Trust Modeling and Service Level Agreement Monitoring in Federated Cloud

Sanjay.H.M[1], GuruPrakash[2]

Associate Professor[1], Professor[2] & Department of information Science[1], Department of Computers[2]
PES College of Engineering[1],Mandya, India, SSIT[2], Tumkur, India (
Address Including Country Name

Abstract *Communication in trusted networks is not absolute until their relation is expressed in a transitive manner. Formulizing trust relationships leads to score reputation of a party or an entity; these evaluations are measured with subjective trust measurement, where subjective trust is described in this paper. The trust between any two parties can be analyzed through their trust linking paths. The properties of evaluating trust on network can be offered as 1. Transitive trust 2. Parallel trust combination 3. Subjective logic. In modern communication of information technology and services, a familiar style being adopted for interaction procedures. The phenomenal growth in business-to-business forum offers people with distributed application sets that are really sensitive for processing and delivering tasks. As a result computer networks fail to meet these uncertain challenges and it degrades quality of services (QOS). Business processing through e-commerce is the recent trend that offers viable applications to customers for fulfilling their business needs. Likewise, people are influenced to use distributed e-commerce application in an enormous way without considering the risk of security as a primary challenge. Cloud computing is a considerable security path, offering services to its users by meeting minimal security needs. Cloud must offer better trusted service to their consumers by building its reputation scores. In this paper assessing of trust becomes a major objective to achieve QoS and better decision-making system in cloud computing. The entities of cloud are CSP's, which delivers the services to consumers, provided by cloud infrastructure provider (CIP). Assessing of trust with respect to CSP and CIP can be accessed on the basis of CSP positive belief on CIP.*

Keywords*: Subjective Logic, SLA, CIP, CSP, Virtual Machines*

I Introduction

Usage of computational resources and liabilities in IT being fascinated over the decade. Cloud is new paradigm in 2000 era, where the policies of cloud define how a service architecture to be prototyped and deployment of its usages. The deployment models of cloud are not stand alone satisfactory for auditing of trust-based modeling. The result of accessing e-commerce, digital banking and many more cloud service action is being federated between its infrastructure and out sourced. A proper SLA monitoring is required to achieve trust between federated and bursted cloud entities. In this paper a newer trust approach towards modelling of cloud is being introduced to carry out the optimal results acquired by different cloud entities. For the consideration of modeling, we assume health care cloud infrastructure as a primary federation, later trust modeling is done through reference of three options Transitive trust principle, Parallel Trust Combination and Subjective Logic. The trust model in this paper is focused mainly on subjective method introduced by Jasong [1] [2] with evaluation of SLA monitoring and observations. The work is compared with SS roys[3] by considering CSP ratings.

II Background

The traditional models concerned to security aspects is platform to create a boundary of trust where an adequate self-control on resources and storing and processing of sensitive information are done. For assessing cloud computing there must be an integration of dynamic based trust and social technological mechanisms to provide accurate trust range. On the off chance that software forms give data about the manner by which data is put away, got to and shared inside a cloud, that data must be trusted if substances that are trusted vouch for the technique for giving the data what's more, evaluating the data. Contingent on the unique circumstance, these elements could be shopper gatherings, examiners, security specialists, controllers, organizations with demonstrated notoriety, set up CSPs, and so forth. Besides, trust connections can be particularly at the focal point of certain security and security arrangements [4].

A. Lacks in User trust: European over viewed in June 2011 about their mentalities on information assurance, it was discovered that specialists and establishments including the European Commission and the European Parliament (trusted by 55% of individuals reviewed) – are trusted more than business organizations. Truth be told, short of what 33% trust telephone organizations, cell phone organizations what's more, Internet specialist co-ops (32%); and a little more than one-fifth trust Internet organizations, for example, web crawlers, long range interpersonal communication destinations and email administrations (22%). Moreover, 70% of Europeans, as indicated by this think about, are worried that their own information held by organizations might be utilized for a reason other than that for which it was gathered. In an ongoing Cloud Industry Forum review, the consequences of 'how would you trust an on the web supplier?' were: notoriety (29%); proposal from trusted gathering (27%); preliminary experience (20%); legally binding (20%); other (4%) [5]**.**

Endeavor IT administrators refer to very much established worries about the difficulties of looking after security, benefit levels, and administration flawlessly over the whole IT esteem chain. They likewise need to make sure the choices they make today about cloud innovation providers don't avert them from improving later on. Henceforth, various basic difficulties should be

tended to with the end goal to energize cloud reception in ventures**.**

B. Absence of Consensus about Trust Management Approaches to be Utilized

There is an absence of agreement about what trust administration approaches ought to be utilized for cloud conditions. The inalienable unpredictability of trust, the subjectivity of a few elements and the trouble of relevant portrayal makes trust estimation a noteworthy test. Artz and Gil [8] give features of trust that can be estimated for appraisal purposes. Institutionalized trust models are required for check and affirmation of responsibility; however none of the substantial number of existing trust models to date is sufficient for the cloud condition [6]. There are many trust models which endeavor to oblige a portion of the elements characterized by and others [9] and there are many trust appraisal systems which intend to gauge them. These will in general be created in seclusion and there has been little coordination among hard and delicate trust arrangements. No appropriate measurements exist for responsibility, just an abnormal state thought to date.

At last, utilization of the cloud is an issue of tradeoffs between security, privacy, consistence, expenses and advantages. Trust is vital to selection of SaaS, what's more, straightforwardness is an essential instrument. Besides, trust systems should be engendered appropriate along the chain of administration arrangement.

