2016 1st International Electrical Engineering Congress (IEEC 2016)
May. 13-14, 2016 in IEP Centre, Karachi, Pakistan

Hybrid Trust Model for Enhancing the Operational Trust in Cloud Computing

Muhammad Faraz Hyder[1] and Muhammad Ali Ismail[2*]

[1,2] High Performance Computing Centre, Department of Computer & Information Systems Engineering,
NED University of Engineering and Technology,
Karachi, 75290, Pakistan
[1]farazh@neduet.edu.pk, [2]maismail@neduet.edu.pk

Abstract: This paper focuses on implementation of various trust mechanisms at different layers of cloud namely physical, virtual and application to enhance the operational trust in cloud computing. The notion is to build an efficient, light weight, pragmatic hybrid trust model for cloud computing. The model proposed in this paper is combination of Certificate and Feedback based Trust models (HCFTM).

Keywords: Trust, Cloud Service, Hypervisor, OpenStack, Hybrid model

I. INTRODUCTION

Cloud computing is an emerging trend in computing and resource management. Establishing trust in cloud system is a complex and challenging problem. In cloud computing trust establishment has to be both identity and properties based due to its dynamic nature, complexity of infrastructure, automated services, application interdependencies, and diversity of stakeholders. Trust in cloud depends mainly upon two factors. One is the operational trust which deals with the operations of cloud service provider and other is automation of different mechanisms for service providers to provide trust.

Trust is a complicated term to define. There is no comprehensive definition for it. It may be defined as Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another [2]. Trusted computing is an emerging field in computing. The aim is to provide the users prof of the trustworthiness of computing services they are using. Its aim is to provide a root of trust to users using the computing facility [3]. The root of trust is the starting point in trust implementation from where the trust is started.

Primarily there are two broader categories of trust in the cloud [4]. A) Implementation of trustworthy mechanisms and tools for Cloud providers; in order to automate the process of maintaining, managing and securing their infrastructure. B) Different methods that provide support to both cloud service providers and users in establishing trust in the operations of the infrastructure by continuous assessment of its operational trust (also known as the operational trust). Operational Trust depends on many factors like scalability, adaptability, availability, reliability and resilience etc [5]. All these properties interns depend on many overlapping factors. The primary focus of this paper is the enhancement of operational trust in cloud computing via providing security mechanisms at different layers of cloud. The notion is to provide efficient and pragmatic trust mechanisms which can cater the trust requirements for cloud computing.

Rest of the paper is organized as follows: the taxonomy of cloud trust models is presented in section 2. Section 3 discusses OpenStack Cloud deployment. Section 4 presents the proposed trust model. Trust implementation at the Physical layer is presented in Section 5. Section 6 provides description about trust implementation at the Virtual layer. Application level trust mechanisms have been discussed in section 7. Section 8 focuses on the analysis of proposed model. The last section concluded the outcome of the paper.

II. TAXONOMY OF CLOUD TRUST MODELS

In this session taxonomy of trust model for cloud computing has been presented. Predominantly Trust models for cloud computing can be classified in five categories as shown in figure 1.

A. Feedback Oriented Models

Feedback trust model calculates the trust of cloud service provider by collecting feedback about the services from the existing customers of the cloud service provider [6-8]. These models aggregates feedbacks received from different cloud customers like Security, QoS etc into Feedback Modules as shown in figure 2. Then there is trust evaluation module which categorized different cloud service provider based upon the feedbacks collected from the customers. Finally there is a Service registry where the cloud service providers list is stored.

In this category three models have been discussed.

