Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2025 SCPE. Volume 26, Issues 2, pp. 641–650, DOI 10.12694/scpe.v26i2.3894

DESIGN OF SECURITY AND PRIVACY MODELS FOR OPTIMIZING THE SELECTION OF CLOUD SERVICE PROVIDERS IN CLOUD COMPUTING ENVIRONMENTS

FAN YANG*, FUQIANG TIAN†, HONGYU WU‡, JUN MOU§, SHILEI DONG¶, AND MAONAN LIN‖

Abstract. In order to solve the problem of difficult access to personalized and high-quality services for cloud users, the author proposes a security and privacy model for optimizing the selection of cloud service providers in the cloud computing environment. This model first divides user nodes into three types based on historical transactions between nodes: familial nodes, unfamiliar nodes, and ordinary nodes; Secondly, in order to protect the privacy information feedback from nodes, a trust evaluation agent is introduced as the subject of trust evaluation, and a trust value evaluation method based on user type is designed; Finally, considering the dynamic nature of trust, a new trust update mechanism based on service quality is proposed by combining transaction time and transaction amount. The experimental results show that compared with the AARep model and PeerTrust model, this model not only has advantages in scenarios with a lower proportion of malicious nodes, but also improves interaction success rates by 12% and 18%, respectively, in harsh scenarios where the proportion of malicious nodes exceeds 72%. This model overcomes the low success rate of interaction between user nodes and service nodes in cloud environments and has strong resistance to malicious behavior.

Key words: Trust model, Personalized cloud services, User type, Privacy protection, Service quality, Update mechanism

1. Introduction. Cloud computing represents the convergence of various computing and networking technologies like distributed computing, parallel computing, and virtualization, delivered over the internet to governments, businesses, and individuals. It offers three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models enable users to access IT resources and services remotely, facilitating tasks such as storage, computing power, and software applications without the need for on-site infrastructure [1].

Cloud computing is an emerging network computing model. Compared with traditional information technology, it has overwhelming advantages such as saving IT investment, fast and simple deployment, on-demand resource allocation, low usage costs, powerful computing power, and unlimited storage capacity. It has been strongly advocated and promoted by governments and enterprises around the world, bringing about significant changes in the computing and business fields. In order to quickly seize the high ground in the field of cloud computing and enhance enterprise competitiveness, global IT giants such as Amazon, Microsoft, Google, Alibaba, etc. are actively developing cloud computing platforms and have successively launched their own cloud computing products. The currently recognized cloud computing platforms include Amazon Simple Storage Service Platform (S3) and Elastic Computing Platform (EC2), Google's App Engine, IBM's Blue Cloud, Microsoft's Azure Cloud Platform, and Alibaba's Alibaba Cloud [2]. With the strong promotion of the government, the domestic cloud computing industry chain has gradually formed, and innovative achievements such as virtualization technology, distributed computing technology, big data processing and mining, and artificial intelligence have begun to be applied. Cloud applications in industries such as transportation and automotive cloud, logistics cloud, medical cloud, and financial e-commerce cloud are emerging and developing [3,4].

With the rapid development and popularization of cloud computing, more and more individual and enterprise users are considering outsourcing their private data to cloud service providers to enjoy affordable data

*Sichuan Zhongdian Oixing Information Technology Co., Ltd, Chengdu, Sichuan, 610000, China (Corresponding author, FanYang9@ 126.com)
†Sichuan Zhongdian Oixing Information Technology Co., Ltd, Chengdu, Sichuan, 610000, China (FuqiangTian5@163.com)
‡Sichuan Zhongdian Oixing Information Technology Co., Ltd, Chengdu, Sichuan, 610000, China (HongyuWu6@126.com)
§Sichuan Zhongdian Oixing Information Technology Co., Ltd, Chengdu, Sichuan, 610000, China (JunMou5@163.com)
¶Sichuan Zhongdian Oixing Information Technology Co., Ltd, Chengdu, Sichuan, 610000, China (ShileiDong9@126.com)
‖Sichuan Zhongdian Oixing Information Technology Co., Ltd, Chengdu, Sichuan, 610000, China (MaonanLin@163.com)

storage and computing services. However, the emergence and development of any new thing is a double-edged sword, and cloud computing is no exception. Compared to traditional information technology, it has enormous technological advantages and commercial potential, but also brings many new problems and challenges [5-6]. Among them, cloud security issues bear the brunt and have become the main factor restricting the further development and application promotion of cloud computing. According to a 2009 cloud computing survey report by Gartner, over 70% of businesses do not adopt cloud computing primarily due to concerns about data security and privacy. In a research report by Gartner and IDC, data security and privacy issues have been consistently listed as the top challenges in cloud computing technology [7,8]. This is because once user data is outsourced to a remote cloud service provider, the data will be detached from the direct physical control of the data user, and user data stored in the cloud will face a dual threat from the cloud service provider and external malicious attackers.

