Advance Journal of Food Science and Technology 12(2): 63-65, 2016
DOI:10.19026/ajfst.12.2839
ISSN: 2042-4868; e-ISSN: 2042-4876

Submitted: August 24, 2015 Accepted: September 11, 2015 Published: September 15, 2016

Research Article

Key Technology of Food Data Security Based on Cloud Computing

[1, 2]Jian Wang, [1]Zhenmin Tang, [1]Wenjuan Shao and [3]Xianli Jin
[1]School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094,
[2]Jiangsu Post and Telecommunications Planning and Designing Institute Co., Ltd., Nanjing 210019,
[3]College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Abstract: At present, the development of electronic information technology has affected all aspects of human society, electronic food data files have been widely used in all walks of life. Therefore, food data security has become one of the most important aspects in the modern society, which can affect our work and life. In this study, it takes the cloud computing overview as a starting point, with the help of cloud computing security risk analysis, exploring the cloud food data security strategy.

Keywords: Cloud computing, electronic information technology, food data

INTRODUCTION

Cloud computing as the core architecture of the next generation computer network application technology regarded by most IT companies and industry insiders, it has changed the traditional habits of people to use their computers. Most of the traditional IT solutions are in the absolute control of the users and most of the food data can be stored in the user's own local physical device. But under the cloud computing environment, almost all of the application software and food data information can be transferred to the cloud computing service provider with its huge server cluster. However, centralized management of food data and services has brought many security challenges to the application of cloud computing. Although cloud computing service providers have the ability to provide a relatively safe and reliable food data center, but the security problem is still the biggest problem in the application and promotion of cloud computing. Under the cloud computing environment, it is very easy to bring uneasiness and distrust caused by the uncontrollable user food data.

The overview of cloud computing: Cloud computing is a kind of concept proposed to meet people's high efficiency calculation. It is actually a kind of interaction model (Table 1) appeared for the needs and services. Service providers can provide services to users through the Internet, at the same time, it can charge the corresponding costs (Bethencourt *et al*., 2007). Therefore, cloud computing technology is the product of grid computing, distributed computing, parallel computing, utility computing, network storage technologies, load balancing and some other related Internet technologies.

The risk of cloud computing security: Cloud computing can be regarded as a public oriented service platform, cloud can store a variety of user's food data and information, at the same time, the users can operate computer at the cloud computing platform, using a variety of software, so as to experience the convenient, fast and efficient service brought by cloud. In the last few years, cloud security issues are mainly manifested in the following aspects:

Illegal users: Cloud platform is the sharing platform, which can allow different users to have operation at the same time, if there are some faults appeared on the platform during the process of having operation, it will cause food data to be intercepted and used by the criminals, the lighter cases can violate the user's food data and information, while the severe cases can cause the enterprise's secret to be leaked out, bringing huge losses to the enterprise (Shor, 1994).

Cloud platform can provide a variety of cloud services, which should be placed on the server end and have the same function of the other network applications, due to the virtual nature of network, confirming the user's identity, ensuring the identity of the legitimacy is the most important task to ensure the cloud security. If hackers intercept the client's user name and password, the hackers will use the customer's

Corresponding Author: Xianli Jin, College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Table 1: Contrast between cloud computing and traditional model

	Traditional method	Cloud computing
Realization method	Buy hardware and software	Supplier service
Commercial process	Equipment and management	Providing services according to user demands
Technical features	Simple	Share
Computational efficiency	Limited scale	Unlimited scale
Whether it can expand or not	Unextensible	Extensible
Operating cost	High	Cheap

Fig. 1: Food data life cycle

identity to log in, casually tampering and getting the customer's information, even exploring the customer's information to the public, therefore, it is very necessary to confirm the password to get certification so as to ensure the identity of the user legitimate, when the customer log in, only in this way can it improve the security of logging the cloud platform (Markus *et al*., 2003).

Food data security: As for food data acquisition process, users are very concerned about whether the security and confidentiality of food data acquisition is perfect or not. Unsafe acts can be including the following: the loss of food data when having communications, arbitrary interception, random changes and some other issues. These problems often occurred during the process of communication, management and preservation. Mainly shown in the following aspects:

Illegal food data operation: Users on the cloud computing platform will have all kinds of operation, in this case, it may cause the user food data to be illegal operated, some of them will cause the user's food data to be modified or deleted, which will cause the loss of user's food data. On the other hand, these illegal operations may be irreversible or destructive, which can bring unestimated loss of benefits for the enterprises and customers.

Transparency: Since cloud computing can only provide users with transmission food data and the location of storing food data storage and the means of communication are transparent for the users, the cloud user's food data will be stored in some position of the cloud and this position may be in a certain place of the earth, therefore, if there is an accident occurred, it may cause unnecessary trouble because of the differences of regulations (Szydlo, 2004).

Using key to transmit food data: Because cloud service can deal with food data in a fast and efficient way, which can also meet the user's needs, it is very important to transmit food data with the security measures. Sometimes, a small fault from the system will enable food data theft, therefore, during the food data transmission process, it must use the key to prevent food data theft.

