ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Eminence Administration System in a united cloud - A Survey

[1] Poralla Mounika, [2] Dr. Shirina Samreen, [3] Dr. G. Vishnu Murthy
[2] Professor, [3] Professor, HOD
[1][2][3] Dept. of CSE, Anurag Group of Institutions, Hyderabad, T.S., India.

Abstract: In the Infrastructure as a Service (IaaS) prototype of cloud computing, computational assets are accessible for lease. Even it presents a price effective answer to indirect system specifications, low trust on the leased computational assets avoid the clients from using it. To reduce the price, computational assets are distributed, i.e., there exists multi-inhabitancy. As the translating medium and other computational assets are distributed, it makes security and privacy issues. A client may not recognize the co-inhabitant as the clients are unknown. The client relies upon the Cloud Provider (CP) to relegate dependable co-inhabitants. Cloud Provider's (CP) interest that it gets maximum utilization of its assets. Cloud Provider permits greatest co-occupancy independent of the practices of client. A powerful eminence administration system motivates the cloud provider's in a united cloud to distinguish the great and harmful clients and allocates the assets in such a way that they do not share the assets. The study provides the accuracy and the proficiency of the eminence administration framework using exact and trial investigation methods.

Index Terms—Virtual network embedding, United cloud, Eminence, Trust, Multi-inabitancy

INTRODUCTION

In this article of A Powerful Eminence Administration System in the United Cloud the main aim Is to evaluate to eminence of the cloud provider and this eminence administrator mechanism encourages cloud provider in united cloud to differentiate good co-tenant bad cotenant and assign resources in such a way that they do not share the resources with co-tenants for this to calculate the analysis we are using analytical method and experimental analysis.

Due to the distributed nature of computational assets resulting in multi-inhabitancy in a cloud, there may be harmful co-tenants. To address the said issue a Eminence Administration System to access the trust metric so as to distinguish great and harmful clients in a united cloud is proposed and to be developed.

Cloud computing is internet based computing which enables sharing of resources. Many clients place their data in the cloud. Correctness of data and security is a prime concern. The problem is ensuring the integrity and security of data storage in Cloud Computing. Security in cloud is achieved by signing the data block before sending to the cloud. Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance.

Enabling the public audit ability for cloud storage is of critical importance so that clients can resort to a Third Party Auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user.

Eminence Administration System:

Eminence Administration System is developed so as to encourage the cloud providers for an accurate segmentation among great and harmful clients so as to ensure good co-inhabitant to good clients

Informally the Eminence Administration System is as follows:

1) There is a finite number of Cloud Provider's(CP) and a finite number of clients. It is assumed that each CP hosts virtual network request from all users. There are three types of CPs,

(a) Rational CP,

(b) Irrational CP and

(c)Opportunistic CP.

There are two types of users,

(a) Great Client: one who does not cause any security or privacy issues and

(b) Harmful Client: one who causes security and privacy issues.

2) a) each CP labels each client as either a good client or a malicious client.

b) It assigns virtual resources to the client.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

c) The clients are partitioned in groups such that in each group all clients share resources with each other, i.e., they are multi-inhabitant.
d) Each CP announces partitions over the clients, i.e., they announce the multi-inhabitant information to the Eminence Administration System(EAS).
3) Next, CPs monitor activities of the clients and report it to the EAS. A CP can either provide a positive or a negative vote for a client. It will be assumed that the united cloud infrastructure will provide the EAS with the means of communication with the individual CPs and using such communication channels CPs regularly provide feedback to the EAS.
The rest of the paper is structured as follows: In Section II, survey report. A comparison of surveyed in Eminence Administration System in a United cloud and concludes the paper and discusses several open research issues in section III.

II. LITERATURE SURVEY

This section is a brief review of the research papers to address various trust challenges and solutions. This is done by conducting survey by the various research papers.

Related Work:

2.1. Deployment of intrusion detection system in cloud.

According to Varun Mahajan and Sateesh K Peddoju [1] The main aim of deployment of intrusion detection system is to detect various attack patterns.
This survey mainly focus on deployment of signature based IDS (Intrusion Detection System) for detection of intrusion at network level and cloud VM instances.
IDS discusses the flow of traffic in provider and self service provider network architecture in open stack environment and use of port mirroring to detect intrusion. To protect the cloud infrastructures from outside and inside attackers the Intrusion Detection System (ISD) both Network IDS and Host IDS, play an important role.

Intrusion Detection System (IDS):

The IDS combined with firewall policies, access control list and data security methods can provide security to cloud environment.
The security of the cloud environment revolves around the ability of the administrator at various levels to deal with the kind of attacks without affecting the performance of the cloud.There are various IDS techniques that can be adopted to generate alerts for specific attacks and the cloud administrator can take necessary mitigation steps.

