Hindawi
Mobile Information Systems
Volume 2022, Article ID 9935244, 8 pages
https://doi.org/10.1155/2022/9935244

Research Article

E-Commerce Network Security Based on Big Data in Cloud Computing Environment

Yifu Zeng,[1,2] Shuosi Ouyang,[3] Tuanfei Zhu,[1,2] and Chuang Li[4]

[1] *College of Computer Engineering and Applied Mathematics, Changsha University, Changsha 410022, Hunan, China*
[2] *Hunan Province Key Laboratory of Industrial Internet Technology and Security, Changsha University, Changsha 410022, Hunan, China*
[3] *School of Accounting, Hunan Vocational College of Commerce, Changsha 410205, Hunan, China*
[4] *School of Computer Science, Hunan University of Technology and Business, Changsha 410205, Hunan, China*

Correspondence should be addressed to Shuosi Ouyang; z20190823@ccsu.edu.cn

Received 21 April 2022; Revised 10 June 2022; Accepted 27 June 2022; Published 31 July 2022

Academic Editor: Yanyi Rao

The popularization and development of big data and cloud computing in e-commerce still face a series of problems, among which the most prominent one is security. How to establish an effective risk assessment system in the cloud computing environment is the primary concern of e-commerce enterprises. This article mainly discusses the network security of e-commerce based on big data in cloud computing environment. Because the servers of the cloud computing platform are deployed on a global scale, all the above nine processes can be carried out in real time, thereby improving the operational efficiency of the enterprise. Moreover, in large-scale e-commerce applications, according to probability statistics, the distribution of all these process steps must be uniformly distributed. Cloud computing is the commercial realization of computing resources, which is essentially a producer-consumer model. Cloud computing can balance the load to the greatest extent and solve various inconsistencies that may exist in the process of data processing. Balanced conflict greatly improved the solution. The speed, at which the case process runs, maximizes the potential of cloud computing on a commercial level. This article makes an effective investigation of information assets in various aspects. In this article, the comprehensive risk value of the system was calculated as 4.4. According to the risk level, this article sets up the electronic commerce system's physical security and access and data backup control vulnerability to resolve problems; another big data reflect is also not allowed to ignore. In view of these problems, this article proposes corresponding improvement strategies responsibility allocation.

1. Introduction

Cloud computing platform, also known as cloud platform, refers to services based on hardware resources and software resources, providing computing, network, and storage capabilities. In the implementation platform of cloud computing, two are currently more popular. One is Google's own MapReduce, Bigtable, and GFS; the other is a Hadoop system, implemented by borrowing Google's technology, including the corresponding MapReduce, Hbase, and HDFS.

The realization of cloud computing relies on software and hardware platforms that can realize virtualization, automatic load balancing, and on-demand. The providers in this field are mainly traditional leading software and hardware manufacturers, such as EMC's VMware, RedHat, Oracle, IBM, HP, and Intel. The main features of these companies' products are flexible and stable cluster solutions and standardized, inexpensive hardware products. Therefore, e-commerce security is not only a network security issue, but also a commercial security issue [1, 2]. E-commerce security is a multidisciplinary discipline that includes not only technologies related to cybersecurity, but also technologies related to commercial security [3]. With big data and cloud computing becoming the mainstream of information technology [4, 5], researching e-commerce security in big data and cloud computing environments has become an urgent academic task [6, 7]. The main concern of commercial transaction security is the various security issues arising [8, 9], which are virtually inseparable and complementary. Without the foundation of cybersecurity, the security of commercial transactions is like a castle in the air; there is nothing to talk about [10, 11]. Commercial transactions are not secure, and even if the network itself is more secure, it cannot meet the special security requirements of e-commerce [12]. This article mainly discusses the network security of e-commerce based on big data in the cloud computing environment and aims to make certain contributions to the network security of e-commerce.

Liu et al. built an economic model that considered the trade-off between system availability and client security constraints. When a brand-building company is a pioneer, both companies have higher security restrictions on their clients. In the mixed market, each company's manager n checks the user's emphasis on security and availability. He believes that with restrictions, users begin to pay more attention to security; managers of companies with lower levels of security restrictions should increase client security restrictions [13, 14]. Bing is increasingly important for activities related to reputation and integrity. Therefore, he proposed an electronic identity (eID)-based cloud service platform architecture [15, 16]. Pop believes that managing large amounts of data processed in distributed systems consisted of data centers that have a significant impact on end users. Therefore, he can effectively implement the management process of such a system by using a unified overlay network interconnected by a secure and efficient routing protocol [17, 18]. Chen et al. believe that providing a highly secured critical infrastructure system should develop scalable [19, 20].

The innovations of this article are as follows: (1) The indicator system, on which the evaluation is based, is analyzed. (2) Corresponding new security policies are formulated for more serious risk locations. (3) A security risk assessment model including asset analysis module, security knowledge base module, and risk assessment calculation module is constructed.