2. Literature Review. Cloud computing services are highly valued by companies for their myriad advantages. Nevertheless, safeguarding data privacy remains a paramount concern for users, as existing laws in this domain exhibit numerous inconsistencies that necessitate refinement. Alkhasawneh, A. et al. explored the legal framework governing privacy concerns in cloud computing, highlighting deficiencies and advocating for additional provisions to enhance consumer experiences, bolster service quality, and fortify personal data protection. The paper concluded with a set of recommendations directed towards both government entities and private companies, aiming to augment the accountability of cloud computing service providers in safeguarding personal data from privacy breaches[9]. Haipeng, S. et al. introduced a novel cross-domain identity authentication protocol with a focus on privacy protection. This protocol offers several key advantages, including a self-authentication key generation algorithm which allows mobile terminals to generate their own public/private key pairs, thus eliminating security vulnerabilities associated with third-party key distribution and custody. Additionally, cross-domain identity authentication is facilitated through blockchain technology, enabling the calculation of alliance keys between edge servers. The protocol ensures simplicity and efficiency in the cross-domain authentication process. Moreover, it ensures the revocability of identity authentication, ensuring that once a mobile terminal is logged out or exits the system, its legitimate identity immediately becomes invalid to uphold the security of system resources. The protocol's security has been demonstrated and its effectiveness verified under the assumptions of the discrete logarithm problem and the Diffie-Hellman problem[10]. Wang et al. introduced an innovative privacy protection approach grounded in K-anonymity principles. This method not only safeguards the query and location privacy of cloud users but also reconciles the tension between privacy protection and service quality. Through simulation experiments, the efficacy of this approach has been validated, affirming its ability to uphold user privacy while maintaining service standards[11]. YiDING et al. investigated a trusted privacy service computation model tailored for common application scenarios of convolutional neural networks. They delved into data and model computation techniques that leverage homomorphic encryption to safeguard data privacy. Additionally, they devised a method for service certificate storage and rights allocation computation utilizing blockchain and smart contract technology, ensuring the transparency, reliability, and traceability of service computation. This research also pioneered a novel cloud environment resource and data service model, facilitating the seamless integration of resources and fostering a sharing economy among resource providers, model owners, and users. Finally, they conducted experimental analyses to scrutinize the efficacy of the privacy protection methods integrated into the model [12].

The author proposes a Trust Model based on User Types and Privacy Preservation for the Personalized Cloud Services (P3Trust) for personalized cloud services. This model first transforms the subject of trust evaluation from selfish user nodes to objective and fair trust evaluation agents. The trust evaluation process is transparent to user nodes and service nodes, and user nodes will not be able to obtain sensitive historical information. It also improves the security of entity privacy information such as identity, interests, and evaluations on the transmission channel, effectively suppressing malicious behaviors such as collusion fraud and malicious recommendations, making the results of trust evaluation more realistic; Secondly, an efficient trust value evaluation method based on user types is proposed. This method divides users into three types based on historical transactions between user nodes and service nodes: familial users, unfamiliar users, and ordinary users. Different trust value calculation methods are used for different user types, which not only improves the efficiency of trust evaluation, but also reasonably solves the initialization problem of trust relationships between new user

Table 3.1: Trust Relationship Table

User	Historical comprehensive trust value	Last transaction interest	Last transaction review	Last transaction request time
u_1	T_{1j}	Q_{1j}	$E(Q_{1j})$	$(t_{11}^{(1)}, \cdots, t_{1n}^{(1)})$
u_2	T_{2j}	Q_{2j}	$E(Q_{2j})$	$(t_{21}^{(1)}, \cdots, t_{2n}^{(1)})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
u_k	T_{kj}	Q_{kj}	$E(Q_{kj})$	$(t_{k1}^{(1)}, \cdots, t_{kn}^{(1)})$

nodes and service nodes; Finally, a trust update mechanism based on service quality is proposed, taking into account the transaction time and amount between user nodes and service nodes. The experimental findings indicate that the trust evaluation outcomes of P3Trust accurately, impartially, and authentically portray the trust dynamics between user nodes and service nodes. Moreover, these results underscore the robustness of P3Trust even in challenging environments, highlighting its reliability and effectiveness.

3. Research Methods.

3.1. Trust Relationship. Trust relationship fundamentally relies on the subjective endorsement of one entity by another, encompassing subjective, ambiguous, and uncertain traits that resist precise measurement. Currently, trust lacks a standardized definition, with trust value serving as the sole quantitative metric for assessing the trust dynamics between user nodes and service nodes.

3.2. Definition and representation of models.

Definition 1: User node. The individuals who make service requests in the system and the processes representing them are represented by U, which represents the set of all user nodes. $u_i(u_i \in U)$represents the i-th user node.