High reliability of food data: Food data centers can be likely to make the food data storage be damaged because of some attacks or non anti-force, which needs to fully consider whether the food data in food data center can have enough reliability. It can be mainly reflected the following aspects: whether the food data have a good backup, whether it has good food data fault tolerance, whether it has the response time to solve problems after the problems occurred.

Operational information records: The cloud platform should provide information recording mechanism through tracing the information, so as to ensure the operation of information can be traced when the error is occurred.

The life cycle of cloud food data: The life security of cloud food data has six development processes, namely: creating the available food data, food data transmission, storing food data in the cloud, sharing cloud food data, making the food data be archived and deleting the food data and so on, which can be shown as follows in Fig. 1:

Cloud food data security strategy: As for users, when users share the enjoyment with the cloud services, the issue of food data security is becoming more and more important. Food data security is to adopt a certain technical method to ensure the food data access can be effectively controlled, so as to ensure these food data can not be leaked, tampered or damaged.

Food data transmission: Confidential information (such as customer information, financial reporting, etc.) is often critical for business customers. Under the cloud environment, these confidential information should be transmitted through the network to the corresponding operation, therefore, it is essential to ensure the security of the food data transmission process (Glen, 2005).

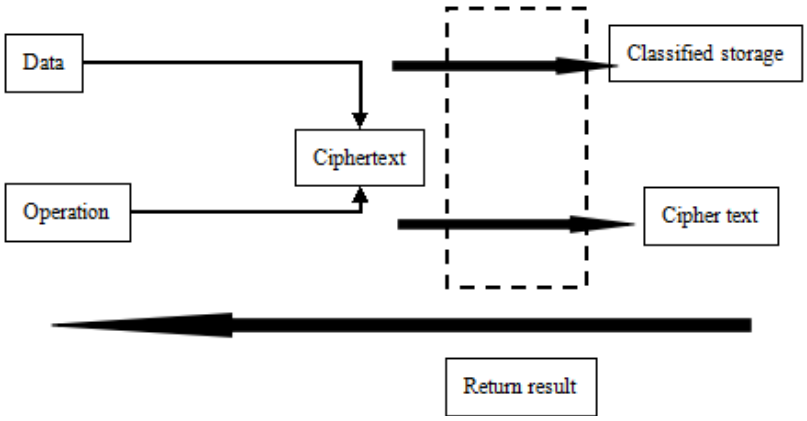

Fig. 2: Schematic diagram of encryption scheme

Meanwhile, food data security strategy can be defined as follows: for some food data, it should use point to point encryption measures, so as to ensure all the food data not be leaked or modified. Using the methods such as HIPSec, SSL and other protocols for transmission encryption, in addition, it also can adopt digital signature and digital certification and so on, which can be used to guarantee the security of food data transmission. Encryption Scheme is as bellows in Fig. 2.

Food data privacy: At present, under the cloud environment, because the food data is usually stored by dispersed way, which made the traditional firewall protection method can not be used, which also can bring a hidden trouble for food data security. But at present, as for the cloud food data privacy issue, it has not got a good method to solve the problem, considering the private cloud can have the ability of protecting the user's food data resources through setting up exclusive firewall, it is suggested that business users should adopt the strategy of building private cloud or mixed cloud to solve this problem.

Food data residue: Food data residue means that after the food data is deleted, on after the physical media still have a residual and these residues can often be recovered by a certain way to recover the deleted food data. This may be used by hackers, malicious users, etc., resulting in the user's food data leakage. Can ensure that the food data of the system in front of the storage space for the release and distribution before storage in the food data completely remove cloud service providers ensure food data security must be solved the problem. So we should use some technical means to remove the expired food data to ensure there is no residual food data effectively.

Food data auditing: As for the problems that occurred in the system of cloud platform, these risks and other issues should be audited effectively, which can not bring security risks to enterprises and users. It is very important to check the legality of food data and information in time. In addition, it is very necessary to consider the saving time for food data encryption, as well as the security of encryption, efficiency, so as to make a certain auditing and ensure the enterprise can make efficient use of the related cloud computing resources.

In a word, as for information security under the cloud environment, when dealing with the corresponding food data security issues, it can ensure the security and privacy of users through the food data isolation, access control, food data storage and other strategies.

REFERENCES

Bethencourt, J., A. Sahai and B. Waters, 2007. Ciphertext-policy attribute-based encryption. Proceeding of the 2007 IEEE Symposium on Security and Privacy. Oakland, pp: 321-334.

Glen, N., 2005. Verified Query Results from Hybrid Authentication Trees. In: Jajodia, S., Wijesekera, D. (Eds.), Data and Applications Security. Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, 3654: 84-98.

Markus, J., L. Tom, M. Silvio and S. Michael, 2003. Fractal Merkle tree representation and traversal. Proceeding of the Cryptographer's Track at RSA Conference (CT-RSA'03), 2612: 314-326.

Shor, P.W., 1994. Algorithms for quantum computation: Discrete logarithms and factoring. Proceeding of the 35th Annual IEEE Symposium on Foundations of Computer Science (FOCS, 1994), pp: 124-134.

Szydlo, M., 2004. Merkle Tree Traversal in Log Space and Time. In: Cachin, C. and J.L. Camenisch (Eds.), Advances in Cryptology-EUROCRYPT 2004. Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, 3027: 541-554.