Data Service Trust Measurement in Cloud Environment

Lin Shi (shiling717@nuaa.edu.cn)
Nanjing University of Aeronautics and Astronautics
Zilong Wang
Nanjing University of Aeronautics and Astronautics
Ning Chen
Nanjing University of Aeronautics and Astronautics
Jie Chen
Nanjing University of Aeronautics and Astronautics

Research

Keywords: Cloud Environment, Data Service, Trusted Measure, Cloud Security, Trust Service

Posted Date: December 18th, 2019

DOI: https://doi.org/10.21203/rs.2.19247/v1

Data Service Trust Measurement in Cloud Environment

Lin Shi[1, 2a*], Zilong Wang[1b], Ning Chen[3c] and Jie Chen[2d]

[1]*College of Economics and Management, Nanjing University of Aeronautics and Astronautics, Nanjing, 211106, Jiangsu, China*

[2]*Jiangsu Financial Information Management Center, Nanjing, 210024, Jiangsu, China*

[3]*Jiangsu Water Conservancy Network Data Center, Nanjing, 210029, Jiangsu, China*

[a] shiling717@nuaa.edu.cn; [b] wangzilong@nuaa.edu.cn; [c] a.cnapt@gmail.com; [d] seba@jscz.gov.cn

[*]*Corresponding author*

Abstract: Highly trusted issues will be one of the main obstacles to a new era of highly trusted cloud computing. In the cloud computing environment, because sensitive applications and user data are put into the cloud, they run in virtual machines in the data center. Among them, due to the existence of access vulnerability, virtualization vulnerability, web application vulnerability, etc., high trust issues arise from data control, identity authentication, lack of information and other related issues. The introduction of trust mechanisms can be very facilitate the solution of related issues, achieve highly trusted quantification, analysis, and modeling of cloud data centers, meet high trust requirements, and provide users with a highly trusted cloud computing environment. This article mainly studies the trust measure of data services in cloud environment. In this paper, the optimization scheme is verified through experiments, and the traditional big data processing scheme, the original Sahara and the optimization scheme are compared in six cases. Overall, the optimization scheme has a significant performance improvement. Compared with the default configuration of Sahara, the configuration of the new interface has increased the throughput in DFSIO by 120%. Using the design of the unified cache management service, Tachyon can reach 13 in specific situations. In the execution time of Sort workloads, the optimization scheme generally decreased by about 50% compared to the original Sahara, and the memory utilization increased from 80% to 96% in our experiments, but in the cache isolation and other areas need to be improved. The results are basically in line with expectations, which also confirms the rational thinking and value of this article on BDAaS performance research.

Key words: Cloud Environment, Data Service, Trusted Measure, Cloud Security, Trust Service

1. Introduction

Since the introduction of the concept of cloud computing, it has received extensive attention from the industry. It combines the advantages of grid computing and service computing, and uses virtualization technology to provide computing and storage resources in the form of services [1]. It adopts a new type of shared storage architecture, has a safe and reliable data storage center, has low requirements on user terminal equipment, can easily realize data sharing between different devices, and can provide unlimited powerful computing and space [2-3]. However, cloud security has become a major obstacle to the rapid and stable development of cloud computing. In terms of technology, all user data is stored in the cloud. Once the cloud service is interrupted due to technical factors, it will cause catastrophic results [4]. The problems of cloud computing in network applications are clearly visible. Although the Internet with the TCP/IP protocol as its core has achieved great success, false identifications and addresses have caused a lot of security problems, making Internet security events happen frequently and credibility. It is greatly reduced, which limits the further development and application of the Internet. Therefore, the development of Internet identity authentication technology also restricts the development of cloud computing [5-6]. In addition, the data security of cloud data

centers is not guaranteed by any trusted third party, and users are anxious about the security issues and loss of control that may occur when data is migrated to the cloud [7]. Considering the security issues in the cloud computing environment, trust is the core of the cloud service interaction process. Some people have introduced the "trust relationship" in social life into the computer field, and proposed to manage "trust". In the following 20 years, universities have conducted a lot of research on the issue of trust and achieved significant results [8-9]. These research foundations provide a new idea for solving security problems in the cloud computing environment.

Cloud computing, as the development and integration of parallel computing, grid computing, and P2P computing, is a business computing model that uses virtualization technology to provide users with computing services, storage services, and software services on demand, which has become increasingly widespread application [10-11]. Users only need to connect to the Internet and directly access services in the cloud through the "cloud", eliminating the need to constantly update their own hardware devices, install software locally, and configure tedious programs [12]. Pay-as-you-need, pay-as-you-collect service principles have made cloud computing application services used by more and more business applications. Business features have injected vitality into cloud computing and promoted the development of cloud computing technology. The ultimate goal of cloud computing is to provide scalable, inexpensive, high-quality computing infrastructure and information services on demand [13]. The virtualized nature of cloud computing makes it possible to use resources efficiently, helping users save time and money, while the commercial nature of cloud computing makes it a success for multinational companies and SMEs. With the vigorous promotion of technology companies, the development of related technologies has become more and more mature, and has already had a huge impact globally [14-15]. Research in academia shows that cloud computing has gained high recognition from the industry. At the same time, its unique virtualization and business features have made it a research hotspot for enterprises and scholars [16].

Jens believes that abstract trust is an important enabler for successfully establishing business relationships and an important factor in determining technology adoption. However, so far, trust has received little attention in cloud computing environments, leading to trust in cloud services and trust prerequisites lack of understanding of dimensions. Although the literature provides a variety of conceptual models of trust for contexts related to cloud computing, which can be used as a reference, especially trust in IT outsourcing vendors and trust in IT artifacts, the nature of trust in cloud computing requires a novel trust conceptual model. First, cloud services have the dual nature of IT artifacts and services provided by the organization. Second, cloud services are provided in the non-personalized cloud market and are built on a cloud service network nested within the cloud ecosystem. In his research, he developed a conceptual model to describe trust in cloud services. The conceptual model combines the duality of trust in cloud service provider organizations and trust in IT artifacts, as well as trust types in non-personal environments and cloud computing ecosystems. Then, using a conceptual model as a perspective, he reviewed 43 empirical studies on trust in IT outsourcing and trust in IT artifacts, which were identified through structured literature searches. The final conceptual model provides a conceptual construction type for trust relationships in cloud services, defines the premise of trust establishment, and presents 19 propositions, describing the relationship between trust constructions and the premises of trust construction and trust establishment. His conceptual model contributed research by integrating two previously unrelated branches into the trust literature and identifying knowledge gaps [17]. In order to analyze the mechanism of trust formation and understand the key conditions for achieving mutual trust and cooperation in the cloud

manufacturing environment, *K* proposes a trust game model based on incomplete information game theory. From the perspective of short-term benefits of service demanders, he analyzed two possible game equilibriums and corresponding conditions. At the same time, a three-game model was constructed from the perspective of the long-term benefits of the service provider, and the possibility of game equilibrium was derived. He obtained the equilibrium of mixed perspectives through comprehensive analysis, verified the existence of game equilibrium through Monte Carlo simulation, and analyzed the influence of different factors on trust games. His simulation results show that the preferences of service demanders can promote the formation of trust between demanders and providers. They satisfy their preferences, make the total trade show a multimodal distribution, and disguise costs and dishonest punishment rates. Increase can promote the formation of trust [18]. Study *D* introduces the privacy and confusion of intelligence and confidential information owned by the insurance and financial industries. He believes that if dictators abuse secret information, there is a privacy risk in the business era. Software outages that corrupt digital data in the name of third-party services. The responsibility of digital confidentiality lies in the isolation of business continuity, improper handling can lead to breach of privacy and its precautionary behavior is prudent in the cloud, where a large amount of data is stored and maintained. Although cloud computing has changed in the field of cloud computing by improving effectiveness, efficiency and optimization of service environment, etc., cloud user data and their identity, reliability, maintainability and privacy of different CPs (cloud providers) may be different. The CP ensures that users' proprietary information is maintained more secretly using current technology [19]. *Fuan* validated the alternative measurement model of brand trust and proved the robustness and measurement invariance of the model in a cross-cultural context. He uses survey data collected from the United States and China to submit to alternative measurement models, and Amos 7.0 is used to test the robustness and stability of the proposed model. His experimental results provide strong support for the stability and robustness of alternative models [20].

