I. J. Computer Network and Information Security, **2016, 1, 43-52**
Published Online January 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.01.06

Secure Allocation of Resources in Cloud Using Trust

Usha Divakarla, K. Chandrasekaran
Department of Computer Science and Engineering, National Institute of Technology Karnataka Surathkal, Karnataka, India-575025
Email: ushachavali@gmail.com, kchnitk@gmail.com

***Abstract*—**Cloud is the recent emerging technology in all aspects. The basic concern with the usage of this Cloud Technology is security. Security poses a major drawback with data storage, resource utilization, virtualization, etc. In the highly competitive environment the assurances are insufficient for the customers to identify the trust worthy cloud service providers. As a result all the entities in cloud and cloud computing environment should be trusted by each other and the entities that have communication should have valid trust on each other. Trust being the profound component in any network has attracted many researchers for research in various ways. The models developed so far are platform dependent and are not valid for heterogeneous platforms. An efficient model which can be ported on any platform is the current research trend in the research world. Our model is platform independent and also helps in calculating trust while migrating to another platform. The result shows that the proposed model is much more efficient in terms of computation time.

***Index Terms*—**Trust, Trust Model, Entropy, Security Issues, Family Gene Algorithm.

I. Introduction

The major influence of any human interaction is Trust. In technology trust has no definite meaning. It is defined as the degree of trustworthiness. The lesser the degree of trustworthiness the more is the risk to the system. Trust is often measured/related to terms like cooperation, confidence and predictability. According to Gambetta[1] trust is the probability that an entity will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of co-operation with it.

The basic principle for any successful relationship is the base value of trust among the entities involved. Trust is one of the obligatory qualities in any relationship. It is due to this trust that any entity could cooperate beyond a system of formal and legal rules.

The basic nature of trust is found as the tension between depending upon another and instituting controls to make sure that other performs. The higher the risk the higher would be the loss. In human science or information technology the trust plays a vital role in reconciling away fears and the willingness to become vulnerable to the other without controlling the other [2].

A. Trust in Cloud Computing Environment

Cloud is the emerging technology for the users to easily work with minimum effort and minimized cost. In every cloud, service is tendered with as pay-as-use term. So users can use the cloud technology to maximize their profit with minimum cost and effort. To ensure proper and efficient secured usage of resource users as well as cloud providers need to trust each other.

Trust being belief of human interaction has many definitions to it. Several researchers have studied the role of trust and reputation in e-commerce, peer to peer networks, grid computing, semantic web, web services, and mobile networks. The valuable information available on trust in various fields is of great benefit to computer scientists and it also has the drawback of presenting a complex notion for trust as there is no common agreement on a single definition of trust. Various researchers have defined trust as attitude, belief, probability, expectation, and honesty and so on. Due to the adoption of cloud computing in the industry, a significant challenge [3] is being raised in managing trust among cloud service providers and cloud service consumers. Several solutions have been proposed to assess and manage trust feedbacks collected from participants [4] [5] due to high significance to the trust management. Due to malicious behavior of user's Trust management experience a setback. Due to confusion in trust definition, trust has been evaluated in very different ways. Some schemes employ linguistic descriptions of the trust relationship, such as Policy Maker, distributed trust model, trust policy language and public-key infrastructure. On the other hand, the quality of trust feedbacks differ from one person to another, depending on how experienced he/she is.

Various models are developed to ensure quality of trust with respect to the domain. The drawbacks like centralized architecture concept, private cloud for security of data, problems with keys due to changed configuration, problems in integration of the proposed layer with the existing configuration likewise. Though these models address security aspects, an improvement with respect to trust models is desirable.

II. Related Work

In any network Trust is the eminent factor that plays a vital role in the security of the network. The more the degree of trustworthiness the less is the risk. Though extensive research has taken place on this trust factor, trust is still the most concentrated factor for any research in distributed networks.

A. Literature Survey

Trust is an eminent factor in any network. Trust management comprises collecting the information necessary to establish a trust relationship and to dynamically supervise the existing trust relationship. The various models for describing trust and trust establishment in Cloud Environment are listed below.

Authors [6] have analyzed the trust in the cloud system in terms of security and privacy. The authors have forecast that remote access control of the resources, transparency in cloud provider's actions and providing security for users would enhance the trust of users in the services and service providers.

Authors [7] have proposed a trust model of cloud security in terms of social security. The social security is divided into three sub areas, namely; multiple stakeholder problem, open space security problem, and mission critical data handling problem. The multiple stakeholders are the client, the cloud service providers, and third parties. The client assigns the operations to cloud providers as written in the Service Level Agreement (SLA). A cloud provider gives the trust to a client based on the contract that is made up of three documents known as Service Policy/Service Practice Statement (SP/SPS), Id Policy/Id Practice Statement (IdP/IdPS) and the contract. A cloud system, thus installed is called a secure cloud by the authors.

Authors [8] proposed a domain-based trust model to ensure the security and interoperability of cloud and cross-cloud environment. They also suggested some trust based security strategies for the safety of cloud customers and providers.

The family gene based cloud trust model [9 ,10] proposed is basically based on the study of various basic operations such as user authentication, authorization management and access control, and proposed a Family-gene Based model for Cloud Trust (FBCT) integrating these operations.

CARE resource broker integrated trust model[11] calculates trust based on three components, namely, Security Level Evaluator, Feedback Evaluator and Reputation Trust Evaluator. Security level evaluation is carried out based on authentication type, authorization type and self-security competence mechanism.. Feedback evaluation has three different stages, namely feedback collection, feedback, verification and feedback updating. The reputation, trust evaluator computes the trust values of the cloud resources based on the capabilities of computational parameters and network parameters

Authors [12,13] have proposed a system of integrating Trusted Computing Platform (TCP) into the cloud computing system which improves the security and dependability of cloud. The TCP is used in authentication, confidentiality and integrity in a cloud computing environment.