C. Trust under Weak Relationships in Cloud

Trust relationship with any point of time immense to be weaker in its delivery chain, this usually takes on a quick services deliverable. When a cloud transaction is initiated, no proper transparency is enabled due to newer business risk and loss of control while passing sensitive information sets. In this thesis we consider medical information synthetic data set to prove the rate of access control preserve the privacy level of a user by enhancing the trust rates mutually between consumer and CSP, as cloud is globally featured entity with its infrastructure. Entities which outsource their business processing as a subcontract never know whether the give outsourced subcontract is again sub-contracted to someone else or else apart if they do so the contract requirements related to data protection may not navigate up to mark to the sub-contractors. As a result in the trust chain customers may not trust on sub-contractors. Due to lack of transparency they are not able to identify the identity of cloud service providers. As a result on-demand and pay-as-you-go models can be stated to weak trust relationships, integrating third parties, exposing the data without the knowledge of actual contractor and finding harder verification.

D. Conclusion of Trust in Cloud

Trust is key parameter in a wide premise like cloud, for the end users, regulators and entities. If the level of trust is lower than cloud adaptability by the consumers is hard. People always worry about their data which is been stored on cloud. They are intensively worried who may access, where their data it will be utilized, whether it's shared with strangers, at last they might feel they have lost the control over their own data sets. Ultimately the usage of cloud services is a questionnaire between security, confidentiality, privacy, cost and compliance. It's an important parameter for the adaption of SaaS and transparency.

III Cloud Computing Example

A better example for cloud computing in recent trends is health care / medical environment, where it provides detail description of the health records to the customers. Now a day's accessing health care system remotely is a challenging task due to sensitive information between entities and customers. Processing this information to the user end can be deployed through cloud services. In this section to assess trust, we consider a health care system which is enabled for mobile cloud users. The health care application allows the patients/users to have virtual reporting, appointments and interaction with entities. The application is hosted on Amazon web services (AWS) using Open Nebula , key features of the application are accessing flexibility remotely anytime and anywhere, providing ease of access to edit the application operations, providing security and scaling up of storage, elasticity and scalability of computing resources. The application contains various components like: active repository, virtual machines (VM) and web interface. VM are said to be virtual desktops. In the proposed model, we consider five different cloud service providers (CSP's) and five Cloud infrastructure providers (CIP) as a multi cloud deployment. The infrastructure i.e. CIP carries the target opinion feedback as an input to the cloud recommender. The cloud recommender checks with the Service Level Agreement (SLA) regulation of the entity and later it recommend the service provider based on Transitive Trust Principal (TTP). As shown in Figure 10 each CIP is constituted of multiple datacenter, as they are distributed geographically. In order to execute multiple VM's the data centers can be capitalized with multiple physical hosts.

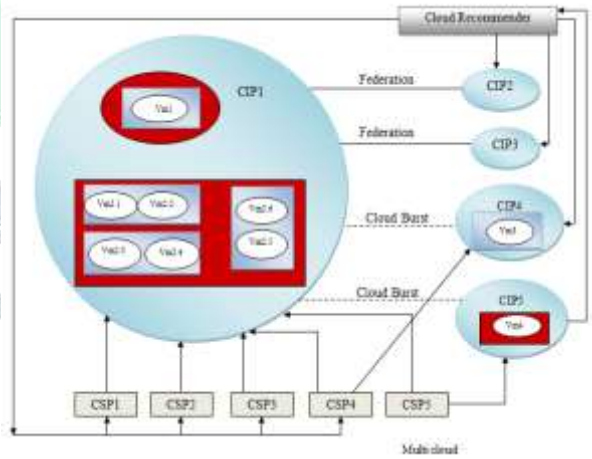

Fig 1: Entities cloud example

Now from the figure 1 consider CIP1 that has three datacenters which is enable with three and one hosts respectively. The CIP1 datacenters constitutes with three and one VM respectively. The establishment of federation between CIP1 and CIP2, CIP1 and CIP3 provides dependency between the infrastructures; this shows CIP 1 is capable of withdrawing the capacity of CIP2 and CIP3. A bursting instance is shown in Figure 1 that defines the scalability of infrastructure and outsourcing it to other clusters from third party. Bursting is an instance where CIP1 bursting CIP4 to reach the SLA requirements of CSP. A cloud recommender (broker) is stated along with all CSP's and CIP's to check the SLA meet up requirements.

Figure 1 provides few options which indicates the deployment of cloud application by CSP on various instance

1) Deployment of application takes it counter with single CIP, associated with all applications on a single physical host. In figure 1 CSP1 provides the set of all its VM 's running on single host
2) Deployment of application is on a single datacenter of CIP. CSP1 and CSP2 runs all its dedicated VM's on similar datacenter of CIP1
3) Usage of federation resources is limited for a single CIP boundary, where CSP1,2 and 3 respectively own its VM's in boundary of CIP1
4) Deployment of application in multiple CIP. In figure 1 CSP4 and CSP5 deploy the application on CIP 1 and CIP 4, CIP 1 and CIP 5 respectively. This situation is also referred to as multi cloud deployment.

