Secure Data Storage for Electronic Commerce Network Payment using Cloud Computing

Shuyan Tang[1,*]

1 Humanities and Law College
Hunan International Economics University
Changsha, Hunan, China

***Abstract* — Advances in cloud computing technology have brought many economic benefits to users. While satisfying the needs of users, cloud computing brings its advantages of low costs, rapid deployment and flexible scale adjustment into full play. Large volumes of data are stored in many types of networks with increasing number of companies and people using cloud computing services, thus putting severe challenge on users' data security and availability. Under these circumstances, our study has analyzed data security of users and found that data storage security is vital to both private and business users. The security challenges brought by cloud computing focus on how to prevent users' data from leaking and how to guarantee users ability to retrieve data efficiently and accurately. In the research status of secure data storage under cloud computing, surveys have shown that experts and scholars have attached great importance to data security. Strategies on secure data transmission and storage based on cloud computing, including encryption and decryption processing, are also discussed in this paper. To protect user data security, structure models have been formulated and secure data storage systems under cloud computing are discussed.**

Keywords - secure data stroage; electronic commerce network payment security; flexible scale adjustment; cloud computing

I. INTRODUCTION

Information technology advanced greatly with the development of social economy and science and technology. Users' deeds for data computing and storage also increased greatly. Compared with traditional model, which computes and stores data based on numerous high-performance servers, cloud computing, the new computing model adapt to users' need of high distribution, low costs and high versatility, can not only provide users with high-speed computing, but also satisfy users' needs for large-scale data storage[1]. Cloud computing service will be needed increasingly, and its application will become wider. As shown in Fig. (**1**), users' need for cloud computing. It shows that the reason for users to choose cloud computing is its cloud host and cloud storage application. In the future, users' needs for cloud computing in business management, application development services and network acceleration services will continue to grow [2]. With the increasing need for cloud service, the focus of cloud computing R&D at the present stage is how to ensure data security and integrity in networks [3]. Started from data storage and application status of cloud computing, and considering the protection of users' data security, a data storage system based on cloud computing should be designed to protect the security of data transmission and security.

With the development of information and network technologies, electronic commerce (e-commerce) has become an important symbol for Internet and information technologies. Meanwhile, the security problem of e-commerce is becoming more and more serious. It has been drawn attention by many scholars and engineering technologists. The e-commerce security protocols are the key technologies to ensure application and growth of e-commerce. The basic security properties of general security protocols include authentication, integrity and confidentiality. More properties are included in e-commerce security protocols e.g. non-repudiation, accountability, fairness, atomicity and anonymity. The design and analysis are more complex for e-commerce security protocols than general security protocols. Practice shows that security vulnerabilities have still existed even if the protocols are designed meticulously, and these vulnerabilities are difficult to find utilizing informal analysis methods. It is a wise choose to analyze e-commerce security protocols using formal methods. Formal analysis can find security vulnerabilities and flaws of the protocols. The analysis results can be used to guide the design of the protocols. Furthermore, the potential problems of the protocols can be mended. So the researches on the e-commerce security protocols and their formal analysis methods have important theories and realistic significance.

Security management platform is also called security operation center, which is a kind of network security management technology becoming popular in recent years. SOC is a management system normally used in nowadays. It can do simple analysis of data and take certain response measurements to some security events, but because traditional SOC's performance usually has a low security, once there are some breakdowns existing in SOC's relational engines, SOC would be gum up, making a greatly damaging effect on enterprise' s management. The application of cloud computing technology improves the defects of traditional SOC system, not only providing mass dynamic data but als

o greatly improving the data processing capability. So the improved SOC can resolve bugs in time, reducing the negative effects on the enterprise. Here, this paper introduces the building of enterprise network security system model based on cloud computing technology and studies the prosperity of cloud computing technology's application and development.

II. THE PROBLEM ANALYSIS OF USERS DATA SECURITY OF CLOUD COMPUTING

Users' date security is among the key issues that need to be addressed with the advance of cloud computing technology [4]. With the popularization of cloud computing service, concerns on cloud computing data security among users have been growing [5]. From the survey result shows in Fig. (**2**), security problem remains to be the most concerned issues of private users. Fig. (**3**) is the survey on business users by IDC in 2010. The result shows that, security risks of computing technology and data supervision risks are the mostly concerned problems of business users. That means could computing security problem is both the concern of private users and business users.