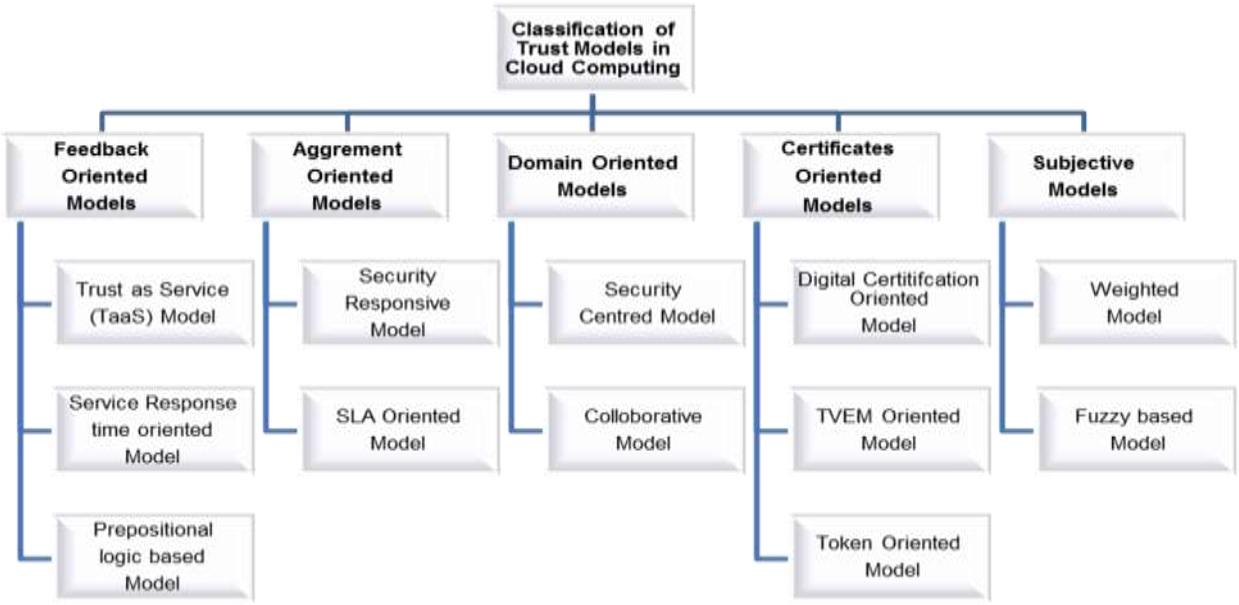

Fig. 1 Classification of Trust Model [19]

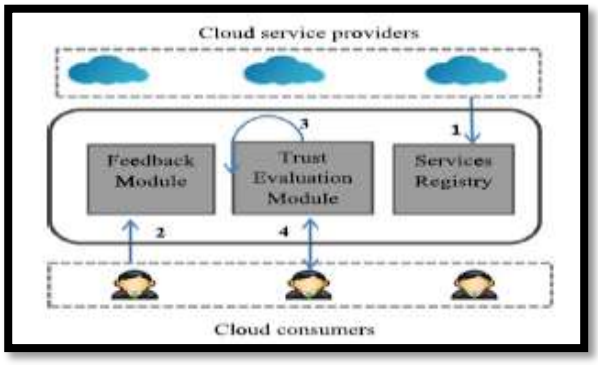

Fig. 2 Feedback based trust model [6]

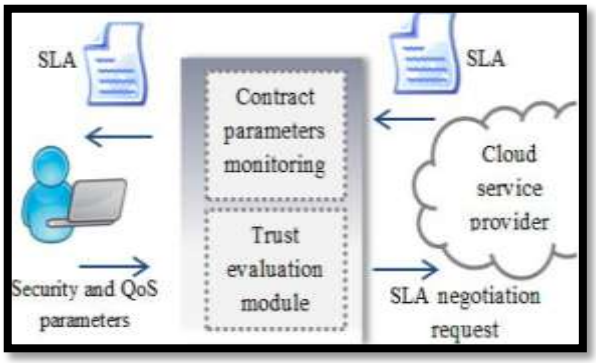

Fig. 3 SLA based trust model [10]

The first one is TEMRT (Trust evaluation model based on response time). In this model the trust is evaluated based upon the service response time of cloud service provider [6]. PLTs (Prepositional logic terms) model estimates the trust based using the feedback from numerous sources [8]. Cloud consumers opinion has been used in "Trust as a service" model for the estimation of trust [7].

B. Agreement Oriented Models

Service level agreement (SLA) model is proposed which attempt to build the trust for cloud users while ensuring that different terms and conditions mentioned in the agreement will fulfill by the cloud service provider [9, 10] as shown in figure 3. SLAs in general include requirement for the uptime of service, quality of service, support level provided by the service provide, contact information of the concerned persons of the service provider. In this category two models have been chosen for discussion. The first one is TMSAW (Trust model for security aware cloud" [10] which focus on the trust mechanisms using SLA.

The second one is SLA based trust model (STM) [9] which explain the importance of SLA with respect to trust establishment in the operations of cloud service providers.