In this example suppose if a diagnostic laboratory wishes to use the healthcare application with the CSP describing all its SLA to reach expected Quality of Service (QoS). SLA proves the QoS at all its level of interaction between CSP and CIP. The execution of VM's at runtime meet the QoS needs for cloud services. QoS like bandwidth and delay issues can also be considered. In this scenario due to multi-cloud deployment the primary QoS is focused on security and scalability of cloud. If SLA are ignored at higher rate, than trust for CIP also drop consecutively that violate SLA. Scalability of cloud for deploying user applications depends on rate of SLA violations, for an instance if SLA between two parties demands the computing resources automatically/dynamically than application receives a request for all its deployment over cloud. In case if the CIP doesn't provides the required computing resources to satisfy the needs of CSP and cloud, than the cloud recommender may choose alternate selection of CIP to recommend the CIP to CSP.

IV Trust Modeling

The following options of trust principles provides a primary note in building better federated trusted cloud zone

Option 1: Transitive trust principle (TTP) based on the target nodes feedback opinion at CIP

Option 2: Parallel combination of trust (PTC) between recommender and direct trust of CSP with CIP to solve uncertainty between CIP's

Option 3: Subjective logic (SL) method to know the opinion of infrastructure based on decision of targets in CIP

The trustworthiness is proved based on CIP that is modeled using its computing resources. In this scenario the results acquired buy control input of target feedback is deployed on all the CIP and its opinion is passed to recommender. The computations are carried at different levels by choosing above options with respect to SLA parameters and CSP satisfactory ratings.

Now consider option 1 TTP, CIP's target opinion is fed to cloud recommender, which believes the recommender has direct trust reference of CIP. In case if the recommender represents that he trusts CIP to CSP than the recommendation is successful. But trust cannot be treated transitive in all part its transactions. In case from figure 1 if CIP1 regulates its option in handling and sharing its computing resources of all its targets and with all its federated CIP, then recommender is not in position to choose the federated CIP. On the other side, if CSP4 has a direct trust with CIP4 without the need of recommender than CIP1 can't provision its computing resources to CSP's, because there is situation of bursting between CIP1 and CIP 4. The transitive trust of the scenario is depicted in Figure 2**.** Incase if CIP4 and CIP5 which has direct trust of CSP 4 and CSP5 respectively, than cloud recommender can't recommend CIP 1, 2 and 3 to share their resources with CSP 4 and 5. Functional trust is derived only when CIP 1 has got at least one direct trust recommendation from CSP with all its federated CIP's.

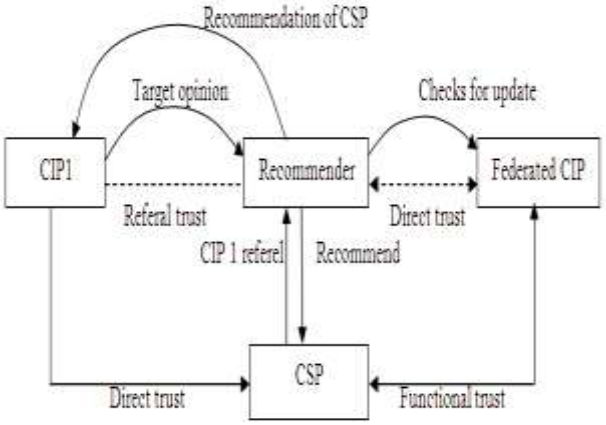

Fig 2: Transitive trust scenario for healthcare

Let us extend the scenario of transitivity a bit. The cloud recommender is not aware of CIP with better target opinion feedback, in this case from figure 1 let us consider CIP5 which is not federated with other CIP, but cloud recommender has fine results with CIP 1 and others. As a result CIP5 who is having direct trust with CSP 5 can recommend itself to cloud recommender as a direct reference. With this instance the cloud recommender can recommend CIP 5 to other CSP's. As an updated result CIP 1 trusts CIP 5 for all its computations and computing resources can be provisioned to all remaining CSP's.

Now consider option 2 i.e. Parallel Trust Combination (PTC), from figure 2 we attained the transitive principal for targets opinions feedback. PTC accounts two or more CIP as a functional trust scope. For an instance the CIP 2 needs a better decision making infrastructure to execute all its computing resources. Now CIP 2 process on a parallel manner with CIP 1 which is federated and has direct trust based on SLA requirements of both. If CIP 2 needs to trust CIP 4 and 5 respectively, either it needs to make a functional trust scope with both recommender and CIP 1. As a result CIP 2 update its trustable CSP's mutually to provision computing resources through CIP 1 which is been evaluated with absolute service provider. Therefore PTC solves the uncertain issues of an entity.

Now option 3 i.e. subjective logic method is a theoretical framework for trust assessment proposed by Josang [2]. The framework defines the belief segment that is relevant to probability theory [10]. The outcome of this framework adds up at least to mark of one and the left out probability is stated for overall outcome representation. In case of

ignorance that takes place in an entity than belief theory is absolute and well compatible with situations for given tasks.

The use of subjective method in this thesis allows representing the opinion of a target feedback in order to recommend suitable computing resources to the end user. Belief uses a metric known as opinion mentioned as W^A_x, A represents overall entity with proposition x, the opinion with respect to probability theory is expressed as $W^A_x = (b^A_x, d^A_x, u^A_x, a^A_x)$ [9] where b^A_x represent the belief , d^A_x represent distrust , u^A_x represent the uncertainty, a^A_x is used as base rate in measuring the weight of uncertainty. The last proposition of base rate can alone handle the probability of distribution between CSP and CIP, the indexes b^A_x, d^A_x, u^A_x, a^A_x can also be featured as b_x, d_x, u_x, a_x determines the proposition of x which belongs to $b_x, d_x, u_x, a_x \in [0.0, 1.0]$. The base rate alone can be used for probability of selecting the CIP and others can be represented as $b_x + d_x + u_x = 1$ [10].

