# Improved Trust Model to Enhance Availability in Private Cloud

Vijay Kumar Damera[1]
Research Scholar, Department of CSE
JNTU Hyderabad, Telangana, India

A Nagesh[2]
Professor, Department of CSE
MGIT Hyderabad, Telangana, India

M Nagaratna[3]
Professor, Department of CSE
JNTUCEH Hyderabad, Telangana, India

***Abstract*—In the process of cloud service selection, it is difficult for users to choose trusted, available, and reliable cloud services. A trust model is a perfect solution for this service selection problem. In cloud computing, data availability and reliability have always been major concerns. According to research, around $285 million is lost per year due to cloud service failures, with a 99.91 percent availability rate. Replication has long been used to improve the data availability of large-scale cloud storage systems where errors are anticipated. As compared to a small-scale environment, where each data node can have different capabilities and can only accept a limited number of requests, replica placement in cloud storage systems becomes more complicated. As a result, deciding where to keep replicas in the system to meet the availability criteria is an issue. To address above issue this paper proposes a trust model which helps in selecting appropriate node for replica placement. This trust model generates comprehensive trust value of the data center node based on dynamic trust value combined with QoS parameters. Simulation experiments show that the model can reflect the dynamic change of data center node subject trust, enhance the predictability of node selection, and effectively decreases the failure rate of node.**

***Keywords*—Trust; trust model; cloud; availability; reliability**

## I. Introduction

Cloud computing provides usable, convenient, and on-demand cloud services in the form of shared computing resource sharing pools. It includes three levels of services: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS), where IaaS provides consumers with comprehensive computer infrastructure services, such as hardware server rental, PaaS is to provide software development platform as a service to consumers, SaaS is to provide software to consumers through the network mode. It is a general practice to choose cloud service providers based on a comprehensive evaluation of QoS metrics [1]. The same is considered here in this work to evaluate the trust value of data center nodes. High availability and high-performance are essential features user expects from cloud service providers[3]. Replication plays an important role for any system to improve availability, throughput and response time for user [24].

In fact, replication is an essential corner stone in data storage not only for cloud computing but also for traditional storage systems [12], [13], [14], [15], because it can relatively impact the performance of cloud storage in terms of storage cost, network usage, response time, etc. [22], [23], [24], [25]. Therefore, maintaining static number of replicas in cloud storage for every data file would be inefficient for storage cost and data availability [16], [17], [18]. As a consequence, the determination of the optimum number of replicas and the suitable nodes for replicas has become a key issue in the cloud computing [19], [20], [21].

To address the above issue this paper proposes a node selection model based on the dynamic trust. The trust value is calculated by direct and recommended trust. In order to reflect trust value more comprehensively the concept of Dynamic Trust Value (DTV) is introduced in this model. Further the concept of information entropy is introduced to solve the problem of weighting of trusted parameters, so that the comprehensive trust value and QoS value are weighted to obtain the optimal node selection for replica placement.

## II. Related Works

For the study of cloud service selection, many scholars at home and abroad have done a lot of work. For example works such as multi-objective genetic algorithm, particle swarm optimization PSO [1], artificial neural network algorithm [2].The application of these methods are generally aimed at a relatively static scenarios. The generation and disappearance of network services in a cloud computing environment are often dynamic, so it is necessary to solve the authenticity judgment of services in a cloud computing environment. Further it is important to solve the problem of degree of understanding of service quality when selecting a service algorithm [3], the trust of cloud services and other problems.

In response to the above problems, at the same time, in order to ensure the success of the service selection algorithm, the research based on the trust degree of the service subject is particularly important. Ma You et al. [4] proposed a new ESOW algorithm for QoS measurement. The ESOW algorithm is based on the user's subjective trust. The two parts of preference weight and objective weight are synthesized. The calculation of user's subjective weight is based on the adaptive SWDM algorithm, and the objective weight is calculated according to the OWDM algorithm. Sarbjeet [5] proposed a method based on the past experience and third-party service recommendation trust evaluation mechanism.

DASA et al. [6] proposed a dynamic trust calculation model that can effectively evaluate the behavior of malicious agent strategies. It mainly analyzes and evaluates all relevant elements to make correct decision. Zhouao et al. [7] proposed a dynamic virtual resource lease method from the perspective of service provider's benefit maximization, from the perspective of price allocation and request urgency. Cao Jie et al. [8] based on the interpersonal relationship in sociology relationship

combined with user satisfaction evaluation, recommendation evaluation and third-party supervision feedback, a new credible measurement model was proposed. Zhang Lin et al. [9] combined relevant ranking factors, attribute factors, and intervals according to the behavior and dynamics of information services factor, penalty factor, and other four factors, a new dynamic trust monitoring model is proposed. Abawajy [10] proposes a distributed trust management framework based on reputation, which can pass the past experience, trust level and first level of honesty to determine the trust value of cloud computing entities.

