

The Study on the Reliable Cloud Computing Safety Strategy Based on the Cloud Computing Environment

Zhao Li^{1, a*}

¹School of computer science, Wuhan Donghu University, Wuhan, HuBei, 430212 China

^a6115480@qq.com

Keywords: Cloud computing; data safety; network safety strategy

Abstract. “Cloud computing” provides the brand-new calculation mode for data analysis processing in the current IT field. In other words, the cloud-end data calculation system constituted by lots of server groups can replace the single operation system with the center of personal computers. In order to further discuss the network safety under the “cloud computing” environment, the effective network safety strategy was proposed.

1. Introduction

With the innovation and development of internet technology in today's society, the scale of network application is gradually expanding. The data processing demands are gradually improving. As the brand-new computing network technology, the cloud computing technology emerged at the right moment. After entering into the cloud computing and cloud storage era, enterprise-level system calculation work starts using distributed storage and deployment mode to complete it. The data security problem of the cloud computing technology is the barrier to obstruct the further promotion and utilization. The security of the cloud data determines the trust degree of users, while the trust degree of users determines the development space of the cloud storage. It is necessary to analyze the key technology in the current cloud computing field and strive for more reliable space for cloud storage.

2. The Data safety strategy analysis under the cloud computing environment.

A. The overall operation performance of the cloud computing.

Two groups of the same data buffer memories are allocated for all physical calculation equipment of the entire cloud computing system. Here, they are named as the CacheA memory and CacheB memory. Then, they are conducted the initial treatment. Each memory is divided for caching. It can be observed from Figure 1 that two groups of memories have users with the same color. When users need to do data calculation and storage, CacheA and CacheB will enter into the normal working state. Under the circumstance, in order to complete initial treatment for Cache memory, it must conduct the timing operation. Once timing is about to reach the established period, it is necessary to select Cache memory to complete the Cache rotation procedure of a period.

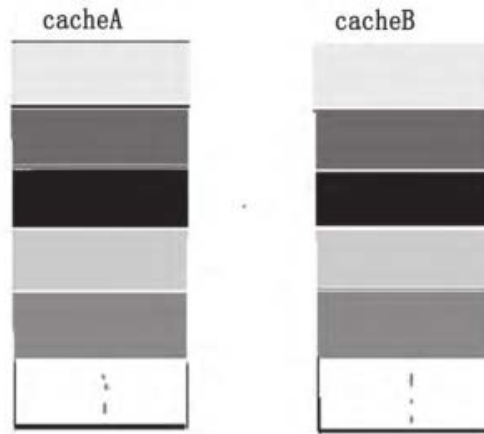


Fig.1 Cache Regional Distribution

The hardware resource division strategy of mutual exchange in the Cache region will make users share Cache region and reduce waste of hardware resources, so as to accelerate the overall operation performance of cloud computing.

B. The Safety Strategy of the Reliable Cloud Model Based on the Cloud Computing Environment

With the popularity of the cloud computing application, an increasing number of users select hardware and software resources that they can apply and also upload their resources to the cloud for other users to download. Meanwhile, users also worry about cloud resource safety. In addition, the hostile attack and stealing of some crackers also make the trust problem between users and CSP become difficult to be solved.

X is set up as a union of credibility, $X=\{x\}$, called as the space of credibility {one-dimensional, two-dimensional or multi-dimensional}. The subjective qualitative trust for the space of credibility X means that any element x has a random number with the stable tendency, $y=UA(x)$, called as the x 's credibility for A . The distribution of credibility on X is called as the trusted cloud.

The proposal of TCCP model opens a new idea to solve such a problem. The cloud computing is combined with the trusted calculation to solve such a problem in the technical level. TCCP model is closely linked with the trusted calculation platform. Throughout numerous safety issues faced by the cloud computing, security of user data and privacy is extremely important. In order to cope with such a safety problem, CSP conducts the encryption processing on internal messages of the cloud. As a result, users are short of the right to know about the uploaded resources. In addition, after users upload their data resources, they lose the control right to these resources. In this way, there is short of information between users and CSP. This obstructs cloud computing development to a large extent. In the three models of cloud computing(IaaS, PaaS, SaaS), only IaaS is transparent to users. In addition, users also have certain control permission. IaaS model is easier to solve a safety problem. The original TCCP model is designed based on such a principle. The management cloud service is used to prevent illegal invaders from tampering the trusted nodes(TNs) in the inner cloud or it will manage TNs as a coordinator. The specific model figure is shown in Figure 2.