The problems of user data security should be addressed in time by cloud service providers; otherwise the problem might become more severe as cloud computing system developing [6]. Specific expressions of data security problems are as following:

(1)Only if cloud service providers create a trustworthy environment for users could make users update various kinds of data to the cloud. We could see that users attach great importance to the security, stability and reliability of cloud computing.

(2)While users store data into cloud, relative cloud service provider should guarantee the completeness and reliability in the storage devices. Besides, cloud service provider should provide various measures ready for use to deal with emergencies so as to guarantee the security and completeness of users' data.

(3)Cloud service providers should have perfect management mechanism for the management of data process after users have update the data to cloud. Once lost control on data management, great losses of users will be thus caused.

(4)Privacy is of great importance to user. In data retrieval and process, the service provider should guarantee that users' privacy should not be invaded.

The new protocol to be proposed should include authentication sub-protocol and payment sub-protocol. The authentication sub-protocol cannot only against personating transaction entities and messages replay attacks, but also resist DoS attacks effectively. Moreover it needs fewer messages to authenticate identities of important entity in the foremost time, as well as session keys used for transaction are negotiated efficiently. The payment sub-protocol is designed by improving the anonymous e-cash payment protocol. To realize its non-repudiation, certificates are used to prove the identities of the transaction entities. To avoid unfairness arisen by the dishonest transaction entities, the transmission of payment receipt is achieved by the trusted party. The proposed protocol uses FTP to transmit electronic cashes and payment receipts, which ensures achievement of accountability and fairness, and enhance the robustness of the protocol. The verification result of the protocol using the new logic indicates that it satisfies authentication, secrecy of key, non-repudiation, accountability, fairness and atomicity.

From the above analysis, we could conclude that cloud computing security has two major aspects: first is to prevent the leakage of users' data so as to avoid causing unnecessary loss of users; second is to guarantee the efficiency and accuracy of data acquisition when user has a specific need for a certain type of data. From the above analysis, we could say that the major task of cloud service provider is to guarantee the security of users' data transmission and storage. Some private data are unavoidable stored when users store data, such as bank account information, users' personal information and private mails. Under this circumstance, following problems should be addressed when users updating date to cloud: how to prevent information from being stolen by other people? How to prevent information from being stolen by internal staff from cloud service providers? How to guarantee the login legitimacy and ready-access at any time? In face of these problems, in-depth study should be carried out by cloud service providers so as to address the data security problem of users.

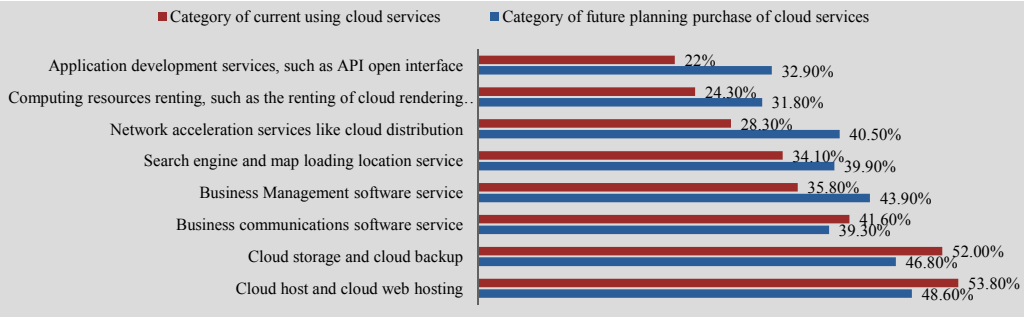

Figure 1. Users' needs for cloud computing.