## III. Proposed Methodology

### A. Basic Definitions

The service feedback results of the system described in this paper can be expressed by the two values namely positives and negatives. Therefore, the trust value of the data center node can be defined as the probability $P$ of providing a good service, that is, using the evaluation information to reflect the probability $P$ of providing a good service as accurately as possible. The process of cloud computing includes three main entities:

**Service Provider:** Represented as $pro_j$, representing the $j-th$ node, this node can provide users with the resources required by the user's cloud service request.

**Service Consumer:** Represented as $user_i$, $i$ represents the $i-th$ service request user, the node can send service request information to the service intermediary, and can provide service history and service results to the service intermediary. As an evaluation of $pro_j$, user $user_i$ vs. $pro_j$ is defined as a binary.

**Service Broker:** Represented as a broker, responsible for processing request response and management, and responsible for processing $user_i$ feedback information, providing $user_i$ with $pro_j$ node evaluation information.

### B. Direct Trust and Recommended Trust

The direct trust value is calculated using the past historical transactions and feedback information of two trading entities[16]. In the process of calculating the trust value, the Bayesian theory [11] is introduced to calculate the trust value of the node.

Suppose that the probability of good service provided by $pro_j$ is $P_j$. After several transactions between the nodes and $user_i$. The evaluated binary "$Positives_{ij}$, $Negatives_{ij}$" is obtained, and the probability density function of $P_j$ is obtained as:

$$f(p|\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \quad 0\leqslant p\leqslant 1, \alpha\geqslant 0, \beta\geqslant 0 \tag{1}$$

In the formula:$\alpha=\text{positives }_{ij}+1, \beta=\text{negatives }_{ij}+1$

The Gama function is represented by:

$$\Gamma(z)=\int_0^{+\infty}\mathrm{e}^{-t}t^{z-1}\mathrm{d}t \tag{2}$$

Then there is a probability density function that can obtain the Bayesian estimate of $P_j$ as:

$$P_{ij}=\int_{P_j=0} f\left(P_j|\alpha_{ij},\beta_{ij}\right)P_j\mathrm{d}P_j=\frac{\alpha_{ij}}{\alpha_{ij}+\beta_{ij}}=\frac{\text{positives }_{ij}+1}{\text{negatives }_{ij}+\text{ positives }_{ij}+2} \tag{3}$$

Then get the direct trust value : $T^{\mathrm{d}t}=P_{ij}$

The recommended trust value refers to the user $user_i$'s trust value for the service provider $pro_j$ is obtained through the recommendation between other related entities, and the related entities are synthesized based on empirical evaluation. During the evaluation, the set of recommended entities is assumed to be R. The associated user-recommended user R in R recommends the two-tuple to $user_k$:

$$\begin{cases}\mathrm{Re}_{-}^{\text{postives}}\ \sum_{k\in R}\ \text{postives }_{kj}\\ \mathrm{Re}_{=}^{\text{negatives}}\ \sum_{k\in R}\ \text{negatives }_{kj}\end{cases} \tag{4}$$

Similarly, through the Bayes principle, the recommended trust value can be obtained:

$$T^{rt}=\frac{\mathrm{Re}_{\text{possives }}^{ik}+1}{\mathrm{Re}_{\text{negatives }}^{k}+\mathrm{Re}_{\text{postives }}^{ik}+2} \tag{5}$$

### C. Time Decay Function

Not all user feedback can truly reflect the trust status between entities. Because over time, old user feedback may not accurately reflect the current trust value. For example, it may be evaluated that the service behavior of the entity has been modified or improved. So at this time set the weight according to the time of feedback to accurately reflect the user's feedback. This can be achieved by setting the time decay function mechanism. Assume that at time $\tau$, after the unit time t, the user feedback trust formula for the attenuation of the value over time is shown in equation (6).

$$f_{ij}(\tau+t)=\begin{cases}f_{ij}(\tau), & f_{ij}(\tau)\geqslant\theta_1, t\leqslant\theta_2\\ f_{ij}(\tau)\mathrm{e}^{-\lambda(t-\theta_2)}, & f_{ij}(\tau)\geqslant\theta_1, t>\theta_2\\ b, & \text{other}\end{cases} \tag{6}$$

In the formula: $\lambda$ is the decay constant, which is used to control the decay rate of the trust value. The value of $\lambda$ can be set according to different service types. At the same time, the user's true intention of evaluating the entity and reducing trust are considered for the update frequency. A start attenuation threshold $\theta_2$ and a stop attenuation threshold $\theta_1$ are set here. When the elapsed time $t$ is greater than $\theta_2$, the trust value decreases gradually according to the attenuation constant, and when the trust value is less than or equal to the stop attenuation threshold at $\theta_1$, the trust value is set to a fixed value $b$, and the trust value will not change with time.

