Research on the key technology of data security protection based on cloud computing

Juan guo[1, a]
[1] ShiJiaZhuang Vocational Technology Institute, 050081, hebei, china
[a] sjzpt_wyh@126.com

Keywords: protection technology, cloud computing, data security

Abstract: cloud computing is the hot topic in the application and the research sphere. And the most IT Enterprises staffs think that cloud computing is the core application architecture of the next generation of computer network technology. Though the appearing of cloud computing bring a lot of advantage, but it also make the challenge of data security. According to the above-mentioned reason, the key technology of data security protection based on cloud computing is the study object of this paper. The definition of cloud computing and the challenges of data security under the surround of cloud computing will be introduced in this paper.

Introduction

The most application software and the data information have distracted to the stupendous data center that cloud computing provided , and it make the storage and management of data become uncontrollable , and it will make the user very worried the data that deposited at the cloud computing environment . According to the above-mention reason, the access control suggestion based on attribute encryption algorithm will be put forward.

Cloud Computing

The interrelated definition of cloud computing. With the development of network application the research , the Utility computing , the grid computing and the on-demand computing had be developed , and these computing manner had resolved the network great collaboration problem . Cloud computing is the novel computing mode that base on the improving of the above-mentioned computing manners. Now the definition of the cloud computing is not be determined [1]. But at the end of the 2007 year, IBM Company put forward that think the content that cloud computing platform. They thought that the cloud computing platform should include the enormous computing resources, the storage area network, the network facilities and the safety equipment. And the most of the cloud application service must be provided by using the internet [2]. and you can find that cloud computing have five features include measured service , on-demand self-service , resource pooling , broad network access and rapid elasticity , the figure of the cloud application service is the figure 1 .

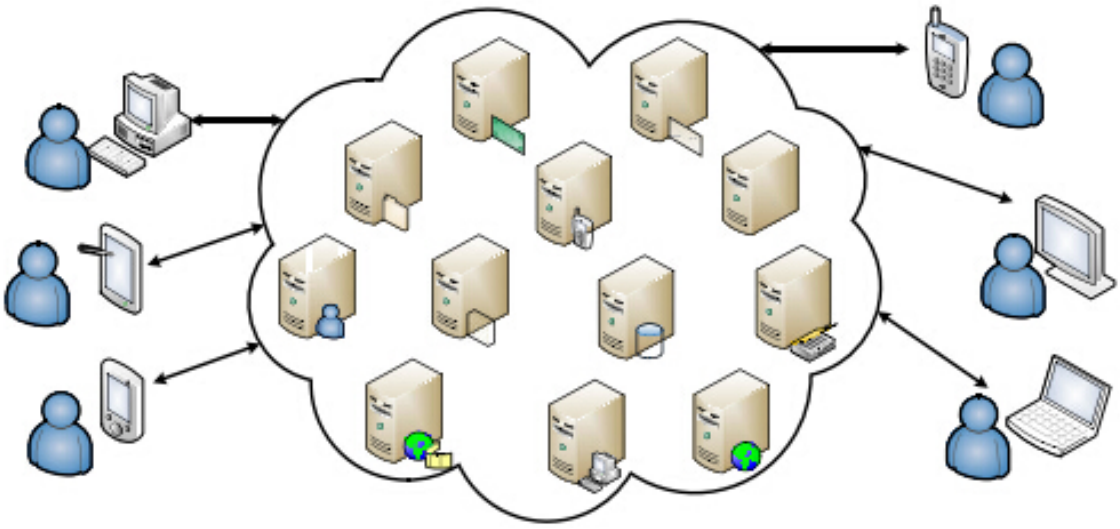

Figure 1 cloud computing service

The model framework of the cloud computing. According to the features and the research achievement of the cloud computing. The system architecture of the cloud computing have be divide into five section that comprise the application layer , the exploitation platform layer , the resources architecture layer , the nucleus layer and the physical layer [3].

Data security

Nowadays , the development of the electronics information technology have influenced many aspects of people , and the electronic data file have get a very wide applications in the most profession , so data security have become the very important aspect of the modern society . In the modern society, everyone is attaches great importance to the security of the private data, they hope that their privacy is will not be find through the network.

The data security protection technologies based on the cloud computing

Symmetric password system . Symmetric password system is the most mature cryptography, and it has been applied in many fields. And it includes the classical cryptography, the data encryption standard and the advanced encryption standard. The encryption and decryption process of the symmetric password system you can find in the figure 2. In the figure 2, you can find more information, and you can know the specific process of the symmetric password system. And the symmetric password system can effectively protect the security of the data.