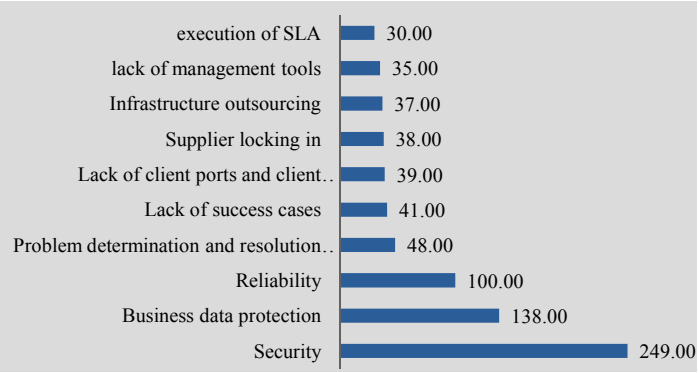

Figure 2. Survey on the most concerned problems of users as for cloud service.

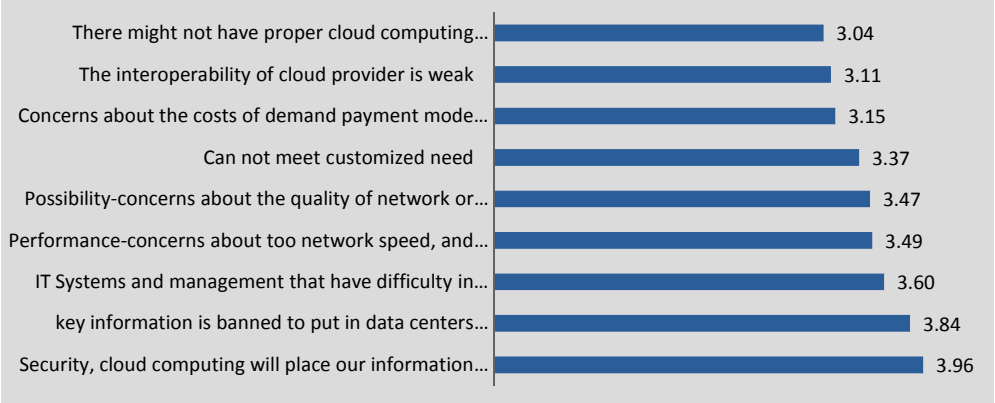

Figure 3. Items of business users concern about cloud.

III. Analysis of Research Status of Secure Data Storage under Cloud Computing Environment

With the development of information technology, cloud computing technology becomes mature gradually. Thus demand for cloud service has been increasing. The result of the above is more and more people have carried out research on cloud computing secure data storage. Fig. (**4**) is the number of published paper about secure data storage under cloud computing environment on CNKI (National Knowledge Infrastructure) from 2008 to 2013. It is a little growth from 2008 to 2009. The growth is a logarithmic one from 2009 to 2013, which means the problem is becoming an increasing concern of experts and scholars. It also means the problem is the one need immediate solution right now. Many experts have already dedicated themselves in the in-depth study on the problem to find out the best method to guarantee data security in cloud service.

During the process, the functions of different network technologies and distributed file systems are also used. Users' data storage by cloud computing is not got from a certain storage device, but through the data access service provided by a cloud storage system.

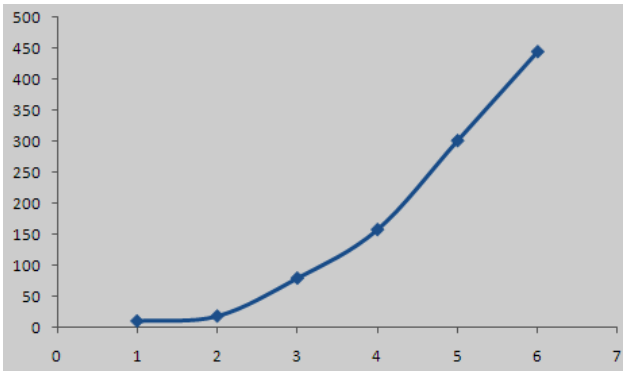

Figure 4. The number of published paper about secure data storage under cloud computing environment on CNKI.