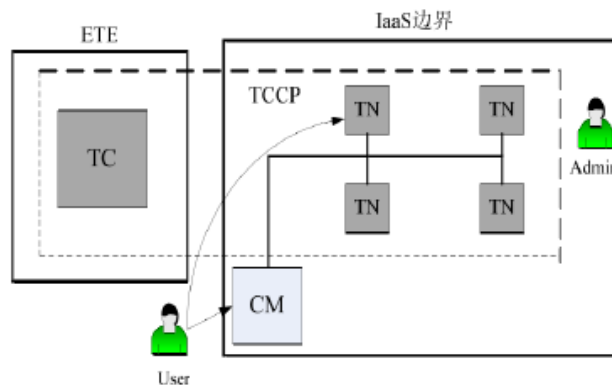


Fig.2 TCCP Model Figure

In this model, every online server needs to verify the status through the TC. Only the status is passed, TC will think it is trusted and add it in TN list. This is an effective method to ensure credibility.

The original one-dimensional reverse cloud computing algorithm uses Cloud(Ex, En, He) to stand for the one-dimensional normal cloud model. 3 cloud parameters are conformed by inputting cloud droplets, namely Ex(expectation), En(entropy and He(hyper-entropy). For example, by inputting the set X of N cloud droplets $X=\{x, x_2, x_3, \dots, x_n\}$, thus

$$\begin{aligned} Ex &= \bar{x} \\ En &= \left(\frac{\pi}{2}\right)^{\frac{1}{2}} \times B \\ He &= (S^2 - En^2) \end{aligned} \quad (1)$$

Where, \bar{x} is the sample mean, B is the first-order sample mean, and 2S is the sample variance, attaining:

$$\begin{aligned} \bar{X} &= \frac{1}{n} \sum_{i=1}^n x_i \\ B &= \frac{1}{n} \sum_{i=1}^n |x_i - \bar{x}| \\ S^2 &= \frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})^2 \end{aligned} \quad (2)$$

Definition 1: The vector model is used to stand for the space of credibility, which can be one-dimensional, two-dimensional or multi-dimensional.

Definition 2: The determination of one-dimensional normal cloud model shows that: the tuple Cloud is constituted by three numerical characteristics (Ex, En, He), where Ex stands for expectation. It refers to the subject expectation distributed in the creditable space and classical sample points with creditability. En stands for the entropy. It means the acceptable cloud droplet range in the subjective creditable concept, showing the vagueness of the trust. He stands for hyper-entropy, showing the randomness of the subjective creditable concept.

Definition 3: The one-dimensional normal cloud model is used to expand the two-dimensional normal cloud model. It is the tuple constituted by six numerical figures(Ex1, Ex2, En1, En2, He1 and He2), where Ex, En and He stand for expectation, entropy and hyper-entropy.

Input: the set of N cloud droplets $\{x_1, x_2, x_3, \dots, x_N\}$; weight set of cloud droplets $\eta = \{\eta_1, \eta_2, \eta_3, \dots, \eta_N\}$.

Output: the qualitative concept represented by N cloud droplets—Ex(expectation), En(entropy) and He(hyper-entropy).

The specific process of the algorithm is shown as follows:

(1) The expectation Ex is calculated in line with the input cloud droplets and weight, where:

$$\begin{aligned} Ex &= \bar{X} \\ \bar{X} &= \sum_{i=1}^N \eta_i x_i \end{aligned} \quad (3)$$

(2) According to input cloud droplets, weight and expectation in (3), entropy(En) is calculated, where:

$$\begin{aligned} B &= \sum_{i=1}^N \eta_i |x_i - \bar{x}| \\ En &= \sqrt{\frac{\pi}{2}} \sum_{i=1}^N \eta_i |x_i - Ex| \end{aligned} \quad (4)$$

(3) According to the cloud droplets, weight, sample mean, and En, hyper-entropy is calculated, where:

$$S^2 = \frac{1}{N-1} \sum_{i=1}^N \eta_i (x_i - \bar{x})^2$$

$$He = \sqrt{S^2 - En^2} \quad (5)$$

(4) After calculating Ex, EN and He of N cloud droplets, the concept of direct creditability and indirect credibility is used to realize the transfer and combination between multiple cloud models. TC is used for representing trusted cloud. Each cloud model can be expressed as TC $i=(i= 1, 2, \dots, n)$.