### D. Calculation of Comprehensive Trust

The calculation of comprehensive trust includes two aspects: the direct trust value $T^{dt}$ and the recommended trust value $T^{rt}$, and the weight between the two can be set according to different service types. Set them to $\alpha, \beta$ and $\alpha + \beta = 1$, in this paper, they are set to 0.5, 0.5 respectively, then the calculation formula of the comprehensive trust $\mathrm{CT}\left(\mathrm{pro}_{r_k}^{j}\right)$ of the data center node $r_k$ is:

$$\mathrm{CT}\left(\mathrm{pro}_{r_k}^{j}\right) = \alpha * \frac{\mathrm{positives}_{ij}+1}{\mathrm{negatives}_{ij}+\mathrm{positives}_{ij}+2} + \beta * \frac{\mathrm{Re}_{\mathrm{positives}}^{ik}+1}{\mathrm{Re}_{\mathrm{negatives}}^{k}+\mathrm{Re}_{\mathrm{positives}}^{k}+2} \tag{7}$$

### E. Dynamic Trust Value

Dynamic Trust Value (DTV), which represents the trend of trust value with respect to change with time. It can reflect the historical change of trust value, and has a pre-judgment indicator for the next node selection, thus improve the efficiency of node selection.

In order to be able to quantify the value of DTV, the least squares data fitting method is introduced. The least squares fitting method is a method to approximate or compare the functional relationship between the coordinates represented by discrete point groups on the plane with a straight line. Assume that the trust degree of $pro_j$ changes with time as $\left\{\left(t_k, \mathrm{trust}_k^j\right) : k \in [1, n]\right\}$, where the node $\left(t_k, \mathrm{tr}\, ust_k^j\right)$ represents the trust value $P_k$ of $pro_j$ at time $t_k$. According to the least squares method, the fitted straight line equation is assumed to be:

$$y_j = \mathrm{DTV}_j * t_k + b \tag{8}$$

The slope of the straight line $DTV_j$ is the Dynamic Trust Value of the defined data center node, $b$ represents the intercept. In order to determine the value of $DTV_j$, $b$, according to the principle of the least square method, all data nodes $(t_k, y_k)\,(k = 1, 2 \ldots n)$. The square sum of the deviation values of all data nodes is minimized, that is:

$$M = \sum_{k=1}^{n} (\ \mathrm{trust}\ _k - y_k)^2 = \sum_{k=1}^{n} (\ \mathrm{trust}\ _k - \mathrm{DTV}_j * t_k - b)^2\, subjectto \min(M) \tag{9}$$

The condition for obtaining the minimum value is that the corresponding binary function takes the extreme value of 0, that is:

$$\frac{\partial M}{\partial \mathrm{DTV}_j} = \frac{\partial M}{\partial b} = 0 \tag{10}$$

After finishing, the normal equations are obtained:

$$\begin{cases} \sum_{k=1}^{n} \mathrm{trust}_k - \mathrm{DTV}_j \sum_{k=1}^{n} t_k - nb = 0 \\ \sum_{k=1}^{n} \mathrm{trust}_k * t_i - \mathrm{DTV}_j \sum_{k=1}^{n} t_k^2 - b \sum_{k=1}^{n} t_k = 0 \end{cases} \tag{11}$$

The linear parameter values $DTV_j$ and $b$ can be obtained by solving the normal equations, namely:

$$\mathrm{DTV}_j = \left(n \sum_{k=1}^{n} t_k * \mathrm{trus}\, t_k - \sum_{k=1}^{n} \mathrm{trust}_k \sum_{k=1}^{n} t_k\right) / \left(n \sum_{k=1}^{n} t_k^2 - \left(\sum_{k=1}^{n} t_k\right)^2\right) \tag{12}$$

$$b = \left(\sum_{k=1}^{n} t_k^2 \sum_{k=1}^{n} \mathrm{trus}\, t_k - \sum_{k=1}^{n} t_k \sum_{k=1}^{n} t_k * \mathrm{trus}\, t_k\right) \left(n \sum_{k=1}^{n} t_k^2 - \left(\sum_{k=1}^{n} t_k\right)^2\right) \tag{13}$$

Then you can get the Dynamic Trust Value $DTV_j$ of $pro_j$'s trust change.