SLA based trust model[14] consists of the SLA agents, cloud consumer module, and cloud services directory. The SLA agent groups the consumers to classes based on their requests, designs SLA metrics, negotiates with cloud providers. Cloud consumer module requests the execution of services. Cloud services directory advertises the cloud provider's services and helps consumers find the appropriate providers.

Multi-tenancy trusted computing environment model (MTCEM)[15] is a two-level hierarchy which supports the security duty separation and also supports three types of stakeholders namely, CSP, customers and auditors. CSP responsibility is to keep infrastructures trusted while the customer assumes responsibility starting from the guest OS, which are installed by the customer on the Virtual Machines provided by the CSP. The auditor monitors the services provided by the CSP.

Authors [16] study states that the existing trust models ignore the existence of a firewall in a network. The authors have proposed a firewall based trust model in the Cloud. Their paper gives the detailed design calculations of the proposed trust model and practical algorithms of measuring and updating the value of dynamic trust.

Watermark-aware trusted environment[17] model is made up of two components, namely the administrative center and the cloud server environment. The administrative center inserts watermark and tailors the Java Virtual Machines (JVM) and the trusted server platform includes a series of cloud servers deployed with the customized JVMs and is used to handle security due to running software on a cloud.

Authors [18] have proposed a system without the involvement of a trusted third party based on the study conducted on identity management in the cloud. The proposed system is based on the use of predicates over encrypted data and multi-party computing.

Security framework model[19] consists of three main entities, namely cloud customers, service integrators and service providers. The Service Integrator acts like a bridge between the customers and service providers. The Service Integrator module consists of security management module, trust management module, service management module and heterogeneity management module. The heterogeneity management module manages the heterogeneity among the service providers.

A reputation system based on a fuzzy-logic was developed by Song [20] which has the ability to handle uncertainty, fuzziness, and incomplete information. The proposed system uses fuzzy logic inference rules to calculate local trust scores and to compute global reputation.

Authors [21] developed a general trust model based on QoS selection and Certain Trust Model which uses QoS parameters like direct trust, user feedback, user preference, etc. to calculate trust of the service provider.

Authors [22] proposed Trust Management Model based on fuzzy set theory called TMFC where direct trust was classified into two types due to difference in their trust assessment.

Authors [23] proposed HITCloud model to handle some of the security issues of the cloud like data integrity, privacy using a feedback mechanism. The feedback from users will be filtered according to their reliability and accuracy of accomplishment, which in turn will be calculated based on node trust and region trust.

Authors [24] proposed Reliability-based Trust Management for Cloud Services which is based on the feedback. Users who have no prior experience with service provider can submit their trust feedback to the trust management system to make a decision to use the service of the provider or not. The feedback from users is filtered according to their reliability, which is calculated based on familiarity and consistency.

Authors [25] proposed multi-faceted trust management architecture for selecting appropriate cloud service providers based on a calculated trust which in turn is dependent on the customer attribute value.

Authors [26] proposed a new trust management architecture which consists of cloud service registry and discovery which helps to register and locate serve provider based on the three service models namely Infrastructure-as-a-service, Platform-as-a-service, Software-as-a-service. Based on the different trust values of the models the selection of service providers is done.

Authors [27] proposed pool oriented resource trust management which calculates the trust of pool of resources that would be used for services. The trust thus calculated is verified and a protocol is developed to initiate communication between the resources in the pool.

Authors [28] proposed a trust based solution to evaluate the Hybrid service model for data credibility. They have proposed two algorithms which handle trust evaluation for both private cloud and public cloud.

Authors [29] have proposed certification based trust model to handle assurance techniques which can manage trust information during production and also handle the third party trust to manage the entire assurance technique.

Authors [30] have proposed a hysteresis based robust trust computing mechanism that computes trust value using a non-linear equation which has more than one state at a given time.

Authors [31] have proposed a trust system based on server response time where the trust computation score lies between -1 and 1 for different levels of services in terms of response time and confidence levels.

Authors [32] have proposed a group signature based trust management for Iaas cloud model. The proposed architecture helps to the resource pool oriented trust management in a cloud infrastructure. A protocol is also devised to synchronize the interaction and behavior of trusted resources.

Authors [33] have proposed a trust system based on the response time. The trust system computes a trust between 0 and 1 for different levels of services and continues to improvise the calculated trust values based on the performance of the system.

B. Shortcomings of Existing Trust Models

Though various Trust Models are developed to solve the trust issue still trust is a major concern. An extensive literature survey reveals some of the drawbacks found in the various trust models explained in the above section. The issues are listed as below:

Trust calculated by model [7] is internal to the organization. The Cloud Service Provider (CSP) has nothing to do with the security of the resources. So the organization has to have a private cloud to secure its data which is not possible with small/medium organizations.

In Family Gene based trust models [9,10] the trust model is just proposed for authentication and is tested by simulation. The model does not deal with security aspects either of data or of resources. A real time implementation is not done.

In CARE [11] resource model conventional scheduling is done through FIFO. So computation/process starves for the necessary resources. The priority of resources for the critical jobs is not taken care.

Authors [12,13] have proposed trusted computing technology for trust evaluation. The basic disadvantage of this model is that the underlying architecture is based on Trusted Computing Platform [TCP] which is difficult to integrate cloud computing with respect to hardware.

Authors [14] have proposed SLA based trust model and no implementation or evaluation has been developed or described. This model is a reputation based trust that has a disadvantage that the user with high scores for reputation can cheat user in fewer transactions even though they receive negative feedback. This model has a centralized architecture, so all the services and reputation information has a single point of failure.

In the Role Based Trust model the trust is based on the roles, ID used for TCP, standard certificate for assurance. The hardware maintains a master key for each machine and it uses master keys to generate unique sub key for every configuration of the machine. The data encrypted for one configuration cannot be decrypted in another configuration of the same machine. If the configuration of the machine changes the session key of the local machine will not be useful.