2. Proposed Method

2.1. E-Commerce Theory. The basic characteristics of e-commerce are universality, convenience, integrity, security, and coordination. In general, therefore, e-commerce security is not only a network security issue but also a business security issue; e-commerce security is an interdisciplinary discipline that includes not only technologies related to network security but also technologies related to business security. E-commerce business model refers to how electronic enterprises use information technology and the Internet to operate their enterprises, applications on the Internet, and on the basis of network security, how to ensure the smooth progress of e-commerce [21]. The value of e-commerce is that consumers shop and pay online through the Internet, which saves time and space for customers and enterprises and greatly improves transaction efficiency. Especially for busy office workers, it also saves a lot of precious time. That is to achieve the confidentiality, integrity, authentication, and forgery of e-commerce. Without the security of the network as the basis, the security of commercial transactions is like a castle in the air. Commercial transactions are not secure, and even if the network itself is no longer secure, it cannot meet the special security requirements or sort out security issues, including related technologies, protocols, architecture, software, and solutions, especially the latest research results of e-commerce security issues. On this basis, the e-commerce security issues in big data and cloud computing environments are analyzed. Among them, the type of e-commerce refers to the classification of e-commerce, and there are five kinds in total; business-to-consumer (B2C), business-to-business (B2B), business process, consumer-to-consumer (C2C), business-to-government (B2G), and consumer-to-government (C2G).

Security issues are an important factor that constrains them. Since e-commerce, security issues have disappeared like ghosts. Broadly speaking, e-commerce security should include information. In order security, there must be a corresponding technology to meet specific security needs. The security issues of e-commerce are mainly manifested in three aspects: information security, transaction security, and property security. Its source code has four levels: hardware level, software level, application level, and environment level. Various measures should be taken to address security challenges and promote the further development of e-commerce in China [22]. Traditional network security consists of three elements: confidentiality, integrity (ensuring that content is not compromised or tampered with, and only authorized individuals identify it), and availability; with the development of services such as online e-commerce, a new element has been added: antirefusal mechanism, that is, documents or transactions signed by individuals on the network cannot be rejected to ensure the normal development of online business. As shown in Figure 1, it is a more complete e-commerce transactional information security application. Among them, there are four elements of e-commerce: shopping malls, consumers, products, and logistics.

2.2. Big Data. Big data refers to the collection of data whose content cannot be captured, managed, and processed by conventional software tools within a certain period of time. The most notable feature of big data is the large scale of data. Internet of Things are rapidly emerging, and cloud computing has arrived. Whether it is instant messaging tools, cloud platforms, or social networks, you can generate large amounts of data anywhere, making the security situation more complex than traditional security. Data integrity challenges and the ability to prevent data loss, theft, and destruction have some technical problems, and traditional security tools are no longer effective. On the other hand, collecting and centrally storing large amounts of corporate data, user data, personal privacy, and user behavior records increases the risk of data breaches. If these data are abused, it will threaten the information security of the enterprise and even personal safety. Analysis of massive data helps

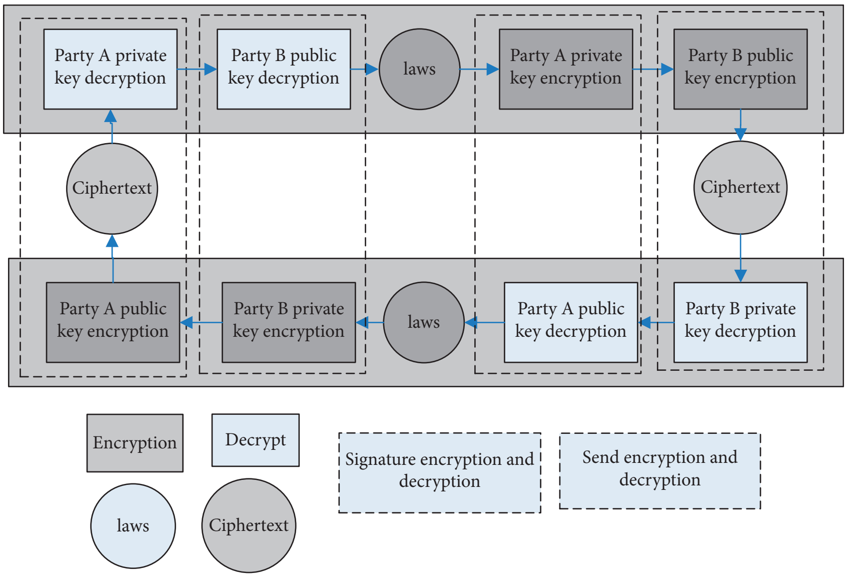
Party A private key decryption
Party B public key decryption
laws
Party A private key encryption
Party B public key encryption
Ciphertext
Ciphertext
Party A public key encryption
Party B private key encryption
laws
Party A public key decryption
Party B private key decryption
Encryption
Decrypt
Signature encryption and decryption
Send encryption and decryption
laws
Ciphertext

Figure 1: A more complete e-commerce transaction information security application diagram.

information security service providers better describe anomalous behavior on the network to identify risk points in the data [23]. Combine real-time security defenses to analyze business data, identify phishing attacks, prevent fraud, and prevent hackers. Traces left by cyber-attacks are often the attack.