C. Domain Oriented Models

Domain oriented models are widely used in Grid but some of them have been suggested for Cloud environment. The fundamental idea behind Domain based trust models for cloud computing is to divide the cloud into sub domains, where each domain is autonomous and then build inter domain trust relationships. Inside each domain there is a trust value assigned and maintained in trust table. When accessing an entity, its trust value is determined from the trust table. A domain based collaborative trust model is proposed by Z. Yang et al [11 12]. It gives the concept of domain agents. This paper focus on the domain based segregation and Firewall mechanism between different domains as shown in figure 4. Trust values are stored in different trust related tables. Two models selected in this category are SCITM (Security & Interoperability trust model [12] and COTM (Collaborative Trust model) [11].

The fundamental theme is to segregate the consumers and service providers into diverse domains.

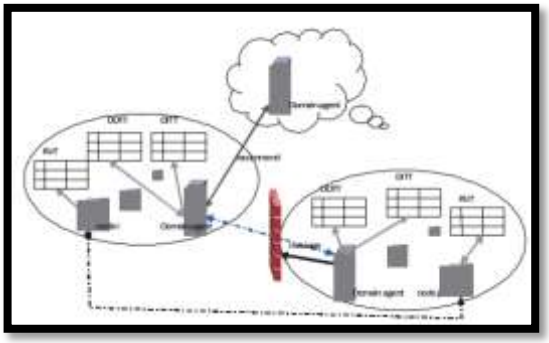

Fig. 4 The Structure of Collaborative Trust Model of Firewall-through based on Cloud Computing [11]

D. Certificate Oriented Models

These models focus on the establishment of trust using digital certificates, keys and token etc issued from trusted third party certificate authorities (CAs) [6, 13,14] as show in figure 5. These certificate and keys are used for building trust in software, infrastructure and platform of cloud service provider (CSP). These certificates provide functionalities like confidentiality, customer's control and vigilance over their data. The models in this category also uses trusted platform module (TPM) for the establishment of trust.

In this category, three models have been discussed. The trusted virtual environment (TVEM) model established trust using the trust processing modules (TPM) [14]. The certificate based model uses certificates issued from different bodies as mean for the establishment of trust [13]. Another model in this category is Ticket based model (TTM) [14].

E. Subjective Models

Trust models in this category use fuzzy logic, set theory, probability as their main method for trust establishment and evaluation [15] [16]. They use concept of classes and subclasses for the trust estimation. These models assign certain weights to different parameters of trust within subclass and class. The values then sum up to calculate the aggregated trust value.

The NWTM "Novel weighted trust model based on cloud" calculates trust through weighted trust algorithms [15]. FCTM ("Fuzzy comprehensive evaluation-based trust model") formulate the result using fuzzy theory [16].

III. THE PROPOSED MODEL

The proposed model implements trust using multiple mechanisms at different layers of the cloud as shown in figure 6. All the mechanisms proposed to be used in this model are light weight as they don't incur substantial processing. The other important aspect of this model is that it is highly pragmatic to implement in the dynamic environment of cloud. The proposed model lies in the categories of feedback and certificate based trust model.

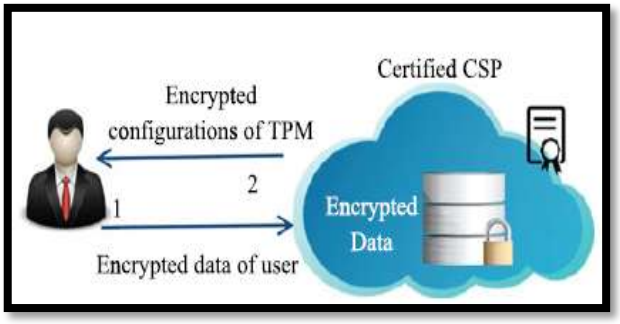

Fig. 5 Certificate based trust model [14]

In this paper, trust mechanism at the physical layer has been focused. Trust mechanisms at the application layer have been discussed in our previous work [18].

IV. TRUST IMPLEMENTATION AT THE PHYSICAL LAYER [Trusted third party Certificate Authority (CA)]

Public Key Infrastructure (PKI) is comprehensive system for the management of public key based encryption, certification and digital signatures. Public key encryption means that there are two keys private key and public key. Private Key is only for the owner, it cannot be shared. While the public key as it name suggest is available to others. When an entity wants to communicate with other, it encrypts the message with the public key of the other party. Since encrypted message can only be decrypted with the private key which is only known by the concerned entity, therefore message can be send in secure and encrypted way.

