also has the capacity to identify strategic and occasional behaviors of collusion attack. It also presents several measurements for the Sybil attacks recognition the "Multi-Identity Recognition" and "Occasional Sybil Attacks".

An Availability Model: The important pre-requisite for the trust administration service is high availability. Thus, it also presents several distributed nodes that are spread in a decentralized way to manage comments given by clients.

A. Assumptions and Attack models

The two assumptions are made. Firstly the trusted third party is handling the TMS and secondly, the communication of TMS is secure because here the concept of securing communication is not focused. Consider the following types of attacks

Collusion attack: Several malicious users are gathered together to give huge number of mischievous feedbacks to increase or decrease the growth of the cloud service trust. This form of attack is also known as collusive attack. Another way of attacking is by using Non-collusive, where specific malevolent consumer gives sum of comments to increase or decrease the growth of cloud trust.

Sybil attack:This attack arises when a single user creates a multiple attack for giving multiple misleading feedbacks on cloud service to affect the trustworthy. If the malicious user tries to download the file more than a restricted times then the Sybil attack will be occurred.

VII. SYSTEM IMPLEMENTATION

Section describes the system implementation and algorithms used in approving the proposed approach. The execution and examinations were produced to accept and think about the execution of both reliability model and the availability model. The platform provides an environment where consumers can give their inputs and request trust evaluation for a specific cloud service. Particularly, the two main components of trust management service (TMS) are "Trust Data Provisioning" and the "Trust Assessment Function".

The Trust Data Provisioning: The responsibility of this element is to collect the trust information and cloud services. The Trust Feedbacks Collector module developed to gather the inputs straightly from clients as history records and saved in the Trust Feedback Database. Firstly, the users must build up their details for the first time when they attempt to utilize the platform through enrolling their credentials at the Identity Management Service (IdM) which stores the information in the Trust Identity Registry. The Identity Info Collector module has developed to gather the aggregate total of established identities among the entire identification behavior.

The Trust Assessment Function: This work is responsible for taking care of trust assessment demands from clients where the reliability of cloud assistance is compared and the factors of trust feedbacks are calculated. The Trust Assessor was developed to compare the trustworthiness of cloud services through requesting the totaled elements weights from the aspects calculator to measure the feedbacks and then count the mean of all comments given to each cloud service.

A. Algorithms Used

The Algorithms that used for the implementation of these modules are listed below along with the procedures.

Particle Filtering Algorithm
This algorithm is mainly used to filter the repeated feedbacks given to a cloud service. This can be done by calculating the weights of each feedbacks trust and resampling technique is performed

Input: The communication of data between consumer and TMS instances.
Output: The replications of the feedbacks are reduced and resampling is performed.
Step 1: Initialize the weights based on the feedback replicas.
Step 2: Generate several set of particle and spread the weights to each particle set based on the priority of weights.
Step 3: Resampling of several particles are performed in the set using weights of each particle.
Step 4: Creates the new set and assign the weights based on possibility of total number of replicas.
Step 5: Estimates the probability of the threshold based on the availability.
Step 6: Recalculate the weight of particle based on the possibility of the TMS feedbacks and calculate the current availability then filters the particle replicas.
Step 7: Go to step 3 and step 4then repeat the iteration.

Credibility weights caching and Trust Results Algorithm

This algorithm is mainly used to calculate the trust of the whole inputs given to the cloud service and stores the trust outcomes in separate caches for consumer and cloud service using credibility weights algorithm.

Input: The user requesting for trust results and giving feedbacks about the cloud service.
Output: Two caches are generated for maintaining the trust results and credibility weights.

Step 1: TMS instances sums up the whole number of trust inputs given by the new specific users.
Step 2: Regulates whether the re-calculation is necessary for integrity component related to the consumers.
Step 3: Computing both the cloud service and end users cache.
Step 4: TMS instances sums up the whole sum of trust inputs given by the cloud server.
Step 5: Regulates whether the re-calculation is necessary for reliability factor related to the cloud server involving the trust outcomes.
Step 6: Computation is repeated again.

Instance Management Algorithm
This algorithm is mainly used to reallocate the original feedbacks that are triggered by the cloud server.