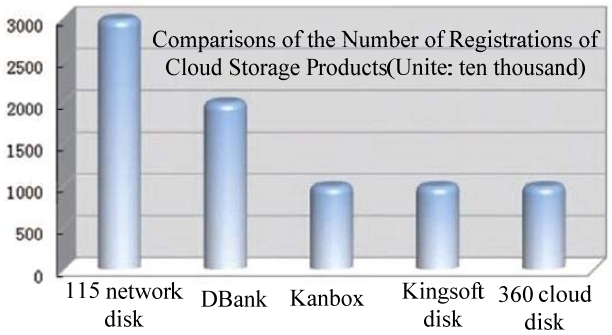

Figure 5. Comparisons of the number of registrations of cloud products in the first half of 2011 in China.

The demands of users are increasing with the development of cloud computing technology. More and more cloud computing service providers emerge with the tide of fashion. Differences do exist among different cloud service providers as for the nature of service and the scale, especially differences in data security protection and risks-handle abilities. Providers are weak in comprehensive strength and have deficiency will be gradually eliminated. When cloud service providers facing troubles, how to process data stored in cloud is unknown. Considering this, users will take data providers and preservers into consideration when choosing cloud providers. From Fig. (**5**), we can see that users most favored cloud service is 115 network disk, followed by DBank. Among the applications of services under cloud computing, the mostly concerned of users is the security of timely service. Users of cloud computing thought that providers should constantly update relative technology of cloud computing and strengthen supervision so as to guarantee the security of cloud service.

IV. SECURITY STRATEGY ON SECURE DATA TRANSMISSION AND STORAGE BASED ON CLOUD COMPUTING

Encryption processing is the commonly used way to guarantee security in data transmission and storage. Data of users can be stored in any storage space in cloud computing secure storage service. After being encrypted, people other than the user cannot acquire or access the information. Data encryption and decryption are used in cloud computing data transmission and storage at present.

At the beginning of user data encryption processing, user receives user's data from key store and extracts data with the public key encryption algorithm. Information verification is included in the process of encryption. Then Asymmetric encryption by secret key is carried out. Finally, data information storing secret key and encrypted user information are together stored into cloud. Continue to repeat the process until the final encrypted data is updated to cloud. This also comes to the end of the whole encryption process. When it comes to the encryption large-capacity data storage for users, two asymmetric encryption processes should be added to the secret key of symmetric encryption algorithm before updating secret key and encrypted data to cloud. In this way, users only have to keep the asymmetric encryption algorithm instead of storing large-capacity data, thus reducing the need for storage room. This will also reduce transmission costs and storage costs and makes users' management of secret keys more convenient.

When decrypting data, the decrypting party need to use the secret key of asymmetric algorithm to encrypt by carrying out piled encryption algorithm of secret key, thus the secret key is restored. Then the restored secret key will restore all the stored data through decryption packet of piled encryption algorithm. Repeat the above steps and all the data packets will be decrypted. After the completion of all data decryption, we will get the most primitive data of users. Problems in the management of secret key of symmetric algorithm will be addressed through the combination of asymmetric and symmetric algorithms. It also can be used to encrypt large-scale data. This strategy could guarantee that every user can conduct asymmetric encryption on data. Besides, the secret data is preserved in certain store of the cloud. When data exchange is needed by the users, they could download corresponding secret key. Besides, users' rights to encrypt the data are also guaranteed. Data encrypted in this way can ensure data security.

As the foundation and core of cloud computing, cloud storage refers to the process of providing data storage service and business access service externally by the combined efforts of various storage devices through relative application devices. During the process, the functions of different network technologies and distributed file systems are also used. Users' data storage by cloud computing is not got from a certain storage device, but through the data access service provided by a cloud storage system. The core of cloud storage is to effectively combine application software and storage devices then alter storage devices into a storage service through application software [7]. As shown in Fig. (**6**), the structure model of cloud storage is composed of four layers; they are access layer, application interface layer, basic management layer and storage layer. Each layer is endowed with different function.

(1)Access layer: mainly to provide users with application interface for cloud storage system login. The layer provides corresponding access type and access means according to different client units.

(2)Application interface layer: characterized by flexibility and changeability. Cloud service providers proved different application service and develop different service interfaces in accordance with business types needed by the users.

(3)Basic management layer: it includes cluster system, distributed file system and network computing. These technologies can realize the coordinated work among different storage devices. It is responsible for content distribution, de-duplication, data compression, data encryption, data decryption and data backup.

