

A Study on Security Technique of Cloud Data Processing in Electronic Commerce

Wei Dai¹, Xuefang Zhang^{*2} and Peng Hu³

¹*School of Economics and Management, Hubei Polytechnic University,
Huangshi 435003, Hubei, P.R.China*

²*School of Economics and Management, Hubei Polytechnic University,
Huangshi 435003, Hubei, P.R.China*

³*School of Mathematics and Physics, Hubei Polytechnic University,
Huangshi 435003, Hubei, P.R.China*

¹*dweisky@163.com*, ^{*2}*zxf1223@126.com (Corresponding Author)*,
³*penghuit@163.com*

Abstract

In the age of e-commerce, the issue of information leakage of internet users is a wide concern. The e-commerce enterprises should be prepared to deal with network data processing security, and to avoid various inconveniences led by the loss of data information. In this study, the "business to customer" (B2C) cloud data processing model is taken as an example to propose a security countermeasure for network data processing based on cloud computing platform. The cloud network computing model is adopted for the automated processing on B2C network data. Based on the network overlapping relationship and model settings, the security workflow of the cloud data computing processing is built. Moreover, the overlapping network plan and flow network technique are considered as the basis of the model, and a diversified security control platform is created by combining with modeling tools.

Keywords: *E-commerce, Cloud data, Information leakage, Security control*

1. Introduction

The global trade and economy is rising in recent years. Commercial trade has become the main trend of the market in many countries. Moreover, technology trade is the development trend of the global economic reform. This is due to the regional openness of Internet platform. Various types of commercial trade networks [1-4] have appeared on the Internet platform and promote the virtualization construction of economic transaction activities. As one of the earliest e-commerce platform in China, "business to customer" (B2C) has difficulty to get rid of customer information security risks in the long term, which has made massive leaks of customer information and brought about a plenty of transaction security issues. In order to promote the sustainable development of e-commerce websites, it is necessary to adopt new technologies to address the security issues of customer information and to create a safe and reliable internet transaction environment for both businesses and customers.

2. Current Status of Information Security of E-Commerce Websites

There are various factors leading to customer information leakage of e-commerce websites

based on B2C platform [5, 6]. A lot of B2C e-commerce websites do not pay sufficient attention to the confidentiality of customer information. Besides, the staff mobility of these websites is high, and hence there have already been plenty of customer information leakage cases caused by the staff of B2C e-commerce websites. The application field of e-commerce technology is gradually expanding, and the e-commerce networks are facing the situation of growing data traffic. Therefore, a single e-commerce platform can no longer satisfy the data processing requirements. As the host platform of e-commerce website, cloud computing network [7, 8] encounters different data operation problems when processing e-commerce data, thereby increasing the data information security risks.

3. Survey on Customer Information Leakage of Jingdong Mall

E-commerce is created in the context of virtualization of global commercial trade. Under E-commerce, the transactions are completed through browser or server. It can be seen from the incidents of customer information leakage of Jingdong Mall that the attacker directly extracted customers' personal information from the backstage of Jingdong, which means that there are two situations leading to such incident. The first one is that the attacker found the vulnerability of the web server and directly invaded the server to steal the customer personal information. The second is that before the attacker attacked the site, he found who wanted to attack the e-commerce website via an illegal underground industry chain like customer information trafficking, and then he sneaked into the company as an employee, worked for some time and stole customer information by setting the backdoor. The specific forms of loophole are shown in Table 1.

Table 1. Jingdong Mall Loophole Type Statistics

Loophole type	XSS scripting attacks	SQL injection	Command execution	Unauthorized access	Design flaw	Others
Percentage	25%	12%	8%	15%	15%	25%

So far, with the development of "business to customer", which is the earliest e-commerce model in China, it has great influence on commercial trade activities. The loophole types that result in the massive customer information leakage account for about 4% of the total. The first thing for Jingdong Mall to do to prevent customer information from being stolen is to find the loopholes of website in time and fix them immediately once they are found, so that the attacker would have no chance to steal the customer information. Today, personal information privacy is highly concerned by the public. Improving the security environment of customer information will bring a better development for the e-commerce websites on B2C platform.