We subject the opinion has internal opinion and external opinion. The internal opinion determines the facts of decision led by target nodes with in CIP and external opinion is led by the decision of all federated CIP's. Both internal and external opinions are evaluated using three operators proposed by Josang, given by Conjunction operator (∧) used for combining opinion of two parties, Consensus operator (⊕) agreement of two and Discount operator (⊗) use for recommendation [10]. Ordering of opinions is based on expectation with respect to trust. The trustworthiness is evaluated on CIP computations with respect to SLA parameters and CSP ratings on CIP resources. It's essential to combine both internal and external opinion to satisfy CSP ratings on CIP. The updated opinion based on internal and external can be represented as W_{IT}, W_{ECIP}, W_{SLA}, W_{CSPR}, where W_{IT} is opinion of internal target nodes of all CIP, W_{ECIP} represents external CIP opinion to the recommender and their federated CIP's, W_{SLA} opinion acquired by SLA observation, W_{CSPR} opinion based on service provider ratings and finally Trust of CIP is represented as T_{CIP}. Trust of CIP is given as:

$$T_{CIP} = \text{Expectation}(W_{(IT \otimes ECIP) \wedge SLA}) \quad (9)$$

The overall Entity trust is represented as ET, and given as:

$$ET = Expectation\ (W_{(ECIP \otimes CSPR) \wedge SLA}) \quad (10)$$

Consider two target nodes I and J of different cluster X and Y respectively, representing internal opinion based on its interaction where $W^I_x = (b^I_x, d^I_x, u^I_x, a^I_x)$ is node I opinion about cluster "x" nodes interaction with target node "I" of any CIP. $W^J_y = (b^J_y, d^J_y, u^J_y, a^J_y)$ is node J opinion about cluster "y" nodes interaction with target node "J" of any CIP and referred as a advice to node "I" . From figure 10, if CIP 1 internal opinion is same as of CIP 2/ CIP 3 as they are federated, that opinion can be followed by discount operator W^{IJ}_x, than W^I_x *and* W^J_y is represented as $W^{IJ}_x = W^I_x \otimes W^J_y$, finally internal target opinion to CIP is represented as $W^{IJ}_{(IT \otimes CIP)}$. To extend a bit the proposition of cluster x with cluster is completely based on mutual decision between I and J with better interactions. The subjective logic parameters proposed by Josang [12] like belief, disbelief , uncertainty and base rate with respect to internal opinion can represented as $W^{IJ}_x = W^I_x \otimes W^J_y = (b^{IJ}_x, d^{IJ}_x, u^{IJ}_x, a^{IJ}_x)$

$$b^{IJ}_x = b^I_J\, b^J_x \quad (11)$$
$$d^{IJ}_x = b^I_J\, d^J_x \quad (12)$$
$$u^{IJ}_x = d^I_J + u^I_J + b^I_J\, u^I_x \quad (13)$$
$$a^{IJ}_x = a^J_x \quad (14)$$

Equal probability between both opinions is required i.e based on the rate of interacting evidence of nodes with its targets. The representation of the evidences is considered as positive and negative relations proposed by Josang [11] and the ordering of opinions with total evidences can be represented by $e_t = r+s$. The internal target opinion can be agreement with its evidences for certain condition is given as follows $W^{IJ}_{x(r,s)} = W^I_x \oplus W^J_y$. Opinion representation for all subjective parameters with proposition of "x" for certain condition is represented as

$$b_x = c\, r / e_t \quad (15)$$

$$d_x = c\, s / e_t \quad (16)$$

$$u_x = e_t / (r\, s + f + 1) \text{ when } e_t \geq 1 \text{ or } u_x = 1 \quad (17)$$

Where c is the certain parameter for the function $c(e_t)$ and f is the function that represents total cluster "x" proposition center for all probability i.e. $f = sqrt\ (c_2^2 - c_1^2)$. The opinion model of CIP has the following rules.

1. The total opinion of any proposition of cluster with higher expectation of probability has got the higher opinion.
2. Uncertainty with lower rate opinion to be the higher opinion
3. Cluster opinion with least base rate to be higher opinion

The Expectation of the overall opinion for cluster x of a CIP is recommended as $E(x) = b_x + a_x u_x$ (18)

V SLA Observations and Monitoring

Observation is one of the satisfying parameter of SLA; it plays its importance in determining the overall opinion over CIP where CIP establishes the SLA with CSPs for their consumer services. A dedicated individual SLA is provisioned for all CSP service which is based on various indicators like CPUs, available free disk space, number of virtual machines etc. the observations made in this section is referred to figure 10 scenario. In order to achieve QOS in cloud environment SLA is processed and performed using monitors proposed by Foster [12]**.** The monitoring of SLA is measured using Open Nebula System that offers various infrastructures from different CIPs and also federate with market place to choose various application deployments overhead.

In this thesis the CIP opinion are measured in three steps. The first step indicates the consensus part between *IT* and *ECIP* based on its federation compatibility. This leads to *ECIP* recommending its consensus opinion to all its federated CIP. In second step the conjunction between CIPs and bursted cloud exists and in the third step the evidence obtained by all the CIP is indicated with trust based on SLA monitoring.