There are various types of IDS techniques such as Signature based detection, anomaly detection methods and Soft Computing Methods such as Artificial Neural Networks, Fuzzy logic, Support Vector Machines (SVM), Generic Algorithm (GA) etc., that can be adopted to achieve the security objectives.

In cloud environment, there are critical network, host and hypervisor components where intrusion can occur.

1) Network Intrusion Detection System(NIDS):

The NIDS is used to detect network level intrusion by comparing the current behavior with the observed behavior. It can use signature and anomaly based methods.
SNORT and suricatare are well known opens source tools for signature based network intrusion detection.

2) Host Intrusion Detection System(HIDS):

The HIDS is used for file integrity checking, log monitoring, root kit detection and generate active response to the alerts generated at the host level. It can be used to detect intrusion in nodes, hypervisors and VM instances in virtualized cloud environment.
Open Source Security Event Correlator (OSSEC) is an open source server-client based HIDS that can be used in cloud with emphasis on the tenant security.

3) Hypervisor Intrusion Detection System:

This type of IDS runs at the hypervisor layer to monitor communication between VMs, hypervisor, VMs and virtual network.
VM introspection (VMI) is an example of hypervisor based IDS technique.

Open Stack Traffic and Networking Details:

To determine the deployment of NIDS in cloud environment, it is important to understand traffic and networking architecture.
The Open Stack environment traffic can be classified into three types:

1) External Traffic:

The external traffic is the traffic flowing from VMs in the tenant network of each Compute Node to the outside world and through the Network/ Controller node at the front end.

2) Internal Traffic:

The internal traffic is traffic flowing from VMs within the Compute Node via physical switch connected between the front and back end.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

3) Local Traffic:

The traffic flowing within VMs of the tenant network in each of the Compute Node through the Open v Switch/Linux Bridge is the local traffic.

The basic networking details of Open Stack Network (neutron) with Linux Bridge and Open v Switch that can be used for intrusion detection at network level.

2.2. Trust in cloud computing

Albert S. Horvath III and Rajeev Agrawal [2] did a survey to measure consumer trust in cloud computing. What they found is that consumers trust cloud computing more than they admit to even themselves. They trust only to the extent that the risk is perceived to be low and the convenience payoff for them is big. [2] examines the issues surrounding the difficulty of the average Internet user to trust cloud service providers with the security of their data. By examining user sentiment they attempt to outline the scope of the problem and suggest how cloud service providers may overcome trust issues. [2] explore the issues of consumer trust in cloud computing by conducting a survey to establish consumer sentiment on trust issues in cloud computing. Finally, [2] analyze the survey results in a way that will be useful for cloud service providers to assess their approach towards customers and make changes.

The investigation into trust in cloud computing has shown several interesting trends.

- Users do not trust current systems
- The government cannot fix trust issues
- Education is key to trust
- Trust cannot be purchased

2.3. Determining service trustworthiness in inter-cloud computing environment

Jemal Abawajy [3] did a survey on determining service trustworthiness in inter-cloud computing environment. He presented a distributed reputation based trust Management System. This survey was carried out by means of determining the service robustness in cloud computing entities.

Here the main aim of the federated cloud computing is to increase ubiquitous and pervasive computing, which needs to access and maintain the robustness of the cloud computing utilities.

A fully distributed framework that enables interested parties to determine the robustness of federated cloud computing entities.

In inter cloud computing, users and computational agents and services often interact with each other without having sufficient assurances about the behavior of the resources they entrust their date and applications with. There is often insufficient information for deciding which resources to use.

Another key problem associated with the formation and operation of inter cloud computing is that what kind of information to collect and how to specify and enforce community trust.

2.4. Establishing trust in hybrid cloud computing Environments

Jemal Abawajy[4] did a survey for Establishing trust in hybrid cloud computing Environments. He presented a distributed reputation based trust management system for hybrid cloud computing system. Establishing trust for resource sharing and collaboration has become an important issue in distributed computing environment. [4]investigated the problem of establishing trust in hybrid cloud computing environments. [4] present a fully distributed framework that enable trust-based cloud customer and cloud service provider interactions. The framework aids a service consumer in assigning an appropriate weight to the feedback of different raters regarding a prospective service provider. Based on the framework, we developed a mechanism for controlling falsified feedback ratings from iteratively exerting trust level contamination due to falsified feedback ratings. The experimental analysis shows that the framework successfully dilutes the effects of falsified feedback ratings, thereby facilitating accurate and fair assessment of the service reputations.