4. Application of Computing Model of E-Commerce Cloud Network Security

The scale expansion of e-commerce websites has brought about a series of information security problems. The server of e-commerce website will lose the high efficiency data processing function when facing massive data information, and encounter a variety of obstacles in the deployment of information resources. Although domestic e-commerce has been divided into multiple patterns, information leakage is still the largest drawback during the popularization period of B2C websites. Retailers do not take sufficient countermeasures to protect customer information, which leads to the personal privacy of customers being stolen and lowers the information security of the customers [9, 10]. The network plan computing model utilizes the overlapping network relationship to provide a broader platform for cloud data processing, so that the operation risks of e-commerce network can be reduced.

4.1. Basic Model of Overlapping Relationship

Faced with a more open network market, the data security issue of e-commerce has attracted wide attention. Crisis of confidence is the outcome of these massive customer information leakage incidents. An automated processing can be implemented on business data based on network overlapping relationship, and provide a plenty of references for data resources deployment. If the overlapping network is chosen to solve the cloud data security issue, the specific circumstances of overlapping relationship must be first clarified. In this study, there are four basic overlapping relationships encountered by the sequence pair (i, j) with partially or completely continuous relationship.

4.1.1. Relation from Finish to Start (FTS): There is the relationship required of time distance LT from the finish of sequence i to the start of sequence j .

4.1.2. Relation from Start to Start (STS): There is the relationship required of time distance LT_i from the start of sequence i to the start of sequence j .

4.1.3. Relation from Finish to Finish (FTF): There is the relationship required of time distance LT_j from the finish of sequence i to the finish of sequence j .

4.1.4. Relation from Start to Finish (STF): It is the relationship required of time distance $LT_i + LT_j$ from the start of sequence i to the finish of sequence j , that is, it is required to complete after a time of LT_i from the start of sequence i , then after a time of LT_j for performing sequence j . The four types of relationship are shown as Table 1, and the combinations of them form more complicated overlapping relationships. The overlapping relationships could be applied to more complex types of processing operations on cloud data. The e-commerce enterprises should choose the data to process in accordance with the actual situation, thereby ensuring the reliability of e-commerce cloud data.