Illusion: To check the SLA monitoring. Consider the health care scenario for cloud described in figure 10. Consider a situation where, medical test reports of various patients distributed among different hospitals and accessing their reports may lead with heterogeneous infrastructure and application deployment which consumes higher rate of

computing resources on each and every CIP, resource with huge amount of Virtual Machines, RAM utilization, CPU execution and usage and available compact space for processing their reports in different infrastructures. For individual hospital the resource request to all CSP is managed with announced SLA. The IT and ECIP opinion obtained as a feedback for resource request to all CSP demands. From the example an instance is created through AWS and provisioned on open nebula platform, where CIP1 deals with all five CSPs to host their healthcare application, the resource demand may occur in similar time frame. There exists a limitation with opinion of other CIPs, where CIP1 can't dominate over the resources of other federated CIPs violating SLA. Due to this situation a private instance is securely created which leads with bursting cloud situation to acquire the resources by CIP 4 and CIP 5.

Dedicated five SLAs been issued to CIP 1, enabled with CSPs i.e. CSP 1 to CSP 5, along indicators of VMs, CPU and so on. Suppose SLA 1 deal with opinion of IT (internal targets) and violating opinion of ECIP (external) in CIP 1 and SLA 1 attached to CSP1, SLA 2 for both IT and ECIP opinions are attached to CSP 2 and so on. Let us consider the monitors that can be associated with specific SLAs. In this case consider five monitors. Monitors are represented by term "M" SLA 1 deals with M1 and M2 for all its indicator types VM and CPU rate respectively, with opinion of IT strictly. SLA 2, 3, 4 and 5 are instanced with M3, M4 and M5 for all indicators of SLA. The internal opinion monitoring is treated with both positive and negative evidences. For an instance, if CIP 1 overall consensus opinion to be considered for CSP1 to CSP 5, than a compliance against ECIP is raised for all its indicator types. Lets assign M1 and M2 with 100 compliances and 20 non-compliances (i.e. r=100 and s=20) for CIP1. So the total evidence based on SLA 1 with respect to CIP 1 is $e_t = r + s = (100+20) = 120$. For SLA 1 we figure out multiple opinions of targets as a single feedback and measured by their constants i.e. $f = sqrt\ (\boldsymbol{c_{2j}^2 - c_{1j}^2}) = sqrt\ (100^2 - 20^2) = 24.49$, here $\boldsymbol{c_{2j}^2 - c_{1j}^2}$ *are the* constant of control input feedback stated in algorithm 4.1. The subjective parameters are computed as follows.

$u_x = 120/(100 * 20 + 24.49 * 24.49 + 1) = 0.0465$ (19)

$a_x = 1-u_x = 0.954$ (20)

$b_x = 0.954*100/120 = 0.79$ (21)

$d_x = 0.954*20/120 = 0.159$ (22)

Consider monitors M1 and M2 associated with SLA 1 to identify opinion of overall CIP1 by its indicators VM and CPU represented as W_{VM} and W_{CP} respectively. In order to obtain opinion of VM along with SLA agreement and CIP 1 conjunction with VM opinion can be represented as

$W_{CIP} \wedge_{VM} = (0.798, 0.159, 0.0465)$

where $a_x > E(x)$ (23)

$W_{CP=}(0.798,0.159,0.0465)$ (24)

The SLA opinion based for CIP1 for all its indicators with conjunction is given as follows

$W_{SLA} = W_{VM} \wedge W_{CP} = (0.798, 0.159, 0.0465)$ (25)

$E(x) = b_x + a_x u_x = 0.79 + 0.954 * 0.0465 = 0.83$ (26)

The opinion of CIP results a better rate when SLA observation are made on CIP

VI Cloud Service Provider Rating

The rating can be defined as; the amount of CSP rating on its satisfaction is computed by the services provisioned by CSP utilizing CIP. Allocation of a dedicated SLA for each CSP, the CSP provides separate ratings based on the indicators of all CIPs services. The importance of CSP rating is to pull out the opinion of over a CIP. An agreement between two CSP and CIP is required to compute the ratings of CSP; the computation can be followed with conjunction and consensus operators. Consider a variable "n" that defines n CSPs that are made available, these CSP provides its mutual opinion with its attached indicators with respective CIP. Finally the *CSPR* is given by

$$W_{CSPR} = W_1^{CSP1,\ CSP2 \ldots CSPn} \wedge W_2^{CSP1,\ CSP2 \ldots CSPn} \ldots \wedge W_m^{CSP1,\ CSP2 \ldots CSPn} \quad (27)$$

Illusion: consider the indicators mentioned as CPU, VMs, space on disk and memory, which has as got the rating instance created by CSP 1. For an instance the CSP 1 provides 50 excellent and 2 worst ratings for all indicators, than r=50 and s=2. We can map the instance based on the opinion of CSP 1 over CIP 1 with respect to all its indicators.

$\boldsymbol{W_{CP}^{CSP1} = (b_{CP}^{CSP1}, d_{CP}^{CSP1}, u_{CP}^{CSP1}) = (0.79, 0.159, 0.02)}$ and this opinion holds good for all the indicators

From the table below different instances of opinion with respect to indicators over CIP 1 by CSPs are mentioned

Table 1: CSP Rating towards CIP

Cloud Service Provider	***Rating***	***Evidences***
CSP 2	*E=100, =10*	*r=100, s= 10*
CSP 3	*E=200, =20*	*r=200, s= 20*
CSP 4	*E=200, =30*	*r=200, s= 30*
CSP 5	*E=250,w=25*	*r=200, s= 25*

E= Excellent rating, w=Worst rating

The opinion for different CSP mapped in the table is given by

$\boldsymbol{W_{CP,\ VM,\ disk,\ mem}^{CSP2} = (0.854, 0.0854, 0.057)}$ (28)

$\boldsymbol{W_{CP,\ VM,\ disk,\ mem}^{CSP3} = (0.995, 0.09, 0.005)}$ (29)

