Risk Management Of E-Commerce Security In Cloud Computing Environment

Yan Li*, Junfeng Li

Jiangxi Science and Technology Normal University, Nanchang, China
*corresponding author's email: Hanter3@163.com

***Abstract*—The emergence of cloud computing technology has changed the traditional business economic model and provided convenience for the application of e-commerce in the financial field. This paper uses cloud computing as the entry point to analyze the security of e-commerce in a cloud computing environment in detail. It also proposes relevant solutions to how e-commerce can ensure the security of its own data in the context of cloud computing. At the same time, it also pays attention to reducing the user's perception of information security risks from the user's perspective, and improving the user's trust, satisfaction and loyalty to the information system.**

Keywords: cloud computing, e-commerce, risk management, security

I. INTRODUCTION

The emergence of cloud computing technology is considered to be a new generation of technological revolution, which has a great impact on the business model and business processes of enterprises. With cloud computing, enterprises can obtain fast, efficient, secure, and reliable cloud services at a lower cost, which allows enterprises to have great flexibility and powerful data processing capabilities. However, compared with the traditional Internet environment, the information security risks in the cloud computing environment are more complicated, and many security risks have emerged. When a customer uses cloud computing, he cannot know exactly where his data is stored or even in which country. The form of data stored in cloud computing is usually all customer data sharing methods, and there is a risk of isolation between customers and between customer data. When catastrophic events occur, customers' data and services will be more difficult to protect and recover. Because there are fewer methods for quantifying information security risks in the cloud environment, a cloud risk analysis and quantification method is proposed based on fault tree and Monte Carlo simulation for the cloud computing environment. For a certain risk in the cloud environment, a fault tree is used to build the relationship between risk and risk factors. The assignment of risk factors uses a probability distribution. The probability distribution of risk results is obtained by Monte Carlo simulation. The inverse cumulative distribution function shows the probability of exceeding a given risk cost. The advantage of this method is that instead of assuming a specific value for the risk factors, it assumes a certain probability distribution. Through the Monte Carlo analysis, the ranking of the risk factors can be known to better control the risk. The probability of this risk helps the enterprise to make risk decisions.

II. INFORMATION SECURITY RISKS IN A CLOUD COMPUTING ENVIRONMENT

Data security protection is a very important point in cloud computing and service providers are on highly integrated, cross-region large-capacity storage space. In cloud computing mode, data protection includes data storage locations, data isolation, and data disaster recovery. Customers are not sure which server their data is placed on, and cloud computing service providers cannot ensure that corporate data is not leaked. In such an environment of data storage resource sharing, even if an encryption method is adopted, cloud computing service providers cannot guarantee effective isolation between data. In addition, when a system failure occurs, cloud computing service providers cannot guarantee the rapid recovery of corporate data.

When e-commerce companies transmit internal data through the cloud computing function, they mainly receive and process data through the cloud computing service provider. Generally, the private data of an enterprise's internal data set is stored in the relevant storage space under cloud computing. These enterprise data centers mainly perform two major tasks. One is to ensure the security of enterprise data during transmission. Strictly screen enterprise data transmission and receive and store it to prevent data leakage. The second is to provide convenience for enterprises to conduct data inquiry and meet the requirements of enterprises for data access.

Cloud computing service providers need to provide relevant information support while not bringing risks to the enterprise's data calculations. All data of the enterprise is stored in the cloud, and these data may be distributed in different regions or countries. There may be differences and legal disputes between local governments in terms of information security supervision, etc. The security and accuracy of the data will be audited. This exists a certain degree of security risks.

The browser is the main client of cloud computing services. Most of the enterprise's work is done in the browser, but currently almost all browsers have vulnerabilities. When the user's technology is not strong and the protection awareness is not high, it can be easily planted with Trojans and viruses. These software vulnerabilities increase the risk of end-user attacks and affect the security of cloud computing in e-commerce applications.

III. E-COMMERCE RISK ASSESSMENT METHOD

A. Qualitative analysis method

The appropriate evaluation method needs to be selected according to the specific system object.