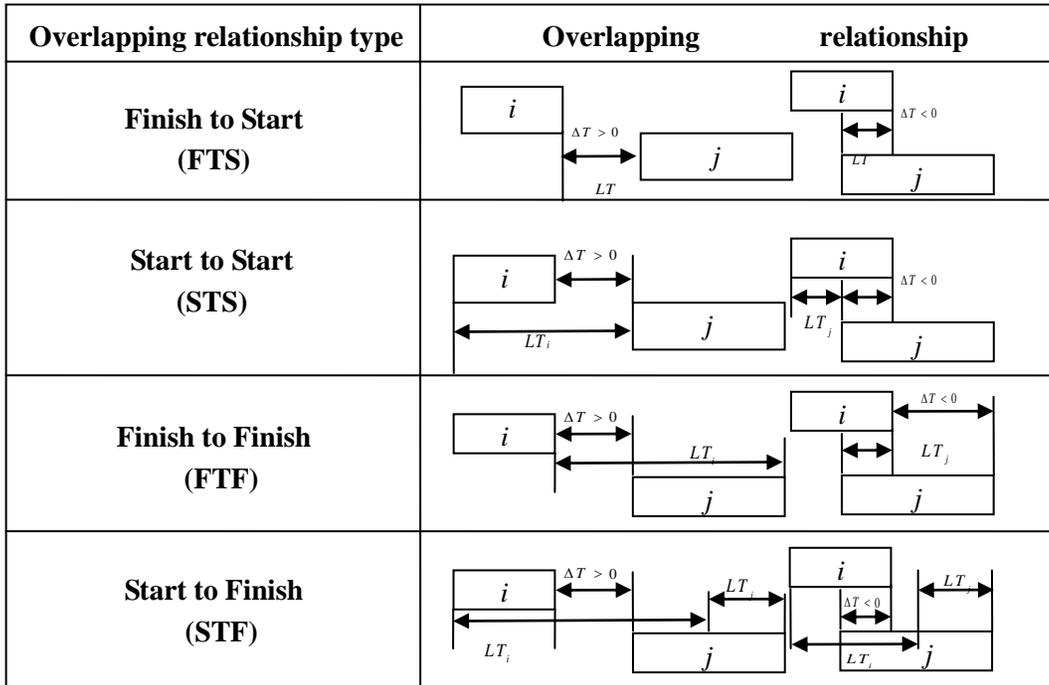


Figure 1. Overlapping Network Relationship

4.2. Delay Time Distance

The network model of the basic overlapping relationship is used, and the cloud data processing flow is relatively complex. There are two situations in the overlapping model of e-commerce cloud data processing: the first one is that the sequence j begins after sequence i finishes; the second one is that sequence j can start before sequence i finishes. Therefore, the time difference from the end of sequence i to the start of sequence j can be utilized to unify various overlapping relationships. The first step is to execute the overlapping. The time delay distance of overlapping sequence pair (i, j) is the time distance from the start of sequence j to the finish of sequence i , which is constrained by the overlapping relationship. It is denoted as $\Delta T(i, j)$. According to the definition, the calculation equation for time delay distance is:

$$\Delta T(i, j) = \begin{cases} LT & (FTS) \\ LT_i - t(i) & (STS) \\ LT_j - t(j) & (FTF) \\ LT_i + LT_j - t(i) - t(j) & (STF) \end{cases} \quad (1)$$

4.3. Relation between Three Network Plans

In order to get rid of the information leakage risks existing in traditional e-commerce

network, the cloud data processing can be based on overlapping network plan and the flow network plan is used as the computing model to help solve a series of security problems in the cloud data processing system. As shown in Figure 1, in overlapping network plan, when $\Delta T(i, j) \geq 0$, sequence i and sequence j does not overlap. When $\Delta T(i, j) < 0$, the two sequences begin to overlap. At this time, $|\Delta T(i, j)|$ is the time distance by which sequence j can start before finishing sequence i . The overlapping network plan is the network plan when there exists the sequence pair (i, j) for $\Delta T(i, j) \neq 0$. When $\Delta T(i, j) = 0$, it means that sequence j is immediately after sequence i in general situation. It is called general sequence pair in the following. The network plan is a general network plan when there is $\Delta T(i, j) = 0$ for all sequence pairs (i, j) . The flow network plan can be seen as an overlapping network plan with STS overlapping relationship between flow processes. The flow step distance is the overlapping time distance, and the corresponding delay time distance $\Delta T(i, j)$ is usually less than 0. Using the network overlapping relationship, the processing flow of e-commerce cloud data can be simplified. The overlapping network is used as the control center to execute data processing operations, thereby guaranteeing the safe use of e-commerce network data.

5. Security Control Platform Based on Framework Manager

For the data processing on e-commerce cloud data, both general network plan and flow network plan are special overlapping network plans, while the overlapping network plan and flow network plan are the extension of general network plan. B2C customer information leakage can cause a variety of abnormalities, and increase the risk of e-commerce websites, which is apparently not conducive to the sustainable development of the new industry. Cloud computing is the improvement of internet-related service. It can provide more network services according to user requirements and to specific time. It focuses on treating the service issues related with the control of virtualized resource.

5.1. Modeling Cloud Data Security

As an important reporting tool in the industry, Cognos for cloud data security modeling is also used in the security processing of e-commerce cloud data, thus enhancing the reliability of B2C data. In the process of creating data model with Cognos Framework Manager [11], by introducing different user groups or roles, different data security access levels are set for the same query object. Therefore, different user groups are allowed to access different data subsets of the same query object. Framework Manager is a client-based modeling tool of Cognos, as shown in Figure 2. The model is a set of related objects associated with each other, and can configure the reporting form for e-commerce data and reflect the authenticity of data information objectively.

