SURVEY OF E-COMMERCE SECURITY MEASUREMENT AND RISK ANALYSIS

Rijvan Beg*
R. K. Pateriya**

Abstract

With the hasty development of E- commerce, Security, issues are arising from people's attention. Electronic commerce services have risen to become more and more well-liked and web environment. Exchange security on network is very important for e-commerce services and it is always the key factor that affects the accomplishment of electronic commerce (e-commerce). In detail two kind of risk analysis methods of the e-commerce security which gauge and assess the e-commerce security risk. And then the risk management strategies of e-commerce security of the e-commerce are addressed. In the end it is pointed out that the study of the risk analysis methods and the management strategies provides an available security framework. This paper present risk analysis measurement and approach for e-commerce. This paper also covers security issues in commercial activities.

KEYWORD: e-commerce; security analysis; CIM model; Fuzzy logic, security issues.

1. Introduction: With the energetic development of internet technology, e-commerce came into being and prompts growth which based on the network and multimedia technology. The e- commerce is through public network, such as internet, open computer network to conduct online transactions, which can fast and effective to implement multiplicity of business process [2].

With the online business enlargement of e-commerce, e-commerce security becomes more and more marvelous. How to create the safe and expedient e-commerce application environment and provide the strong protection of information security has become a spotlight of e-commerce [1].

E-commerce is faced with various risks. The materialization of e-commerce may not only exaggerate the occurrence possibility and the dent of various types of risks, but also bring new risks in the area of financial services. With observe to e-commerce risk management of e-commerce, the western developed countries by research and practice, have accumulated rich experiences and a lot of standardized norms, however, the research and practice of e-commerce risk management in e-commerce are relatively backward [3].

2. Problem Faced in E-Commerce: Appropriate to the complexity and vulnerability of the internet, the development of e-commerce based on internet is faced with serious security problems. Usually, there are several kind of security risks as follows [5-6].

- Information Tempering: By a variety of technical ways and means, network attackers usually tamper with and destroy the internet software make the information system fail, and they also often copy, tamper with, delete or insert transmitting information in order to undermine the integrity of information.

*CSE Department, Moulana Azad National Institute of Technology, Bhopal

- Data Access Risk.: Data access risk primarily is the result of both the data revision and deletion from the unauthorized access to the database system and the operational mistakes of the staff in the e-commerce [1].
- Fake Information: When attacker master the law of network information and decrypt business information of banks, they can become justifiable users of imitation or use fake information to betray other users [1].
- Online Payment Risk: Online payment has always been regarded as the most decisive factor restricting the e-commerce development of banks, because many customer worry about the security and snub to use online payment [1].
- Security Issue Related to E-commerce: With survey to the security of e-commerce applications, it s useful to discern between client –side security issue, server-side security issue, and transaction security issue. In this section, I will take the security system in online banking for example [3].

A. **Client** –side Security Issues: From the user's point of view client-side security is emblematic the major concern. In general client-side security requires the use of traditional computer security technologies, such as proper user authentication and authorization, access control, and antivirus protection. With observe to communication services, the client may furthermore require server authentication and non repudiation of receipt [3]. In addition, some applications may require anonymity (e.g. anonymous browsing on the web). Following figure 1 is the survey of customer access online banking security setting in banks.

Client Terminal / Banks	Account Information input area	Cipher Information input area	Cipher Verification
Industrial and E-commerce of India	General Control	Security ActiveX Control	Yes
Agriculture Bank of India	General Control	Security ActiveX Control	Yes
Bank of India	General Control	General Control	No
Transportation Bank of India	General Control	Security ActiveX Control	Yes

Figure 1. Data based on Indian online banking webpage access test. 2007[3]

data analysis show that the client-side security protection for online banking dose need improvement. Most banks use single cipher security setting system is vulnerable to virus and cyber attacks. One of the important characteristic of online banking is that it can offer safe and personalized customer service anytime, any wear and anyhow. With out sound security protection will cause online banking transaction fail. Client-side safety protection is weakest part of online banking service providers[3]. The application of encryption to provide authentication and privacy of online transaction, cryptography provides the basis for achieving access control, transaction authorization data integrity and accountability.