Definition 2: Service nodes. The individuals and representative processes that provide services to user nodes in the system, represented by O as the set of all service nodes, and $o_j(o_j \in O)$as the j-th service node.

Definition 3: Trust evaluation agents. Individuals deployed by cloud computing authorities who can fairly and objectively evaluate the trust level of U in O on behalf of user nodes, represented by A as the trust evaluation agent in the cloud environment.

Definition 4: Personalized services. Services that reflect the U feature and are of interest, or services that reflect the O feature and are good at, are represented by Q_{ij} as the personalized service vector for the last request of o_j by u_i, and $E(Q_{ij})$ as the evaluation vector for the personalized service Q_{ij} by ui[13,14].

Definition 5: Trust Relationship Tables (TRTs). The trust information table saved by the trust evaluation agent records the historical interaction information between U and O, and its structure is shown in Table 3.1.

Definition 6: Historical related direct trust. The current direct evaluation of U on O based on the direct interaction experience between U and O history is quantitatively represented by historical related direct trust values.

Definition 7: Historical related indirect trust. The current indirect evaluation of U on O based on the similarity between U and the reference node is quantitatively represented by historical related indirect trust values [15].

Definition 8: Comprehensive trust related to history. The overall evaluation of U on O is obtained by combining the direct evaluation of U on O and the indirect evaluation of U on O, and is quantitatively represented by historical related comprehensive trust values.

3.3. Trust Model Design. The design concept of a trust model for personalized cloud services based on user type and privacy protection is that the trust evaluation agent is the main body of trust evaluation, and the trust evaluation agent adopts corresponding trust value evaluation methods based on user type to dynamically obtain the degree of trust of user nodes in service nodes. The goal of this model is to enhance the accuracy of trust assessment while protecting the privacy of user nodes, and help them obtain high-quality services to improve resource utilization. Based on the historical transactions between user nodes and service nodes, the

Table 3.2: Classification of User Nodes and Their Trust Value Evaluation Methods

Customer type	Is there a historical transaction record	$\geqslant T_b$	$\leqslant t_b$	Service Node O
Family nodes	Yes	Yes	Yes	$O = \{o \mid T_o^{(n)} = \max_{j=1}^{n}(T_{oj}^{(n)})\}$
Unknown node	No			$O = \{o \mid T_o^{(n)} = \max_{j=1}^{n}(R_{(N\_user,o_j)}^{(o\_user)})\}$
Ordinary node	Yes	No	Yes	$O = \{o \mid T_o^{(n)} = \max_{j=1}^{n}(T \oplus R_{(o_j)})\}$
	Yes	Yes	No	
	Yes	No	No	

trust evaluation agent defines user nodes as familial nodes, unfamiliar nodes, and ordinary nodes, and the trust value evaluation method for each type of node is different, as shown in Table 3.2.

Definition 9: Family nodes. User nodes in the system who have had historical transactions with service nodes, and whose historical comprehensive trust value is greater than the minimum trust value Tb acceptable to the user node, and whose transaction time interval does not exceed the time threshold tb. The trust evaluation method between family nodes and service nodes is shown in section 3.3.1.

Define 10: Unfamiliar nodes. The user node that requests service for the first time has no historical transactions with the service node, that is, a new user node. The trust evaluation method between unfamiliar nodes and service nodes is shown in section 3.3.2.

Definition 11: Ordinary nodes. All user nodes in the system, except for familial and unfamiliar nodes. The trust value evaluation method between ordinary nodes and service nodes is shown in section 3.3.3.

3.3.1. Trust evaluation of family nodes on service nodes. If the user node is a family node and its transaction interval is within the time threshold range of ($|t_n^{(1)} - t_{(n-1)}^{(1)}| \leqslant t_b$) , it indicates that the user node has requested a transaction again in a short period of time. Generally, the user node's interests (that is personalized needs) will not change significantly; Secondly, when the historical transaction trust value of a user node is not less than its minimum acceptable trust value ($T_{so_j}^{(n-1)} \geqslant T_b$), it indicates that the transaction record has high reference value. Therefore, the trust evaluation agent selects the appropriate service node for the family node among the service nodes it has traded with. Trust has a time-dependent characteristic, which is reflected in the fact that family nodes are more willing to trust recent transaction records. Therefore, the author introduces a time decay function and defines it as follows 3.1:

$$S^{(n)} = \frac{t_n^{(1)} - t_{n-1}^{(1)}}{\sum_{j=1}^{k}(t_j^{(1)} - t_{j-1}^{(1)})} \tag{3.1}$$

where $t_i^{(1)}$ represents the i-th transaction request time; The larger the $S^{(n)}$, the longer the time interval between the last transaction between the family node and the service node and the current transaction.