The Active Bundle Scheme[18] proposed based on Identity Management model approach is independent of a third party, it is less prone to attack as it reduces the risk of correlation attacks and side channel attacks, but it is prone to a denial of service as an active bundle may also be not executed at all in the remote host

Though a lot of work is done in trust area still no researcher has proposed any trust model for trusting the resources in the cloud. As resources are the entities in cloud, the security of these entities is very essential. Though the security as a whole is taken care by the service provider still security of the resources in the cloud is at stake. It is noted from the Existing Models that trust plays an important part of the security in the

cloud, but trust as a whole in terms of services provided is taken into account. When an entity enters the cloud the trust is calculated by the service provider in accordance with the other resources.

From the above details it is very clearly known that researchers have till now not considered the availability/non-availability of resources for any transaction. Thus a strong Trust model is needed to calculate Trust in Cloud Environment based on the availability of resources as the resources are the main basis for any transaction in the Cloud. Hence a new Trust Model is proposed in the next section to handle this problem.

From literature survey it is very clearly known that researchers have till now not considered the availability/non-availability of resources for any transaction. Thus a strong Trust model is needed to calculate Trust in Cloud Environment based on the availability of resources as the resources are the main basis for any transaction in Cloud. Hence a new Trust Model is proposed in the next section to handle this problem.

III. Proposed Trust Model

Trust is the belief of one entity on other entity to work in coordination or to complete a specific task successfully. Though this trust till date is not standardized, researchers define this trust in their own way. Based on this trust value the basic security shield is formed though not completely. For users to distinct between cloud providers in terms of offered trust, there should be some mechanism to evaluate trust services by independent third parties.

A. Conceptual Diagram of the Proposed Model

To ensure a strong trust value in cloud environment we have proposed a Trust Model. The Fig.1 is conceptual diagram of the proposed model. The diagram has components like Trust Admin, Trust Feedback, Dynamic Trust Calculator, Trust Selection Algorithm, Trust Calculative Model, Effective Trust Value and Trust Moderator. The detailed description of these components is given below.

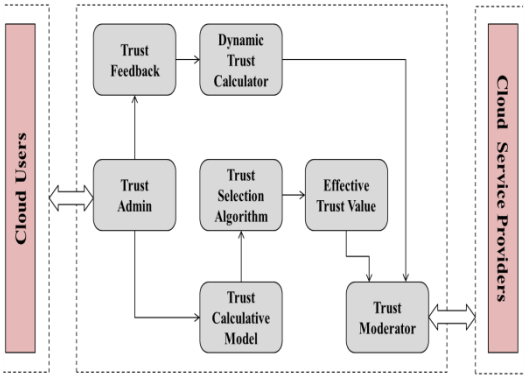

Fig.1. Conceptual Diagram of proposed Trust Model

*Trust Admin***:** Basic Trust value is needed to enter any domain. Trust Admin initializes the minimum/basic trust required to enter the system. Trust Admin also administers the overall basic trust of the user/ resources in the system. In migration also Trust Admin plays an important role in calculating the basic trust of the user/resources using the Trust Feedback component.

Trust Calculative Model: Many Trust models are developed, but are always very specific for a specific scenario. Our trust model is a generic model. Here trust is calculated mathematically. The mathematical detail is as given below:

We propose to calculate the trust value based on usage values which in turn are calculated in terms of availability and non-availability.

The trust value calculation is briefly described as below:

i. Trust relationship established between two entities is based on usage and the entities are represented as customer and resources. The notation for the relationship is given as {Customer: resource, usage}

ii. Trust is a collaboration of certainty and uncertainty. If the resource is available it is allocated to the customer and the customer performs the action else if not available the trust of the customer on the resource is minimized.

iii. The degree of the trust can be represented by a real number called Trust Value. Trust value represents availability/non-availability.

iv. Customer may have variation of trust values based on the availability of the resources.

Principle-1: Trust Using Entropy

Thus by the basic understanding of the trust, we further define the trust value based on usage. If the trust value is calculated based on availability that the resource is allocated for the customer for his action to be performed, then T{customer: resource, usage} denote that the trust of the customer on the requested resource is based on the availability/non-availability. Then the probability P{customer: resource, availability} will be the availability of the resource to the customer for some action to be performed. Using entropy model [34] of the Information theory the new trust value thus defined is as:

$$\boldsymbol{T\{customer: resource, usage\}} = \begin{Bmatrix} \boldsymbol{1 - H(p)},\ \boldsymbol{for}\ \ 0.5 < p < 1 \\ \boldsymbol{H(p) - 1},\ \boldsymbol{for}\ \ 0 < p < 0.5 \end{Bmatrix} \quad (1)$$

Where $H(p)=-p\log_2(p)-(1-p)\log_2(1-p)$ and p=P{customer: resource, usage}. When p=1 the customer is allocated the available resources and the trust value is high. When p=0 the customer is not allocated the resources due to unavailability and the trust is very low.

Principle-2: Dynamic Direct Trust Value

Evaluating Trust in dynamic cloud environment is a necessary factor as cloud is dynamic in nature. Here trust is calculated based on the number of successful

transactions made so as to take into account the availability of resources for every successful transaction.

$$\boldsymbol{i_t = \sum_{n=0}^{n=1}(rn * cn)} \quad (2)$$

where r_n is initial resource trust value
c_n is initial customer trust value.

After successful transactions, the new trust value will be

$$\boldsymbol{D_t = i_t + \sum_{i=0}^{i=n} \text{ti/ No. of transactions}} \quad (3)$$

Where t_i is No. of successful transactions and D_t must always be greater than the initial trust value as i_t is the initial trust required to perform any transaction.

Principle-3: Trust Value for Migration

The new trust value calculated for the customer on resources is stored in central table which can be retrieved by all Cloud Service providers (CSP).