The innovations of this paper: (1) In terms of high service quality, it will analyze and establish a resource scheduling model in the cloud computing environment, quantify the user's application preferences, the user utility in the multidimensional QoS space, and the objective function of multidimensional QoS optimization. An immune cloning algorithm with objective optimization capabilities will propose a cloud resource scheduling algorithm based on application preferences, which will build an efficient, stable, and fast resource scheduling theory in a cloud computing environment. (2) In terms of high trustworthiness, the trustworthiness in the cloud computing environment will be defined, the trustworthiness attributes will be quantified, the measure of trustworthiness will be realized, and the theoretical standards for achieving trustworthiness in various situations will be analyzed. A general theoretical approach to enhance system reliability in a cloud computing environment through the use of virtualization technology, and theoretically determine the number of virtual machine nodes required to achieve high reliability, which will build a multi-dimensional, dynamic, and flexible reliability theory. (3) In terms of high trustworthiness, it will quantify the measurement of trust on specific content between trusted entities, mine malicious recommended trust information between entities, improve the accuracy of recommended trust information, and model a multi-angle spatial attenuation of recommended trust information evaluation method, and a multi-stage time decaying direct trust information evaluation method, based on the interaction history and interaction content between trusted entities, to achieve dynamic management of trust, will build a multi-angle, multi-stage, efficient, accurate, and timely in a cloud computing environment trustworthiness theory.

2. Proposed Method

2.1 Cloud Computing

(1) Cloud computing concept

Cloud computing inherits the main technologies and concepts of distributed computing, grid computing, utility computing and virtualization. Cloud computing provides users with efficient and convenient on-demand computing services. It is based on a configurable virtual computing resource pool (including the network, server, storage, application software, services, etc.), users can quickly use these resources with only a small amount of necessary management work, greatly improving the efficiency of large-scale storage and computing. A large number of concurrent network computing and services are connected in the cloud computing environment. It uses virtualization technology to maximize the use and expansion of the capabilities of each virtual machine, integrates its respective resources through the cloud computing platform, and provides supercomputing and storage capabilities. Its architecture, standards, system platform, and software services are all open. These services are not centralized, but are distributed on tens of thousands of different servers in various places. At present, resources and services in the cloud computing environment are already on a large scale and are still growing rapidly. It needs to be dynamically combined or expanded to provide multiple services under the complex conditions of considering resource constraints, service goals, and diversified service implementation methods. Different information service applications to meet the individual needs of users.

(2) Cloud computing services

In view of the fact that cloud computing technology provides software and hardware resources as IT services to users with different needs, for this reason, academia and industry have proposed a cloud delivery model SPI (Software Platform Infrastructure) to represent the three types of basic services provided by cloud computing technology. It is infrastructure as a service, platform as a service, and software as a service.

(a) Infrastructure as a Service (IaaS). IaaS refers to the provision of supporting services such as computing, storage, and networking for users based on traditional IT infrastructure such as servers, storage, and networks. Computing services include both scalable virtual machine environments and high-performance computing capabilities. Storage services are diversified storage modes, such as block storage mode, object storage mode, and database storage mode. The storage capacity supports both traditional shared storage systems and distributed storage systems. Network services are common firewall services, load balancing services, and content distribution networks.

(b) Platform as a Service (PaaS) Cloud computing service providers achieve the goal of PaaS by building a platform or environment that meets the basic needs of application development, operation, and testing. In PaaS, the basic elements of the development platform such as operating system, middleware, and environment variables are all deployed and operated by cloud service providers, and they are provided to external users in the form of service instances.

(c) Software as a Service (SaaS). SaaS refers to application software that cloud service providers will uniformly deploy in a cloud computing environment and deliver it to users as service instances via the Internet. Customize specific application software services. In the cloud computing environment, PaaS provides a scalable IT infrastructure to the maximum extent and is transparent to users. Therefore, users do not have to order the required IT infrastructure, they can quickly build their own PaaS private platform on IaaS, and they can even directly deploy SaaS software services on IaaS or PaaS. In

summary, IaaS, PaaS, and SaaS provide users with diverse services at different levels through a unified technical architecture and specific software technologies. The cloud computing service architecture is shown in Figure 1.

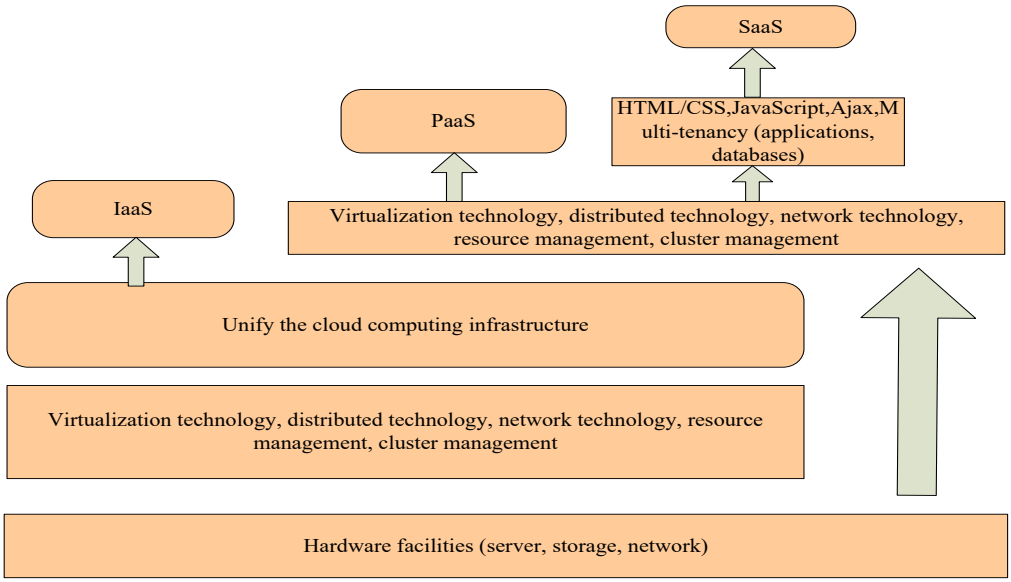

Figure 1. Cloud computing service framework

2.2 Cloud Computing Security Technology

Software as a service (SaaS) providers in cloud computing share program services based on the cloud computing environment for users. However, users' applications and information are all in the hands of service providers, and their credibility and confidentiality may be difficult to guarantee. Although cloud computing service providers are working hard to improve the security of their own system platforms, cloud service security still faces many problems that need to be solved urgently. Therefore, corresponding methods are urgently needed to solve the many hidden dangers faced by cloud computing services, so as to ensure that the customer's information is not leaked, including the reliability, integrity, and confidentiality of customer information. In order to enable the cloud computing service platform to have a trusted execution environment and a secure authentication process, it is urgent to study data confidentiality protection, user privacy protection, information integrity authentication, trusted cloud computing, information authentication, and access control in the cloud computing environment. And other issues. Based on the summary of the above research issues, the following related technical requirements are required in terms of cloud computing data security protection:

(1) Identity authentication technology

Cloud computing is an emerging technology. Through web technology, several users can access cloud applications. Too many users need to let cloud service providers adopt identity authentication technology and improve the identity authentication mechanism to ensure that legitimate users can access cloud applications and data.

(2) Access control technology

As the data of several users are stored in the cloud, cloud service providers need to use related authentication access control technology, so that users can only access their own data, and cannot access other user data without obtaining relevant permissions. At the same time, cloud computing service providers must do good data isolation work to prevent unauthorized cloud workers from accessing user data.

(3) Data transmission security technology

For the user's information transmission process, the problem of reliable information transmission involves information loss, illegal alteration, and leakage. For customers, information is stored in the cloud. Due to the characteristics of cloud computing, it is not possible to know exactly where the information exists. Although cloud service providers will implement corresponding protection measures, if the protection measures are not perfect, it will also cause loss and tampering during data transmission. And other security risks. In order to ensure the secure transmission of data in the cloud and users, as well as in the cloud, it is necessary to introduce traditional web security technologies to ensure the security performance of user data transmission during network transmission and establish a secure communication mechanism. By introducing the security technology involved in the cloud computing environment, we can understand that whether it is on the cloud platform or the user platform, there are many security risks in data security issues during the authentication process of cloud computing. So constructing an authentication architecture that guarantees the credibility of the platform is crucial to building a credible cloud computing environment. On this basis, firstly, a mutual trust relationship needs to be established between the user terminal and the cloud computing platform. The establishment of the mutual trust relationship is the prerequisite for eliminating the problem of information leakage and the foundation for realizing the trusted cloud computing security technology. If users do not regard the cloud computing platform as a trusted object, they will not operate the cloud software to hand over their data to the cloud for processing, so it will greatly hinder the development of cloud computing, which involves the credible cloud problem naturally becomes the top priority of cloud computing research. Conversely, if the end users connected to the cloud computing platform cannot prove their legitimacy and security, the cloud service provider will not allow them to access the cloud illegally. If they access, it may cause unnecessary losses to the cloud. There are many ways to solve these problems, and the concept of trusted cloud computing is proposed in the process of solving the above problems. As the name implies, it applies the integrity measurement technology of the trusted computing certification terminal to the cloud computing environment. However, it is not enough to build a trusted platform at both ends of the cloud computing environment. In some way, the trusted information is transmitted to the other platform in a certain form and the other platform judges it correctly, the platform authentication architecture in the cloud computing environment is really realized. By introducing the concept of remote authentication, cloud terminals and end users can use different authentication methods to verify to the challenger that the security of the data transmitted by their platform is reliable. For security problems that are prone to occur during user data transmission, relevant digital signatures, data encryption, and Web security technologies are introduced to ensure that data is not tampered with or lost during the data transmission process.

