ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

Cloud Services: A Platform for Credibility Based Trust Management in Cloud Environment

P. Sowjanya, Ch. Dileep Chakravarthy

M.Tech, Dept. of Information Technology, S.R.K.R Engineering College, Bimavaram, A.P, India

Assistant Professor, Dept. of Information Technology, S.R.K.R Engineering College, Bimavaram, A.P, India

ABSTRACT: In this environment of multi cloud providers, the assurances are not enough for the cloud users to select the trustworthy cloud service providers. Trust is one of the most concerned obstacles for the adoption and growth of cloud computing. Determining the credibility of trust feedbacks is mostly neglected. In this paper, we present the importance of trust management in cloud environments. It also describes the feedback based trust issues where trust calculation is done through feedback of cloud users. It is important to identify the feedback based attacks because less submission of fake feedbacks can also compromise the whole trustworthiness of service provider. Also, we propose a method for the trusted service using three topological metrics, including in-degree, out-degree and reputation measures. The proposed method has been evaluated in different challenging situations where obtained results show the increase in accuracy of proposed method using the advice of trusted service providers.

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

I. INTRODUCTION

Cloud Computing has been emerged as new computing way in which two main players. Cloud service providers and cloud end-users. There are several definitions proposed to define exactly what is cloud computing by different authors. Cloud computing is a relatively new business model in the computing world. According to the official [9] NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with
minimal management effort or service provider interaction."

[1], [3] The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three "service models", and four "deployment models" that together categorize ways to deliver cloud services. Cloud computing provide several advantages such as rapid elasticity, location independence, device diversity etc. However, there are many open issues which are obstacles in adoption and growth of cloud computing such as security, privacy, vendor-lock in, trust etc.

Trust Management is widely used in various sectors such as wireless system, e-commerce sector, human sociology etc. In cloud environment, trust evaluation is very important to find the trustworthy of service provider. One major source for trust estimation of service provider is ratings submitted by cloud customers. This paper presents different kinds of attacks when trust calculation done through feedbacks submitted by cloud users.

My paper in the next section describes about what is trust, requirements of trust in cloud environment and types of trust. Then after distinguishes the different parameters used for trust evaluation and last section describes feedback base trust evaluation attacks, proposed solution by different authors and the summary of attacks and possible occurrences of attack in different stages of trust management. Currently, the Internet puts a huge effect on the society and creates a new revolution in the 21st century where everything and everyone are getting online.[4] The cloud computing is a kind of information service made based on a grid and distributed computing. It is relatively a new term in information

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

technology, firstly popularized in 2006 by Amazon's EC2. It is a large-scale parallel and distributed computing architecture which promises to bring with itself the great benefits to all types of computing activities and it plays a central role to meet today's business requirements. Also, it is a pervasive computing paradigm that has revolutionized how computer infrastructures and services are delivered.

The cloud computing can be seen as one of the latest major evolutions in computing which offers the unlimited possibility to use ICT in various domains. It is the next generation of computer system which extends the network architecture into dynamic and large scale capacity by using the visualization techniques. Major advantages such as the cost reduction and flexibility ensure the cloud computing to be a much-sorted technology in the computing industry. It needs various forms of interactions with entities that are seldom known, and, some parts might never be met. The cloud is a back to the future proposition that was foreseen in the 1950s and is as old as the computing itself. In the cloud environments, the consumers make complex decisions, requiring trust for several services and various reasons. [5]The Cloud based computation services have grown popularity in recent years. It is the Internet-centric providing all the resources and services such as storage, computation, and communication. One of the key promises of the cloud is the speed and ease with which the organizations can temporarily access the additional compute resources. Although the cloud computing services are increasing and gaining popularity, the dread about the usage of the cloud services is still an open issue. The cloud computing offers many advantages by allowing users to apply the infrastructures and software's that are provided by the cloud providers with pay-per-use fashion and low cost. It supports four types of service delivery models, for example, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Expert as a Service (EaaS).