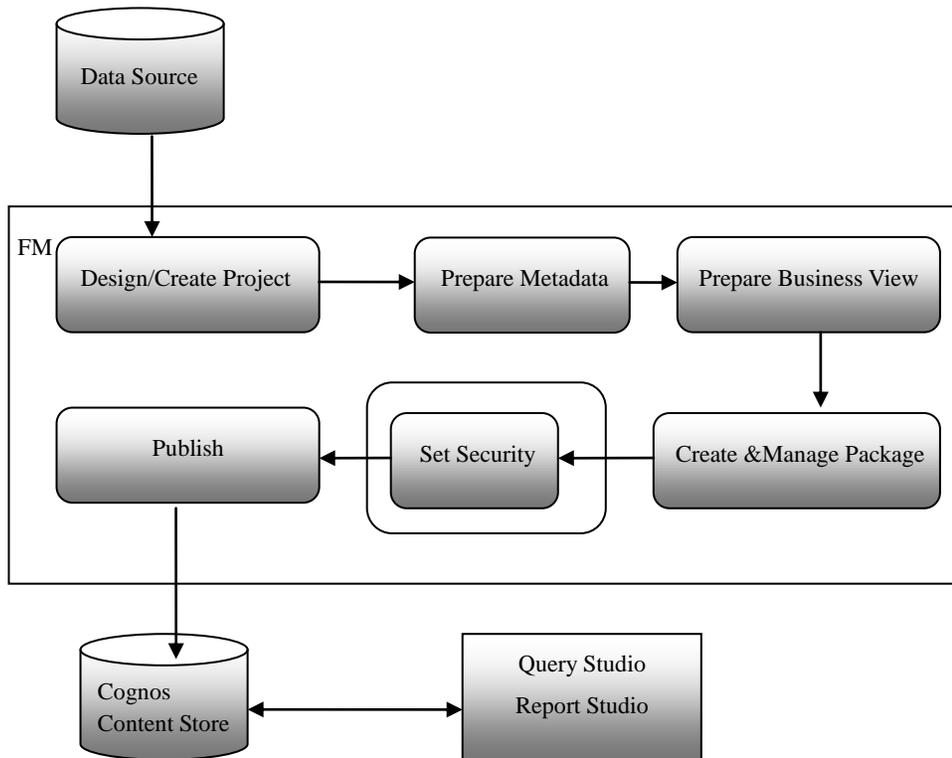


Figure 2. Framework Manager Workflow

In Framework Manager, security control is a method to control the access to Cognos product data and metadata. If it is set to be safe in FM, then access by selected users, user groups or roles to the content is controlled. The security control in FM can be divided into three types.

5.1.1. Data Security: It is used to constrain the returned data, which is used in specific query object. When the report developer is developing the report based on the query object, which data is returned to the customer is controlled.

5.1.2. Object Security: According to the setting, the users have access to one object, or do not have access to an object, or one object is hidden from some users. The object here refers to the query object, query term or filter criteria.

5.1.3. Packet Security: The packet security in FM means that whoever has the authority to use the packet in Cognos Studio (QueryStudio, ReportStudio *etc.*) or whether there is the authority to operate a report using the packet in Cognos Connection.

5.2. Cloud Technology Application

In the customer information leakage incident of Jingdong Mall, although the customer information is not stolen directly from the target website, it may be indirectly accessed by coincidence due to the connectivity of internet. The automatic detection of program code stored in cloud database can be used to actively give an alarm when discovering abnormal data to remind the users to re-examine the data to perform a

second transfer command. Hybrid cloud is a comprehensive type of e-commerce. The technique has a higher operating efficiency in cloud computing processing and can execute data security processing, which helps the users detect the security factor of the collected data. These are key issues of consideration when creating modern e-commerce.