Using $\lim_{x \to -\infty} e^x = 0$, define the time decay factor $\Delta t^{(n)} = e^{-S(n)}$ to measure the freshness of transactions.

Based on the comprehensive time related characteristics, the trust evaluation agent calculates the historical related direct trust value $\widehat{T}_{so_j}^{(n)}$ based on historical transaction records, which is defined as the following equation 3.2:

$$\widehat{T}_{so_j}^{(n)} = T_{so_j}^{(n-1)} * \Delta t^{(n-1)} \tag{3.2}$$

Among them: $\widehat{T}_{so_j}^{(n-1)}$ represents the comprehensive trust value of the previous transaction, $\Delta t^{(n-1)}$ is the time decay factor, and $\widehat{T}_{so_j}^{(n-1)}$represents the reference value of historical transactions for this transaction. According to equation 3.2, the trust evaluation agent calculates the historical related direct trust values between the family node and the service node that has been traded, as shown in Table 3.2. The maximum $\widehat{T}_o^{(n)}$ is selected as the basis for this transaction of the family node. In theory, this trust value evaluation method can improve the efficiency and accuracy of trust value evaluation.

3.3.2. Trust evaluation of service nodes by unfamiliar nodes . One of the hotspots in trust research is how to initialize the trust relationship between unfamiliar nodes (new users) and service nodes in a cloud environment. In social networks, there is a saying that "different paths do not conspire", which is reflected in the following two aspects in cloud environments:

1) Strange nodes are more willing to refer to the historical transaction records of nodes with similar interests;

2) Strange nodes are more willing to refer to the historical transaction records of nodes with similar evaluations. Indirect trust relationship is the basis for trust evaluation agents to help unfamiliar nodes determine service nodes by referring to the historical transactions of other nodes when they have insufficient understanding of the service node.

The author proposes an indirect trust value evaluation method based on interest similarity and evaluation similarity to initialize the trust relationship between unfamiliar nodes and service nodes.

1) Interest similarity. In social networks, when unfamiliar nodes request personalized services, they are more willing to refer to the historical transaction records of nodes with similar interests. Therefore, the similarity of interests between unfamiliar nodes and reference nodes is an important influencing factor in indirect trust evaluation. Interest similarity refers to the degree of similarity between personalized demand vectors of any two nodes. Let $Q(N\_user) = (n\_q_1, n\_q_2, \cdots, n\_q_n), Q(O\_user) = (o\_q_1, o\_q_2, \cdots, o\_q_n)$ be the personalized demand vectors for the unfamiliar node N_user and the reference node O_user, and use the cosine similarity between Q(N_user) and Q(O_user) to represent the interest similarity between N_user and Q_user (3):

$$P\_Sim^{(Q)}_{(O\_user)}(O\_user) = \frac{Q(N\_user) \cdot Q(O\_user)}{|Q(N\_user)| * |Q(O\_user)|} \tag{3.3}$$

2) Evaluate similarity. Similarly, when a stranger node requests personalized services, in addition to considering nodes with similar interests, they are also willing to refer to the historical transaction records of nodes with similar evaluations. Therefore, the evaluation similarity between the stranger node and the reference node is another important influencing factor in indirect trust evaluation.

Evaluation similarity refers to the degree of consistency between any two nodes in evaluating the same behavior. Let $S' = \{S'_1, S'_2, \cdots, S'_n\}$ be the public service provided by the trust evaluation agent, and the evaluation vectors for N_user,O_user.and S' after interaction are $E^{(s')}(Q(N\_user)) = (e(n\_q_1), e(n\_q_2), \cdots, e(n\_q_n))$, $E^{(s')}(Q(O\_user)) = (e(o\_q_1), e(o\_q_2), \cdots, e(o\_q_n))$.

Trust relationships originate from social networks, which have subjective characteristics, uncertainty, and fuzziness. The essence of the above characteristics of trust relationships is their gray nature. Therefore, the gray correlation coefficient between $E^{(S')}(Q(N\_user))$ and $E^{(S')}(Q(O\_user))$ is used to define the evaluation similarity between N_user and Q_user 3.4.

$$E\_Sim^{(Q)}_{(N\_user)}(O\_use) = \frac{\Delta_{min} + \rho\Delta_{max}}{\Delta + \rho\Delta_{max}} \tag{3.4}$$

Among them: ρ for the resolution coefficient, it is usually taken as 0.5; Δ_{Min}, Δ_{Max}, Δ is the minimum difference, maximum value, and absolute difference between the two poles of $E^{(S')}(Q(N\_user))$ and $E^{(S')}(Q(O\_user))$