Consumers' feedback is an excellent source to assess the overall trustworthiness of cloud services. Several researchers have known the significance of trust management and proposed solutions to assess and manage trust based on feedbacks collected from participants. In reality, it is not unusual that a cloud service experiences malicious behaviors e.g., collusion or Sybil attacks from its users. This paper focuses on improving trust management in cloud environments by presenting novel ways to ensure the credibility of trust feedbacks. In particular, Consumers' feedback is a good source to assess the overall trustworthiness of cloud services. Several researchers have recognized the significance of trust management and proposed solutions to assess and manage trust based on feedbacks collected from participants. In particular, we distinguish the following key issues of the trust management in cloud environments**.** The adoption of cloud computing raises privacy concerns.

Customers can have dynamic interactions with cloud providers, which may involve sensitive information. There are several cases of privacy breaches such as leaks of sensitive information e.g., date of birth and address or behavioral information e.g., with whom the consumer interacted, the kind of cloud services the consumer showed interest etc.. Undoubtedly, services which involve consumers' data e.g., interaction histories should preserve their privacy. It is not unusual that a cloud service experiences attacks from its users. Attackers can disadvantage a cloud service by giving multiple misleading feedbacks or by creating several accounts. Indeed, the detection of such malicious behaviors' poses several challenges. Firstly, new users join the cloud environment and old users leave around the clock. This consumer dynamism makes the detection of malicious behaviors a significant challenge. Secondly, users may contain multiple accounts for a particular cloud service, which makes it difficult to detect Sybil attacks. Finally, it is difficult to guess when malicious behaviors occur.

II. LITERATURE SURVEY

[1],[2],[7] Over the past few years, trust management has been a hot topic in the area of cloud computing some of the research efforts use policy-based trust management techniques. For example, Ko et al propose Trust Cloud framework for accountability and trust in cloud computing. In particular, Trust Cloud consists of five layers including workflow, data, system, policies and laws, and regulations layers to address accountability in the cloud environment. All of these layers maintain the cloud accountability life cycle which consists of seven phases including policy planning, sense and trace, logging, safe-keeping of logs, reporting and replaying, auditing, and optimizing and rectifying. Brandic et al. propose a novel approach for compliance management in cloud environments to establish trust between different parties. The approach is developed using a centralized architecture and uses compliant management technique to establish trust between cloud service users and cloud service providers. Unlike previous works that use policy-based

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

trust management techniques, we assess the trustworthiness of a cloud service using reputation-based trust management techniques. Reputation represents a high influence that cloud service users have over the trust management system, especially that the opinions of the various cloud service users can dramatically influence the reputation of a cloud service either
positively or negatively.

Cloud Service Provider Layer
This layer consists of different cloud service providers who offer one or several cloud services, i.e., IaaS, PaaS, and SaaS, publicly on the Web (more details about cloud services models and designs can be founding. These cloud services are accessible through Web portals and indexed on Web search engines such as Google, Yahoo, and Baidu. Interactions for this layer are considered as cloud service interaction with users and TMS, and cloud services advertisements where providers are able to advertise their services on the Web.

Trust Management Service Layer
This layer consists of several distributed TMS nodes which are hosted in multiple cloud environments in different geographical areas. These TMS nodes expose interfaces so that users can give their feedback or inquire the trust results in a decentralized way. Interactions for this layer include: i) cloud service interaction with cloud service providers, ii) service advertisement to advertise the trust as a service to users through the Internet, iii) cloud service discovery through the Internet to allow users to assess the trust of new cloud services, and iv) Zero- Knowledge Credibility Proof Protocol interactions enabling TMS to prove the credibility of a particular consumer's feedback.

Zero-Knowledge Credibility Proof Protocol
Since there is a strong relation between trust and identification as emphasized in, we propose to use the *Identity Management Service* (IdM) to help TMS in measuring the credibility of a consumer's feedback. However, processing the IdM information can breach the privacy of users. One way to preserve privacy is to use cryptographic encryption techniques. However, there is no efficient way to process encrypted data. Another way is to use anonymization techniques to process the IdM information without breaching the privacy of users. Clearly, there is a trade-off between high anonymity and utility.

