Research on the Optimal Design of Computing Security based on Cloud Computing

Fan Yang[1, a], Yutai Rao[2, b]
[1] *Department of Electrical and Information Engineering, Hubei Radio & TV University, Wuhan, Hubei, 430074 , China*
[2] *Department of Electrical and Information Engineering, Hubei Radio & TV University, Wuhan, Hubei, 430074 , China*
[a]*email: yangfan_sheep@163.com,* [b]*email:2079406@qq.com*

Abstract

This paper analyzes the current problems in the data security and privacy of cloud computing. On the basis, this paper mainly research about the legitimacy and validity of research cloud computing process. First of all, this paper understand the concept of cloud computing technology, according to the working principle of the structure model of the cloud computing service analyzes the existence of data security and privacy. Cloud computing service providers for cost savings, or application access layer has invasion of illegal users, so cloud computing task submitted by the legitimate user will not be executed or not executed completely, and the users will get that a random outcome, and task submitted by illegal users may be was carried out. Research on the remote computing verification problem, analysis of the existing research on security work, found that the existing calculation in advance and the second validation of remote computing method for cloud computing users spending too big, this paper combines the characteristics of cloud computing mass data processing, puts forward the remote computing verification method based on the third-party certification, efficient and low consumption to ensure security.

Keywords: computing validation; cloud computing; Optimal Design

1 Introduction

At home and abroad in recent years, the development of cloud computing has

received widespread attention. With the development of cloud computing, the people's current computer hardware design, use, and buying patterns will change dramatically. Cloud computing provide storage resource and computing resources to users as needed to, users no longer need to invest in updating equipment ,but only pay the cost of the actual use of cloud computing resources .

Domestic and foreign scholars generally agree that cloud computing is the next generation Internet service platform; however, it also means that cloud computing security and privacy problem to be solved. Breaks through the traditional computing model, cloud computing users lose the ability to completely control data, the data is no longer stored on a personal computer but distant cloud computing server, data calculation is not from the user to control complete personal computer, but from cloud computing to finish. The new computing model for data calculation process are very vulnerable to attacks, will cause the user data security and privacy exposed, such as, whether to carry out the user's computing tasks, whether to feedback to the user the correct calculation result, whether cloud computing will disclose personal information.

This paper researches remote computing verification problem , analyzes the existing research on security work, finds that the existing calculation in advance and the second validation of remote computing method for cloud computing users spending too big, combining the characteristics of cloud computing mass data processing , puts forward the remote computing verification method based on the third-party certification, efficient and low consumption to ensure security.

2 Methods of the Remote Computing Verification

For data calculation process is likely to suffer from to attack, more mature study is less, which mainly include two aspects of remote computing verification and validation of computing. [7] proposes distributed computing protocol, the protocol makes the server can send some advance calculation results to the user without receiving the input data, let the user himself verify by calculation results and the remote computing results in turn. [8] and [9] define the concept of formal

verification calculation, users not only get the calculation results ,can also get the second calculation result, and verify by the two results. Due to the limited computing and communication resources, cloud computing terminal users can't take complex computation authentication every time, because it will face a very expensive cost and low efficiency.

3 Methods Optimization Design

The aforementioned algorithm is commonly used in the distributed processing system. And in processing data, the algorithm's performance is stable. But when processing large data, the algorithm will become slow, can not meet the customers' demands. And big data computing requirements tend to be higher. When handling large data for the user the attack may be more not easy to find, because the time data processing needs is longer, and whether the results are correct or not needs time to determine. Therefore, a method is need, can deal with distributed data, and can handle large data at the same time.

For now, the cloud customer terminal hardware conditions of processing large data is not enough. So a third party is need between cloud services and the customer terminal , it should have hardware conditions to handle large data. The third party can store big data and deal with data calculation, the third party can also authenticate legal user's identity and legal cloud server.

Then, on the basis of the previous algorithm, this paper optimizes them.

First of all, determine the qualified third party which approved by the cloud server and users. When the user requests to calculate, the third party starts authentication. After the third party to confirm the identity of the user, further to confirm the user's request time and transaction. After confirmed, looking for the same transaction history in the user access list saved in the third-party server, if any, the transaction processing results of the list will be sent back to the user. If there is no the same transaction in the list, then the third party will find out the most similar to the first five transaction results in the list with the transaction committed to return to the user.

After the user receives the results returned by the third party, he can choose

whether to verify the result, if he want to verify the results, the third party will handle the request in advance and sent the user's calculate request to the cloud server, after the cloud server has processed, the result is returned to the third party, which will be validated by a third party, the processing result comparing with the results of cloud returns. When alignment is correct, the third party returns the results to the user.