When a customer wants to migrate to a different service provider the initial trust of the customer with the new CSP is calculated as :

$$\boldsymbol{M_t = \frac{i_t + D_t}{0.5}} \quad (4)$$

Where 0< Mt for availability
Mt < 0 for non-availability

i_t is initial trust by (2)
D_t is the dynamic trust by (3)
0.5 is the minimum trust required by any entity for a successful transaction.

Thus in the Trust Calculative Model trust is calculated using any of the above defined principles and thus a trust value is arrived which is forwarded to Trust Selection Algorithm to check for the accurateness.

Trust selection Algorithm: It is known from the previous researchers that Genetic Algorithm [35] is the best selection algorithm which gives near optimal solutions which are suitable for many practical problems where input data are approximate, but the basic disadvantage of genetic algorithm is it does not yield exact optimal solutions when the population size is considerably large. So the algorithm used for trust selection is the Family Gene Genetic Algorithm [36]. The algorithm adapted is as shown below.

Algorithm 1 Adapted Family Gene Genetic Algorithm

Input: population, Trust value
Output: Best trust value inform of IP address retrieved, System Computation time

1: Initialize P population of n elements.
2: Use a fitness function to evaluate the current solution
3: Use genetic operators (Cross over, Mutation, Selection) to create new generations.
Go to 2 until the population does not pass the fitness criteria
4: Incorporate the Trust Model developed on the new population along with the new fitness function.
5: Find the best population from the newly incorporated population.

*Effective Trust Value***:** The trust values generated by Trust Calculative Model and Justified by Trust Selection algorithm are finalized here so as to assign the trust value required to allocate resources based on availability for the transactions to be performed by the customer/user. Once the thus calculated trust is assigned the user can access the resources that are termed available due to the trust value for any transaction as required by the user.

*Trust Moderator***:** Trust Moderator assigns the final trust value to the existing customer who has requested for the specific resources and during migration the trust value of the customer.

Trust Feedback: In case the customer wants to shift his cloud service provider then his current trust value is stored in central table called Trust Feedback.

Dynamic Trust Calculator: In case of migration the new trust value is calculated using (4) of the Trust calculative Model and the new trust by migration is sent to the Trust Moderator for the assignment of the trust.

B. Working Process of the Proposed Trust Model

In the above section we have described the proposed Conceptual Diagram of Trust model developed. The working process between the components in the proposed Conceptual Diagram is as shown below:

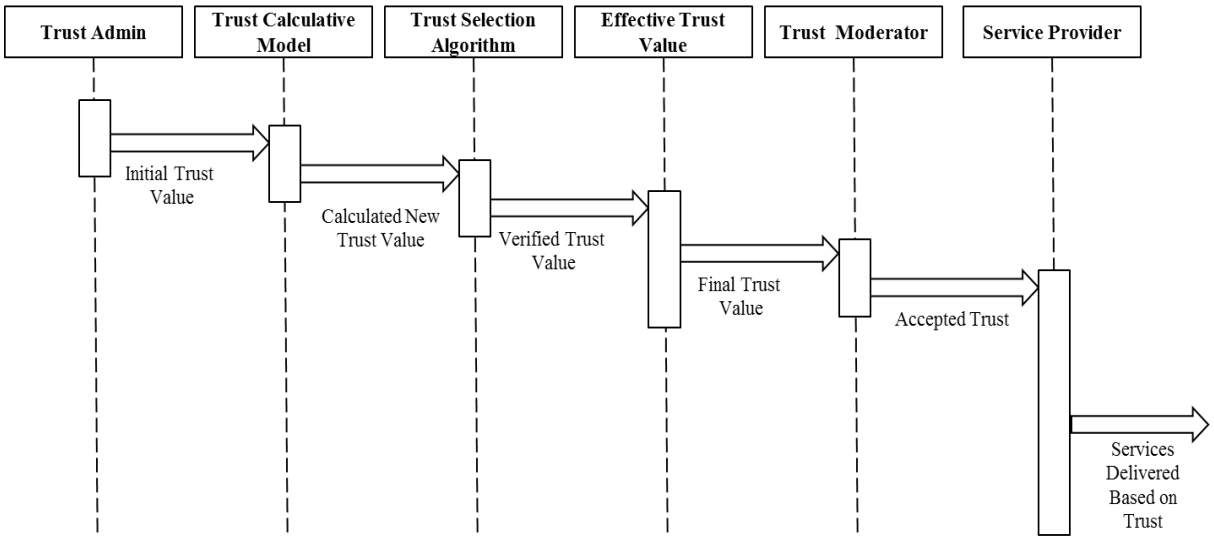

Fig.2. Working Process of the Proposed Trust model

The Fig.2 sequence diagram describes the sequences of steps performed in calculating trust by a service provider to processes the request of the customer for available resources to complete his transaction. Trust Admin defines the initial trust required to enter the system. Trust calculative model incorporates the mathematical model proposed and generates trust values. Trust selection algorithm justifies the trust values generated by the trust calculative model and then these trust values are sent to effective trust value. In effective Trust Value based on the scenario the final trust value is generated and sent to Trust Moderator who in turn assigns the trust value for the customer and resource. Based on the trust value assigned by the Trust Moderator the Service provider processes the request of the customer for resources for the transaction. Trust Selection Algorithm Uses Family Gene Genetic Algorithm to justify the trust calculated by the Trust Calculative Model. Effective Trust Value finalizes the final trust value. This final trust value is assigned/passed on to the Service provider by the Trust Moderator who in turn assigns the resource to the requested customer based on this final trust value. In case of migration the trust value stored retrieved by the Trust Feedback and this is sent to the Dynamic Trust Calculator who in turn calculates the dynamic trust and the sends it to the Trust Moderator for final assignment of Trust by CSP.

IV. Proof Of Concept

In this section a brief conceptual explanation is given for the trust and the trust evaluation scheme. The trust is calculated based on usage values of availability and no availability.