2.3 Trusted

(1) Credible definition

The definition of trusted computing is very broad, and whether it is application software, system software, or chips can be included in the definition of trusted computing. With the grim situation of Internet information security, it has programmed a popular direction for Internet security research. A hot topic in trusted computing research is the question of what is trusted computing. At present, the relevant definitions of trusted computing include the following definitions. According to the relevant definition of the Trusted Computing Group (TCG): If a system can work in a predictable manner and achieve a set goal in a limited number of steps, then the system is credible. Through software behavior to demonstrate trusted computing, TCG believes that software is credible if a software system can work

in its predicted direction and achieve its stated goals. A trusted software system can have the ability to protect data security and the ability to measure system integrity.

By predicting the behavior of software entities, credibility is defined: if an entity always moves in the expected direction and in an expected manner, then this entity is credible. This is the behavior of TCG organizations using entities to define credibility. Some people believe that the services provided by computer systems are trustworthy based on existing knowledge. The concept of trust here includes two elements. The first is that the services provided by the system are trustworthy. The second is that this credibility is verifiable. The credibility here mainly refers to the reliable performance and security of the system. Through some researchers' definition of the concept of trust: trusted computing software is a computer system that can judge the credibility, security, and availability of a platform. There are many aspects to credibility, such as accuracy, reliability, security, and so on.

(2) Trusted Computing Platform

The use of relevant definitions and technologies of trusted computing requires the establishment of a trusted computing terminal. According to the definition of the TCG organization, the root of trust of a trusted computing terminal must be reliable, which is the foundation for realizing a trusted computing terminal. A set of roots of trust can describe the characteristics of the platform and provide relevant evidence of the credibility of the platform. A trusted computing terminal usually consists of three components: a trusted measurement root RTM, a trusted storage root RTS, and a trusted report root RTR.

RTM measures the reliability of trusted platforms, and RTS retains the summary of trusted metrics and the calculation of the digest sequence. RTR can accurately represent the ability of trusted storage roots to grasp information. A trusted computing platform is a platform trusted by users. Its trusted foundation is built in the trusted computing module TPM, which provides a variety of security functions for trusted platforms, such as ensuring the security of private keys; detecting malicious code; preventing malicious code from using private keys; and ensuring the security of encryption keys. TGC also implements the public key authentication function, the integrity measurement function, and the certification function through the chip. The trusted computing terminal utilizes the security performance of the above TPM chip to implement functions such as terminal identity authentication, data security storage, and integrity measurement. As shown in Figure 2, it is a flowchart of trusted platform authentication.

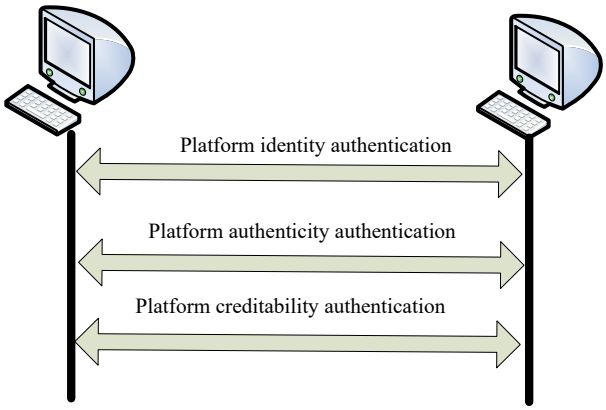

Figure 2. Trusted platform authentication flowchart

(3) Weighted combination method of evidence classification based on new conflict metrics

In order to accurately measure the degree of conflict between evidences, a classic evidence conflict coefficient K and improved evidence coincidence were introduced to establish a new method

for calculating the evidence conflict coefficient.

The formula for improving the coincidence degree of evidence is:

$$c_{12} = \sum_{i=1}^{N} \min\left(m_1'(A_i), m_2' A_i\right) (1)$$

Among them, A_i is a single-subset focal element, N is the number of single-subset focal elements, and $m_1'(A_i) = \sum_{A_i \in A} m(A)/|A|$ is a Pignistic probability function of the single-subset A_i.

The new evidence conflict factor is:

$$K_{ij}^c = \sqrt{k_{ij} \cdot (1 - c_{ij})} \quad (2)$$

When $\overline{K}_i > K_{ave}$ and $\overline{K}_i > 0.5$, the evidence m_i is the conflict evidence, of which

$$\overline{K}_i = \left(\sum_{j=1, i \neq j}^{n} K_{ij}^c \right) / (n-1), \quad K_{ave} = \left(\sum_{i=1}^{n} \overline{K}_i \right) / n .$$

In order to effectively solve the problem of synthesizing highly conflicting evidence, the improvement of the second type of improvement method (that is, adjusting the basic credibility distribution of the original evidence source) for reference, the improved D.S theory algorithm is established. The algorithm first uses the new conflict coefficient to determine the conflict evidence, and then combines the new conflict coefficient with the degree of evidence certainty to define the reward function, determine the normal evidence weight, define the penalty function, determine the conflict evidence weight, and use the normalized evidence weight. After the weighted average of evidence, the weighted average evidence was synthesized *n*-1 times using the Dempster synthesis formula.

The greater the degree of certainty of non-conflict evidence, the more credible the evidence, the more conducive to decision-making, and the greater the weight should be given; the greater the certainty of conflict evidence, the less weight should be given in order to reduce the impact of conflict evidence on the composite result. This paper introduces the calculation method of evidence certainty proposed by Wang Lu et al. And improves it.

Let m_1, m_2,. m_n. The piece is the mass function under Θ. The degree of certainty of the evidence m_i is:

$$Q(m_i) = \exp(-S(m_i) + P(m_i) - 1) (3)$$

Among them, $S(m_i) = s(m_i) / \sum_{i=1}^{n} s(m_i)$, $s(m) = -\sum_{\theta \in \Theta} BetP_m(\theta) \log_2 (BetP_m(\theta))$ are the entropy of the evidence, stipulating that when $BetP_m(\theta) = 0$, $BetP_m(\theta) \log_2 (BetP_m(\theta)) = 0$,

$BetP_m(\theta) = \sum_{\theta \in B \subseteq \Theta} m(B)/|B|$, $P(m_i) = P(m_i) / \sum_{i=1}^{n} P(m_i)$, $P(m) = \sum_{A \subseteq \Theta} (|\Theta| - |A|)/(|\Theta| - 1) \cdot m(A)$

are the accuracy of the evidence. However, the accuracy of the evidence calculated by formula (3) is low.

Use formula (1) to calculate $Q_1 = 0.189$, $Q_2 = 0.717$. The observation shows that the degree of certainty of the evidence E_2 should be 1.

Therefore, the following corrections are made to the certainty of formula (1):

$$Q'(m_i) = \exp(-s(m_i) + p(m_i) - 1) \quad (4)$$

Use formula (4) to calculate $Q_1' = 0.27$, $Q_2' = 1$. The calculation results are consistent with the actual.