2157-1481/20/$31.00 ©2020 IEEE
DOI 10.1109/ICMTMA50254.2020.00172

Scientific and reasonable assessment methods can make the results of risk assessment more credible and make the results more accurate. Evaluation methods can be divided into three categories according to the principle of qualitative or quantitative: qualitative analysis method, quantitative analysis method, and the combination method. The most commonly used method is the qualitative analysis method, because this method requires the analyst's experience, knowledge, and even intuition in the classification of the risk assessment element size or level. This method is highly subjective. The interview results of the interviewees are carried out, and the theoretical derivation and frame analysis are carried out accordingly. The survey results are obtained through the coding of the surveyed data. Common qualitative analysis methods are: expert scoring method, fault tree analysis method, event tree analysis method, causal analysis method, safety checklist method, etc. Compared with the quantitative analysis method, the qualitative analysis method is easier to operate and can dig out some ideological content to make the evaluation result more comprehensive and profound. However, the discrepancy in the subjectivity of the appraiser's experience and knowledge may cause the analysis results to be inaccurate. At the same time, the method requires relatively higher appraisers.

B. Quantitative analysis method

Quantitative analysis method is to use mathematical indicators to assign risk factors, and use numerical analysis to effectively assign the potential loss level of the system, so as to comprehensively evaluate the security risks of the system by integrating indicators from various aspects. The entire risk process is quantified, including asset value, the severity of the threat, the possibility of the vulnerability being exploited, and the impact of the established security measures, etc. are given a reasonable amount of value to judge the level of risk . Common quantitative analysis methods include: factor analysis, cluster analysis, time series models, neural networks, grey correlation analysis, and risk models based on complexity theory. Quantitative analysis method is characterized by accurate calculation and grading of risks, but it is difficult to guarantee the accuracy of the index data in the process of quantitative analysis. For complex systems, the amount of calculation for quantitative analysis is huge, and the calculation process is prone to errors, making it difficult to implement quantitative analysis.

C. Comprehensive assessment method

Qualitative analysis and quantitative analysis have different emphasis on accuracy and precision. The former has high accuracy but lower accuracy, and the latter has higher accuracy but lacks certain accuracy. The calculation amount of the two is also very different, so the quality requirements of the evaluator are also different. Although the calculation amount of the former method is not large, the requirements of the evaluator's ability are high. The quantitative analysis calculation process is complicated and the calculation amount is huge. The results of Qualitative analysis are relatively more subjective, while the results of quantitative analysis are relatively objective and the observations are more intuitive. When assessing the risk of a complex information system, a comprehensive assessment method combining quantitative and qualitative measures is usually used. The environment of the information system in the actual evaluation process is relatively complicated, and many factors are involved. It is necessary to solve the information security problem under the condition of multi-attribute decision making. This requires that while considering factors such as the length of time to process security events, whether the load is balanced, and the like, an effective solution can be determined that can not only meet the guarantee of quality, but also handle security events with the highest efficiency and lowest cost. In the evaluation process, judgment factors are generally extracted from actual system applications. These indicators may have contradictions in the process. In practice, the quantitative description of indicators is often difficult to define, and direct and accurate comparison and analysis between different indicators is not possible. Therefore, it can only be evaluated based on experience and knowledge. Simply using qualitative or quantitative analysis methods cannot effectively evaluate system security, so the current assessment of information system security mostly uses a combination of quantitative and qualitative comprehensive evaluation methods.

D. Risk assessment process

The process of risk assessment includes: assessment preparation, asset identification, threat identification, vulnerability identification, security measure confirmation, risk analysis calculation, and risk assessment result document. Threat source has various attributes such as threat subject, resource, motivation, and approach. The content of the threat can be specifically described from these different attributes. From the perspective of the source, threats can be divided into human factors and environmental factors. The different motivations of threats divide human factors into malicious and non-malicious ones. From the perspective of environmental factors, threat factors can be divided into force majeure factors and physical factors. Threats can directly or indirectly attack information systems, damaging the integrity, confidentiality, or availability of the system. It may also be an incidental or deliberate event. Before categorizing threats, you should consider the source of the threat, and then categorize the threat according to its source in its manifestation.

IV. Risk management process

The related concepts of risk can be divided into several types: (1) risk is the possibility of loss; (2) risk is a calculation of the size of the possible loss; (3) Risk is the magnitude of possible consequences and losses. Although these definitions are different, in summary, the composition of risk can be summarized into the following three factors: potential loss, the size

of the loss, and the uncertainty of the loss. Risk analysis is to identify and estimate the risks existing in a project or event. It is an important step in risk management. Risk analysis includes risk identification and risk estimation. Risk identification refers to the risk of a given project or event, all the risk-producing factors identified, risk estimation is through the relevant theory to calculate the probability of the risk and the risk of the possible loss, so as to obtain the risk value of the event.

Risk management is the process by which managers take appropriate risk control measures through analysis and assessment of risks. The process of keeping risk within the reach of the enterprise at an acceptable cost. The process of risk management, as shown in Figure 1. Risk management processes are divided into two main components, risk assessment and risk control, which can be broken down into sub-processes.