4 Test results

Simulation experiment is to verify the proposed method can improve the validation work when the mass data processing. The program to deal with affairs put on Baidu cloud server, the program is based on the Eclipse development platform, with triple loop structure, each cycle at the same cycles which is 10^n, integer $n \in [1,12]$. With the PC, users respectively use literature [7], literature [8] [9] and this paper‘s methods to access the program of the cloud server , and record the access results and response time. Three methods on the correctness and completeness of the execution result difference is not big, which illustrates the correctness and integrity of the paper’s algorithm in remote computing results have no obvious improvement. Three methods on the response time of performance is shown in figure 1, the results show that when the data level is less than 6, the response time of the algorithm in this paper is higher than the other two; when the data level is between 6 to 7, the response time of the three algorithms is roughly balance; But when the data is orders of magnitude greater than 7, response time of the algorithm in this paper are much smaller than the other two algorithms. That is to say, before the data level in 7, the paper’s algorithm did not improve response time, but when the data scale is more and more big, the response time of the algorithm in this paper is much shorter than the other two algorithms, improvement is obvious.

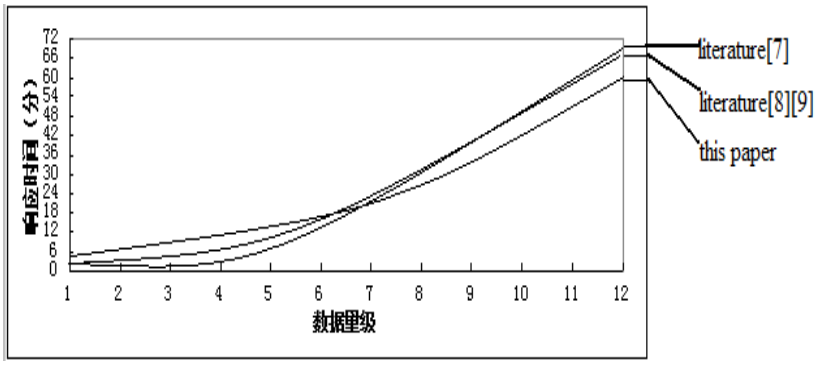

Fig.1. The experimental results

5 Conclusion

From the perspective of remote computing verification, this paper analysis of the existing research on security work, found that the existing calculation in advance and the second validation of remote computing method for cloud computing for users spending too big, this paper combines with the characteristics of cloud computing mass data processing and puts forward the remote computing verification method based on the third-party certification, the third party is responsible to ensure the authenticated user legal , jointly by legitimate users and authentication institutions select common tasks and submitted to the third party , the third party take a common task in advance calculation method for validation.

Acknowledgements

In this paper, the research was sponsored by the Science and Technology Research Program of Hubei Provincial Department of Education (Project No.B2014187). Associate Professor Yutai Rao of Hubei Radio & TV University is the Corresponding Author of this paper, his email is 2079406@qq.com.

References

[1]Buyyaa R，Chee S Y，Srikumar V，et a1．Cloud computing and emerging

IT platforms：vision，hype，and reality for delivering computing as the 5th utility[J]．Future Generation Computer Systems，2009，25(6)：599-616．

[2]Luis M V，Luis R—M，Caceres J，et a1．A break in the clouds：towards a cloud definition[J]．ACM SIGCOMM Computer Communication Review，2009，39(1)：50—55．

[3]Wang L，Laszewski G V．Cloud computing：a perspective study[J]．Journal of New Generation Computing，2010，28(2)：137—146．

[4] Kouzes RT，Anderson GA，Elbert ST，Go．on I，Gracio DK．The changing paradigm of data．intensive computing．Computer，2009，42(1)：26-34，[doi：10．1 109/MC．2009，26]

[5]U·S·Department of Commerce．The NIST definition of cloud computing．National Institute of Standards and Technology． 2011．

[6] Chert K，Zheng W M．Cloud computing：System instances an d current research． Journal of Software，2009，20(5)：1337—1348 (in Chinese with English abstract)．

[7] P. Golle and I. Mironov. Uncheatable distributed computations. In The Cryptographers' Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001.

[8] L. Wei, H. Zhu, Z. Cao, W. Jia, and A.V. Vasilakos. Seccloud: Bridging secure storage and computation in cloud. In 30th International Conference on Distributed Computing Systems Workshops (ICDCSW'10), Genova, Italy, June 21-25, 2010.

[9] R. Gennaro, C. Gentry, and B. Parno. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In 30th International Cryptology Conference (CRYPTO'10), Santa Barbara, California, USA, August 15-19, 2010.