Cloud Service Consumer Layer
Finally, this layer consists of different users who use cloud services. For example, a new startup that has limited funding can consume cloud services. Interactions for this layer include: i) *service discovery* where users are able to discover new cloud services and other services through the Internet, ii) *trust* and *service* interactions where users are able to give their feedback or retrieve the trust results of a particular cloud service, and iii) *registration* where users establish their identity through registering their credentials in IdM before using TMS. Our framework also exploits a Web crawling approach for automatic cloud services discovery, where cloud services are automatically discovered on the Internet and stored in a *cloud services repository*. Moreover, our framework contains an *Identity Management Service*, which is responsible for the *registration* where users register their credentials before using TM Sand proving the credibility of a particular consumer's feedback through ZKC2P. Thus, we propose a *Zero*-Knowledge Credibility Proof Protocol to allow TMS to process IdM's information (i.e., credentials) using the Multi- Identity Recognition factor. In other words, TMS will prove the users' feedback credibility without knowing the users' credentials.

III. ATTACK MODELS

COLLUSION ATTACKS
Also known as collusive malicious feedback behaviors, such attacks occur when several vicious users collaborate together to give numerous misleading feedbacks to increase the trust result of cloud services or to decrease the trust result of cloud services. This type of malicious behavior can occur in a non-collusive way where a particular malicious user gives multiple misleading feedbacks to conduct a self-promoting attack or a slandering attack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

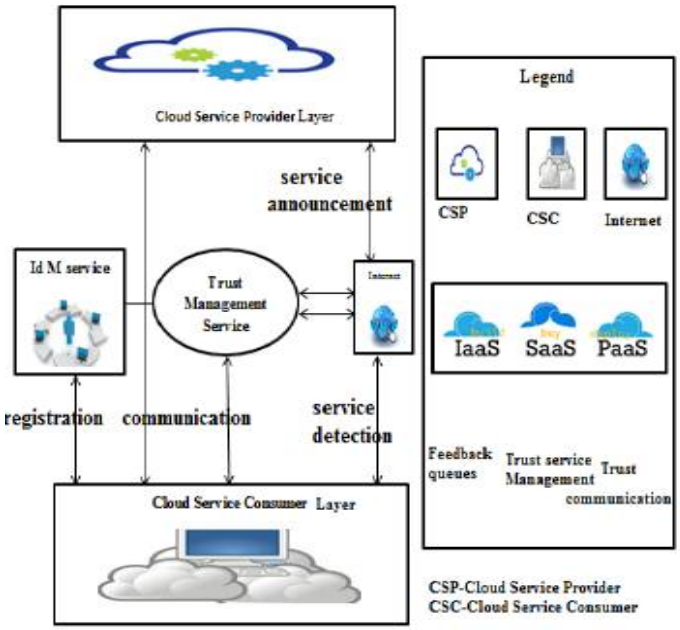
SYBIL ATTACKS

Such an attack arises when malicious users exploit multiple identities to give numerous misleading feedbacks for a self-promoting or slandering attack. It is interesting to note that attackers can also use multiple identities to disguise their negative historical trust records.

FEEDBACK COLLUSION DETECTION

Feedback Density Malicious users may give numerous fake feedbacks to manipulate trust results for cloud services. Some researchers suggest that the number of trusted feedbacks can help users to overcome such manipulation where the number of trusted feedbacks gives the evaluator a hint in determining the feedback credibility. However, the number of feedbacks is not enough in determining the credibility of trust feedbacks.

ARCHITECTURE



TRUST MANAGEMENT FACTORS

We can evaluate trustworthiness based on below classified trust parameters. We may categorize the trust related parameters in three categories.

A. IDENTITY BASE TRUST PARAMETER

All the security related parameters like Authorization level, User protection level, Data security level, Data Recovery level etc. are involved in identity base trust management parameters.