2.5. A Trust Management Model to Enhance Security of cloud computing Environments.

Xiaodong Sun and Guiran Chang[5] did survey on A Trust Management Model to Enhance Security of cloud computing Environments. They introduced TMFC including direct trust measurement and computing, connecting and trust chain incorporating where the issue of recommended trust similarity has been addressed to prevent the behavior of associated cheat of middle nodes. The content of research could be summarized as follows: First, A formal model TMFC was proposed where direct trust was firstly classified into two typed due to the differences on their own trust assessment attributes whose degree was all expressed as the subjective trust valuation set. They equipped the proposed TMFC construction with the new definition of trust according to the natures of cloud systems and way addressing trust evaluation similarity exposed by malicious middle nodes;

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

2.6. Hysteresis-based Robust Trust Computing Mechanism for Cloud Computing

Mohamed Firdhous and ALT [6]developed Hysteresis-based Robust Trust Computing Mechanism for Cloud Computing that computes the trust scores for a cloud computing system based on any QoS parameter.

The proposed mechanism computes the trust scores using a non linear hysteresis function that can be in more than one state at any given time. The hysteresis function makes the trust computing mechanism more stable due to its special properties, such as the shape, the large input range and inherent memory.

The proposed system has been tested using simulations and the results were compared against that of entropy based mechanism.

2.7. Trust-oriented Research Methods in Cloud Environment

Yan Wan, Jiantao Zhou[7] developed Trust-oriented Research Methods in Cloud Environment. According to [7] there is a challenges in cloud environments is trust crisis and its influence on the development of cloud computing. For that [7] analyzes the similarities and differences between cloud computing and other distributed environments.

[7] proposes the concept of trust and three different directions of trust-oriented research in cloud environments, and analyzes difficulties and hot spots for trust-oriented research in cloud environment.

2.8. Financial Option Market Model for Federated Cloud Environments

Adel Nadjaran Toosi and et al.[8] developed Financial Option Market Model for Federated Cloud Environments. According to [8] to maintain Quality of Service (QoS) to customers who reserve the resources in advance and may or may not be using the resources at a future date makes the resources wasted, if not allocated to other on-demand users. Therefore, a need for a mechanism to guarantee the resources

to reserved users whenever they need them, while keeping the resources busy all the time is in very high demand.

The concept of federation of Cloud service providers has been proposed in the past wherein resources are traded between the providers whenever need arises.

[8] propose a financial option based

Cloud resources pricing model to address the above situation. This model allows a provider to hedge the critical and risky situation of reserved users requesting the resources while all the resources have been allocated to other users, by trading (buying or outsourcing) resources from other service providers in the Cloud federation. using financial option based contracts between Cloud providers in a Cloud federation, providers are able to enhance profit and acquire the needed resources at any given time.

It would also help creating a trust and goodwill from the clients on the Cloud service providers by less number of QoS violation.

2.9. Developing Trust in Large-Scale Peer-to-Peer Systems

Bin Yu and et al.[9] developed Developing Trust in Large-Scale Peer-to-Peer Systems. According to Bin Yu and et al.[9] paper discusses the design of reputation mechanisms and proposes a novel distributed reputation mechanism to detect malicious or unreliable peers in P2P systems.

It illustrates the process for rating gathering and aggregation and presents some experimental results to evaluate the proposed approach and also it considers how to effectively aggregate noisy (dishonest or inaccurate) ratings from independent or collusive peers using weighted majority techniques.

Furthermore, it analyzes some possible attacks on reputation mechanisms and shows how to defend against such attacks.

2.10. WIM: A Wage-based Incentive Mechanism for Reinforcing Truthful Feedbacks in Reputation Systems

Huanyu Zhao et al.[10] developed A Wage-based Incentive Mechanism for Reinforcing Truthful Feedbacks in Reputation Systems. According to [10] The success of current trust and reputation systems is on the premise that truthful feedbacks are obtained.

To ensure trustworthiness, incentive mechanisms are critically needed for a reputation system to encourage rational peers to provide truthful feedbacks.

They model the feedback reporting process in reputation system as a reporting game. [10] propose a Wage-based Incentive Mechanism (WIM) for enforcing truthful report in self-interested P2P networks.

Their contributions in this work are multifold.

1. Assuming peers in reputation systems are selfinterested, they model the feedback reporting problem to the reporting game.
2. They design a wage-based incentive mechanism for enforcing truthful report. Different from most existing schemes, our algorithm does not require the peers to verify the information truthfulness. The solution requires only localized wage payment scheme.
3. To gain better understanding of landscape in their scheme, initial characteristics of our scheme are investigated.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

4. They design and conduct extensive simulation evaluation and the results demonstrate clearly that our scheme enforces the truthful report and renders lying costly.
They design, implement, and analyze incentive mechanisms and players' strategies. The extensive simulation results demonstrate that the proposed incentive mechanisms reinforce truthful feedbacks and achieve optimal welfare.