(4)Storage layer: the main function of this layer is to realize logical virtualization management of storage devices, centralized management of data, status monitoring of data and system maintain and update.

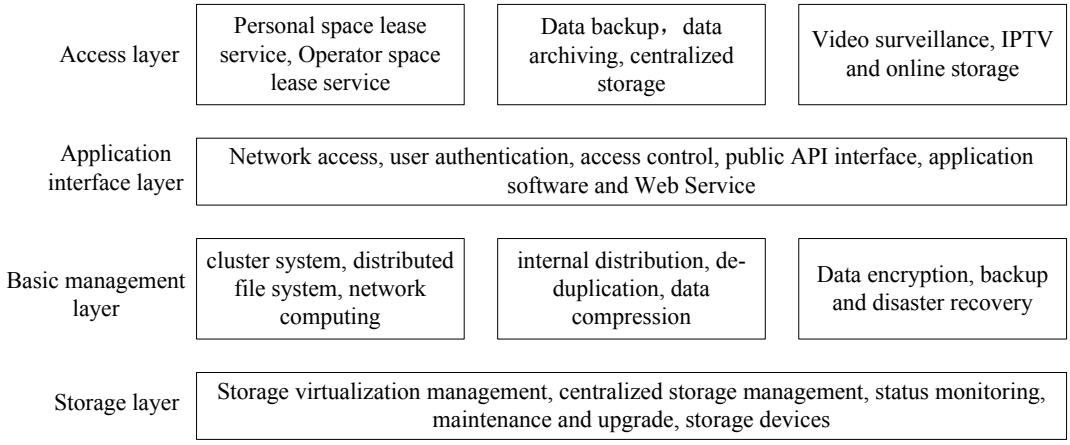

Figure 6. Structure model of cloud storage.

The design of secure data storage system under cloud computing environment consists of storage cloud, control center, the user interface and Client, as shown in Fig. (**7**).

(1)Cloud Storage：mainly include two parts, public data storage cloud and private data storage cloud. The function of storage cloud is to store all the data and operations of user without having to proved arithmetic function. Private cloud, by providing business users with a private data storage platform, can guarantee data security. Storage space can be saved by dividing cloud storage into private cloud and public cloud. Besides, it could solve problems of cloud platform that worry the users. Private cloud provides users with secure platform. The way to achieve private cloud: Linux system with Xen is installed into the physical machine in the clusters. At the same time, all the physical machines open SSH services together. The controller of cloud service provider manages private cloud through Xen and SHH. The relationship among cloud components are shown in Fig. (**8**).

(2)Control center: conducting data process and computing. Data process and computing includes data encryption, data decryption, data compression and data index.

(3)User interface: mainly to guarantee that different cloud service user can use different service interface. Its functions are user data format conversion, user authority management and user authentication.

(4)Client: it is the end user of data. Node server can provide service for client by sending service request to control center. Control center will conduct operation after receiving request. Then it will retrieve data for client from the storage cloud. Cipher text is used in the transmission from control center to storage cloud so as to guarantee the safety of data transmission [7-8].

Combining the above-mentioned researches, the thesis summaries the requirements of the e-commerce protocols and concludes the protocols design rules. The rules provide references for the design industrial standards of e-commerce protocols, and guide the design and application of the protocols. Implementing above rules, a typical micro-payment protocol is analyzed and redesigned. Micro-payment is a kind of the typical application of e-commerce. Its security and efficiency are regarded as the key factors in its design and implementation. The thesis studies the NMP protocol based on the conventional hash chains firstly. Some shortness or flaws are found in it, including user's malicious overdraft and executive timeliness. In addition, the use of conventional Hash chains has length limitation, so it is not easy to renew the authentication root of a Hash chain. That means the micro-payment protocols based on conventional Hash chains have low working efficiency and security. In response on the above problems, this thesis proposes a new micro-payment protocol based on self-updating Hash chains. A comparison between the proposed protocol and the NMP protocol shows that the former not only solve the latter's problems, but also improve efficiency and fairness. The analysis results show that the storage and communication load of the former is only 80 bytes longer than the latter, whereas the average computation efficiency of the former is 125 times higher than the latter under a transaction accomplishment of 10000 electron shares.