3) The synthesis of historical related indirect trust values. In order to initialize the trust relationship between unfamiliar nodes and service nodes, an indirect trust value evaluation method is proposed. The trust evaluation agent combines the interest similarity $P\_Sim^{(Q)}_{(O\_user)}(N\_user)$ and evaluation similarity $E\_Sim^{(Q)}_{(O\_user)}(N\_user)$ of N_user and O_user, as well as the historical comprehensive trust value $T^{(n-1)}_{(O\_user)}$ of O_user. According to equation 3.5, the historical related indirect trust value $\widehat{R}^{(O_1 user_j)}_{(N\_user,O_i)}$ of O_user and each service node is calculated, as shown in equation 3.5:

$$\widehat{R}^{(O_1 user_j)}_{(N\_user,O_i)} = P_{Sim^{(Q)}}{}_{(O\_user)}(N\_user) * T^{(n-1)}_{(O_{user})} * E_{Sim^{(Q)}}{}_{(O\_user)}(N\_user) * \Delta t^{(n-1)} \tag{3.5}$$

As shown in Table 3.2, the trust evaluation agent selects the $T^{(n)}_O$ with the highest historical indirect trust value as the basis for the initial transaction of the unfamiliar node, and feeds back the service node

information to the user node. The trust evaluation method proposed by the author for unfamiliar nodes and service nodes provides a solution to the problem of initializing the trust relationship of new user nodes, with high accuracy [16].

3.3.3. Trust evaluation between ordinary nodes and service nodes . For ordinary nodes, they are not unfamiliar nodes, but their historical transaction records do not meet the requirements of family nodes. Therefore, they not only have their own historical transaction records, but also refer to the historical transaction records of other nodes to evaluate trust relationships. Therefore, trust evaluation agents cannot only evaluate the trust relationship between them and service nodes based on $\widehat{T}_{(o_j)}^{(n)}$ or $\widehat{R}_{(user,o_j)}^{(other\_users)}$. On the basis of the previous text, the author proposes a historical related comprehensive trust value evaluation method to evaluate the trust relationship between ordinary nodes and service nodes, and defines the historical related comprehensive trust value according to equation 3.6.

$$\widehat{T} \oplus \widehat{R}_{(o_j)} = \alpha \widehat{T}_{(o_j)}^{(n)} + (1-\alpha)\widehat{R}_{(user,o_j)}^{(other\_users)} \tag{3.6}$$

Among them: α is a historical related direct trust factor; $\widehat{T}_{(o_j)}^{(n)}$ is the historical related direct trust value; $\widehat{R}_{(user,o_j)}^{(other\_users)}$ is the indirect trust value related to history. Finally, as shown in Table 3.2, the trust evaluation agent selects the largest $\widehat{T}_{O}^{(n)}$ as the basis for this transaction of the ordinary node.

3.4. Trust Update Mechanism Based on Service Quality. Given the dynamic nature of trust in cloud computing environments, the trust relationship between any two nodes is not static. Therefore, after the transaction between the user node and the service node is completed, it is necessary to update the trust relationship between the user node and the service node in a timely manner [17]. The author proposes a new Quality of Service based Trust Updating Mechanism (QoS UM). The steps of QoS UM are: After the user node completes the transaction with the service node, the user node pays the fee to the service node and provides feedback on the service evaluation. The trust value update mechanism is activated, and the trust evaluation agent updates the TRT based on the user node's satisfaction with the transaction. Firstly, the evaluation of the service by the user node is the most important reference factor for trust updates. Therefore, the trust evaluation agent defines the satisfaction $N^{(Q)}$ of the user node with this transaction based on the Q and E(Q) of the user node according to equation 3.7, as follows:

$$N^{(Q)} = Q * E(Q)^T \tag{3.7}$$

Secondly, the transaction volume between user nodes and service nodes can reflect the quality of service provided by the service node. Therefore, the transaction volume between user nodes and service nodes is one of the important factors for trust updates. The transaction volume related factor $M^{(n)}$ is defined according to equation 3.8:

$$M^{(n)} = \frac{(M_n)^{\omega}}{\sum_{j=1}^{p}(M_j)^{\omega}} \tag{3.8}$$

Among them: ω represents the adjustment factor for transaction volume, taking values based on actual circumstances; M_j represents the j-th transaction amount between the user node and the service node.

Finally, user nodes are more willing to trade with service nodes that can cooperate stably in the long term. If the transaction time between user nodes and service nodes is longer, it reflects that the service node can provide high-quality services. Therefore, the transaction time between user nodes and service nodes is another important reference factor for trust updates. The transaction time related factor $I^{(n)}$ is defined according to equation 3.9:

$$I^{(n)} = \frac{(t_n^{(2)} - t_n^{(1)})^k}{\sum_{j=1}^{n}(t_j^{(2)} - t_j^{(1)})^k} \tag{3.9}$$

Among them: κ Represents the adjustment factor for trading time, taking values based on actual circumstances; $t_i^{(1)}$ represents the request time for the i-th transaction; $t_i^{(2)}$ represents the end time of the i-th transaction.