For the research needs of this paper, after the calculation of the Dynamic Trust Value $DTV_j$, it is normalized and converted into the following formula:

$$\mathrm{TCV}_i = \frac{\mathrm{TCV}_i - \min\{\mathrm{TCV}_k\}}{\max\{\mathrm{TCV}_k\} - \min\{\mathrm{TCV}_k\}} \tag{14}$$

The trust value can be converted to the range of [0, 1]. Since the Dynamic Trust Value of trust degree (DTV) reflects the change trend of trust degree, the level of $DTV$ reflects the change of trust degree, so it can be based on the value of $DTV$. It is used to predict the value of future trust. The higher the $DTV$, the higher the trust value of the data center node. On the contrary, it indicates that the node provides false information, so that the trust is in a downward trend.

At the same time, when choosing the range of Dynamic Trust Values, the range of different trust change trend values will be normalized to the interval of [0, 1]. Choosing different intervals will not have much impact on the experimental results. However, in order to reflect the user's true trust feedback behavior, this paper selects the range of Dynamic Trust Values pertaining to e-commerce platforms such as eBay and Amazon [-0.875, 0.875].

### F. Quality of Service (QoS)

QoS describes the ability of a product or service to meet consumer demand. To achieve better availability of cloud the following aspects, such as processing time, storage capacity, link capacity and type of operating system are considered as QoS parameters. They reflect service availability from different perspectives. This paper considers the QoS attributes of data center nodes from four aspects: Processing Capacity, Storage Capacity, Link Capacity and Operating System. The calculation of service performance can be calculated through user feedback or a third-party monitoring mechanism.

Assuming that there are a group of $n$ services that meet the functional requirements, the vector of each group corresponding to the QoS attribute is set as: $Q_j = (q_p, q_s, q_l, q_o)$

$j = 1, 2, 3 \cdots, n, q_p, q_s, q_l, q_o$, respectively represent the processing capacity, storage capacity, link capacity and type of operating system of the j data center node. Because the value span between these attributes is relatively large, all QoS attributes need to be converted to normalization. $q^+, q^-$, respectively represents the value after the positive and negative QoS attributes are normalized, and their normal conversion methods are:

$$q^- = \begin{cases} \frac{q^{\max} - q}{q^{\max} - q^{\min}}, q^{\max} - q^{\min} \neq 0 \\ 1, q^{\max} - q^{\min} = 0 \end{cases} \tag{15}$$

$$\mathrm{q}^+ = \begin{cases} \frac{q - q^{\min}}{q^{\max} - q^{\min}}, q^{\max} - q^{\min} \neq 0 \\ 1, q^{\max} - q^{\min} = 0 \end{cases} \tag{16}$$

Equation (15) shows that the attribute is negatively correlated with performance, that is, the larger the attribute value, the worse the performance, such as processing capacity and storage capacity; Equation (16) indicates that the attribute is positively correlated with performance, that is, the larger the attribute value, the better the performance and reliability. $q^{\max}$ and $q^{\min}$ respectively represent the maximum and minimum values in the attribute group. Then the $QoS$ value can be obtained by linearly weighting each attribute:

$$Q = w_1 * q_p + w_2 * q_{\mathrm{s}} + w_3 * q_l + w_4 * q_o \tag{17}$$

### *G. Optimal Node Selection Strategy based on Information Entropy*

The optimal node selection in the cloud computing environment is not only related to the QoS value, but also closely related to the trust value and the value of feedback by the user. It is a comprehensive reflection of the user's service quality. In previous studies, the analysis was only from the perspective of pure QoS. Some of them considered the trust value, but only considered the trust of the interaction process, and quantified the trust value as a single QoS value. This lacks in-depth study of service credibility. This paper believes that the optimal node selection should be considered in combination with both trust and QoS. Only considering any single aspect is unreasonable. At the same time, it is aimed at existing research where it only quantifies trust into a single value to evaluate the trust degree, which does not reflect the problem of trust degree changing with time. This paper integrates the Dynamic Trust Value (DTV) into the calculation process of node selection, and combines the concept of information entropy to determine the parameter weight between trust and QoS, so as to obtain the optimal node selection strategy.

Information entropy is a concept used to measure the amount of information. It is often used to give a rough measure of the uncertainty of information. Information entropy is a measure of the uncertainty of the result before the event. After the event, It is a measure of information obtained from the event. Therefore, the information entropy of an event is not only a measure of the amount of information of an event, but also can be included as relevant information in the event itself [12].

