Analysis and Research on the calculation of user data security and privacy services in the cloud

ZHOU Xianlin[1,a]

[1]Collage of Mathematics and Software Science, Sichuan Normal University, Sichuan Chengdu, 610066 China

[a]zhouxianlin1027@163.com

Keywords: cloud computing; cloud storage; data security; data encryption

Abstract. The problem of data security is one of the main problems plaguing the development of cloud computing, in view of the current cloud computing user data safety storage applications demand increase, need to greatly improve the data read-write efficiency problems, put forward the use of symmetric encryption and asymmetric encryption algorithm combining encryption, decryption scheme, suitable for large-scale data using a symmetric key encryption the symmetric key is itself, rather than the characteristics of high safety, give full play to the advantages of both computing environment in the clouds, to achieve a safe storage and good reading and writing data storage strategy to achieve high efficiency; the premise of asymmetric key encryption system in data security, the efficiency of the algorithm is close to the encryption system the symmetric key levels.

Introduction

In recent years, cloud computing is a new computing model, have become a new research and application field, gets more and more attention. Its development is gradually changing the whole IT industry and academia, the computers as the performance tool, software as a service model, in the provision of high performance computing for users at the same time, the use of low cost, rapid deployment, flexible adjustment of scale advantages, in the form of service for customers to provide mass data storage requirements [1,2]. In the traditional model, the enterprise data is usually focused on local storage and processing, so that enterprises not only need to configure the hardware infrastructure, also need the system configuration of professional maintenance personnel; implementation and maintenance cost is high. With the rapid development of IT technology, makes a lot of data distribution in Internet servers become possible. So as to provide services for the purpose of cloud computing mode emerge as the times require [3].Cloud computing services use charging way. According to the actual resources used by the user according to the amount of payment, and quota payment services compared to traditional cost saving, more competitive. With the popularization of the cloud computing model, how to let the "cloud" in the data transmission can be safely and efficiently in the network. In the cloud computing environment, user data is stored in the cloud server, how to ensure that every user of the stored data is opaque to other people, that data is not leaked [4], data security has become more and more challenges. The need for storing encrypted cloud data on the server, but the encryption methods being used to improve the safety need to sacrifice efficiency, how to realize a kind of safety and efficiency in both high encryption methods to ensure security of data stored in cloud computing, is a realistic problem urgently needed to resolve. In this paper, the data storage service model based on cloud computing, with the feature of low cost and performance full of dynamic, this paper put forward a data storage and transmission scheme of service oriented, combined with the use of symmetric encryption algorithm and non symmetric encryption algorithm, the data encryption and decryption method, to solve the data security issues of cloud computing services in application.

Unconstrained integer programming problem can be described as:

$$\min f(x_1, x_2, ..., x_n)$$
$$s.t. a_j \le x_j \le b_j, (j = 1, 2, ..., n)$$
$$x_j \in Z, (j = 1, 2, ..., n) \quad (1)$$

Wherein: a_j and b_j is an integer and they are the bounds of variable x_j; n is the number of variables x_j.

Defined delt $a_j = (b_j - a_j)/(l_j - 1)$, l_j is the number of values of the variables x_j, $j = 1, 2, ..., n$. Feasible solution space is shown in Figure 1.

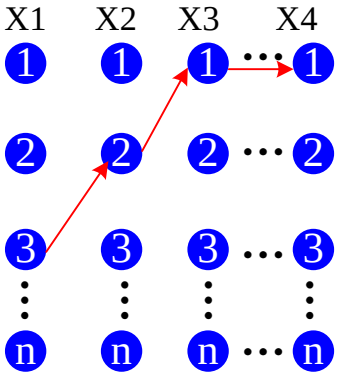

Figure1. Feasible solution space

In Figure 1, x_j has l_i nodes, and each variable in a node of a column, which can form a solution $(x_1, x_2, ..., x_n)$ of the optimization problem. Node number of each column 1 ~ l_j is defined as the code of the selected nodes of the j-th variable node. A set of solution is as follows:

$$(x_1, x_2, ..., x_n) = (a_1 + (m_1 - 1)\square delta_1, a_2, +$$
$$(m_2 - 1)\square delta_2, ..., a_n + (m_n - 1)\square delta_n)$$

n variables constitute the decision problem with n-level; the j-th level (the j-th variables) has l_j nodes; at the beginning m ants are on the first level; the j-th level select the probability of the i-th node.

$$P_{ij} = \tau_{ij} / \sum_{i=1}^{l_j} \tau_{ij} \quad (2)$$

τ_{ij} is the intensity of attracting of the i-th node on the j-level. Update equation is as follows:

$$\tau_{ij}^{new} = \rho \tau_{ij}^{old} + \frac{Q}{f} \quad (3)$$

Wherein: ρ represents the attenuation coefficient of intensity; generally 0 5 ~ 0.9; Q is the positive number; f is the value of objective function.