Normalize the revised evidence certainty to the relative certainty of evidence:

$$Q^n(m_1) = Q'(m_1) / \sum_{i=1}^{n} Q'(m_i) \quad (5)$$

Combining the evidence conflict coefficient with the degree of evidence certainty, the defined reward function and penalty function formula are as follows:

$$w_i = \frac{1 - \overline{K}_i}{\sum_{i=1}^{n} (1 - \overline{K}_i)} \exp(Q''(m_i) - 1) \quad (6)$$

Define the penalty function:

$$w_i = \frac{1 - \overline{K}_i}{\sum_{i=1}^{n} (1 - \overline{K}_i)} \cdot (1 - Q^n(m_i)) \cdot \exp(-Q''(m_i) - 1) \quad (7)$$

Normalize the weight of evidence:

$$w_i' = w_i / \sum_{i=1}^{n} w_i \quad (8)$$

The weighted average of the original evidence is obtained by using the normalized evidence weight, and the weighted average evidence is:

$$m'(A) = \sum_{i=1}^{n} w'(m_i) \cdot m_i(A) \quad (9)$$

3. Experiments

3.1 Experimental Design

(1) Simulation process description

Introducing the trust mechanism, CloudSim's resource simulation scheduling work mode is shown in Figure 3.

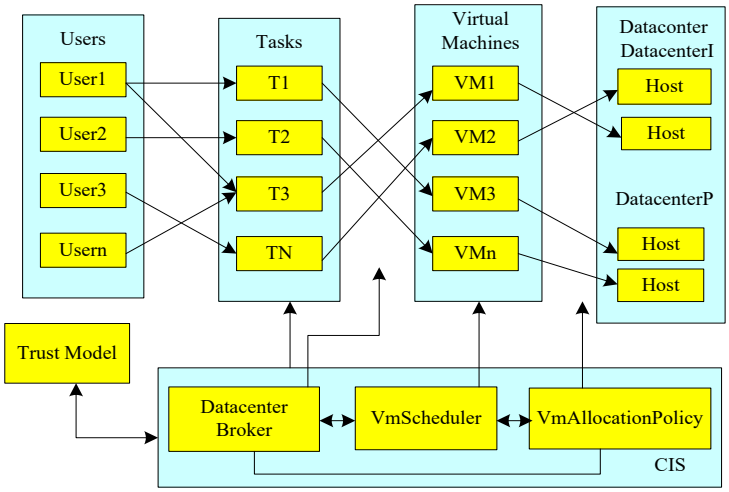

Figure 3. CloudSim resource scheduling simulation diagram

As shown in Figure 3, the resource simulation scheduling is divided into three levels: the first layer of users-a VM (VirmalMachinel task list, the second layer of VM lists-a DataCenter list, and the third layer of DataCenter lists-a Host. Its core modules are CIS and DataCenterBroker, both of them implement resource discovery and message interaction. The user-developed scheduling algorithm and trust algorithm can be implemented in the DataBroker method. Since the trust object studied in this article is the cloud service request user and service provider. The virtual machines in the list can be regarded as their own service resources published by the service provider in the cloud center, and the trust model can be added to the first level of the service resource simulation scheduling. So this article adds the trust model to the DataBroker class and extends the DataBroker class. Let the trust model participate in the service resource scheduling process to ensure the safe use of cloud resources. The service resource scheduling system that this article intends to implement does not consider other factors of the service resource, and only studies to verify the trust model in the service resource scheduling system. Assess accuracy and dynamic adaptability. According to the bindCloudletToVm method code in the DataBroker class. In the source code, only a single task is bound to run on the specified virtual machine, and the task and virtual machine are not processed accordingly. According to the trust model proposed in this article, including the trust calculation, trust decision, and trust update process, the extension to bindcloudlettovm method is described in detail.

(2)Experimental environment and parameter settings

This article uses Netlogo software to simulate a cloud file storage system, mainly to implement file download services. In the simulated cloud file storage system, cloud file resources are divided into four categories: images, audio, video, and text; each type of resource is divided into large, medium, and small scales. CSPs are divided into three categories: honest CSPs, malicious CSPs, and random CSPs. Among them, honest CSPs always provide genuine and trusted services, malicious CSPs always provide false and untrusted services, and random CSPs randomly change between good and bad. In the same way, CU is also divided into three categories: honest CU, malicious CU, and random CU; among them, honest CU always provides real evaluation, malicious CU always provides false evaluation, and random CU constantly changes between good faith and malicious. The ratio of honest, malicious, and random entities is 7: 1: 2. Within each simulation time step, the CU will make a service request, and the CSP responds to the service request. After the interaction is completed, the CU evaluates the CSP's service. The system calculates and updates the trust based on the CU's satisfaction evaluation and the QoS attribute of the interaction itself. The initial direct trust value for the entity is set to 0.5.

4. Discussion

4.1 Analysis of Trusted Models

(1) Analysis of trust value decay and time change

Table 1. Simultaneous virus disinfection time for virtual machines

Number of antivirus virtual machines (sets)	Antivirus average time (s)
1	191
2	333
3	788
4	1357
5	1547

Many trust models regarding the time factor are aimed at the interaction time between the cloud user entity and the cloud service provider entity. This interaction time can effectively express that the trust value between entities changes with time. The time factor used in this paper mainly considers two aspects: one is the time interval between the entity's last interaction time and the current time; the other is the number of entity interactions hum,as shown in Table 1.

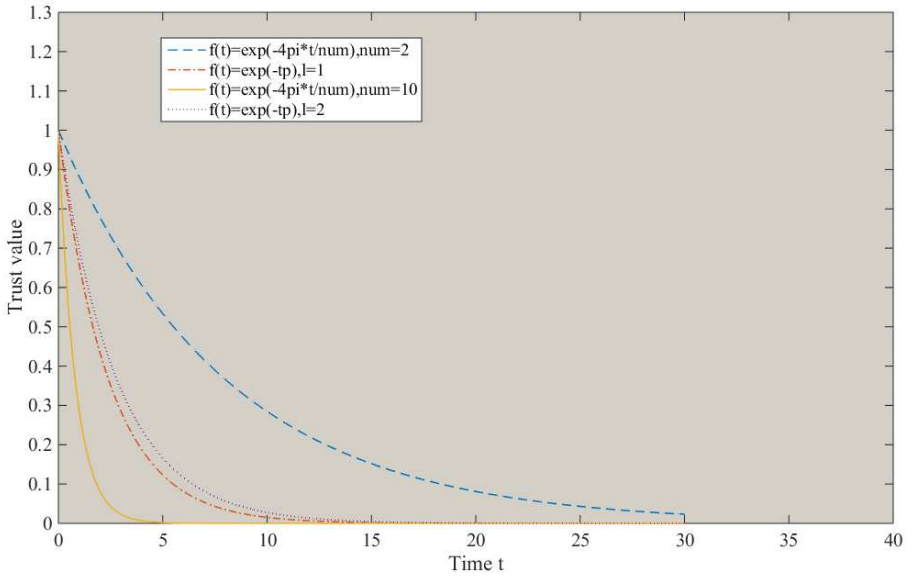

Figure 4. Trust value decay versus time

As shown in Figure 4, the difference in the total number of historical interactions greatly affects the rate of trust decay. The greater the number of interactions, the slower the rate of trust decay, and vice versa. From the comparison chart of num = 2 and p = 2, it can be seen that when the number of interactions is small, the decay rate is faster.

(2) Analysis of the relationship between trust change and time

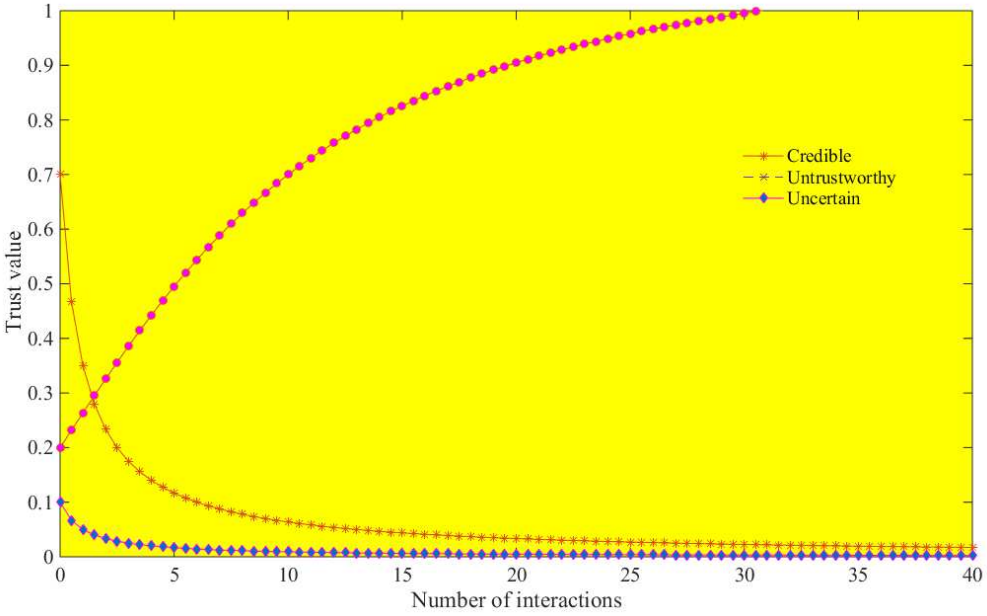

Figure 5. Relationship between trust change and time

As shown in Figure 5, when only the time factor is considered, the larger the time interval between the last service interaction, the smaller the proportion of trusted and untrusted, and the larger the proportion of uncertainty, which is consistent with the actual life law. It can be seen that the time factor model proposed in this paper is more scientific than $Trust_x Y(t) = Trust_x Y(t_0) \times e^{\frac{(t-t_0)}{\lambda}}$.