B. Server-side Security Issues: Divergent to that, server-side security is typically the major concern from the service providers point of view. Server-side security requires proper client authentication and authorization, non- repudiation of origin, sender anonymity (e.g., anonymous publishing on the web), audit trail and accountability, as well as reliability and availability

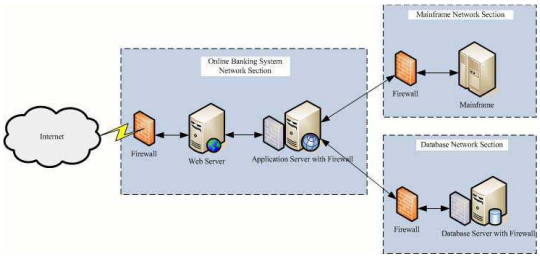

Figure2. Firewall of online banking system

C. Transaction Security Issues: Transaction security is equally important for both the client and server side. Transaction security requires various security services, such as data authentication, access control, data confidentiality, data integrity, and non-repudiation services. In addition, certain application may also require transaction anonymity guaranties [3]. Figure shows the data process of online banking system.

3. Approach Used For Security Measurement and Risk Analysis: With a variety of qualitative and quantitative methods, the risk analysis determines the importance of elements of e-commerce security risks, and assesses its impact on all aspects of the e-commerce system, so that staff of the e-commerce project implementation can focus on major risks, and control effectively the e-commerce system risk as a whole, two types of risk analysis methods are discussed in the following.

A. Risk Matrix: Risk matrix is the most direct and effective way of risk analysis. The occurrence probability of risk and the loss of assets are respectively regarded as the levels of rows columns, with the degree higher, high, medium, low, and lower. The number at the cross of the matrix shows the risk. Supposing that risk probability and loss degree are in the lower order from 10 to 0, respectively 10, 8,6,4,2, then the risk is the product of two factors. Risk analysis matrix is shown in TABLE I.

RISK ANALYSIS MATRIX

PROBABILITY / LOSS DEGREE	HIGHER	HIGH	MEDIUM	LOW	LOWER
HIGHER	10,10	10,8	10,6	10,4	10,2
HIGH	8,10	8,8	8,6	8,4	8,2
MEDIUM	6,10	6,8	6,6	6,4	6,2
LOW	4,10	4,8	4,6	4,4	4,2
LOWER	2,10	2,8	2,6	2,4	2,2

B. Risk Analysis Based on CIM: **Fuzzy logic** is a form of multi-valued logic derived from fuzzy set theory to deal with reasoning that is approximate rather than precise. In contrast with "crisp logic", where binary sets have binary logic, the fuzzy logic variables may have a membership value of not only 0 or 1 – that is, the degree of truth of a statement can range between 0 and 1 and is not constrained to the two truth values of classic propositional logic.[1] Furthermore, when linguistic variables are used, these degrees may be managed by specific functions.

Fuzzy logic emerged as a consequence of the 1965 proposal of fuzzy set theory by Lotfi Zadeh. Though fuzzy logic has been applied to many fields, from control theory to artificial intelligence, it still remains controversial among most statisticians, who prefer Bayesian logic, and some control engineers, who prefer traditional two-valued logic.

1). Trapezoidal fuzzy number: In the domain X, the trapezoidal fuzzy number is as follows:

$$A^{*}(x)=\begin{cases}\dfrac{x-a}{b-a}, & a\le x\le b\\ 1, & b\le x\le c\\ \dfrac{d-x}{d-c}, & c\le x\le d\\ 0, & \end{cases}$$

2). CIM Model: CIM model (control interval and memory model) is a kind of risk analysis model put forward by American scholars coopor and chapman. There are two types: the serial response model and the parallel response model, which were respectively the serial or parallel some of variable probability distribution [1].

If an event has n risk factors and the occurrence of each factor will separately influence the event, then the probability distribution model with n risk factors is called parallel response model[1].

3) E-commerce Risk Assessment of E-commerce Based on CIM mode: The is indicated by a function of the probability of risk event and its impact, that is, R=f(P,I), where R shows risk, P the probability of risk event, I the impact of risk incidents. In view of the characteristic of all risk factors in e-commerce of e-commerce, the CIM model is applied to e-commerce risk assessment of e-commerce as follows:

A) Constructing risk factor sets and judgment sets: Risk factor sets and judgment sets of bank e-commerce are constructed, and different judgment sets can be established for the occurrence probability of risk factors and the impact of risk factors. Assumption that the risk factors set is Fi = (f1,f2,…….,fn), i= 1,2,3 and the judgment set is J = (j1,j2,……,jm), the qualitative comments in the judgment set are expressed by trapezoid fuzzy number.