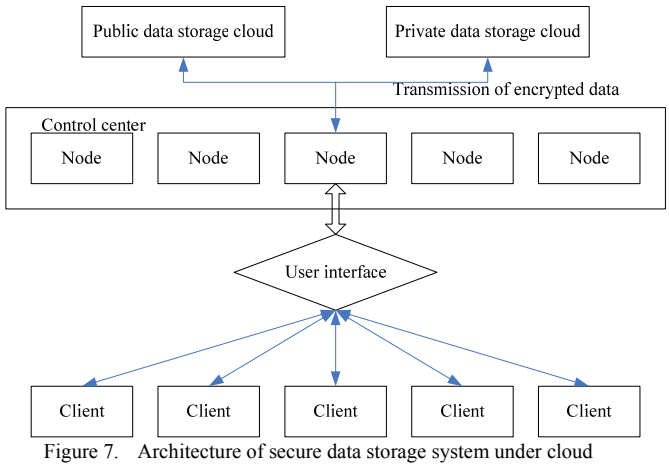

Figure 7. Architecture of secure data storage system under cloud computing environment.

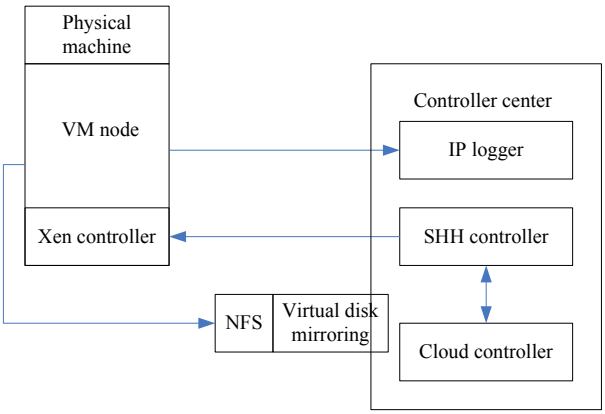

Figure 8. Relationship among cloud components

V. CONCLUSION

Cloud computing is characterized by high-performance, low costs and high storage capacity. Problems facing the security of data storage in cloud computing is becoming severer while cloud computing is advancing. This paper analyzed data security in cloud computing and found out that the problem is the concern of both private user and business user; it also studied the current research status of cloud computing data storage, and found out from the searching on CNIK that the subject is a hot study focus of experts and scholars; introduction of security strategy for safe data transmission and storage based on cloud computing was also made in this paper, showing that data encryption and decryption are the major measures of safe data transmission and storage; finally, the paper studies the structure model of cloud storage. In order to create a safer system, the design of secure data storage system model was made in this paper.

REFERENCES

[1] Chen Siluo, "The design and construction of distributed network security management platform". Beijing: Beijing University of Posts and Telecommunications,2008.

[2] Huang Decai,Qi Huachun, "The research of Page Rank". Computer Engineering, vol. 32, pp.145-146, 2006.

[3] Wangdong, Lei Jingsheng,Lizhuang, "The upgraded page sorting algorithm based on Page Rank". Computer Engineering and Design, vol. 29, pp. 5921-5923, 2008.

[4] Wang Xuesong, "Lucene+Nutch Search engine's development. Beijing". Post and Telecom Press, vol. 1, pp. 368-375, 2008.

[5] H. Ahn, K. Kim, "Bankruptcy prediction modeling with hybrid case based reasoning and genetic algorithms approach", Applied Soft Computing, vol.9, no.2, pp.599-607, 2013.

[6] W. He, Z. Wang, H. Jiang, "Model optimizing and feature selecting for support vector regression in time series forecasting", Neurocomputing, vol.72, no.1-3, pp.600–611, 2012.

[7] Cao, L., Tay, F., "Support vector machine with adaptive parameters in financial time series forecasting", IEEE Transactions on Neural Networks, vol.14, pp.1506–1518, 2013.

[8] Hastie, T., Rosset, S., Tibshirani, R., Zhu, J., "The entire regularization path for the support vector machine", Journal of Machine Learning Research, vol.5, pp.1391–1415, 2009.