2.11. Robust Reputation Management Using Probabilistic Message Passing

Erman Ayday and Faramarz Fekri[11] developed . Robust Reputation Management Using Probabilistic Message Passing. According to [11] In a typical reputation management system, after each transaction, the buyer (who receives a service or purchases a product) provides its report/rating about the quality of the seller for that transaction. In such a system, the problem of reputation management is to compute two sets of variables:
1.The (global) reputation parameters of entities who act as sellers, and
2.The trustworthiness parameters of the entities who act as the raters (i.e., buyers).[11] introduce an iterative probabilistic method for reputation management. The proposed scheme, referred to as RPM, relies on a probabilistic message passing algorithm in the graph-based representation of the reputation management problem on an appropriately chosen factor graph.
In the graph representation of the problem, the sellers and buyers are arranged as two sets of variable and factor nodes, respectively, that are connected via some edges. Then, the reputation and trustworthiness parameters are computed by a fully iterative and probabilistic message passing algorithm between these nodes in the graph. They provide a detailed evaluation of RPM via computer simulations. We observe that RPM iteratively reduces the error in the reputation estimates of the sellers due to the malicious raters.
Comparison of RPM with some well-known and commonly used reputation management techniques (e.g., Averaging Scheme, Bayesian Approach and Cluster Filtering) indicates the superiority of the proposed scheme both in terms of robustness against attacks (e.g., ballot-stuffing, bad-mouthing) and computational efficiency.

2.12. A multi-dimensional trust and reputation calculation model for cloud computing environments

Ashish Singh and Kakali Chatterjee[12] developed A multi-dimensional trust and reputation calculation model for cloud computing environments. According to [12]
The Cloud Computing (CC) is an Internet-based technology which offers a shared pool of highly available, virtualized, dynamically scalable, and configurable computing resources.
They analyze the current trust issue associated with the cloud. To enhance the trust and reputation for the cloud computing we explored a novel and effective multi-dimensional trust and reputation calculation model for the cloud computing environment. [12] present a novel multi-dimensional trust and reputation calculation model for the cloud computing, in which they integrate multiple trust factors that increase the novelty of the model. Additionally,[12] dynamically assign a weight for each trust and reputation factor using the Weighted Moving Average and Ordered Weighted Averaging (WMA-OWA) combination algorithm. The proposed model overcome the issues of the previous existing models.

III. COMPARISON AND CONCLUSION

• ***This table includes the comparision and conclusion***

TABLE: THE HIGHLIGHTING FEATURES, REQUIREMENTS AND LIMITATIONS OF THE EMINANCE ADMINISTRATION SYSTEM IN A UNITED CLOUD

Protocol	Highlighting Features	Requirements	Weaknesses/ Overheads
Varun Mahajan and Sateesh K Peddoju [1]	The signature based detection is useful for cloud administrator to detection of pattern of attacks and take mitigation step.	To detect various attack patterns there are different deployment scenarios and detection methods of Intrusion Detection System(IDS) a cloud administrator can adopt.	Need to improve the performance of IDS and various unknown attacks

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Albert S. Horvath III and Rajeev Agrawal [2]	Measures consumer trust in cloud computing		Consumers trust
Jemal Abawajy [3]	A fully distributed framework that enable interested parties determine the trustworthiness of federated cloud computing entities.	Needs mechanism for selecting trustworthy clouds to peer with and outsource applications for execution or data for storage.	problem associated with the formation and operation of inter cloud computing is that what kind of information to collect and how to specify and enforce community trust.
Jemal Abawajy[4]	Fully distributed framework successfully dilutes the effects of falsified feedback rating, thereby facilitating accurate and fair assessment of the service reputation.	There will be a need to access and maintain trustworthiness of the cloud computing entities.	One of the main challenge in reputation system is to identify false feedback.
Xiaodong Sun and Guiran Chang[5]	a trust management model based on fuzzy set theory and named TMFC including direct trust measurement and computing, connecting, and trust chain incorporating	A formal model TMFC was proposed where direct trust was firstly classified into two typed due to the differences on their own trust assessment attributes whose degree was all expressed as the subjective trust valuation set	a host of tasks remains to be done. It still have to continue working on the measurement of trust degree and further amelioratin g and improving our model.
Mohamed Firdhous and ALT (6)	Hysteresis functions are immune to small changes and hence can be used to protect the system from sporadic attacks		investigate further into the security of the system with special reference to identifying malicious requests and isolating them