Table 4.1: Experimental Parameter Settings

Parameter	Parameter values	Parameter	Parameter values
Number of service nodes	100	α	0.5
Number of user nodes	50	T_b	0.3
Types of interests	3	τ	0.5
ψ	0.5	t_b	0.003
ω	2	κ	2

The trust evaluation agent obtains the service quality NMI_{so_j} of this transaction by integrating the satisfaction $N^{(Q)}$, transaction volume related factor $M^{(n)}$, and transaction time related factor $I^{(n)}$ of this transaction, which is defined as the following equation 3.10:

$$NMI_{so_j} = N^{(Q)} * M^{(n)} * I^{(n)} \tag{3.10}$$

The trust evaluation agent integrates historical transaction records and the service quality of this transaction, and updates the trust relationship according to equation 3.11. The following equation 3.11:

$$T_{so_j}^{(n)} = \psi * \widehat{T}_{so_j}^{(n)} + (1 - \psi) * NMI_{(so_j)} \tag{3.11}$$

Among them: ψ represents the weight of historical transaction records, taking values based on actual circumstances.

4. Result analysis. This section verifies the effectiveness and correctness of P3Trust through simulation experiments. As a reference, both the PeerTrust model and AARep model were implemented simultaneously [18].

4.1. Experimental Environment. The simulation experiments were conducted on a hardware setup consisting of an Intel Core2 Quad processor clocked at 2.83 GHz with 2.00 GB of RAM. The software environment utilized for the simulation experiments comprised Windows XP operating system and the Matlab 7.1 simulation platform. The experimental scenario is file download service, personalized service attribute vector: Download service=[file quality response time download speed], user interest vector: Interest vector=[0.5 0.2 0.3]. The evaluation index is the transaction success rate between user nodes and service nodes η. define it as the following equation 4.1.

$$\eta = N_{(T_{so} \geqslant \tau)} / \sum N \tag{4.1}$$

Among them: τ is the minimum acceptable comprehensive trust value; $N_{(T_{SO} \geqslant \tau)}$ represents a trust value that exceeds the minimum acceptable comprehensive trust value τ total number of times; $\sum N$ represents the total number of transactions.

In real situations, there are many types of service nodes, and this experiment sets the following two types of service nodes:

1. General node: This type of service node can provide high-quality services based on the corresponding services registered in the trust evaluation center.
2. Malicious nodes: The services provided by these service nodes do not match the service information registered in the trust evaluation center [19].

The experimental parameter settings are shown in Table 4.1.

This experiment sets the following three types of user node transaction situations:

1. 40% of transactions are related to family nodes;
2. 20% of transactions are first-time transactions, that is transactions with unfamiliar nodes;
3. 40% of transactions are ordinary node transactions.

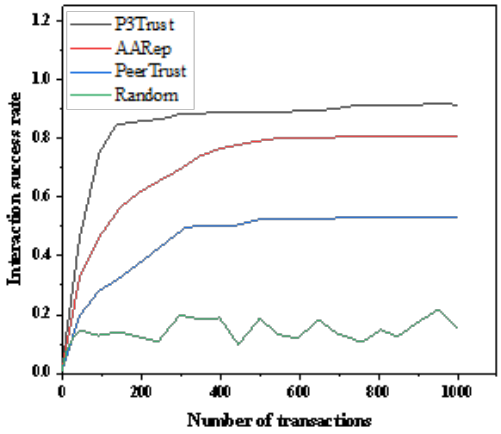

Fig. 4.1: Comparison of interaction success rates under 30% malicious nodes

During each simulation cycle, user nodes make personalized requests to the trust evaluation agent to download resources they have never owned. The trust evaluation agent first searches for TRT and determines the type of user node; Then, corresponding trust evaluation methods are used to evaluate the trust relationship between user nodes and service nodes, and suitable service nodes are selected for user nodes; Finally, after the transaction is completed, the user node evaluates the service and feeds it back to the trust evaluation agent. The trust evaluation agent updates the trust relationship based on QoS UM and saves it in the TRT.

4.2. Experimental Results.

4.2.1. Efficiency and accuracy of P3Trust trust assessment . This section examines the efficiency and accuracy of trust assessment in P3Trust, and compares it with the PeerTrust model, AARep model, and random selection model [20]. In scenarios where the proportion of malicious service nodes is 30% and 70%, the curves of the interaction success rate obtained through P3Trust model, PeerTrust model, AARep model, and Random model with respect to the number of transactions are shown in Figure 4.1 and Figure 4.2, respectively.