Let us consider a real case scenario where the cloud resources are allocated to the customer based on the trust pre-calculated in the SLA. When a customer wants to request for more resources he has to modify the SLA or it is completely at the discrete of the Service Provider. The Below example depicts how the developed trust model can minimize this allocation problem to an extent.

Now consider the below scenario as shown in Fig.3. A layered approach is adapted for the trust evaluation. Assume C1, C2, C3, C4 are the customers using the cloud services. Based on their functional requirement they are connected to the respective Cloud Service Provider through a common Interface. CS1, CS2, CS3, CS4 are the different Cloud Service Providers who provide cloud services in form of Saas, Paas, Iaas. These service providers have a common platform where they share common resources like servers, software, platform, processors for computation, etc. R1, R2, R3, R4, R5 are the different resources available in the cloud provided by the cloud service provider to the customer.

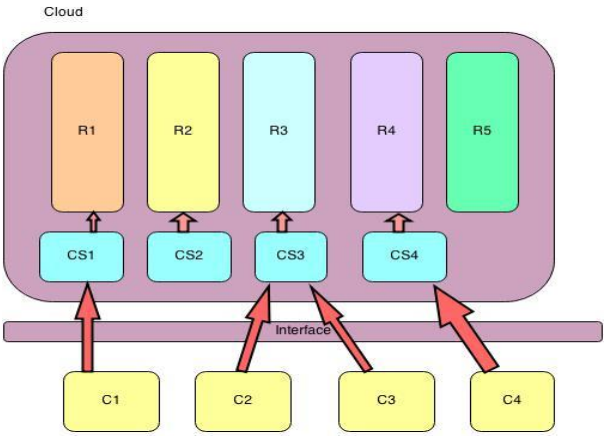

Fig.3. Layered approach for trust evaluation.

When a customer (C1) who wants to use Software as a Service enters the cloud using the interface and based on his functional requirements he is connected to the service provider CS1 who in turn is connected to the resource R1 which is software. The allocation of the resources to the service provider is done through a common agreement between them.

Now if we prioritize the resources available in the cloud on common platform as software:1, server:10, patform:4, processor:6 and etc. on a scale from 1 to 10 where 10 is of higher priority and is of lowest priority. Based on the priority of the resource and basic trust value calculated using the proposed trust equations, of the customer the service provider allocates the requested resources to the customer. If two customers C4 and C3 request for services as Paas and Iaas respectively, they are connected to CS4 and CS3 respectively who in turn are connected to Resources servers(R3) and platform(R4). As CS4 requires partial memory for the application to be stored and CS3 requires memory for the storage of data by customer the priority of these resources and the trust values of the customer is taken into consideration and based on the new trust value calculated the resource is allocated. There is probability that the customer C3 would not be allocated the required memory due to unavailability of the resource as it is allocated to customer C4. Thus this model helps in migration as the service providers use the common resources and the trust calculated is stored in the trust feedback for new calculations.

Thus the probability of allocation is dependent on the availability of the resources. If the resource is available then it is allocated to customer based on his trust value which is designed in the SLA agreement between the customer and service provider.

A. *Theoretical Conclusion*

This solution helps the customer to migrate from one service provider to other without any change in the data format of the customer. Thus interoperability is achieved in the cloud with minimum effort from customer as well as the Service provider

V. Experimentation

To evaluate the correctness of the proposed Trust Model proposed, the mathematical components were simulated using simulation tools like MATLAB and the effectiveness of the mathematical model on a cloud platform was tested using the Aneka Software. The next successive sub-sections give a brief description of the platforms used for evaluation.

A. *Using MATLAB*

MATLAB (matrix laboratory)[37] developed by MathWork is a fourth-generation high-level programming language and interactive environment for numerical computation, visualization and programming. Using MATLAB we can perform matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, interfacing with programs written in other languages, including C, C++, Java, and Fortran, etc. It has numerous built-in commands and math functions that help us in mathematical calculations, generating plots and performing numerical methods.

Using MATLAB we have implemented the mathematical model to check the correctness of the model. From MATLAB experiment it is understood that the Trust value calculated using the mathematical model is accurate.

B. *Using ANEKA*

Aneka [38] is a Cloud Computing platform rendering Platform-as-a-Service for developing distributed applications on the Cloud. Aneka provides developers with a rich set of APIs for exploiting resources and expressing the business logic of application.

The Aneka based computing cloud is a collection of physical and virtualized resources connected through a network, either by the Internet or private intranet. One of the key features of Aneka is the ability of providing different ways for expressing distributed applications by offering different programming models; execution services are mostly concerned with providing the middleware with an implementation for these models.

Using Aneka Platform we have created 3 users and one server. The users are treated as clients. We have implemented our Trust Model using Family Gene Genetic Algorithm in .NET frame work. The Project is run from client machine using the thread concept supported by Aneka.

C. *Results and Analysis*

Our Mathematical Model was simulated using MATLAB software. The experimental results are as below:

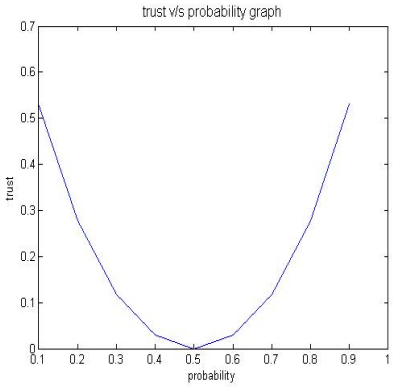

Fig.4. 1-H(p) values

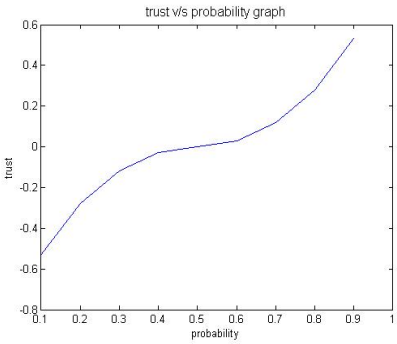

Fig.5. H(p)-1 values

The Fig.4 shows that for every increase in probability value due to Entropy the trust decreases and at a particular point of probability value 0.5 the trust becomes zero and again increases with increase in probability value. This shows that the trust increases with increase in probability.