B. CAPABILITY BASE TRUST PARAMETER

Capability of cloud resources like RAM, speed of processor, Bandwidth, latency are involved in capability base trust management parameters.

C. BEHAVIOR BASE TRUST PARAMETER

In behavior based trust management, need to identify behavior based parameter like availability, Success Rate, Feedback.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

IV. ALGORITHMS USED

ALGORITHM 1: PARTICLE FILTERING BASED ALGORITHM

Initialization: compute the weight distribution *Dw*(*A*(*stms*)) according to prior knowledge on replicas, e.g., the IP address of server hosting replicas etc.

Generation: generate the particle set and assign the particle set containing *N* particles generate initial particle set *P0* which has *N* particles, *P*0 =(*p*0;o; *p*0;1;…….*p*0;*N*-1) and distribute them in a uniform distribution in the initial stage. Particle *p*0;*k*(*A*(*stms*)0;*k*;*weight*0;*k*) Assign weight to the particles according to our weight distribution *Dw*(*A*(*stms*)).

Resampling:

Resample *N* particles from the particle set from a particle set *Pt* using weights of each particles. Generate new particle set *Pt*+1 and assign weight according to *Dw*(*A*(*stms*))

Estimation: predict new availability of the particle set *Pt* based on availability function
A(*stms; t*).

Update:

recalculate the weight of *Pt* based on measurement
m,*wt*;*k*=Π(*Dw*(*A*(*stms*)*t*,*k*)) (1/√2πσy)exp(_*δA*(*stms*)2*t*,*k*/2*σ*2*y*),
where *A*(*stms*)*k* = *mA*(*stms*) - *A*(*stms*)*t*,*k* calculate current availability by mean value of *pt*(*A*(*stms*)*t*)
6. Go to step 3 and iteration until convergence

ALGORITHM 2: TRUST RESULTS & CREDIBILITY WEIGHTS CACHING

Input: *s*, **Output**: *T r*(*s*)
Count |*Vc*(*c; s*) |*Cache* /*TMS instance counts the total number of new trust feedbacks given by a particular consumer*/
if |*Vc*(*c; s*) |*Cache* ≥ *eCache*(*c*) **then** /*TMS determines whether a recalculation is required for credibility factors related to the consumer*/
Compute *J* (*c*); Compute *B*(*c*)
Compute *Mid*(*c*); Compute *Cr*(*c, s*)
end if
Count |*V*(*s*) |*Cache* *TMS instance counts the total number of new trust feedbacks given to a particular cloud service*/
if |*V*(*s*)|*Cache* ≥ *eCache*(*s*) **then** /*TMS determines whether a recalculation is required for credibility factors related to the cloud service including the trust result*/
Compute *D*(*s*); Compute *Cr*(*c; s*)
Compute *T r*(*s*)
end if

ALGORITHM 3: INSTANCES MANAGEMENT ALGORITHM

1. **Initialization:** *tmsid*(0) computes *Op*(*stms*) for all trust management service nodes if any
2. **Generation:** *tmsid*(0) estimates *Ntms* and generates additional trust management service nodes if required
3. **Prediction:** *tmsid*(0) predicts new availability of all trust management service nodes *A*(*stms; t*) using Algorithm 1
4. **Replication:** *tmsid*(0) determines *r*(*stms*), and generate replicas for each trust management service node
5. **Caching:** *tmsid*(0) starts caching trust results (consumer side) and *tmsid*(*s*) start caching trust results (cloud service side) using Algorithm 2
6. **Update:** All *tmsid*(*s*) update the frequency table
7. **Check Workload 1:** *tmsid*(0) checks whether *ew*(*stms*) is triggered by any *tmsid*(*s*) before reallocation
if *Op*(*stms*) ≥ *ew*(*stms*) and *V*(*stms*) ≥ *V*(*meantms*) **then**
go to next step
else
go to step 3
end if
8. **Reallocation:**
   - *tmsid*(0) asks *tmsid*(*s*) which triggered *ew*(*stms*) to reallocate all trust feedbacks of the cloud service that has the lowest |*V*(*s*)| to another *tmsid*(*s*) that has the lowest *V*(*stms*)
   - perform step 6