TABLE I. INFORMATION ENTROPY AND WEIGHT CALCULATION

| Index | Service Quality | Trust Value |
|---|---|---|
| Value | 0.6 | 0.8 |
| Initial Value | 0.4 | 0.2 |
| Information Entropy | 0.9708 | 0.7205 |
| Weights | 0.426 | 0.574 |

According to the calculation principle of information entropy, the information entropy determined by the quality of service $QoS_j$ is:

$$H\left(\mathrm{QoS}_j\right) = -\mathrm{QoS}_j \log \mathrm{QoS}_j - (1 - \mathrm{QoS}_j) \log \left(1 - \mathrm{QoS}_j\right) \tag{18}$$

The information entropy determined by the trust value is:

$$H\left(\mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right)\right) = -\mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right) \log \mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right) - \left(1 - \mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right)\right) \log \left(1 - \mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right)\right) \tag{19}$$

Then the weight of the quality of service $QoS_i$ can be determined:

$$\delta_1 = H\left(\mathrm{QoS}_j\right) / \left(H\left(\mathrm{QoS}_j\right) + H\left(\mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right)\right)\right. \tag{20}$$

And the weight of trust value $\delta_2 = 1 - \delta_1$

Among them, $\mathrm{CT}\left(\mathrm{pro}_{\mathrm{r}}^{\mathrm{j}}\right)$ means the degree of reliability of the subject j, and 1-$\mathrm{CT}\left(\mathrm{pro}_{\mathrm{r}}^{\mathrm{j}}\right)$ indicates the undeterminable component; $QoS_j$ is the evaluation of the service quality of the subject j, and $1 - QoS_i$ is the uncertain component of its service quality.

For example, a service subject's (service quality, trust value) is (0.6, 0.8), then their information entropy is (0.970, 0.720), then the weight indicators of the two are: 0.4, 0.5, see Table I for details.

After the weights are calculated, the calculated trustworthiness value is trend-corrected according to the $DTV_j$ value, so that the trustworthiness value can more accurately reflect the trustworthiness of the node. According to the dynamic trust value of trustworthiness, the correction formula is as follows (21).

$$\overline{\mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right)} = \begin{cases} \mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right) + \left(1 - \mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right)\right) \times \\ \mathrm{DTV}_j \mathrm{DTV}_j > 0.5 \\ \mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right) \mathrm{DTV}_j = 0.5 \\ \mathrm{CT}\left(\mathrm{pro}_{r_k}^j\right) * e^{DTV_j - 0.5} \mathrm{DTV}_j < 0.5 \end{cases} \tag{21}$$

When the normalized Dynamic Trust value of trust degree $DTV_j$ is equal to 5, we know that the change of trust value is in a relatively stable state at this time, so we do not change the trust value, and make a difference when the value of $DTV_j$ is greater than or less than 5. The treatment is to punish some of the service providers' false information caused a decline in the trend of the change in trust, while the increase in the value of the trend of the change in the degree of trust changes

the value of the trust appropriately. According to the revised trustworthiness value,QoS value and information entropy, the calculation weight is determined to obtain the comprehensive value of optimal node selection:

$$\Delta = \delta_1 * \mathrm{QoS}_j + \delta_2 * \overline{\mathrm{CT}\left(\mathrm{pro}_{r_k}^{j}\right)} \tag{22}$$

The following is a data center node selection strategy process based on the dynamic trust value:

1) The service broker receives the node selection request from the service user ($user_i$).
2) The service intermediary selects the data center node provider ($pro_j$) that meets the user's functional requirements by analyzing the service request.
3) According to formula (7), the service consumer obtains the comprehensive trust value through the direct trust value and the indirect trust value.
4) According to equation (8), the Dynamic Trust Value DTV of the node provider is obtained.
5) According to formula (17) to obtain the quantified QoS value of the overall service quality and formula (21) to modify the trust value, and through the information entropy calculation to obtain the corresponding weight.
6) According to equation (22), the overall evaluation value of the optimal node selection can be obtained.
7) Choose the node with the largest overall evaluation value as the best choice for replica placement.

## IV. Results and Discussions

For this work simulation method is opted to verify the effectiveness of the node selection model proposed in this paper based on Dynamic Trust. The experiments were run on the cloud simulation software CloudSim3.0 [13]. CloudSim is a new universal and extensible simulation framework that supports seamless modeling and simulation, based on a specific environment and configuration, by extending its basic functions, can conduct experiments on cloud computing infrastructure and management services.

When CloudSim starts the simulation, you first need to create a data center (Datacenter), create resources such as CPU and memory in the data center, you can map user requests to the appropriate service provider (DatacenterBroker) through CIS (CloudInformationService), according to service selection Strategy for resource allocation. The operating environment is the Eclipse integrated development platform based on java development, and the CloudSim simulation program runs on the Intel Pentium dual-core G630, 2.7GHz, 2GB memory, Ubuntu18.04 64 bit Operation System on the desktop.