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Yan Wan, Jiantao Zhou[7]	analyzes the similarities and differences between cloud computing and other distributed environment	require a service provider to provide the evidence of trusted execution	strengthen studying trust issues of each hierarchy in the cloud architecture
Adel Nadjaran Toosi and et al.[8]	using financial option based contracts between Cloud providers in a Cloud federation, providers are able to enhance profit and acquire the needed resources at any given time.	need for a mechanism to guarantee the resources to reserved users whenever they need them, while keeping the resources busy all the time is in very high demand	In this model, it did not consider strategies regarding selling options.
Bin Yu and et al.[9]	presents some experimental results to evaluate the proposed approach also it considers how to effectively aggregate noisy ratings from independent or collusive peers using weighted majority techniques.	It illustrates the process for rating gathering and aggregation	goal is to develop a robust distributed trust model for large and dynamic P2P systems and help peers manage the risk that is involved with unknown parties in large-scale P2P systems.
Huanyu Zhao and et al.[10]	A Wage-based Incentive Mechanism (WIM) for enforcing truthful report in self-interested P2P networks.	To ensure trustworthiness, incentive mechanisms are critically needed for a reputation system to encourage rational peers to provide truthful feedbacks	
Erman Ayday and Faramarz Fekri[11]	RPM iteratively reduces the error in the reputation estimates of the sellers due to the malicious raters	The proposed RPM is a robust mechanism to evaluate the quality of the service of the SPs from the ratings received from the raters.	

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Ashish Singh and Kakali Chatterjee[12]	proposed model solves the current trust issue present in the cloud as well as the model compute accurate and reliable trust value for the CS	To addresses the issues, the paper present a novel,multi-dimensional trust and reputation calculation model for the cloud computing	

REFERENCES

1. Varun Mahajan, Sateesh K Peddoju, - "Deployment of Intrusion Detection System in Cloud" Department of Computer Science and EngineeringIndian Institute of Technology Roorkee, 2017.

2. Albert S. Horvath III, Rajeev Agrawal, -"Trust in Cloud Computing" Computer Systems Technology North Carolina A&T State University, Greensboro, NC,2015

3. Jemal Abawajy,-" Determining Service Trustworthiness in Inter loud Computing Environments", Deakin University School of Information Technology, 2009

4. Jemal Abawajy, -"Establishing Trust in Hybrid Cloud Computing Environments", Senior IEEE Member School of Information Technology Deakin University, Melbourne, Australia,2011.

5. Xiaodong Sun, Guiran Chang, Fengyun Li, - "A Trust Management Model to enhance security of Cloud Computing Environments", School of Information Science and Engineering Northeastern University Shenyang, P. R China,2011.

6. Mohamed Firdhous_y, Suhaidi Hassan_, Osman Ghazali, - "Hysteresis-based Robust Trust Computing Mechanism for Cloud Computing", InterNetWorks Research Laboratory, School of Computing, Universiti Utara Malaysia, Malaysia, Faculty of Information Technology, University of Moratuwa, Sri Lanka.

7. Yan Wan, Jiantao Zhou, - "Trust-oriented Research Methods in Cloud Environment", College of Computer Science Inner Mongolia University Huhhot, China, 2013.

8. Adel Nadjaran Toosi, Ruppa K. Thulasiram and Rajkumar Buyya, - "Financial Option Market Model for Federated Cloud Environments", Cloud Computing and Distributed Systems (CLOUDS) Laboratory Department of Computing and Information Systems, 2012.

9. Bin Yu, Munindar P. Singh, Katia Sycara, - "Developing Trust in Large-Scale Peer-to-Peer Systems", in Multi-Agent Security and Survivability, 2004 IEEE First Symposium on, Aug 2004, pp. 1–10.

10. H. Zhao, X. Yang, and X. Li, "An incentive mechanism to reinforce truthful reports in reputation systems," J. Netw. Comput. Appl.,vol. 35, no. 3, pp. 951–961, May 2012.

11. E. Ayday and F. Fekri, "Robust reputation management using mprobabilistic message passing," in Proceedings of the Global Communicationsm Conference, GLOBECOM 2011, 5-9 December 2011, Houston, Texas, USA, 2011, pp. 1–5.

12. Ashish Singh and Kakali Chatterjee, "A multi-dimensional trust and reputation calculation model for cloud computing environments", Computer Science & Engineering National Institute of Technology Patna-800005 Bihar (India), 978-1-5090-5942-3/17/$31.00 c 2017 IEEE