As shown in Figure 4.1, in the interaction scenario of 30% malicious service nodes, except for the Random model which is irregular, the other three models can all lead to an increase in interaction success rate. When trading around 600 times, the interaction success rate of the PeerTrust model can remain stable at around 0.5, the interaction success rate of the AARep model can remain stable at 0.7-0.8, and the P3Trust model can remain stable at around 0.9 after trading around 200 times. This is because P3Trust provides a reasonable trust value initialization method. In the harsh scenario of 70% malicious service nodes, the P3Trust model still has a higher interaction success rate than the other three models, as shown in Figure 2. Therefore, P3Trust can improve the accuracy of trust assessment while improving the efficiency of trust assessment [21].

4.2.2. Robustness of P^3 Trust. This section examines the ability of P3Trust to withstand harsh environments and analyzes its differences in resistance to harsh environments compared to the PeerTrust model, AARep model, and Random model. The curves of the success rate of interaction with the proportion of malicious nodes after 2000 transactions for P3Trust model, PeerTrust model, AARep model, and Random model are shown in Figure 4.3.

From Figure 4.3, it can be seen that as the proportion of malicious nodes increases, the interaction success rate of the other three trust models decreases continuously, except for the random model which is irregular. P^3 Trust can achieve an interaction success rate of around 0.8 in a good environment with a malicious node proportion of about 20%, and in a harsh environment with a malicious node proportion of about 72%, P^3 Trust maintains an average transaction success rate that is 12% and 18% higher than AARep and PeerTrust [22].

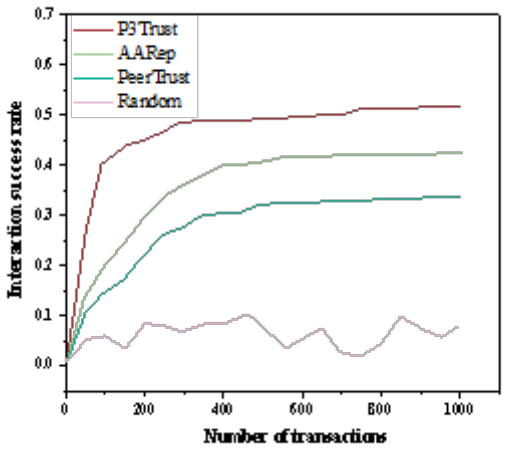

Fig. 4.2: Comparison of interaction success rates under 70% malicious nodes

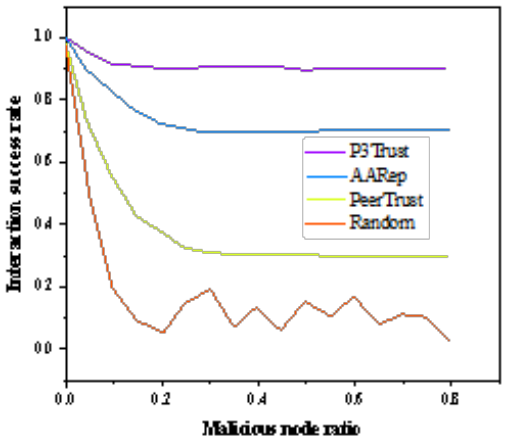

Fig. 4.3: Comparison of interaction success rates under different malicious nodes

Respectively, the reason is that the subject of trust evaluation in the P3Trust model is a fair and objective trust evaluation agent, and an efficient trust value evaluation method has been proposed. Therefore, the P3Trust model has strong resistance to harsh environments.

5. Conclusion. Through the discussion of existing trust models in cloud environments, the author proposes a trust model for personalized cloud services based on user types and privacy protection - P3Trust. The model first classifies user nodes based on historical transactions between nodes; Secondly, in order to improve the efficiency and accuracy of trust evaluation, a trust evaluation agent was introduced as the main body of trust evaluation to protect the privacy information feedback from nodes, and a trust value evaluation method based on user type was proposed; In addition, in order to reflect the dynamism of trust and improve the integrity of trust models, fully considering the transaction time and transaction amount of cloud services, the

author proposes a trust update mechanism based on service quality. The simulation results show that compared with existing trust models, P3Trust has significant improvements in the effectiveness and robustness of curbing malicious behavior, and improves the accuracy of trust evaluation.