(3) Analysis of the static trust relationship before and after the trust model is applied

Table 2. E values when Cloud Desktop starts

Cloud Desktop	Non-SVMIM startup total time(s)	SVMIM startup total time(s)	E value
1	36	113	3.47
2	82	124	2.41
3	146	134	0.87
4	322	165	0.76
5	726	274	0.45
6	1366	312	0.37

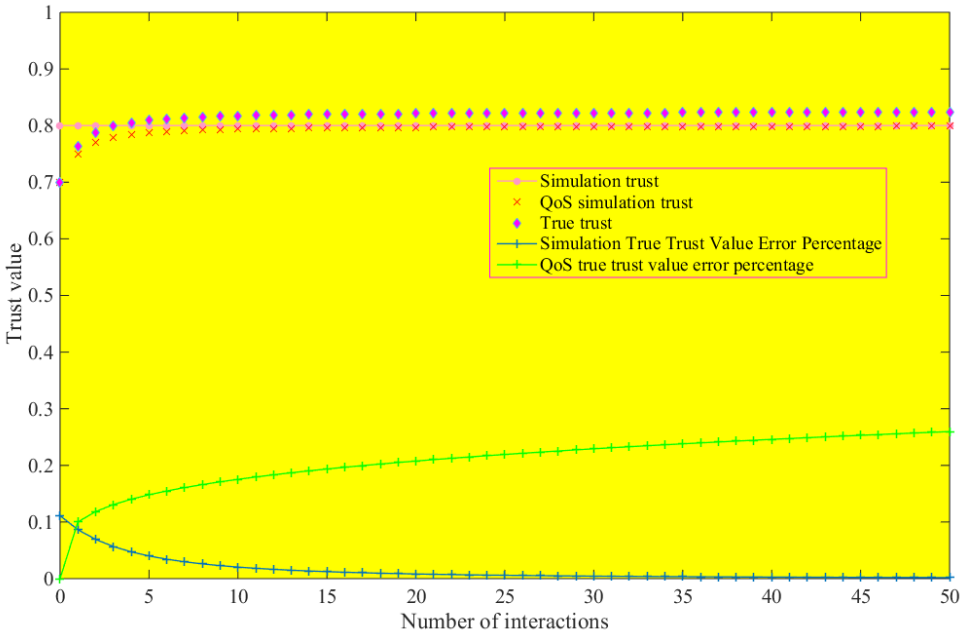

Figure 6. Static trust relationship diagram before and after the trust model is applied

As shown in Table 2, the more Cloud Desktop instances running on a physical server, the more obvious the SVMIM performance advantage. As shown in Figure 6, the trust model proposed in this paper has high accuracy in the evaluation of static trust relationships, a high degree of fit between the simulated trustworthiness and the true trustworthiness relationship curve, and the trust measurement error remains at 10 %, and as the number of interactions gradually increases, the error percentage also decreases.

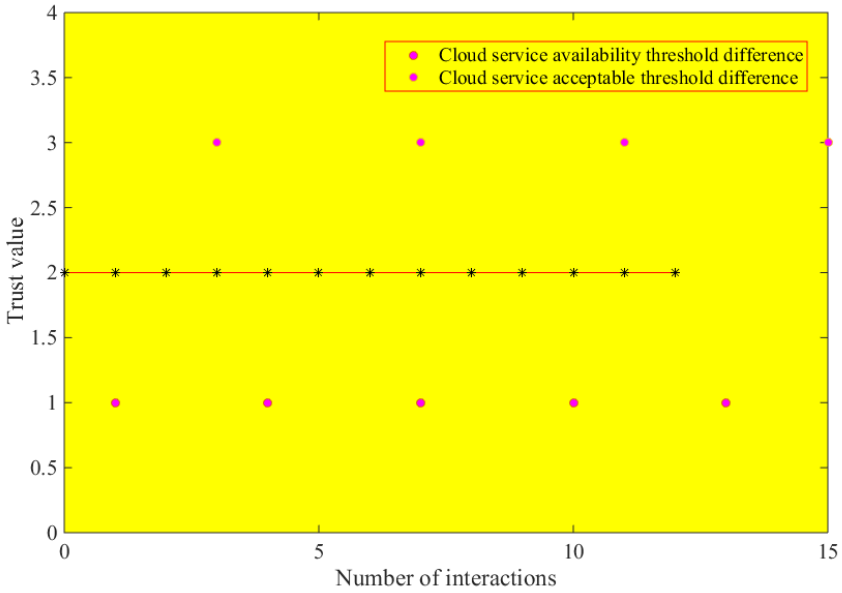

Figure 7. Difference graph of service availability change

As shown in Figure 7, those above the cloud user acceptable threshold difference are unacceptable by the entity, this service interaction evaluation is untrustworthy evaluation, and the others are credible evaluations. When the availability of cloud services changes, the entity's trust value with the cloud service provider is constantly changing. When the service availability change value is within the

acceptable range of the cloud user, the service provider's trust metric value also increases. When the service availability change value exceeds the acceptable range for the cloud user, the trust metric value of the service provider decreases, and the graph shows that the rate at which the trust value increases is less than the rate at which the trust value decreases. This is consistent with the change rule of communication trust in real life. Two types of entities are simulated. One is an entity with a higher initial trust value of trust = 0.8, and its trust value changes when the ratio of trusted services is 1.0, 0.33, and 0.1 respectively; the other is an initial trust value for entities with low trust = 0.5, their trust values change when their trusted service ratios are 1, 0.5, 0.25, and 0.1, respectively.

5. Conclusions

Trust research is a key issue in the field of cloud computing security. Due to the nature of trust and the commercial nature of cloud computing, cloud users and cloud service providers are constantly changing. To ensure the security of cloud center service resources, an appropriate trust management system needs to be provided, to establish a good trust relationship between cloud users and cloud service providers.

The main contributions of this paper: (1) Propose a trusted QoS evaluation model based on service awareness to solve the dynamic and security issues of service resources in cloud computing environment. In this trusted model, the interaction number of entities, the time distance and the exponential function are combined to design the attenuation function of the trust degree, the correlation ratio theory is introduced to calculate the similarity between the direct evaluation and the recommendation evaluation. Finally, we synthesize the trust degree of QoS feedback and measure the trust degree of entities. The validity of the trusted model was verified by Matlab tool simulation. (2) The trusted model proposed in this paper is applied to the service simulation module of cloud simulation platform CloudSim, and the CloudSim class is extended. By analyzing the simulation experiment results, it is easy to know that the simulation experiment results are consistent with the simulation results of Matlab tools, which verifies the reliability model is applied to the accuracy and dynamic adaptability of service resource scheduling.

The future work of this article is mainly as follows: (1) This article only analyzes and designs the application of "trust as a service". There is currently no actual cloud platform for development and implementation. And the security protocol involved in the module is just a simple verification protocol, and no novel security protocol is proposed for the cloud computing environment. The next step is the actual development of the cloud trust platform, including web page design and implementation, virtual machine configuration and scheduling, virtual machine and web data interaction control. (2) In the simulation experiments, we consider the VM as a service provider for trust measurement. In fact, each service provider has multiple areas of trust services. The trust value should be considered comprehensively. Next, we need to improve the experiment. With broker as a service provider, VM is a cloud service in different fields it provides. (3) This article focuses on the application of trust mechanism before service interaction, but does not consider the application of trust during service interaction. The next step will focus on the application of the trust mechanism in the service interaction process.

Abbreviations used in this paper

CPs (cloud providers)

SPI (Software Platform Infrastructure)

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Declarations

Availability of supporting data: We can provide the data.