PKI also provides digital certificate services. In that case an entity wants to get the digital certificate; it sends requests to the PKI server/ Certificate Authority (CA) server giving information about itself like organization name, address, country etc. Another important information send is the public key of the entity. Once the request is received by the PKI server, it endorses the Public key by signing it with its private key. Now, the certificate is returned to the requestor. The Requestor can now use this digital certificate. Now when digital certificate is presented to others; they can verify it because it is endorsed by the CA. CA's digital signature is verified through public key of CA.

Trusted third party certificate authority (CA) has been incorporated for providing the digital certificates to different nodes used to build the OpenStack cloud like controller, compute, network etc as shown in figure 8.

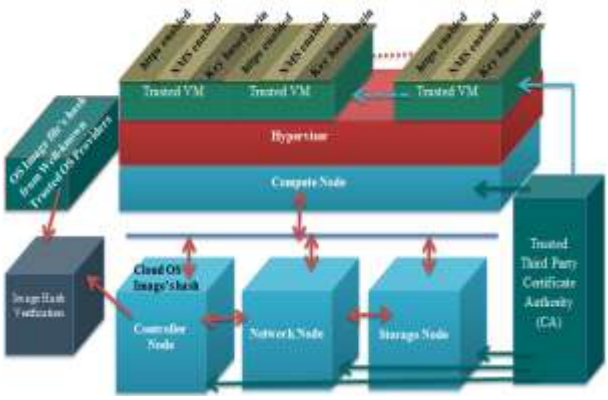

Fig. 6 The Trusted Cloud VM Mechanism

Fig. 7 Certificate issued to the host machine

The digital certificate provided by CA will served as verification of these nodes as cloud customers have trust in these third parties CAs issuing certificate. Similarly, CA also provides digital certificate to different virtual machines (VMs) launched for customers. Through these digital certificates, customers can verify VMs as trusted while contacting the CAs. These CAs issue Public key (PKI) Certificates for physical and virtual machine authentication and verification.

V. ANALYSIS OF PROPOSED MODEL

The proposed Hybrid Certificate and Feedback based Trust model (HCFTM) is predominantly combination of Certificate and Feedback based Trust approaches. The model has been named as it uses digital certificates for providing trust at the physical and virtual layers and hash verification feedback mechanism at the application level. The proposed model implements trust at physical, virtual and application layers of cloud using existing industry standards.

The Physical layer of cloud has been secured using Digital Certificate. Digital Certificates issued by trusted third party Certificate Authority (CA) are used for the verification of Physical Nodes of the deployed cloud. The CA issued certificate for the Compute, Controller, Storage and Network nodes of Cloud. This helps in the verification of physical nodes cloud service provider (CSP). Digital Certificate issued for particular physical machine will provide transparency and trust in the operations of CSP from the perspective of cloud users. The process of obtaining digital certificate begins with generating request for obtaining the certificates from trusted third party authority (CA). The request contains information about the organizations, machine specifications, location etc. The CA signs the public key of machine. Cloud customer can easily verify these certificates.

A comparative analysis of proposed model HCFTM with existing trust protocols in the domain of Feedback and Certificate class is presented in table 1.

Table 1 Comparisons of proposed HCFTM model with existing Trust Models

Assessment Parameters	**Feedback Class Models**			**Certificate Class Models**			**Proposed Model**
	TEMRT [6]	PLT [8]	TAS [7]	TVEM [14]	CTM [13]	TTM [12]	**HCFTM**
Encryption	×	✓	×	✓	✓	✓	✓
Certification Mechanism	×	×	×	✓	✓	✓	✓
QoS	✓	✓	✓	×	×	×	×
Ease of Deployment	✓	✓	✓	✓	✓	×	✓
Trusted Third Party	×	×	×	✓	✓	✓	✓
Multi-layer Protection	×	×	×	×	✓	×	✓
Feedback Mechanism	✓	✓	✓	×	×	×	✓

VI. CONCLUSIONS

The proposed model provide substantial, pragmatic trust mechanism for cloud computing. The model is combination of Certificate and Feedback based trust model. Different Trust mechanisms have been implemented at the Physical, Virtual and Application layer of cloud for enhancing the operational trust in cloud. All the mechanisms used for the trust implementation are also useful in the context that none of the method put substantial processing burden on any resource of the cloud.