Input: The number of affected feedbacks in the cloud server.
Output: The feedbacks that are triggered in the cloud server can be reallocated.
Step 1: Initialize TMS instance 0 and compute the operation for all TMS nodes.
Step 2: The TMS 0 estimates the N particle set of Trust mainframe service and creates additional TMS nodes if necessary.
Step 3: Predicts the TMS instance 0 which provides new availability threshold of all TMS nodes based on Algorithm 1.
Step 4: The TMS instance 1 determines replications and create reduplication for each trust administration service nodes.
Step 5: Instance 0 begins caching result on consumer side and TMS instance s begins caching result at server side based on Algorithm 2.
Step 6: All the TMS nodes of server updates the frequency table.
Step 7: Instance 0 checks whether the workload 1of the TMS instance is provoked by any TMS before reallocation.
Step 8: If the TMS instance is triggered go to next step otherwise go to step 3.
Step 9: TMS instance 0 asks TMS instance server s which triggered the workload of the TMS to re-locate all the trust inputs of the cloud server that has the lower feedback and the new trust inputs given to specific cloud server and another TMS instance s has the lowest trust feedbacks of TMS, perform step 6.
Step 10: TMS Instance 0 computes functions for all the trust mainframe service node check whether workload 2 of the TMS is triggered for any instance s after reallocating.
If the Op is greater than workload of TMS and server trust feedback is greater than mean value of trust result then go to step 2, otherwise go to step 3.

VIII. CONCLUSION

Cloud administration user's input is a decent source for evaluating the whole cloud administrations trustworthy. The malicious end users cooperate each other i) By providing several misleading trust feedbacks makes disadvantage for cloud service or ii) By creating several number of accounts and trapping the clients to trusting cloud service that is not really trustworthy and providing the feedbacks that mislead the users about trust. The novel approaches are developed by the proposed system is used to support in identifying the reputation-based attacks and permitting clients to viable recognize reliable cloud service. Specifically, the credibility models not only distinguish deluding trust inputs from collusive attacks but also distinguish Sybil assaults regardless of the attacks that occur in a long or short time period. An availability model also built up at desired level to manage trust management service. Several trust feedbacks are gathered to valid the proposed system. The exploratory results exhibit the applicability of the methodology used and demonstrate the ability to identify such malicious practices.

IX. FUTURE SCOPE

In future, the experimental outcomes are used to consolidate the various administrations of trust strategies such as recommendation and notoriety to boost the credit results in efficiency. Another focus is on performance optimization.

REFERENCES

[1] Talal H. Noor, Quan Z. Sheng, Lina Yao, SchahramDustdar, and Anne H.H. Ngu, "Cloud Armor: Supporting Reputation-based Trust Management for Cloud Services", in IEEE Computer Society, vol. 27, no. 02, pp. 367-380, 2016.

[2] S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud Trust Management for Hadoop," in Proc. CLOUD'12, 2012.

[3] 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.

[4] J. Huang and D. M. Nicol, "Trust Mechanisms for Cloud Computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.

[5] Kai Hwang, Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", in IEEE Internet Computing, vol. 14, no. 05, 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] Mohamed Nabeel, Elisa Bertino, " Privacy Preserving Delegated Access Control in Public Clouds", in IEEE Computer Society, vol. 26, no. 09, pp. 2268-2280, 2014.

[8] Ivan Damgard, JesperBuus Nielsen, and Daniel Wichs, "Universally Composable Multiparty Computation with Partially Isolated Parties", in the theory of cryptography, vol. 5444, pp. 315-331.

[9] Kan Yang, XiaohuaJia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", in IEEE transaction on Parallel and Distributed Systems, vol. 24, no. 09, pp. 1717-1726, 2013.

[10] R. Koetal., "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in Proc. SERVICES'11, 2011.

[11] T. H. Noor and Q. Z. Sheng, "Trust as a Service: A Framework forTrust Management in Cloud Environments," in Proc. of WISE'11, 2011.

[12] T. H. Noor, Q. Z. Sheng, A. H. Ngu, A. Alfazi, and J. Law, "CloudArmor: A Platform for Credibility-based Trust Management of Cloud Services," in Proc. of CIKM'13, 2013.

[13] T. Noor and Q. Z. Sheng, "Credibility-Based Trust Management for Services in Cloud Environments," in Proc. of ICSOC'11, 2011.

[14] 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.

[15] 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.

[16] C. Dellarocas, "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms," Management Science, vol. 49, no. 10, pp. 1407–1424, 2003.

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