Competing interests

These no potential competing interests in our paper. And all authors have seen the manuscript and approved to submit to your journal. We confirm that the content of the manuscript has not been published or submitted for publication elsewhere.

Funding

This research is supported by the National Social Science Foundation of China (Key Programs) (Grant No. 18AGL028)

Author's contributions

All the authors take part in the discussion of the work described in this paper, did the experiments of the paper and Lin Shi wrote the paper.

Acknowledgements

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

References

[1] Mark Ng. Examining social exchange among Chinese service workers: The mediating effect of trust in organization[J]. Asia-Pacific Journal of Business Administration, 2016, 8(2):163-176.

[2] Crocker, Joanna C, Boylan, Anne‐Marie, Bostock, Jennifer. Is it worth it? Patient and public views on the impact of their involvement in health research and its assessment: a UK‐based qualitative interview study[J]. Health Expectations, 2017, 20(3):519-528.

[3] Zhao, Na, Zhou, Mingjie, Shi, Yuanyuan. FACE ATTRACTIVENESS IN BUILDING TRUST: EVIDENCE FROM MEASUREMENT OF IMPLICIT AND EXPLICIT RESPONSES[J]. Social Behavior & Personality An International Journal, 2015, 43(5):855-866.

[4] Mark J. Rice, John L. Smith, Douglas B. Coursin. Glucose Measurement in the ICU: Regulatory Intersects Reality*[J]. Critical Care Medicine, 2017, 45(4):741-743.

[5] P Kelbich, A Hejčl, J Procházka. Comment on the study 'Cerebrospinal fluid lactate: measurement of an adult reference interval' by Sally D Slack, Paul Turley, Victoria Allgar and Ian B Holbrook[J]. Annals of Clinical Biochemistry, 2015, 53(Pt 1):180-181.

[6] Xiaoyong Li, Huadong Ma, Member. T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services[J]. IEEE Transactions on Information Forensics & Security, 2017, 10(7):1402-1415.

[7] MA Manfu, WANG Mei. Trust evaluation model based on service level agreement in cloud[J]. Journal of Computer Applications, 2015, 35(6):1567-1572.

[8] X.-C. Zhang, J.-T. Xi, J.-Q. Yan. Research on digital measurement technology based on point cloud data of complex surfaces[J]. Computer Integrated Manufacturing Systems, 2005, 11(5):727-731+737.

[9] Jing Xu, Guannan Si, Jufeng Yang. An Internetware dependable entity model and trust measurement based on evaluation[J]. Scientia Sinica, 2013, 43(1):108.

[10] Tobias Häberle, Lambros Charissis, Christoph Fehling. The Connected Car in the Cloud: A Platform for Prototyping Telematics Services[J]. IEEE Software, 2015, 32(6):11-17.

[11] Gustavo Gutiérrez-Carreón, Thanasis Daradoumis, Josep Jorba. Integrating Learning Services in the Cloud: An Approach that Benefits Both Systems and Learning[J]. Journal of Educational

Technology & Society, 2015, 18(1):145-157.
[12] Dalmazo, Bruno L, Vilela, João P, Curado, Marilia. Online traffic prediction in the cloud[J]. International Journal of Network Management, 2016, 26(4):269-285.
[13] Mohammad Al-Rubaie, J. Morris Chang. Reconstruction Attacks Against Mobile-Based Continuous Authentication Systems in the Cloud[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(12):1-1.
[14] Shanjiang Tang, Bu-Sung Lee, Bingsheng He. Fair Resource Allocation for Data-Intensive Computing in the Cloud[J]. IEEE Transactions on Services Computing, 2016, PP(99):1-1.
[15] Bushra AlBelooshi, Ernesto Damiani, Khaled Salah. Securing Cryptographic Keys in the Cloud: A Survey[J]. IEEE Cloud Computing, 2016, 3(4):42-56.
[16] Christian Esposito, Alfredo De Santis, Genny Tortora. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?[J]. IEEE Cloud Computing, 2018, 5(1):31-37.
[17] Jens Lansing, Ali Sunyaev. Trust in Cloud Computing: Conceptual Typology and Trust-Building Antecedents[J]. ACM SIGMIS Database, 2016, 47(2):58-96.
[18] K. Bi, Z. Niu, N. Zhao. Trust formation mechanism in cloud manufacturing environment based on incomplete information game theory[J]. Computer Integrated Manufacturing Systems, 2016, 22(1):95-103.
[19] D. Chandramohan, T. Vengattaraman, P. Dhavachelvan. A secure data privacy preservation for on-demand cloud service[J]. Journal of King Saud University, 2015, 29(2):144-150.
[20] Fuan Li, Lan Xu, Tiger Li. Brand trust in a cross-cultural context: Test for robustness of an alternative measurement model[J]. Journal of Product & Brand Management, 2015, 24(5):462-471.

Lin Shi, doctoral candidate, was born in Zhenjiang, Jiangsu, P.R. China, in 1982. He received the Master's Degree from University of Electronic Science and Technology, P.R. China. His research interest include computational intelligence, information security and big data analysis.
E-mail: shiling717@nuaa.edu.cn

Zilong Wang is a Professor at the Nanjing University of Aeronautics and Astronautics, from where he has also received his PhD. His research interest focuses on industrial economics and management, big data analysis. He has received several research funding from important Chinese research institutions as the National Natural Science Foundation of China and Aeronautics Science Foundation.
E-mail: wangzilong@nuaa.edu.cn

Ning Chen, Master of Engineering, was born in Nanjing, Jiangsu, P. R. China, in 1979. He received the Master`s Degree from Hohai University, P. R. China. His research interest include Information- Collection, Information -Security, Auto-Control.
E-mail: a.cnapt@gmail.com

Jie Chen was born in Changzhou, Jiangsu, P.R. China, in 1979. He received the Master`s Degree from Nanjing University, P.R. China. His research interest include computational intelligence, software design and application.
E-mail: seba@jscz.gov.cn