For such kind of integer programming model, usually the heuristic algorithm is used to find suboptimal solutions: such as the job scheduling algorithms like classic Min-min, Max-min, suffrage, X sufferage. Grid scheduling also uses such models. With the rapid development of modern optimization methods, taboo search, simulated annealing genetic algorithm, ant colony optimization algorithm and artificial neural network algorithm are used in grid scheduling and improved with the follow-up study. Subsequently there are some models considering the economic benefits, and some economic parameters like price of machines, operating budgets and the latest job completion time are added. The form of such models is at follows:

$$\begin{aligned} &\min \sum_i \sum_j x_{ij} t_{ij} P_j \\ &s.t. \sum_j x_{ij} t_{ij} P_j \le B_i \\ &\sum_j x_{ij} t_{ij} \le D_i \\ &x_{ij} \in \{0,1\}, \sum_{1 \le j \le m} x_{ij} = 1 \end{aligned} \quad (4)$$

Such scheduling model has the following problems: firstly, the target solution is limited as variables 0-1, and essentially it is a linear integer programming problem. Theoretically the integer linear programming problem can be transformed into a linear programming problem, but from the point of view of computing the achievement of this transformation is quite difficult. Secondly, these models usually use more heuristic algorithm to search local optimal solution for different input conditions, The convergence speeds may be quite different and it is difficult to ensure scheduling efficiency.

Therefore, this thesis uses the network utility maximization model (NUM) and proposes the Cloud Utility Maximization, (CUM).

The basic NUM model can be expressed as following:

$$\begin{aligned} &\max \sum_s U_s(x_s) \\ &s.t. Rx \le c \end{aligned} \quad (5)$$

Wherein, R is a routing matrix; vector c is the maximum transmission bandwidth of each link; Us is the utility function of the s-th service, and the utility function is generally a smooth, concave increment function, and also it is only depend on the obtained bandwidth xs; target solution vector x and each component xs represent the allocated bandwidth of the s-th service network. NUM optimization problem is often convex programming, and the global optimal solution can be got. Through the reverse engineering analysis, the network bandwidth allocation according some utility function is verified, which can ensure the requirements of different fair policy.

Experiment

CUM l model can be applied to the cloud environment with a larger scale. Figure 6 shows the application mode.

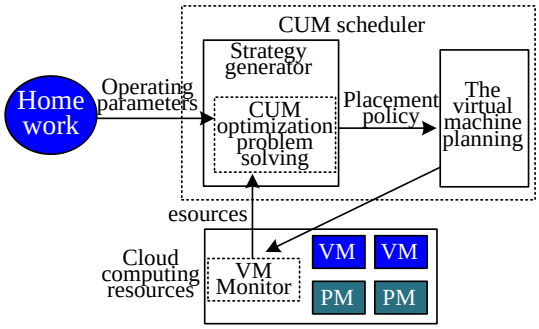

Figure2. Application scenario of CUM in the cloud

In Figure 2, CUM global scheduler (CUM scheduler) real-time receive the computing resource usage sent by the virtual machine monitor (VM Monitor). According to the job and remaining resources to determine the maximized effectiveness of the virtual machine placement policy, create the virtual machine and assign jobs to the virtual machine. Compare with the job scheduler in traditional clusters and grid computing environment, firstly CUM scheduler determines the virtual machine placement strategy, namely the instance of how many instances of physical computing resources into a virtual machine, and then assign the jobs to a virtual machine for execution. In a real cloud environment, the jobs preprocessing module can be increased in the front of CUM scheduler. Through the user bids and the user's preference the job level is divided, and it is set from the high and low. The value of willing to pay wi are set with different value. After grading the jobs are submitted to CUM scheduler for scheduling. CUM model uses the utility maximization as the

optimization objective and this optimization approach has achieved good results in the computer network bandwidth allocation. The carried business of the computer network has the following characteristics: at the same time there are a lot of business reached for service, and the quality of service requirements are different, and in the peak the network resources are basic full load. So when evolving cloud computing, users' demand for computing resources are as common as the demand on the network, and the scheduling advantage of CUM model becomes more apparent.

Summary

Cloud computing A new force suddenly rises., in various fields have a good prospect, but thecomputing environment data dependence on Internet cyber source in the cloud, the data security problem is particularly prominent. Security question users of cloud computing, and enterprisedata cannot be safely and conveniently transplanted into cloud computing environment mediumto a series of problems, leading to the popularity of cloud computing difficulties. In order to effectively solve these problems, this paper data storage service model based on cloud computing, by a combination of symmetric and non symmetric encryption both encryption and decryption scheme, implemented a storage security and good reading and writing data storage strategy in high efficiency. With the development of cloud computing technologies and mature,and legal aspects of legislation and related system of continuous improvement, is one of thedifficult problem of cloud computing, data storage security in cloud computing environment will be conquered, I believe that in the near future, cloud computing is just like any other application environment on the Internet, a profound influence on our the way of life.

References

[1] Joerg Christian Wolf, Phil Hall, Paul Robinson, Phil Culverhouse. Bioloid based Humanoid Soccer Robot Design, 2007.

[2]Wu Chuan-yu, He Lei-ying, Design and Realization of Instructional RPPR-Robot, Research and Exploration in Laboratory.2007, 26(10)

[3]Y. Geng, J. Chen, K. Pahlavan, Motion detection using RF signals for the first responder in emergency operations: A PHASER project, 2013 IEEE 24nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), London,Britain Sep. 2013

[4]Y. Geng, J. He, K. Pahlavan, Modeling the Effect of Human Body on TOA Based Indoor Human Tracking[J], International Journal of Wireless Information Networks 20(4), 306-317