REFERENCES

[1] Mell P, Grance T (2009) A NIST definition of cloud computing. National Institute of Standards and Technology. NIST SP 800-145.[Online].Available http://www.nist.gov/itl/cloud/upload/cloud-defv15.pdf.

[2] Rousseau D, Sitkin S, Burt R, Camerer C (1998) Not so Different after All: a Cross-discipline View of Trust. Academy of Management Review, 23(3):393-404.

[3] Trusted Computing Group ; 2014 [Online] http://www.trustedcomputinggroup.org/.

[4] I. M. Abbadi "Clouds trust anchors", Proc. 11th IEEE Int. Conf. Trust, Security and Privacy in Comput. and Commun. (IEEE TrustCom-11), pp.127 -136 2012.

[5] Abbadi IM. Operational trust in clouds' environment. In: MoCS 2011: proceedings of the workshop on management of cloud systems. IEEE, p.141–5. 2011.

[6] Firdhous, M., Ghazali, O. and Hassan, S. (2011) A Trust Computing Mechanism for Cloud Computing. Proc. ITU, The Fully Networked Human?-Innovations for Future Networks and Services (K-2011), Cape Town, December 12–14, pp. 1–7. IEEE, New York, USA.

[7] Noor, T.H. and Sheng, Q.Z. (2011) Trust as a Service: A Framework for Trust Management in Cloud Environments. Web Information System Engineering–WISE, Sydney, Australia, October 13–14, pp. 314–321. Springer, Berlin.

[8] Habib, S.M., Ries, S. and Muhlhauser, M. (2011) Towards a Trust Management System for Cloud Computing. 10th Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), Changsha, November 16–18, pp. 933–939. IEEE, New York, USA.

[9] Alhamad, M., Dillon, T. and Chang, E. (2010) SLA-Based Trust Model for Cloud Computing. 13th Int. Conf. Network-Based Information Systems (NBiS), Takayama, Japan, September 14– 16, pp. 321 324. IEEE Computer Society, Los Vaqueros.

[10] Sato, H., Kanai, A. and Tanimoto, S. (2010) A Cloud Trust Model in a Security Aware Cloud. 10th IEEE Int. Symp. Applications and the Internet (SAINT), Korea, July 19–23, pp. 121–124. IEEE, New York, USA.

[11] Yang, Z., Qiao, L., Liu, C., Yang, C. and Wan, G. (2010) A Collaborative Trust Model of Firewall-Through Based on Cloud Computing. 14th Int. Conf. Computer Supported Cooperative Work in Design (CSCWD), China, April 14–16, pp. 329–334. IEEE, New York, USA.

[12] Li, W. and Ping, L. (2009) Trust Model to Enhance Security and Interoperability of Cloud Environment. 1st Int. Conf. Cloud Computing (CloudCom), China, December 1–4, pp. 69–79. Springer, Berlin.

[13] Bezzi, M., Kaluvuri, S.P. and Sabetta, A. (2011) Ensuring Trust in Service Consumption through Security Certification. Proc. Int. Workshop on Quality Assurance for Service-Based Applications, Switzerland, September 14, pp. 40–43. ACM, New York, USA.

[14] Krautheim, F.J., Phatak, D.S. and Sherman, A.T. (2010) Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Cloud Computing; 3rd Int. Conf. Trust and Trustworthy Computing, Germany, June 21–23, pp. 211–227. Springer, Berlin.

[15] Zhaoxiong, Z., He, X. and Suoping,W. (2011) A novel weighted trust model based on cloud. Adv. Inf. Sci. Serv. Sci., 3, 115–124.

[16] Li, W., Lingdi, P., Qinlong, Q. and Qifei, Z. (2012) Research on trust management strategies in cloud computing environment. J. Comput. Inf. Syst., 8, 1757–1763.

[17] Ahmed, M. and Xiang, Y. (2011) Trust Ticket Deployment: A Notion of a Data Owner'S Trust in Cloud Computing. 10th Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom),China, November 16–18, pp. 111– 117. IEEE, New York, USA.

[18] M. F. Hyder and M. A. Ismail, "Application Level Trust Mechanisms for Enhancing the Operational Trust in a Cloud," Cloud Computing (ICCC), 2015 International Conference on, Riyadh, 2015, pp. 1-6.doi: 10.1109/CLOUDCOMP.2015.7149631.

[19] A. Kanwal, R .Massod, "Taxonomy of Trust Models in Cloud Computing". The Computer Journal Advance Access, 2014.