Fig.5 shows that with at a threshold of probability value 0.5 the trust starts increasing to positive which clearly indicates the availability of resources due to increase in the trust value. Thus the priciple-1 shows that with every availability of resources the trust increases.

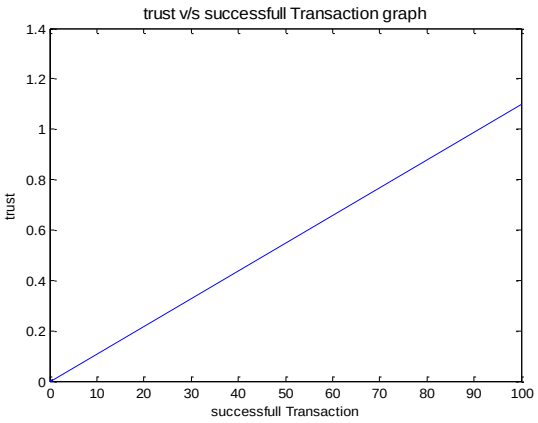

Fig.6. Dynamic trust after every successful transaction

We have considered in our experiment a minimum of 100 transactions. The Fig.6 shows that with every successful transaction the trust increases. This shows the availability of resources for the successful transactions which in turn increase the trust value. The graph shows that trust value increases with every successful transaction; we have considered the upper threshold of trust value as 1. Any increase in trust value above 1 is considered as trust value 1.

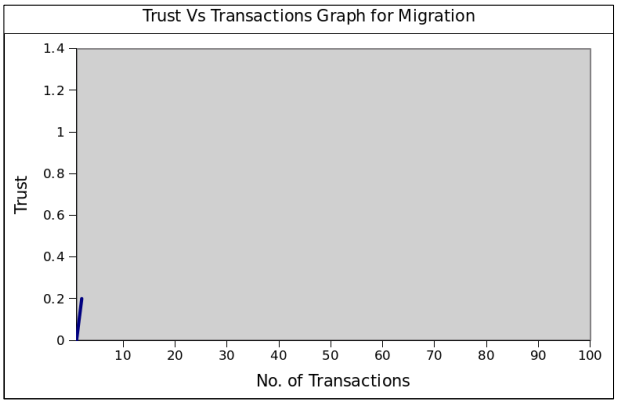

Fig.7. Dynamic trust after every unsuccessful transaction

Fig.7 depicts that for every unsuccessful transaction the initial trust value drops down to 0.2 but for every successful transaction the trust increases. Our experiments shows that the minimal trust required for requesting resources for transaction to happen is 0.2. So to calculate the dynamic trust again after every unsuccessful transaction the minimum trust required is 0.2 whereas minimum trust required for every successful transaction is 0.5.

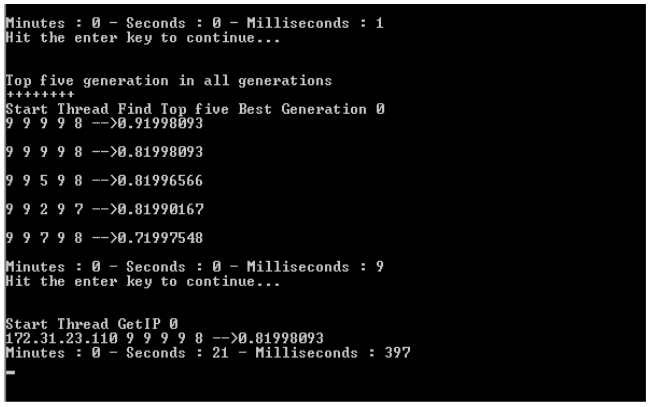

Fig.8. Time taken by Genetic Algorithm

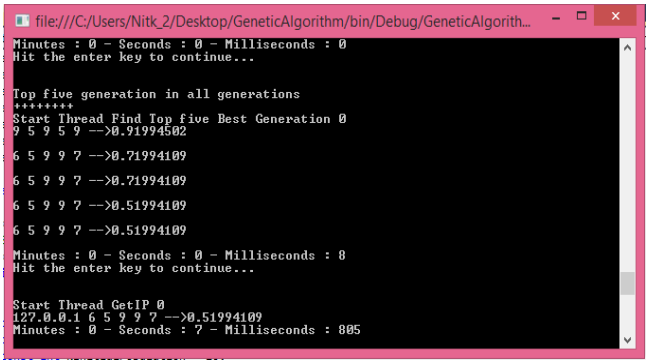

Fig.9. Time taken by Family Gene Genetic Algorithm

Our trust model was implemented using the Genetic Algorithm(GA) and Adapted Family Gene Genetic Algorithm (FGA) in Aneka Cloud Platform. Our experiment concluded that the selected IP with the best fitness value has the best trust value. The time for completing the GA process for 1000 population size was 21 seconds 397milliseconds whereas the time taken for complete execution of Family Gene Genetic Algorithm with trust incorporated was 7 seconds 805 milliseconds. Fig.8 and Fig.9 shows the results of the genetic algorithm and family gene algorithm respectively which tells that Family Gene Genetic Algorithm gives better optimal solution.