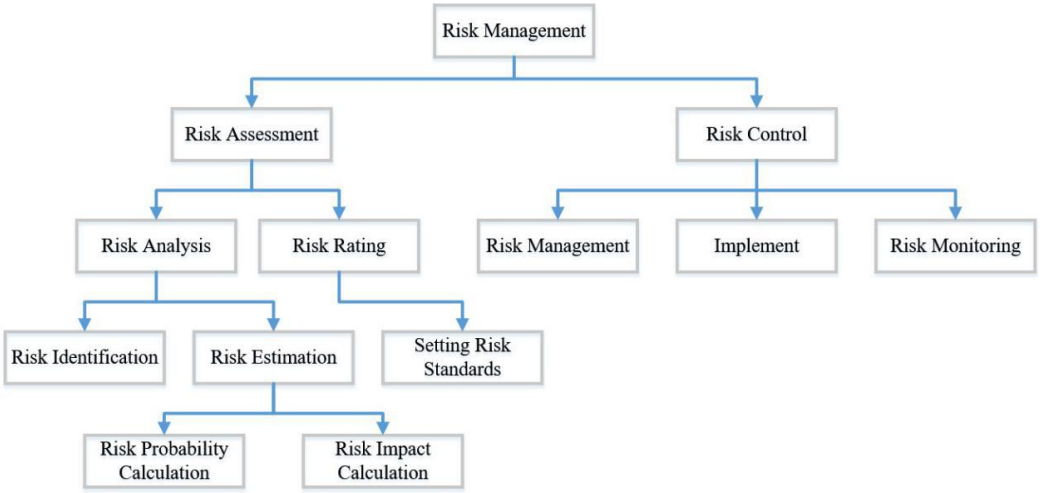

Fig.1 Risk Management Process Map in Cloud Environment

V. Conclusion

In the cloud computing environment, the user's perception of information security risk is also changing and deepening gradually, and the user's perception of information security risk has become an important factor in the user's willingness to use the information system. The research of this paper emphasizes that enterprises should combine information security risk analysis with information security risk awareness when carrying out information security risk management, and study the model of information security risk assessment and risk decision-making. In view of the mutual impact of information security risk factors, the paper puts forward the information security risk assessment model based on network analysis method which is not only beneficial to enterprises to grasp the size of internal information security risks, and reduce the loss of enterprise information security risks. At the same time, the user's information security risk awareness is reduced from the user's perspective. This paper analyzes the cloud computing architecture, analyzes the information security risks of cloud computing, and puts forward a risk management method based on cloud risk analysis.

Acknowledgements

This paper is the result of the 2018 scientific and technological research project of Jiangxi Provincial Education Department, "Construction research on the security risk assessment model of e-commerce in cloud computing environment" (project number GJJ180604)

References

[1] Zhang X, Wuwong N, Li H, et al. Information security risk management framework for the cloud computing environments[C]//2010 10th IEEE international conference on computer and information technology. IEEE, 2010: 1328-1334.

[2] Townsend M. Managing a security program in a cloud computing environment[C]//2009 Information Security Curriculum Development Conference. ACM, 2009: 128-133.

[3] Juncai S, Shao Q. Based on Cloud Computing E-commerce Models and ItsSecurity[J]. International Journal of e-Education, e-Business, e-Management and e-Learning, 2011, 1(2): 175.

[4] Saleh A A E. A proposed framework based on cloud computing for enhancing e-commerce applications[J]. International Journal of Computer Applications, 2012, 59(5).

[5] Labuschagne L, Eloff J H P. Electronic commerce: The information-security challenge[J]. Information Management & Computer Security, 2000, 8(3): 154-157.

[6] Udo G J. Privacy and security concerns as major barriers for e-commerce: a survey study[J]. Information Management & Computer Security, 2001, 9(4): 165-174.

[7] Ngai E W T, Wat F K T. Fuzzy decision support system for risk analysis in e-commerce development[J]. Decision support systems, 2005, 40(2): 235-255.

[8] Warren M, Hutchinson W. A security risk management approach for e-commerce[J]. Information management & computer security, 2003, 11(5): 238-242.

[9] Zhou Z, Hu C. Study on the e-government security risk management[J]. International Journal of Computer Science and Network Security, 2008, 8(5): 208-213.

[10] Palmer M E, Robinson C, Patilla J C, et al. Information security policy framework: best practices for security policy in the e-commerce age[J]. Information Systems Security, 2001, 10(2): 1-15.