In this experiment, according to the different trend values of the trust degree of the node provider SP, the SP is divided into three categories:

1) Class A: The Dynamic Trust Value of SP is monotonously increasing. For example, due to the improvement of technical quality, the value of trust gradually increases.
2) Type B: The Dynamic Trust Value of SP's trust degree is relatively stable, that is to say, this type of SP provides stable cloud service functions and has good trust.
3) Type C: The Dynamic Trust Value of the SP is monotonously decreasing. For example, the SP provides a cloud service product with a false function description, which leads to the decrease of the trust value.

TABLE II. Simulation Parameters

| Parameter | | Default Value | Description |
|---|---|---|---|
| Operating Parameters | CloudletNum | 100 | Total number of tasks |
| | VmNum | 500 | Total number of SP |
| Algorithm Parameters | Num_luser | 100 | Total number of SC |
| Weights | $\alpha$,$\beta$ | 0.5 | Trust Weight |
| | $w_i$ | 0.25 | QoS weight parameters |

In order to conduct metric comparison, two test indicators are set: success rate and predicted success rate.

Within a certain time interval T, the CIS (CloudInformationService) in the CloudSim simulator provides the number N of service providers to all SCs according to the selection strategy, where the number of SPs that successfully interact with the SC is S (here, there is no fraud Behavior), the success rate is:

$$\theta = \frac{S}{N} \times 100\% \tag{23}$$

Where: $\theta$ is the average degree of cooperation between network nodes.

Within a certain time interval T, the CIS in the CloudSim emulator provides the number of service providers N to all SCs according to the selection strategy, encountered a situation where the node happened to be in the blacklist, or encountered during the interaction deception, the total number of times in both cases is M, then the model's predicted success rate is:

$$\varphi = \frac{N - M}{N} \times 100\% \tag{24}$$

In the formula: $\varphi$ can reflect the model's ability to predict the next step.

In the verification test, it is assumed that the number of SP subjects is 500 and the number of SC subjects is 100 in a cloud environment. The trust value of each virtual machine starts to be randomly generated. The node selection policy input parameters, namely, CloudletNum, vmNum, num_user, $\alpha$, $\beta$, $w_i$ are shown in Table II.

In the table, CloudletNum represents the total number of tasks requested by users in the CloudSim simulation environment, and the tasks from different users are relatively independent; vmNum is the number of virtual machines; num_user represents the number of users; $\alpha$ and $\beta$ are the direct trust weights and recommendation Trust weights, respectively. The data results of each group are averaged after 10 times.

**Case Study 1:** In a cloud environment, the nature of data center node is highly dynamic. It is assumed that a service node rj is malicious, but the resource may be used to

cover its important service transactions. Good service quality establishes good trust. After a period of time, the service provider lowers the standard of service quality in order to reduce costs, but due to the establishment of early trust, the poor post-service has a higher trust value. So, it is necessary to introduce the trust time decay mechanism. When there is no transaction in the middle of a period of time, the trust value will decrease with time. Also set a decay constant, you can set the credibility decay speed according to different service types. The service occurs in a malicious time period, and a larger attenuation constant can be set. Fig. 1 shows the attenuation of the trust value under different attenuation constants, namely, type1($\lambda$=y1=exp(-0.025x)), type2($\lambda$=y2=exp(-0.05x)) and type3($\lambda$=y3=exp(-0.1x)). Simulation results show that the larger the attenuation parameter, the faster the attenuation rate.

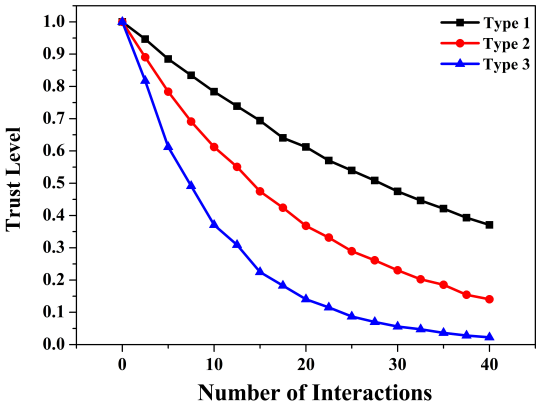


Fig. 1. Change of Trust under Different $\lambda$ Values.