$W^{CSP4}_{CP,\ VM,\ disk,\ mem} = (0.86,\ 0.129,\ 0.0051)$ (30)

$W^{CSP5}_{CP,\ VM,\ disk,\ mem} = (0.99,\ 0.08,\ 0.07)$ (31)

The entity trust between CIP 1 and CSPR with support to equation 10 can be represented as

$ET = Expectation\ (W_{(ECIP \otimes CSPR) \wedge SLA)}) = (0.901,\ 0.108,\ 0.03142)$ (32)

The above Entity trust leads with higher belief rate and close to the base rate for all iteration. The base rate a_x computed satisfies at higher rate when compared with CSP rating of belief parameter. The average result of base rate computed for all indicators with uncertainty of indicators considered is given by

$Average(a_x) = a_x^{CSP1 \cdots} a_x^{CSP5} = 0.995+0.94+0.94+0.93+0.98/5 = 0.95,\ where\ (a_x > b_x)$ (33)

VII Evaluation of Trust Model

In this chapter we have considered Open Nebula representing in figure 3 integrated with AWS market place attached to 15 VM's with 10 instances. The instances are covered accounting with Amazon, azure storage and SoftLayer for host instance creation and represented in figure 4. The system represents a cloud burst with existing local resources of a private cloud and is connected with remote CSP. The infrastructure is formulated with clusters, hosts, virtual networks and zone regions and it is represented in figure 5. The subjective opinion of the internal cloud is evaluated with respect to overall base rate of that entity. The Azure location for storage availability is deployed on each host (potential bigger in capacity for load balancing). The templates are created and attached for single administrator with hybrid implications. The VM templates are initiated with all instances at a time. The scheduler can place VM's as external cloud by lookup to any other host. The instance of the entire host after initiating VM is refreshed on its priority of opinions. For an instance in figure 6, let's consider softlayer which is private cloud burst after scheduling is fixed per host, even after that the base rate of the entire cloud entity remains the same and in figure 7 the same is depicted with Azure constantly running over three VM's. Finally the internal opinion of all the target hosts are equal with their base rates, this can be justified by shutting down all the host instances at the same time.

Fig 3: Represents the infrastructure for hosting cloud burst

Fig 4: Host instance creation after cloud burst

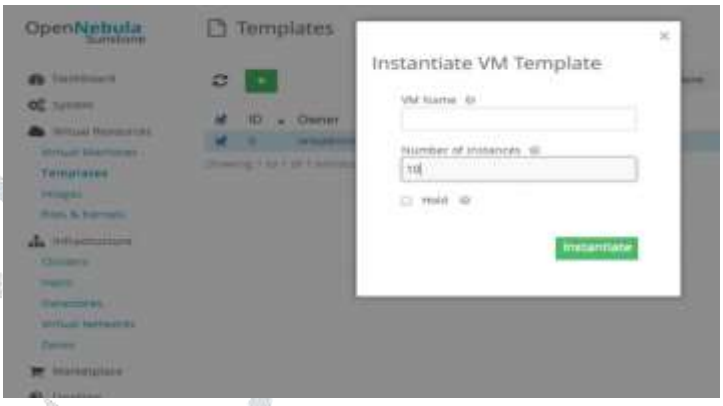

Fig 5: VM template attached to single administrator

Fig 6: Integration of all instances as hybrid

Fig 7: Softlayer instance hosting private cloud

Fig 8: Azure instance running remotely for all three machines

After setting the instances the base rate of the entire hosts remains the same due to negotiable assessment. Now let's connect the Amazon market place with Open Nebula prototype, to find the accuracy of different targets, we have consumed real data sets. Let us consider the marketplace host for all interactive target hosts base rate for different entities that's been set up varies with respective region. Consider the ratings of a mobile seller (green mobiles), the ratings differ from region to region based on user prediction on seller trust. The data sets collected ranges between 1 to 5 ratings; now for all the host instances created we normalize 10 users out of 518 who have rated green mobiles. The first 10 user are listed in the table 4.1 below. Base on different user perspective and cloud dimensions the host instances running on any private cloud manage only one instance at a time. Therefore for convenience we choose the rating as positive and negative till the i^{th} transaction of the hosts. We compare the work with S.S. Roy approach [6]. Considering our model and S.S.Roy approach, both of it takes the i^{th} rating in order to predict the additional increment of i+1. The instances of the entire host running on a federated rate must be able to satisfy previous i^{th} rating by fulfilling the belief over the base rate that ranges between 0 and 1 [considering 0.5 is minimum base rate a_x]. The graph in the figure 9 shows the error predicted by the entire time stamp for a single seller (green mobile). The conclusion of our results provides that our subjective error prediction rate is minimum when compared to S.S. Roy approach [6] and its represented in table 4.2.