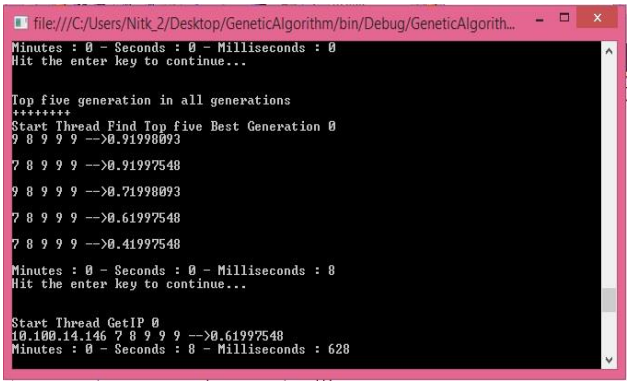

Fig.10. Time taken by Family Gene Algorithm for population size 100000

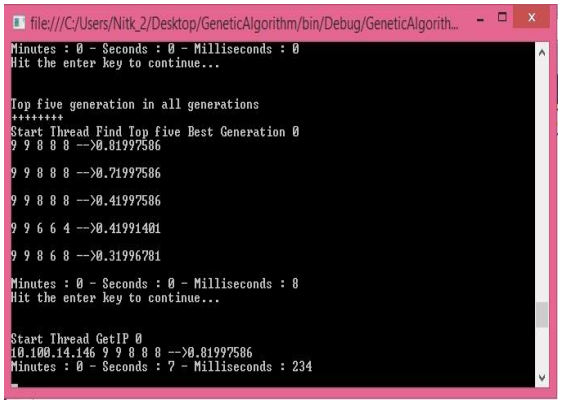

Fig.11. Time taken by Family Gene Algorithm for population size 10000000

From Fig.10 and Fig.11 it is visible that as the population size increases the computation time taken by FGA decreases. From the experiment it is evident that Family Gene Algorithm is the best algorithm for optimal solution when the population size is large.

From the experiments conducted, it is concluded that a strong trust model can solve the first step of secure allocation of resources. The trust model proposed would enhance the security of the resources as it is based on the availability. Experiments also depict that the selected family gene algorithm gives optimal trust value when incorporated.

VI. Conclusion

Trust being the one of the important factor in cloud environment for the basic security of entities needs more attention. Though trust is prominent factor still it poses to be off-track when security is considered. A strong Trust model is needed to signify the importance of trust. Our model proposes a strong trust value for dynamic change as well as trust value for migration. Migration poses major problem in Cloud environment. Our Proposed model reduces the risk of migrating to other clouds using the proposed trust platform. The implementation of the trust using the family gene algorithm has proved that trust when incorporated properly in any system can yield better results than system without trust. Our future work includes formulating and implementing the End-to-End Trust in the dynamic environment using the proposed Trust Model and also to find the performance of the system with the End-to-End Trust thus implemented.

References

[1] Gambetta D,G(Ed).1988. “can we trust trust?”In D.G Gambetta(Ed), Trust 213-237,NewYork:Basil Blackwell

[2] Sheikh MahbubHabib, Sebastian Ries, Max M ¨uhlh ¨auser, “Towards a Trust Management System for Cloud Computing”, International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11

[3] Seyyed Yasser hashemi, Parisa Sheykhi Hesarlo,” Security, Privacy and Trust Challenges in Cloud Computing and Solutions”, International Journal of Computer Network and Information Security, 2014, 8, 34-40

[4] Conner, W., Iyengar, A., Mikalsen, T., Rouvellou, I., Nahrstedt, K.: “A Trust Management Framework for Service-Oriented Environments.” In: Proc. of WWW 2009, Madrid, Spain (April 2009)

[5] Hwang, K., Li, D.: “Trusted Cloud Computing with Secure Resources and Data Coloring.” IEEE Internet Computing 14(5), 14–22 (2010)

[6] Khaled M Khan and Qutaibah Malluhi, "Establishing Trust in Cloud Computing," IT Professional, vol. 12, no. 5, pp. 20 - 27, 2010.

[7] Hiroyuki Sato, Atsushi Kanai, and Shigeaki Tanimoto, "A Cloud Trust Model in a Security Aware Cloud," in 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT), Seoul, South Korea, 2010, pp. 121 - 124.

[8] Wenjuan Li, Lingdi Ping, and Xuezeng Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," in International Conference on Electronics and Information Engineering (ICEIE), vol. 1, Kyoto, Japan, 2010, pp. 14-19.

[9] Tie Fang Wang, Bao Sheng Ye, Yun Wen Li, and Yi Yang, "Family Gene based Cloud Trust Model," in International Conference on Educational and Network Technology (ICENT), Qinhuangdao, China, 2010, pp. 540 - 544.

[10] Tie Fang Wang, Bao Sheng Ye, Yun Wen Li, and Li Shang Zhu, "Study on Enhancing Performance of Cloud Trust Model with Family Gene Technology," in 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 9, Chengdu, China, 2010, pp. 122 - 126.

[11] Paul D Manuel, Thamarai Selve, and Mostafa Ibrahim Abd-EI Barr, "Trust management system for grid and cloudresources," in First International Conference on Advanced Computing (ICAC 2009), Chennai, India, 2009, pp. 176-181.

[12] Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform," in International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 1, Changsha, China, 2010, pp. 942 - 945.

[13] Zhidong Shen and Qiang Tong, "The security of cloud computing system enabled by trusted computing technology," in 2nd International Conference on Signal Processing Systems (ICSPS), vol. 2, Dalian, China, 2010, pp. 11-15.

[14] Mohammed Alhamad, Tharam Dillon, and Elizabeth Chang, "SLA-based Trust Model for Cloud Computing," in 13th International Conference on Network-Based Information Systems, Takayama, Japan, 2010, pp. 321 - 324.

[15] Xiao Yong Li, Li Tao Zhou, Yong Shi, and Yu Guo, "A trusted computing environment model in cloud architecture," in Ninth International Conference on Machine Learning and Cybernetics (ICMLC), vol. 6, Qingdao, China, 2010, pp. 2843-2848.

[16] Zhimin Yang, Lixiang Qiao, Chang Liu, Chi Yang, and Guangming Wan, "A Collaborative Trust Model of Firewall-through based on Cloud Computing," in 14th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Shanghai, China, 2010, pp. 329 - 334.