B) Quantifying the fuzzy evaluation of risk factors: The expert evaluation method is used to determine fuzzy evaluation of the judgment set of the occurrence probability of risk factors and the impact of risk factors of e-commerce. Fuzzy evaluation of risk factors by the fuzzy way is processed to get the probability distribution range and the impact distribution range, at the same time calculate expectation of individual risk factor judging the individual risk factor[1].

C) CIM Calculation: CIM model is used to calculate the probability distribution range and the impact distribution range of all types of e-commerce risks of e-commerce, by which the expectation of the overall risk can be calculated to assess the e-commerce risk of e-commerce [1].

4. E-Commerce Risk Management Strategies of E-Commerce's: Because of the importance of e-commerce security, it is necessary for e-commerce to be provided with the complete and effective e-commerce risk management strategy to forecast and control effectively the risk which e-commerce probably are confronted. The strategies mainly include the following [1].

A. Physical Security: Physical security is a prerequisite for the security of e-commerce systems. It can protect computer system, e-commerce server, and communication links and so on from the various risks.

B. Virus Surveillance: The firewall technology can provide the security, control and identify the accesses to a variety of sites, and it also does a good job in the regular detection of virus, the antivirus, and the dynamic guard.

C**. Data Defense:** For many e-commerce carrying out a e-commerce, the data are their important assets, so the steal or damage of the will lead to irreparable losses. Therefore, it is of great significance for the security and the operation of e-commerce system to strengthen protection of e-commerce transaction and related data[1].

D. Application Defense: Strengthening the application is an integral part of the security model. As strengthening the protection of the operating system can only offer some protection, the developers of e-commerce system have the responsibility to join protection into application in order to provide regions visited by applications with special protection[1].

E. Establishment of Internal Control System: The internal control system mainly consist of the organizational control system, the control system of development and maintenance, data access control and backup system, application control system, and daily management system. At the same time, the security audit is applied to the comprehensive assessment of the security of e-commerce system of e-commerce and the prediction of e-commerce risk in order

that e-commerce are directed to improve the safety measures, and the emergency mechanism to deal with the risk.

F. Personnel Training: The e-commerce implementation of e-commerce needs a large number of human resources with computer network knowledge and business knowledge and laws and regulations, so e-commerce should recruit or train this kind of talents to promote the rapid development of e-commerce.

G. Improvement of Management Strategies: With the information system audit and the external evaluation of information security, e-commerce must create condition to strengthen the collaboration between risk management department and e-commerce sector and take some measures to improve the status of all kind of risks. E-commerce must attach importance to the unified measurement of the traditional financial risk and e-commerce security risk, and constantly improve the ability to control the overall risk of the risk management department.

5. Conclusion: In this paper we have study of various e-commerce security measurement and risk analysis such as CIM model and risk matrix. But also suffered some security problem such as accuracy of matrix values, also observed some heavy computational in security measurement. Now we have proposed a new technique for risk measurement of e-commerce

6. References

1. Li Bo, Xu Congwei, (2009) "E-commerce Security Risk Analysis and Management Strategies of Commercial Bank", international forum on information technology and application, ieee computer society.
2. Yuanqiao Wen, Chunhui Zhou, Juan Ma, Kezhong Liu, (2008) "Research on E-Commerce Security Issues", international seminar on business and information management, ieee computer society.
3. Lu Tao, Lei Xue, (2007)" Study on Security Framework in E-Commerce".
4. Wang Liping, (2007) "Study of the Electronic Business Security Risk Management in E-Commerces", journal of Zhongnam university of electronic and law, (1) pp,75-78.
5. Luis Navarrow, (2001) "Information Security Risk and Managed Security Service", information security technical report, 6(3) pp. 28-36.
6. B. Fernandez-Muniz, J. M. Montes-peon, C. J. Vazquez-ordas, "Safety Management System: Development and Validation of Multidimensional Scale", Journal of Loss prevention in the process industries, no.20, 2007, pp. 52-68.
7. Nie Jin, Lei Xue (2006) "Chiness Online Banking Security Analysis". The fifth wuhan international conference on e-business. Volume I, pp. 662-665.
8. China Internet Network Information Center, The eighteenth statistics reporter of the development Chinese internet, jan. 2006.
9. China internet network information center, (2007) the nineteenth statistics reporter of the development Chinese internet.