Table 2: Ratings and review by users

ID	Seller ID	Ratings	Review
1	1	5	"great seller thank you"
2	2	4	"happy with delivery."
3	3	5	"Wonderful transaction. Book in great condition, well packaged and received very quickly. A super seller! Thank you very much."
4	4	5	"Just as expected"
5	5	1	"Received damaged item. seller refused to refund sending a number of rude, angry E-mails accusing me of lying. Only when i submitted a claim and sent E-mail of complaint to Amazon did seller eventual agree to refund. Sent damaged item back and, unbelievably, seller further accused me of watching and damaging the whole box set! Seller was rude, arrogant and unco-operative throughout. STAY AWAY!!!"
6	6	5	"thank you"
7	7	2	"Order cancelled by seller and refund given. However, this was advised by Amazon. No communication from the seller and this is reason for 2 stars. I think that a quick note from the seller with an apology would have been appropriate in the circumstances. Hopefully I can still obtain elsewhere."
8	8	5	"Very happy"
9	9	5	"none"
10	10	5	"delighted with the cd, arrived promptly and was in excellent condition, thankyou very much"

Table 3: Error prediction rates for all the private hosts after federation

Approach	Amazon seller provider	Azure provider	Softlayer	Physical host
S.S.Roy	0.12756	0.09278	0.09415	0.14004
Our approach	0.12567	0.04878	0.05848	0.02848

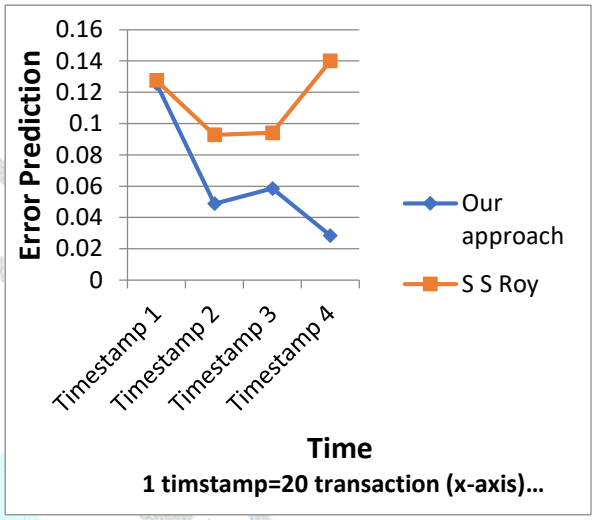

Fig 9: Error prediction for all the entity instances for one seller

Finally the result observations validates that for a federated cloud running many instances irrespective of region requires bursting support. Our approach figures out with minimal error rate to other trust model [6], based on the real time evidences found. The accuracy rate to be consensus while meeting multiple hosts, which to be similar and positive for the selection of trust model.

A. Monitoring of SLA

The main focus of this evaluation depends on the federated cloud scenario, when bursting occurs between one or more CIP's. Monitoring of SLA is an individual parameter choice indicating only SLA presence in the trust factors. The trust features are led with two issues, one is Compliant and the other is non-compliant. For choosing this SLA as a parameter in federated environment, consideration of cloud dimension resources are necessary as they are related with CIP 1 as constant reference of CIP 1 from figure 1. The dimensions of resource demands are increased additively by all CSP's and from figure 1 health care example, CIP1 is the only infrastructure to provide the needful demands of CSP and CIP1 is chosen to be a compliant perimeter along with SLA, as a result this increases the alertness of evidences positively which is followed by CSP's for CIP1. When SLA violations are out reached with all its said properties than the cause can be due to the over flow service capacity of CIP1

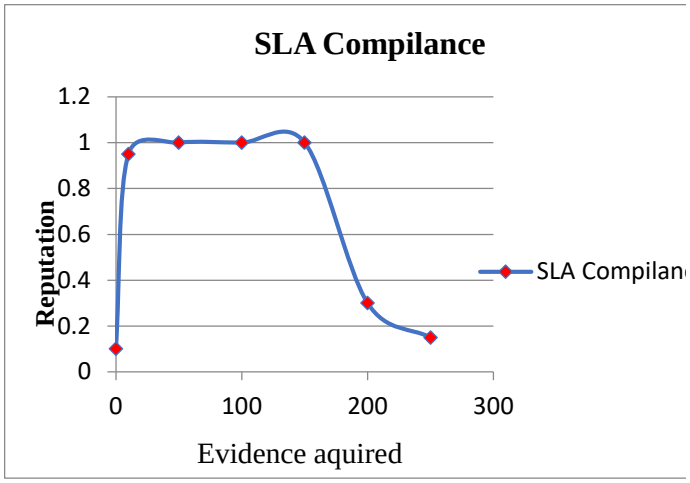

Fig 10: SLA compliance monitoring for positive and negative evidences

The results from figure 10 represent additive increase of reputation due to positive evidences managed by all CSP's. The total positive evidences found to be achievable by CIP1, only when CSPs gain positive evidences. The SLA meet up can be up to maximum 1 for first 150 and it linearly decreases with next 50.

B. Assessment for CSP Ratings (CSPR)

We consider CSPR as an individual parameter that exist with federated trust cloud. The CSPR rating is evaluated with respect to positive and negative evidences. Here in the federated scenario form figure 11 the CSPs expect its computing resources with CIP1 and rate the CIP1 with external opinion and recommendation. The indicators of computing resources are considered. CIP1 rating is situated with all CSPs, here the reputation of CIP1 is estimated by CSP initially and later CSP2 to CSP5 are estimated. In case if SLA violations are highlighted than CSPs rate CIP1 with decreased negative range. Here CSP1 positive and negative evidences are fixed to 250, 150 as positive and 100 for negative.

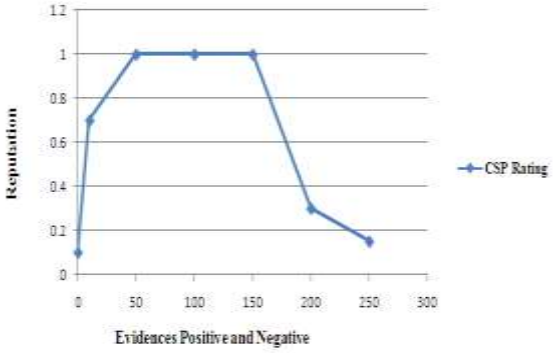

Fig 11: Reputation evaluated based on CSP rating

From the results it is observed that the mutually received evidence and ratings by other CSPs to CSP1 is increased with positive ratings till the reputation is reached to 150.