If subject A and subject B have no direct transaction, the subject A should evaluate the subject B for trusted grade. The evaluation method is shown as follows:

The similarity of the cloud is calculated as follows:

$$\delta_i = \frac{1}{n} \sum_{j=1}^n \mu_{ij} \quad (6)$$

$$\text{Where } \mu_{ij} = \exp \frac{-(x_i - Ex_j)^2}{2En_j^2} \quad (7)$$

If TC is the multi-dimensional cloud, thus the similarity is shown as follows:

$$\delta_j = \frac{1}{n} \sum_{i=1}^n \exp \left(- \sum_{i=1}^n \frac{-(x_{ik} - Ex_j)^2}{2En_j^2} \right) \quad (8)$$

(6) According to three eigenvalues, the objective credibility is judged. The judgment method is shown in Table 1.

Table 1 The Relevant Numerical Eigenvalues of the Credit Line

Trust objects	Ex	En	He
A	5.32857	0.554338	1. 23 346
B	5.6284	0. 28863 5	0.726125
C	5.12578	0.0114133	0.476382
D	5.1175 6	0.0882431	0.527223
E	5.11811	0.0813816	0.526637

From the perspective of Ex, En and He, Ex of C is maximal, showing that C has the highest satisfiability. Meanwhile, He of C is minimal, showing that stability of C's satisfiability is the highest. As a result, we should select C as the transaction object. Based on the above-mentioned algorithm, we can find out the higher object with the higher credibility for transaction(the object with the larger Ex and the smaller He will have the relatively high credibility). In this way, transaction security can be greatly improved.

3. Conclusions

As an implementation mode of utility computing, cloud computing owns three interactive modes, including IaaS, PaaS and SaaS, provides public cloud, private cloud, community cloud and mixture cloud, and forms five public features of pay-as-you-go, ubiquitous access, rapid deployment, resource abstraction and standard service. It is the service paradigm that provides "instant use as required, on demand, rapid deployment, instant release and good quality with cheapness". The abstract and virtual technology, resource dispatching and rapid deployment technology, mass data processing technology, high-performance data storage technology, and large-scale multi-tenant technology can be used to realize and optimize industrial distribution, promote professional division, improve resource utilization, reduce initial investment, reduce operation costs and create the new industrial value. As a result, the cloud computing fundamentally changes people's production mode and lifestyle. By combining the trusted concept with the cloud safety technology, the author studied

the safety strategy problem of trusted cloud under the cloud computing environment, thus the safety problem under the cloud computing environment can be improved to some extent.

Acknowledgements

This paper is supported by Youth Foundation of Wuhan Donghu University.

References

- [1] Liu Yuan, the Discussion on the Network Safety Problems under the Cloud Computing Environment[1] Technology and Market, 2017, (09): 157-158;
- [2] Gong Jianfeng, the Data Integrity Protection Model Construction of Cloud Computing Based on the Multi-level Safety Strategy[J], Computer and Digital Engineering, 2017, (08): 1625-1628;
- [3] Rong Chunyang, the Computer Network Safety Strategy under the Cloud Computing Environment[J], Technology Wind, 2017, (14): 86;
- [4] Liu Dong and Wang Wenting, the Study on the Cloud Safety Protection Strategy Design Based on the Cloud Computing Environment[J], Telecommunication Network Technology, 2017,(08): 54-57;
- [5] Li Bohan and Wang Fengzhu, the Data Safety under the Big Data Cloud Computing Environment[J], Electronic Technique and Software Engineering, 2017, (15): 213