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

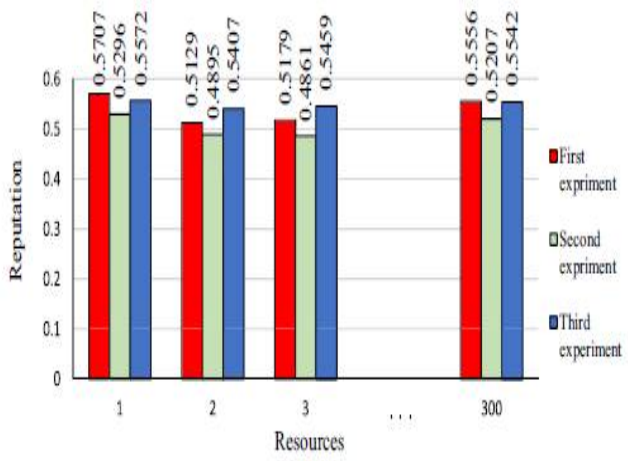
9. **Check Workload 2:** *tmsid*(0) computes *Op*(*stms*) for all trust management service nodes and checks whether *ew*(*stms*) is triggered for any *tmsid*(*s*) after reallocation
if *Op*(*stms*) ≥ *ew*(*stms*) and *V*(*stms*) ≥ *V*(*meantms*) **then**
go to step 2
else
go to step 3
end if

ATTACKS IN TRUST MANAGEMENT

In this section we summaries different phases of occurrence of some attacks in trust management system. Newcomer attack and Sybil attack mostly occur in login phase. Discrimination attack and Intoxication attack occur in transaction phase and Collusion and Sybil attack can occur in trust evaluation phase. Trust accuracy is based on quality of assessment from all feedbacks.

V. EXPERIMENTAL RESULTS

In this paper, the experiments are developed by using Mat lab R2013b and performed on a desktop computer with a configuration such as Intel CPU Core i5, 4 GB RAM, and Windows 7 operating system. In order to test the performance of the proposed method, we use a standard evaluation technique in the cloud environment. In this section, the efficacy of our approach is investigated. We present the details of the extensive experiments on random datasets to evaluate the performance of our approach. The dataset contains 300 resources with different characteristics. we use three sets of different weights which are shown in three sets in different experiments. Next, according to the obtained results, we select one of the reputations to evaluate the trusted service. Also, we present the results of the selection of the trusted service using the proposed formula. Finally, we compare our methods to other works in the related studies.



We propose several results for the reputation evaluation using different weights. As a first experiment, we consider the reputation weights as Weight1 ¼ 0.3, Weight2 ¼ 0.4, and Weight3 ¼ 0.3. As a second experiment, to investigate the other situations, we change the weights of reputation to Weight1 ¼ 0.3, Weight2 ¼ 0.3, and Weight3 ¼ 0.4. As a third experiment, we consider the weights of reputation as Weight1 ¼ 0.4, Weight2 ¼ 0.3, and Weight3 ¼ 0.3. We measure the impact of the different trusted service methods and compare the behavior of the implemented methods. There are two methods to recognize the trusted service. We evaluate each of them with two different reputation thresholds. The experiment was conducted for 300 services in the Cloud environment. We analyze the different weights and alpha values. With a hybrid measurement with different alphas, the values are changed only marginally. We consider the subjective alpha values as a ¼ 0.2 for each criterion. We consider reputation weights as Weight1 ¼ 0.3, Weight2 ¼ 0.4 and Weight3 ¼ 0.3. We consider this case as a more efficient solution than others. Also, we evaluate this approach

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

using three different reputation thresholds, including 0.6, 0.65, 0.7 and consider the TS1 and TS2 of lTS > 50. The obtained results for the trusted service selection using the two methods.