Finally the result observations validates that for a federated cloud running many instances irrespective of region requires bursting support. Our approach figures out with minimal error rate to other trust model [3], based on the real time evidences found. The accuracy rate to be consensus while meeting multiple hosts, which to be similar and positive for the selection of trust model.

VIII Conclusion

The issue and challenges faced in federated environment due to cluster heterogeneity and their multiple targets identification is addressed. A control input is resulted with cluster constants and subjected to total target identification and coverage. Trust modeling is achieved based on few options, all these options represent the perspective of federated and bursting situations in cloud. The options considered are transitive, parallel and subjective methods. Our proposal with consideration of internal target opinion and external CIP opinion satisfies different IaaS provider's credibility and reputation. Entity trust is achieved through the following opinion factors like belief, uncertainty and base rate. The SLA requirements are satisfactory after an opinion is generated with agreement, negotiation and recommendation. Finally, the infrastructures cluster opinion is considered to be the primary fact for complete deployment overhead. Error prediction of our approach proves with a minimum error prediction for all the entity considered with respect to their heterogeneous instances. The SLA compliance being a challenging issue for generating total positive and negative evidences in order to create the reputation along.

References

[1] Josang.A, "Robustness of Trust and Reputation Systems", Springer, pp. 253–262 210, 2012

[2] Josang.A, Ismail.R, Boyd.C, "A survey of trust and reputation systems for online service provision". Decision Support Systems. 43, 618–644, 2007

[3] Sudipta Singha Roy, Tamjid Haque Sarker, M. M. A. Hashem, "A Novel Trust Measurement System for Cloud-based Marketplace", Proceedings of International Conference on Electrical Information and Communication Technology, IEEE,2015

[4] Li W, Ping L, "Trust Model to Enhance Security and Interoperability of Cloud Environment", Cloud Computing, Lecture Notes in Computer Science, Springer, 5931:69-79, 2009

[5] Marsh S, "Formalising Trust as a Computational Concept". Doctoral dissertation, University of Stirling, 1994.

[6] Banerjee S, Mattmann C, Medvidovic N, Golubchik L, "Leveraging architectural models to inject trust into software systems". In: Proc. SESS '05, ACM, New York, NY, USA, 1-7.

[7] Marco Dorigo, "Ant colony optimization theory: A survey", RIDIA, Université Libre de Bruxelles, CP 194/6, Ave. F. Roosevelt 50, 1050 Brussels, Belgium November 2005

[8] Artz.D, Gil.Y, "A survey of trust in computer science and the semantic web". Web Semantic Science. World Wide Web 5, 58–71 2007

[9] Guoyuan Lin, Yuyu Bie, Min Lei, Kangfeng Zheng , "ACO-BTM: A Behavior Trust Model in Cloud Computing Environment", Atlantis press.Com,2014

[10] Josang A, "A logic for uncertain probabilities". International Journal on Uncertain. Fuzziness Knowledge based systems. 9, 279–311, 2001

[11] A. Josang, R. Hayward, S. Pope, "Trust Network Analysis with Subjective Logic", Proceedings of the 29 Australasian Computer Science Conference (ACSC2006), Volume 48, Hobart, Australia, January 2006

[12] H. Foster, "Service monitoring configurations with SLA decomposition and Selection", ACM Proceedings on Applied Computing, 2011

[13]Huang.J,Nicol.D.M."Trust echanisms for cloud computing. J. Cloud Computing". Advance Systems.Apple, 2013

[14] Noor.T.H, Sheng.Q.Z, "Trust management of services in cloud environments", ACM Computing. Survev, 2013

[15] Josang.A, Robin Hankin, "Interpretation and fusion of hyper opinions in subjective logic". In Information Fusion (FUSION), IEEE, 2012.

[16] R. Calheiros, R. Ranjan, A. Beloglazov, C. De Rose, and R. Buyya, "Cloudsim: A toolkit for modeling and simulation of Cloud Computing environments and evaluation of resource provisioning algorithms," Software: Practice & Experience, vol. 41, no. 1, pp. 23–50, 2011.

[17] Hwang.K, "Trusted cloud computing with secure resources and data coloring. Internet Computing. IEEE 14, 14–22, 2010.

[18] Conner.W, Iyengar .A , Mikalsen. T, Rouvellou. I, Nahrstedt.K. "A Trust Management Framework for Service-Oriented Environments" , Proceedings of WWW , Madrid, Spain April 2009

[19] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O' Reilly Media, USA, 2009.

[20] Santos.N, Gummadi.K.P, Rodrigues.R. "Towards trusted cloud computing", Proceedings of the conference on Hot topics in cloud computing. 2009: 3-3.

[21] Peter Mell, Tim Grance, "The NIST Definition of Cloud Computing". National Institute of Standards and Technology, Information Technology Laboratory, Version 15, 10-7-09:2, 2009.

[22] Li W, Ping L, "Trust Model to Enhance Security and Interoperability of Cloud Environment", Cloud Computing, Lecture Notes in Computer Science, Springer, 5931:69-79, 2009

[23] A. Josang, R. Hayward, S. Pope, "Trust Network Analysis with Subjective Logic", Proceedings of the 29 Australasian Computer Science Conference (ACSC2006), Volume 48, Hobart, Australia, January 2006