Figure

Figures

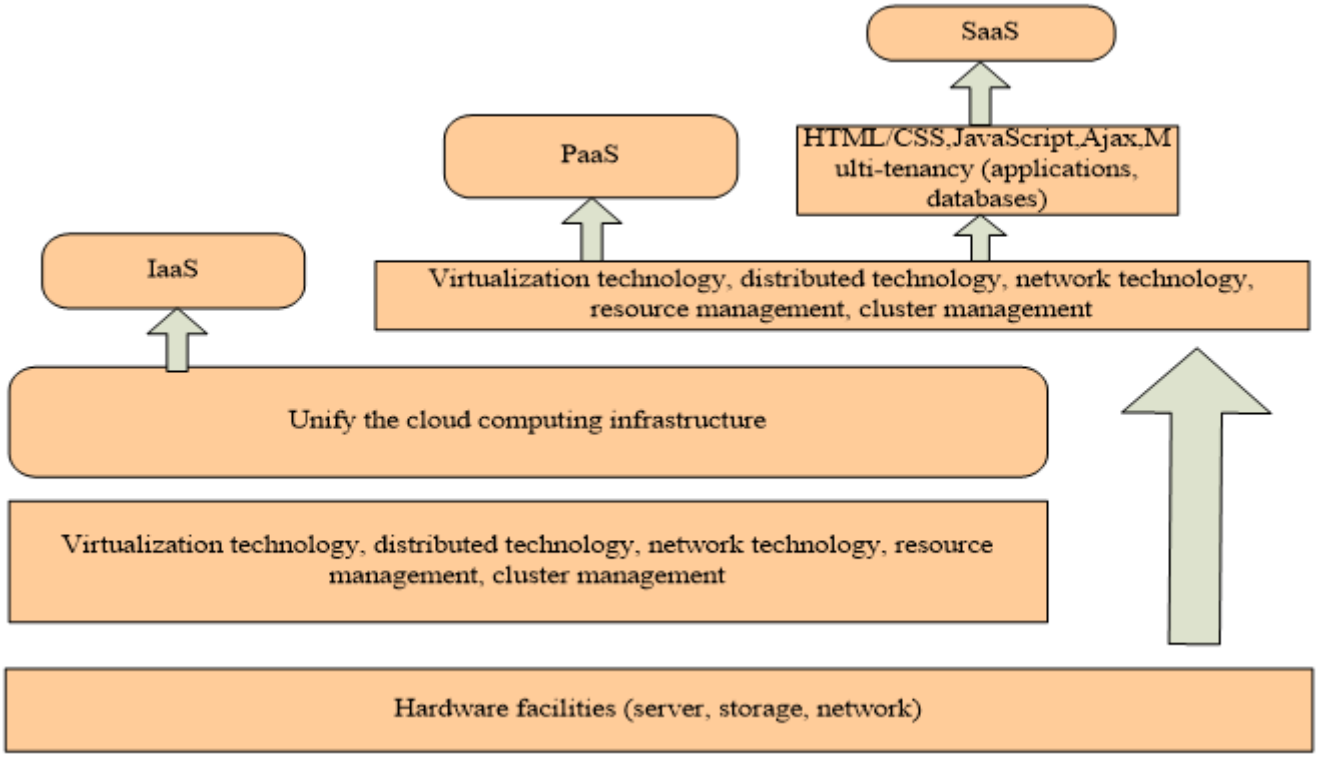

Figure 1

Cloud computing service framework

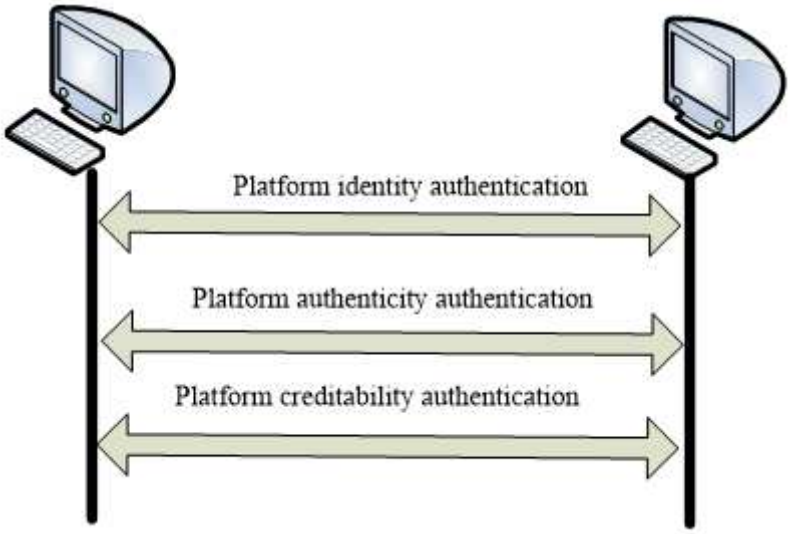

Figure 2

Trusted platform authentication flowchart

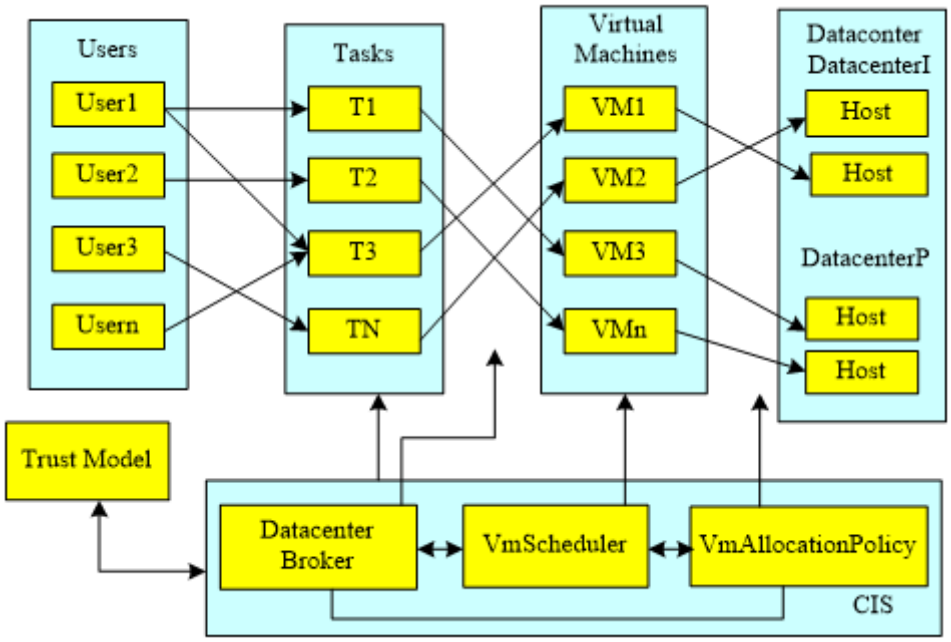

Figure 3

CloudSim resource scheduling simulation diagram

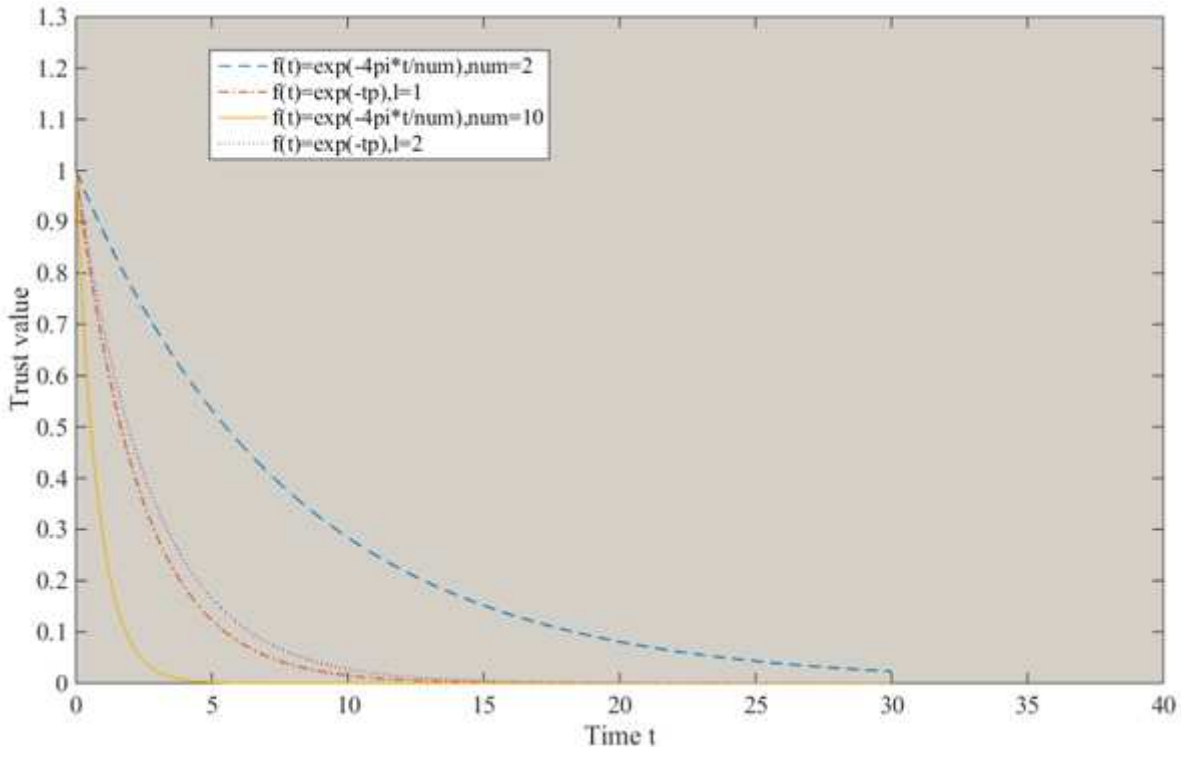

Figure 4