VI. CONCLUSION AND FUTURE WORK

I worked about a new method for the trusted service identifiscation in the cloud environment. We have explained how the reputation value is calculated based on the credential attributes such as accessibility, dependability, and ability. Also, we calculate the trust value using three topological measures including in-degree, out-degree and reputation, while the weights of the trusted services are varied in the Cloud environment.

Furthermore, we conclude that the number of the trusted services have a direct relationship to the reputation. If we increase the threshold of reputation value, the fewer number of the trusted service will be selected. Also, we show that the accuracy of the proposed method using the advice of the trusted service is increased. In the future, we plan to investigate the impact of other algorithms on the trust as well as the reputation evaluation. Also, the formal verification and specification of the proposed trust evaluation mechanism in the Cloud environment is still very challenging.

REFERENCES

[1] Sheikh Mahbub Habib, Sebastian Ries, Max Muhlhauser, Towards a Trust Management System for Cloud Computing, IEEE Trust, Security and Privacy in computing and Communications(TrustCom), Pages 933-939, 2013
[2] B.Kezia Rani, Dr.B.Padmaja Rani, Dr. A. Vinaya Babu, Cloud Computing and Inter-Clouds-Types, Topologies and Research Issues, ELSEVIER, Volume 50,Pages 24-29, 2015
[3] Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries and Max Muhlhauser, Trust as a Facilitator in Cloud Computing: A survey, Journal of Cloud Computing,1:19,2012
[4] Rajkumar Buyya, Christian Vecchiola, Thamarai Selvi, Mastering in Cloud Computing, Morgan Kaufmann, May 2013
[5] Maricela-Georgiana Avram, Advantages and challenges of adopting cloud computing from an enterprise perspective, ELSEVIER, Volume 12, Pages 529-534, 2014
[6] Soon-Keow Chong, Jemal Abawajy, Masitah Ahmad, Isredza Rahmi, Enhancing Trust Management in Cloud Environment, ELSEVIER, Volume 129, Pages 314-321, 2014
[7] Dawei Sun, Guran Chang, Lina Sun, Xingwei Wang, Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments, ELSEVIER, Volume 15, Pages 2852-2856, 2011
[8] Khald M. Khan and Qutalbah Malluhi, Establishing Trust in cloud computing, Qatar University, IEEE IT professional, Volume 12(5), 2010
[9] Talal H. Noor and Quan Z. Sheng, Trust as Service: A framework for Trust Management in Cloud Environments, Springer, Volume 6997, Pages 314-321,2011
[10] Rizwanna Shaikh, Dr. M. Sashikumar, Trust Model for Measuring Security Strength of Cloud Computing Service, ELSEVIER, Volume 45, Pages 380-389, 2015
[11] Paul Manuel, Thamarai Selvi Somasundaram, A Novel Trust management System for Cloud Computing – IaaS Providers, ResearchGate Journal of Combinatorial Mathematics and Combinatorial Computing, 79:3-22, 2011
[12] Soon-Keow Chong, Jemal Abawajy, Isredza Rahmi A. Hamid, Masitah Ahmad, A Multilevel Trust Management Framework for Service Oriented Environment, Elsevier, 129:396 405, 2013
[13] Dongxia Wang, Tim Mullerr, Yang Liu and Jie Zhang, Towards Robust and Effective Trust Management for Security: A Survey, ACM, 2014
[14] Satyajeet N Srujan Kotikela, Mahadevan Gomathisankaran, CTrust: A framework for Secure and Trustworthy application execution in Cloud Computing, International Conference on Cyber Security", 2012
[15] Manoj Kumar Muchahari, Smriti Kumar Sinha, A New Trust Management Architecture for Cloud Computing Environments, IEEE International Symposium on Cloud and Services Computing (ISCOS0), 2012
[16] Edna Dias, de Sousa, R T, de Carvalho , R.R., de Oliveira Albuquerque R., Trust Model for Private Cloud, IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic(CyberSec), 2012.