**Case Study 2:** Fig. 2 shows the change of the trust value of the three types of service providers during the interaction of the service subjects. From the figure, it can be seen that the class A SP is in the increasing trend as the number of interactions are increasing and its credibility has been maintained with a growing trend. The Trust value of the B-type SP increases with the number of interactions, but when it reaches a certain level, it will be in a relatively stable state. The Trust value of C-type SP begins to increase with the number of interactions. The trust value also increases. Although the C-type SP maintains a high trust value in the early stage, due to the provision of false services, the trust level in the later stage decreases, which ultimately leads to a lower level of trust value.

**Case Study 3:** Fig. 3 shows the comparison of the three different strategies namely the node selection method based on the Dynamic Trust Value, the node selection method based on trust degree, and the node selection method based on non-trust degree. It is an indicator of success, so its success rate has a greater advantage than the latter. But at the same time, the node selection method based on the dynamic trust has always maintained a better growth trend, because its DTV which effectively reflected the change trend of trust. This method has the ability to predict, to a certain extent can filter out false information, thereby improving the success rate of node selection in a better way.

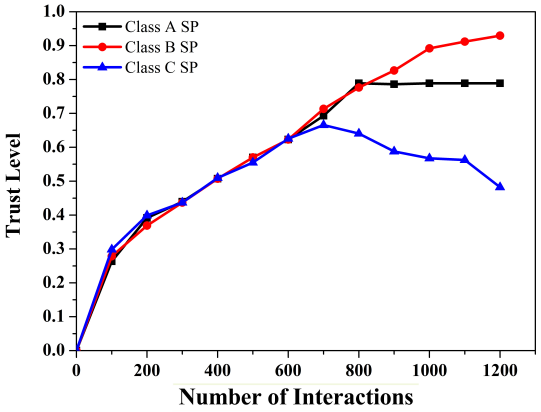


Fig. 2. Comparison of Different SP's under Dynamic Trust.

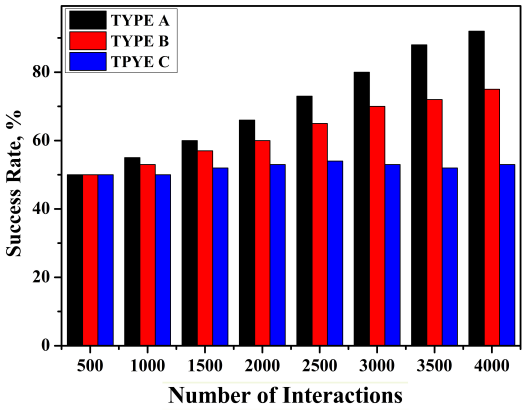


Fig. 3. Comparison of Node Selection Rate of Different SP's.

**Case Study 4:** Fig. 4 shows the comparison of the prediction success rate among the three methods namely the node selection method based on the Dynamic Trust Value, the node selection method based on trust degree, and the node selection method based on non-trust degree. The proposed method DTV has a certain predictive ability for node selection, so the prediction success rate has always shown a relatively stable growth state, while the node selection method based on trust does not predict the success rate after reaching a certain level. Again, this is because the trust-based node selection method does not contain the Dynamic trust evaluation and lacks continuous predictive ability. The trust-based node selection method has no consideration of trust factors, so it has the great blindness that led to the development of the prediction success rate in molar shape. The experimental results show that the model based on the DTV proposed in this paper effectively improves the prediction ability of node selection for replication.

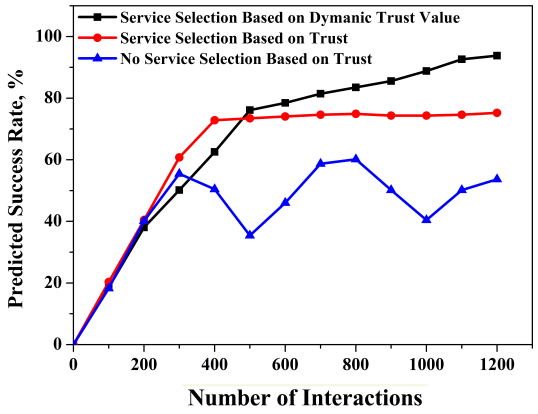


Fig. 4. Comparison of Predicted Success Rate of Proposed Model with Others.

## V. Conclusion

In the cloud computing environment, this paper aims at the problem of replica placement in data center nodes for enhanced availability. The node selection for replica placement is a difficult process. Based on the proposed trust model it improves the ability to predict service quality of data center node and increases the accuracy of data center node selection for replication. The concept of Information Entropy is introduced to avoid the shortcomings that only perform simple weighted analysis of trusted parameters, and effectively improves the success rate of node selection. Experimental analysis shows that this method can better meet users' service quality and trust in node selection. Further the data center node which gets selected for replication using this model exhibits less failure rate, there by enhances availability in cloud.