Trust value decay versus time

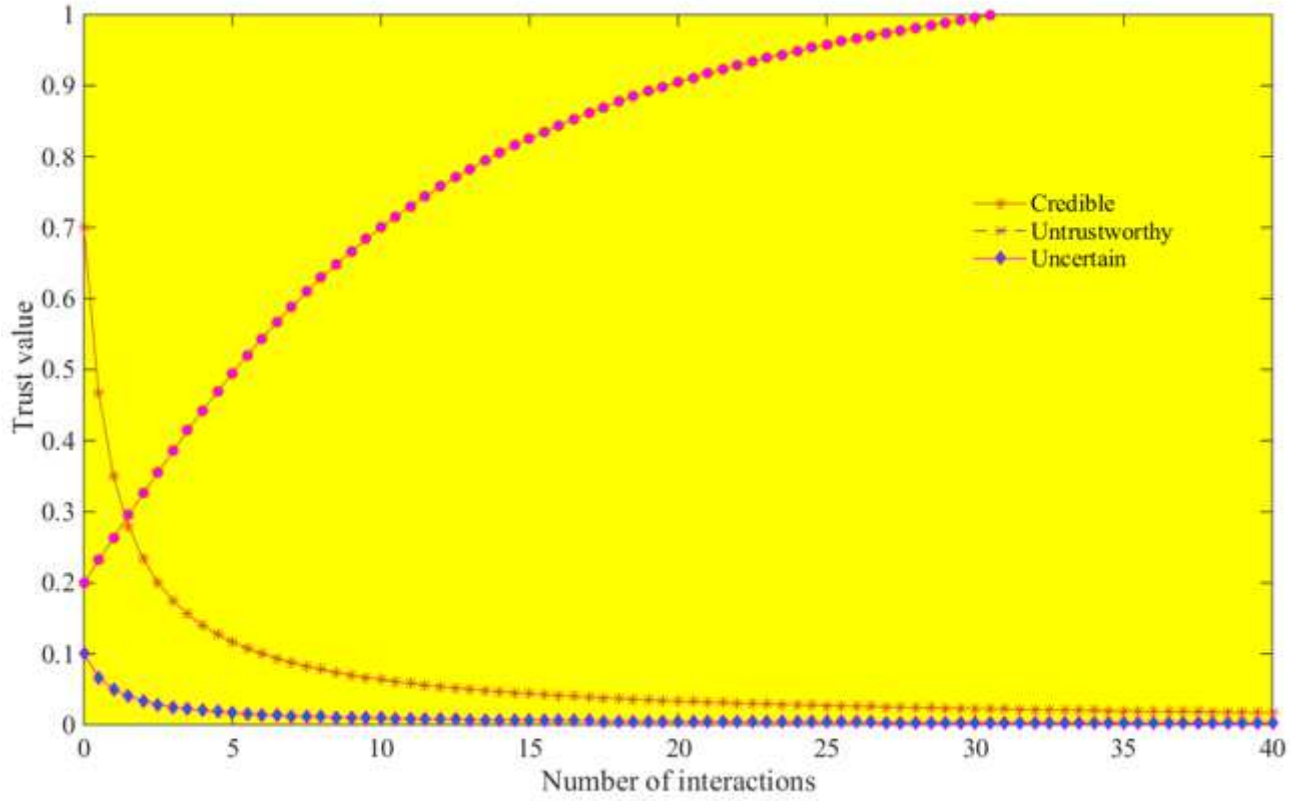

Figure 5

Relationship between trust change and time

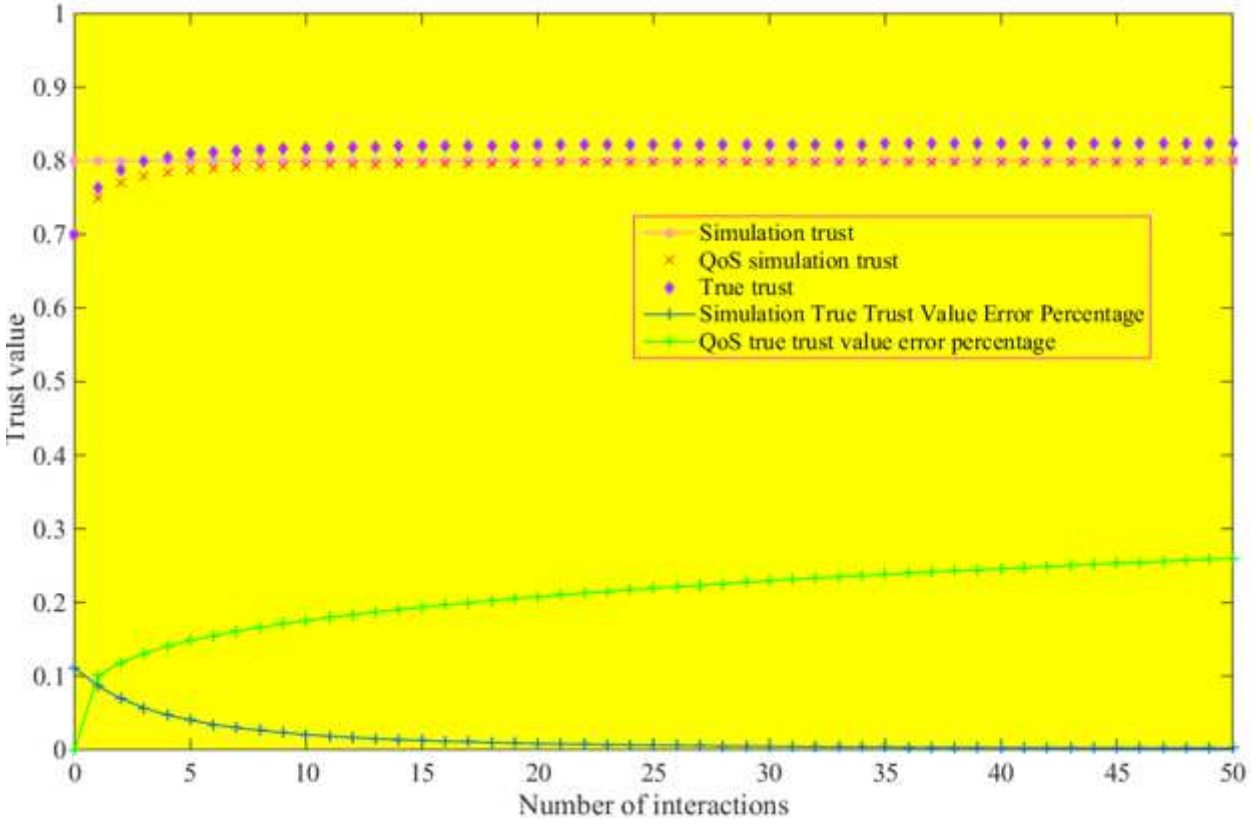

Figure 6

Static trust relationship diagram before and after the trust model is applied

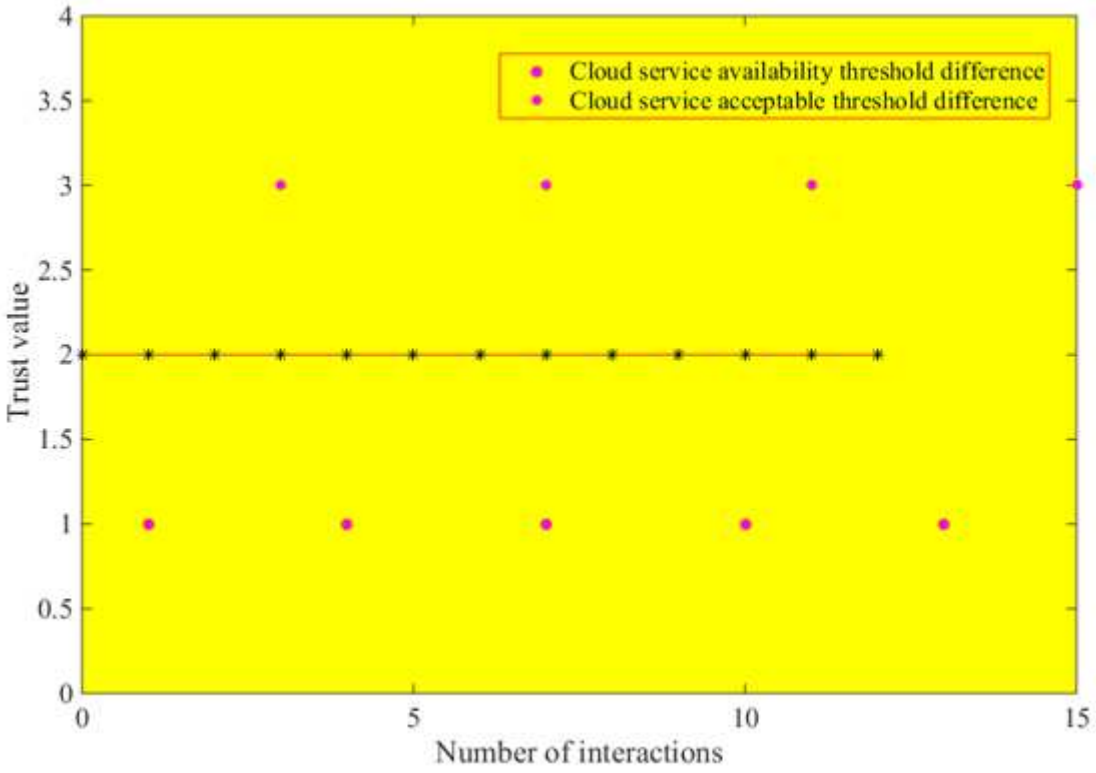

Figure 7

Difference graph of service availability change