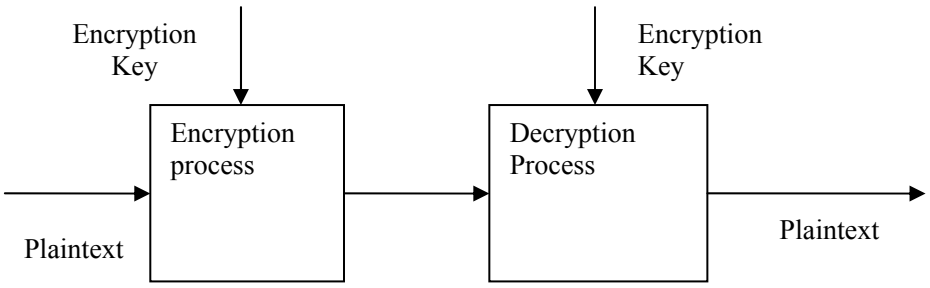

Figure 2 symmetric encryption systems

Asymmetric encryption systems . The encryption key have be divided two section s that include the open encryption key and the private encryption key [4]. And the open encryption key is be registered in a credible communal database, the private encryption key is be protected by the users. In the process of encryption, the side of information transmitted use the open encryption key make the information be encrypted, the side of information accepted use the private encryption key achieve the decryption of the encrypted information .And you can find more information in the figure 3.The asymmetric encryption system can eliminate the rigid requirement of users exchanging encryption key.

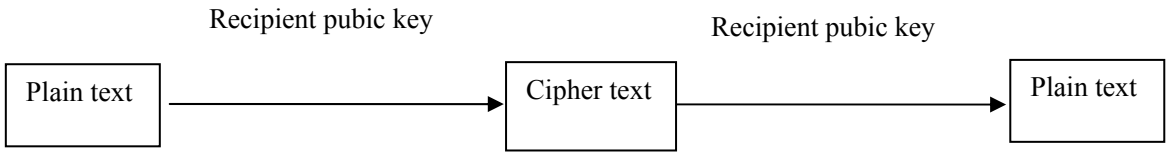

Figure 3 asymmetric encryption systems

The encryption algorithm that based on attribute. According to the access structure of the cipher text and the relation between the attribute collections, the attribute-based encryption algorithm can be divided to two categories that include cipher text-policy attribute-based encryption and the key-policy attribute-based encryption. The cipher text and the access structure of the cipher text are corresponding to each other, but the key is corresponding to properties collection. In the process of decryption, the properties collection of the decrypting party must conform the access structure that be set up in the process of information encryption. But in the key-policy attribute-based encryption, the encryption key is corresponding to the access structure and the cipher text is corresponding to the properties collection.

Hash Tree. This manner had been put forward by Ralph Merkle in 1979. Essentially, this method is a binary tree. The leaf node of the hash tree is representing hashes, and the non-leaf node represents the leaf node getting on concatenation achieved hashes. And every leaf node must be get on concatenation. And the all leaf nodes of the hash tree are provided with correlation.

Conclusion

The cloud computing is the center architecture of the computer network application technology. Cloud Computing changes the custom what the method of using computer thoroughly. The surroundings of cloud computing, almost all the application software and the information of data are divert into a bulky server farm by the provider of cloud computing. The centralized management of data and serve has a lot of challenge about security to the application of cloud computing. The article is mainly have a research that the data security which is based on cloud computing, which in connection with the feature just as the virtual and large-scale and dynamic configuration of cloud computing. These scheme can effectively support the dynamic operation, the verification of consistency and integrity，the security access control of data file under the environment of the clouding computing .

References

[1] R. Buaya, C.S. Deo, S. Revenual. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities[C]. Dalian:10th IEEE Ante alternation Conference on High Performance Computing and Communications (HPCC 2008), Sept. 25-27, 2008.

[2] Fay Chang, Jeffrey Dean, San jay Hematomata, et al. Big table: a distributed storage system for structured data[J]. New York: ACM Transactions on Computer Systems (TOCS), 2008, Volume 26 Issue 2 .

[3] Buaya R., Revenual S. The Grid bus toolkit for service oriented grid and utility computing: an overview and status report[C]. Grid Economics and Business Models, 23 April 2004, pp19-66.

[4] Chimeric FM, Enuf G, Sure S. An Approach to a Cloud Computing Network[C]. Technical University of Ostrava: 2008 IEEE First International Conference on Applications of Digital Information and Web Technologies, 2008, pp113-118.