## References

[1] Wand et al., "Particle swarm optimization with skyline operator for fast cloud-based web service composition ", Mobile Network s and Applications, 2013 , 18(1) :116-121.

[2] Zhang et al., "Preference-aware QoS evaluation for cloud web service composition based on artificial neural networks", Web Information Systems and Mining , 2010 , 18(1) :116-121.

[3] H U Chunhua et al., "Services selection based on trust evolution and union for cloud computing", Journal on Communications, 2011 , 32 ( 7 ) :71-79.

[4] MA You et al., "Web service quality metric algorithm employing objective and subjective weight", Journal of Software. 2014 , 25 (11) : 2473 -2485.

[5] Sarabjeet S et al., "Trust evaluation in cloud based on friends and third party's recommendations", RAECS Conference. Panjab University Chandigarh: IEEE, 2014 :1-6.

[6] Das A et al., "Secured trust : a dynamic trust computation model for secured communication in multi agent systems", IEEE Transactions on Dependable and Secure Computing , 2012 , 9( 2) :261-274.

[7] Zhou et al., "Dynamic virtual resource renting method for maximizing the profits of a cloud service provider in a dynamic pricing model" , International Conference on Parallel and Distributed Systems. Seoul :IEEE, 2013: 118-125.

[8] Cao , Jiang Huowen et al., "Trust-aware dynamic level scheduling algorithm in cloud environment", Journal on Communications , 2014 , 35(11) :40-49 .

[9] Zhang Lin and Wang Hai-yan, "Dynamic trust monitoring model supporting behavior in information services", Journal of Nanjing University of Posts and Telecommunications, 2013 , 33(1) :68-73.

[10] Abawajy J., "Determining service trustworthiness in intercloud computing environments", Proceedings of the 10th International Symposium in Pervasive Systems, Algorithms, and Networks. National Cheng Kung University: IEEE, 2009 :784 -788 .

[11] Josang A and Ismail R., "The beta reputation system", Bled Electronic Commerce Conference. Bled Slovenia: IEEE, 2002: 324-337.

[12] Huang Ying-jie et al., "Hybrid particle swarm optimization based on entropy for flexible job shop scheduling problems", Journal of Hunan Universit y: Natural Sciences, 2012 , 39(3) :48-52.

[13] Rahul M., "Study and comparison of CloudSim simulators in the cloud computing", The SU Transactions on Computer Science Engineering &. its Applications, 2013 , 1(4) :111-115.

[14] Tjang C et al., "Research on evaluation of SaaS SP service quality based on SLA", In Journal of Computer Engineering, 2013, Page:31-36.

[15] Dantas J et al, "Eucalyptus-based private clouds: availability modeling and comparison to the cost of a public cloud", 2017, Page:1130–1140

[16] Fan W., Perros, H., "A novel trust management framework for multi-cloud environments based on trust service providers", Knowl. Based Syst.70, 2014, 392–406.

[17] Rajendran, V.V., Swamynathan, S., "Hybrid model for dynamic evaluation of trust in cloud services", Wirel. Netw., 2015, 1–12.

[18] Jabbar, S., Naseer, K., Gohar, M., Rho, S., Chang, H., "Trust model at service layer of cloud computing for educational institutes", J. Supercomput., 2015,1–26.

[19] Chiregi, M., Navimipour, N.J., "A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities", Comput. Human Behav. 60, 2016. 280–292.

[20] Selvaraj, A., Sundararajan, S., "Evidence-based trust evaluation system for cloud services using fuzzy logic", Int. J. Fuzzy Syst., 2017, 1–9.

[21] Lynn, T., van der Werff, L., Hunt, G., Healy, P., "Development of a cloud trust label: a Delphi approach", J. Comput. Inf. Syst. 56, 2016, 185–193.

[22] Tang, M., Dai, X., Liu, J., Chen, J., "Towards a trust evaluation middleware for cloud service selection", Future Gener. Comput. Syst. 74, 2017, 302–312.

[23] P. T. Endo, M. Rodrigues, G. E. Gonçalves, J. Kelner, D. H. Sadok, and C. Curescu, "High availability in clouds: systematic review and research challenges", J. Cloud Comput., vol. 5, no. 1, Oct. 2016, p. 16.

[24] Vijay Kumar, A Nagesh and M Nagaratna, "SLA-Based Trust Model to Enhance Availability in Private Cloud", International Journal of Advanced Science and Technology, 29(05), 2020, pp.13941 - 13954.

[25] J. Riley, J. Noss, W. Dillingham, J. Cuff, and I. M. Llorente, "A High-Availability Cloud for Research Computing," Computer, vol. 50, no. 6, 2017, pp. 92–95.