6. Conclusions

In this study, the objective is to study the customer information security of e-commerce website based on B2C platform. By analyzing the countermeasures for protecting the customer information of the existing e-commerce websites based on B2C platform, the possible risks of actual application are pointed out. The work provides a reliable guidance for ensuring customer information security and for completing the management system of customer information in e-commerce websites based on B2C platform. Using SPI interface technology in e-commerce cloud data processing can build diversified cloud data processing model for users, and satisfy all requirements of deployments and utilization of e-commerce data resources.

Acknowledgements

This study has been financially supported by Humanities and Social Science Youth Fund Project of Ministry of Education (No.13YJCZH028).

References

- [1] R. B. Li, J. Y. Liu, S. Yuan and Y. L. Du, "Study on Application Software Update of the Micro-Navigation Computer by Serial Port", *Mini-micro Systems*, vol. 12, no. 10, (2010), pp. 3-4.
- [2] N. He, W. M. F. Yun, C. P. Liu and J. Pei, "Research on Sensor Technology Face to Wireless Sensor Network", *Computer Applications and Software*, vol. 19, no. 10, (2011), pp. 32-33.
- [3] P. Li, L. K. Zeng, A. Z. Shui, X. L. Jin, Y. C. Liu and H. Wang, "Design of Forecast System of Back Propagation Neural Network Based on Matlab", *Computer Applications and Software*, vol. 17, no. 6, (2010), pp. 12-14.
- [4] B. L. Shi and W. Wang, "The Survey of the Research on Data Warehouse and Data Mining", *Computer Applications and Software*, vol. 15, no. 11, (2009), pp. 8-10.
- [5] J. H. Chen, "Network Security Data Transfer Method Research Based on Cloud Computing", *Computer Simulation*, vol. 29, no. 8, (2012), pp. 139-141.
- [6] Z. B. Gan, C. Zeng, K. Li and J. J. Han, "Construction and Optimization of Trust Network in E-Commerce Environment", *Chinese Journal of Computers*, vol. 35, no. 1, (2012), pp. 7-37.
- [7] L. Xu, Y. Y. Zhang, J. Wu and B. Y. Fang, "Network technology research under cloud computing environment", *Journal on Communications*, vol. 33, no. 1, (2012), pp. 16-221.
- [8] M. M. Fu, "Application of Fuzzy Comprehensive Analysis to Information Security Evaluation", *Journal of Southwest Jiaotong University*, vol. 45, no. 3, (2010), pp. 440-444.
- [9] D. P. Zhang, K. Cai, M. Zhang and Z. Xu, "The Research of Cloud Computing Data Security Support Platform Architecture", *Journal of Computer Research and Development*, vol. 48, no. S3, (2011), pp. 261-267.
- [10] C. F. Yang, G. Wang and J. H. Si, "Build New Generation EAI Based on SOA", *Computer Applications and Software*, vol. 22, no. 10, (2005), pp. 122-123.
- [11] "IBM Cognos&Business Intelligence", <http://publib.boulder.ibm.com/infocenter/cogic/v1r0m0/index.jsp>, (2010).

Authors



Wei Dai, he received his M.S.E. in Computer Science and Technology (2006) and PhD in Computer Application Technology (2012) from Wuhan University of Technology. Now he is full researcher of informatics at Economics and Management Department, Hubei Polytechnic University. His current research interests include different aspects of Intelligence Computing and Information Systems.



Xuefang Zhang, she received her B.B.M. in Finance (2004) and M.Ec in Industrial Economics (2007) from Huazhong Agricultural University. Now she is full researcher of informatics at Economics and Management Department, Hubei Polytechnic University. Her current research interests include different aspects of Financial Engineering and Information Computing.



Peng Hu, he received his B.S. in Mathematics (2003) from Hubei Normal University and M.Sc. in Information Sciences (2010) from Hubei University. Now he is full researcher of informatics at Mathematics and Physics Department, Hubei Polytechnic University. His current research interests include different aspects of Artificial Intelligence and Information Coding.