REFERENCES

[1] Tricomi, G., Merlino, G., Panarello, A., & Puliafito, A. (2020). Optimal selection techniques for Cloud service providers. IEEE Access, 8, 203591-203618.
[2] Mohamed, A. M., & Abdelsalam, H. M. (2020). A multicriteria optimization model for cloud service provider selection in multicloud environments. Software: Practice and Experience, 50(6), 925-947.
[3] Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2022). Privacy-aware cloud service composition based on QoS optimization in Internet of Things. Journal of Ambient Intelligence and Humanized Computing, 13(11), 5295-5320.
[4] Rahimi, M., Jafari Navimipour, N., Hosseinzadeh, M., Moattar, M. H., & Darwesh, A. (2022). Toward the efficient service selection approaches in cloud computing. Kybernetes, 51(4), 1388-1412.
[5] Gupta, I., Gupta, R., Singh, A. K., & Buyya, R. (2020). MLPAM: A machine learning and probabilistic analysis based model for preserving security and privacy in cloud environment. IEEE Systems Journal, 15(3), 4248-4259.
[6] Kumar, R. R., Kumari, B., & Kumar, C. (2021). CCS-OSSR: a framework based on hybrid MCDM for optimal service selection and ranking of cloud computing services. Cluster Computing, 24(2), 867-883.
[7] Reddy, M. I., Rao, P. V., Kumar, T. S., & K, S. R. (2024). Encryption with access policy and cloud data selection for secure and energy-efficient cloud computing. Multimedia Tools and Applications, 83(6), 15649-15675.
[8] Ermakova, T., Fabian, B., Kornacka, M., Thiebes, S., & Sunyaev, A. (2020). Security and privacy requirements for cloud computing in healthcare: Elicitation and prioritization from a patient perspective. ACM Transactions on Management Information Systems (TMIS), 11(2), 1-29.
[9] Alkhasawneh, A. , & Khasawneh, F. . (2023). Legal issues of consumer privacy protection in the cloud computing environment: analytic study in gdpr, and usa legislations. Int. J. Cloud Comput., 12, 40-62.
[10] Haipeng, S. , Yu'An, T. , Congwu, L. I. , Lei, L. , Qikun, Z. , & Jingjing, H. U. . (2022). An edge-cloud collaborative cross-domain identity-based authentication protocol with privacy protection. Chinese Journal of Electronics, 2021, 1-11.
[11] Wang, T. , Xu, L. , Zhang, M. , Zhang, H. , & Zhang, G. . (2022). A new privacy protection approach based on k-anonymity for location-based cloud services. Journal of Circuits, Systems and Computers, 31(05), 2343-2358.
[12] YiDING, WeiSHEN, Hai-shengLI, Qiong-huiZHONG, Ming-yuTIAN, & JieLI. (2022). Blockchain trusted privacy service computing model for cnn. Acta Electronica Sinica, 50(06), 1399-1409.
[13] Nezafat Tabalvandani, M. A., Hosseini Shirvani, M., & Motameni, H. (2024). Reliability-aware web service composition with cost minimization perspective: a multi-objective particle swarm optimization model in multi-cloud scenarios. Soft Computing, 28(6), 5173-5196.
[14] Wu, Q., He, K., & Chen, X. (2020). Personalized federated learning for intelligent IoT applications: A cloud-edge based framework. IEEE Open Journal of the Computer Society, 1, 35-44.
[15] Wu, Q., Chen, X., Zhou, Z., & Zhang, J. (2020). Fedhome: Cloud-edge based personalized federated learning for in-home health monitoring. IEEE Transactions on Mobile Computing, 21(8), 2818-2832.
[16] Kashevnik, A., Lashkov, I., Ponomarev, A., Teslya, N., & Gurtov, A. (2020). Cloud-based driver monitoring system using a smartphone. IEEE Sensors Journal, 20(12), 6701-6715.
[17] Gill, S. H., Razzaq, M. A., Ahmad, M., Almansour, F. M., Haq, I. U., Jhanjhi, N. Z., ... & Masud, M. (2022). Security and privacy aspects of cloud computing: a smart campus case study. Intelligent Automation & Soft Computing, 31(1), 117-128.
[18] Gill, S. H., Razzaq, M. A., Ahmad, M., Almansour, F. M., Haq, I. U., Jhanjhi, N. Z., ... & Masud, M. (2022). Security and privacy aspects of cloud computing: a smart campus case study. Intelligent Automation & Soft Computing, 31(1), 117-128.
[19] Murthy, C. V. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain based cloud computing: Architecture and research challenges. IEEE access, 8, 205190-205205.
[20] Wang, J., Yan, Z., Wang, H., Li, T., & Pedrycz, W. (2022). A survey on trust models in heterogeneous networks. IEEE Communications Surveys & Tutorials, 24(4), 2127-2162.
[21] Papenmeier, A., Kern, D., Englebienne, G., & Seifert, C. (2022). It's complicated: The relationship between user trust, model accuracy and explanations in ai. ACM Transactions on Computer-Human Interaction (TOCHI), 29(4), 1-33.
[22] Ramu, N., Pandi, V., Lazarus, J. D., & Radhakrishnan, S. (2020). A novel trust model for secure group communication in distributed computing. Journal of Organizational and End User Computing (JOEUC), 32(3), 1-14.

Edited by: Bradha Madhavan
Special issue on: High-performance Computing Algorithms for Material Sciences
Received: Nay 10, 2024
Accepted: Jun 25, 2024