Junning Fu, Chaokun Wang, Zhiwei Yu, Jianmin Wang, and Jia Guang Sun, "A Watermark-Aware Trusted Running Environment for Software Clouds," in Fifth Annual China Grid Conference (ChinaGrid), Guangzhou, China, 2010, pp. 144 - 151.

[17] Rohit Ranchal et al., "Protection of Identity Information in Cloud Computing without Trusted Third Party," in 29th IEEE International Symposium on Reliable Distributed Systems, New Delhi, India, 2010, pp. 1060-9857.
[18] Hassan Takabi, James B.D Joshi, and Gail Joon Ahn, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," in 34th Annual IEEE Computer Software and Applications Conference Workshops, Seoul, South Korea, 2010, pp. 393 - 398.
[19] Shanshan Song, Kai Hwang, and Yu-Kwong Kwok. Riskresilient heuristics and genetic algorithms for security assured grid job scheduling. IEEE Trans. Computers, 55(6):703-719, 2006
[20] Fatima Zohra Filali, Belabbes Yagaubi, "Global Trust: A Trust Model for Cloud Service Selection", International Journal of Computer Network and Information Security, 2015, 5, 41-50.
[21] Xiaodong Sun ,Guiran Chang, Fengyun Li," A Trust Management Model to enhance security of Cloud Computing Environments", Second International Conference on Networking and Distributed Computing,2011
[22] Hamzeh Mohammadnia, Hassan Shakeri," HITCloud: Novel Hierarchical Model for Trust Management in Cloud Computing", First International Congress on Technology, Communication and Knowledge (ICTCK 2014),Iran, 978-1-4799-8021-5/14, IEEE-2014.
[23] Wenjuan Fan, Harry Perros," A Reliability-based Trust Management Mechanism for Cloud Services", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 978-0-7695-5022-0/13, IEEE-2013.
[24] Sheikh Mahbub Habib, Sebastian Ries, Max Muhlhauser, "Towards a Trust Management System for Cloud Computing", International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, 978-0-7695-4600-1/11, IEEE-2011.
[25] Monoj Kumar Muchahari, Smriti Kumar Sinha, "A New Trust Management Architecture for Cloud Computing Environment", International Symposium on Cloud and Services Computing, 978-0-7695-4931-6/12, IEEE-2012.
[26] Gansen Zhao, Haiyu Wang, Chunming Rong, Yong Tang, "Resource Pool Oriented Trust Management for Cloud Infrastructure", International Conference on Availability, Reliability and Security, 978-0-7695-5008-4/13, IEEE-2013.
[27] Nadia Bennani, Khouloud Boukadi, Chirine Ghedira-Guegan, "A trust management solution in the context of hybrid clouds", IEEE 23rd International WETICE Conference, 978-1-4799-4249-7/14, IEEE-2014.
[28] Marco Anisetti, Claudio A. Ardagna, Ernesto Damiani, "A Certification-Based Trust Model for Autonomic Cloud Computing Systems", International Conference on Cloud and Autonomic Computing, 978-1-4799-5841-2/14, IEEE-2014.
[29] Mohamed Firdhous, Suhaidi Hassan, Osman Ghazali, "Hysteresis-based Robust Trust Computing Mechanism for Cloud Computing", TENCON-2012, 978-1-4673-4823-2.
[30] Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan, "A Trust Computing Mechanism for Cloud Computing with Multilevel Thresholding", 6th International Conference on Industrial and Information Systems, ICIIS 2011, 978-1-61284-0035-4/11.
[31] Haiyu Wang, Gansen Zhao, Qi Chen,Yong Tang, "Trust Management for IaaS with Group Signature", Fourth International Conference on Emerging Intelligent Data and Web Technologies, 978-0-7695-5044-2/13, IEEE-2013.
[32] Mohamed Firdhous, Osman Ghazali , Suhaidi Hassan, "A TRUST COMPUTING MECHANISM FOR CLOUD COMPUTING", ITU-T Kaleidoscope Academic Conference, 978-92-61-13651-2/CFP1138-E-CDR.
[33] T M Cover and J A Thomas,' Elements of Information Theory', Newyork:Wiley, 1991
[34] Noraini Mohd Razali, John Geraghty, "Genetic Algorithm Performance with Different Selection Strategies in Solving TSP", Proceedings of the World Congress on Engineering 2011 Vol II , WCE 2011.
[35] Jianhua, Li ;Xiangqian, Ding ; Sun'an, Wang ; Qing, Yu ,"Family genetic algorithms based on gene exchange and its application", Journal of Systems Engineering and Electronics, IEEE-2006.
[36] Gowtham Bellala, "A quick Tutorial on MATLAB", http://web.eecs.umich.edu/~aey/eecs451/matlab.pdf
[37] http://www.manjrasoft.com/aneka_architecture.html

Authors' Profiles

Usha Divakarla is currently pursuing Ph.D in Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, India. She obtained her B.E from Bangalore University, Karnataka and M.Tech from Maharshi Dayanand University, Haryana. She has teaching experience of 6 years and industrial experience of more than 2 years. Her areas of interest include Cloud Computing, Trust Management, Cloud Security

K. ChandraSekaran is currently Professor in the Department of Computer Science and Engineering, National Institute of Technology Karnataka, having 26 years of experience. He has more than 120 research papers published in various reputed International journals, con ferences which include IEEE, ACM, Springer etc. He has received best paper awards and best teacher awards. He serves as a member of various reputed societies, including IEEE (Senior member), ACM (Senior Member), CSI, ISTE and Association of British Scholars (ABS). He is also a member in IEEE Computer Society's Cloud Computing STC (Special Technical Community). His areas of interest include Computer Networks, Distributed Computing (includes Cloud Computing and Security) and Business Computing and Information Systems Management.

How to cite this paper: Usha Divakarla, K. Chandrasekaran,"Secure Allocation of Resources in Cloud Using Trust",International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.1,pp.43-52, 2016.DOI: 10.5815/ijcnis.2016.01.06