2.3. Cloud Computing. Cloud computing is a type of distributed computing. It refers to decomposing the huge data computing processing program into countless small programs through the network "cloud and then processing and analyzing these small programs through a system composed of multiple servers to obtain the results and return them to the user. Cloud computing is the commercial implementation of computing resources. It is essentially a producer-consumer model. Cloud services are considered to be a valuable commodity economy, and cloud users can provide products to consumers according to their own needs. Suppliers and points are purchased from suppliers worldwide based on certain payment methods. In the short term, the impact of cloud computing on individuals is relatively small. Perhaps many of the previous technologies introduced cloud computing to enterprises first, especially, which are the most direct changes: they will be worrying. Whether it will eventually expand individuals remains to be seen [24].

The characteristics of cloud computing are ultralarge scale, high reliability, versatility, and high odd scalability. With the rise of an environment, a new trend in the application of cloud computing services the economic, business, management, and e-commerce fields. It is an electronic outsourcing based on cloud computing technology. Enterprises only need to access the e-commerce cloud service provider, established by the software library, to obtain the required management procedures and business database information. There is no investment to establish a complete set of internal software and procedures. The cost is relatively low, and only a certain rent is required. When the enterprise's existing IT resources can meet the business needs, uninterrupted business and the enterprise do not need to invest in new equipment or pay high cloud. Any idle IT resources in IT can help with this task. In fact, the business operation mode of the enterprise is to use the cloud computing platform to virtually establish various resources distributed throughout the country and realize resource sharing at the application layer. Businesses do not need sharing. Cloud computing has a wide range of applications, including cloud IoT, cloud security, cloud storage, private cloud, cloud gaming, and cloud education.

2.4. Risk Assessment Model. After asset analysis, it is necessary to separately examine the threats and vulnerabilities faced by individual assets, so that the risk of integrating all assets can be obtained from them. The theoretical model of risk assessment is shown in Figure 2.

Regardless of the size of the enterprise, when operating an e-commerce system, a series of security controls are preconfigured to prevent potential security risks or to improve control measures against security attacks that have occurred. Existing control measures improve the results of systemic risk assessments by reducing the likelihood of threats occurring and reducing the destructive effects of threat impacts. In the risk assessment process, the actual existing security measures need to be included in the risk calculation, so as to obtain the risk value that is most consistent with the information assets in the current tense. The risk assessment result information of a single information asset is stored in a unified database, and the comprehensive risk assessment module in the evaluation model performs effective reasoning according to certain inference rules, and combines the object. Get the overall risk profile of the system and explain the results accordingly. The following is a breakdown of the identification of threats and

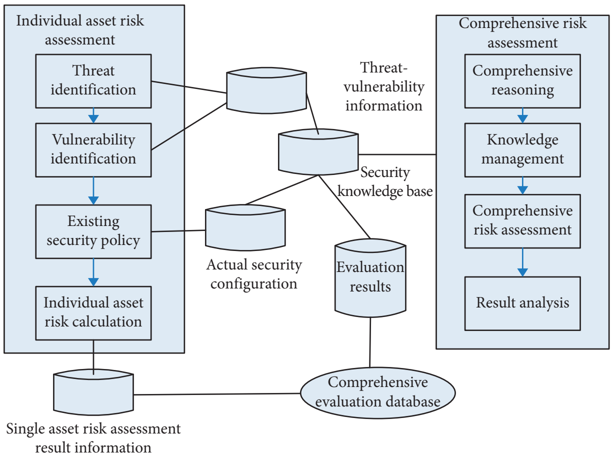
Individual asset risk assessment
Threat identification
Vulnerability identification
Existing security policy
Individual asset risk calculation
Threat-vulnerability information
Security knowledge base
Actual security configuration
Evaluation results
Comprehensive risk assessment
Comprehensive reasoning
Knowledge management
Comprehensive risk assessment
Result analysis
Comprehensive evaluation database
Single asset risk assessment result information

FIGURE 2: Risk assessment model diagram.

vulnerabilities in a single asset risk, the impact of existing security strategies, and the classification of risk levels, combined with qualitative and quantitative methods.

2.4.1. Estimation of the Events. Under the influence of existing security measures, the probability of a threat event is affected by four factors: whether the asset is attractive, whether the asset is easier to convert into compensation, the technical size of the threat, and whether the vulnerable points are easy to be used and threatened. The probability of defining the occurrence of threat T is $P(T)$. From the above four factors, we can define four factors as $P(A)$, $P(B)$, $P(C)$, and $P(V)$. The threat event $P(T)$ and is as follows:

$$P(T) = P(A) * P(B) * P(C) * P(V). \tag{1}$$

Since $P(A)$ and $P(B)$ are directly related to asset attributes, $P(C)$ and $P(V)$ are directly related to the attributes of the vulnerable points. We can combine these four items, respectively.

$$P(T) = P(A) * P(V), \tag{2}$$

where $P(A)$ is the correction factor associated with the asset and $P(V)$ is the probability that the vulnerable point is utilized. Therefore, the probability of estimating the probability of a threat event is to determine the correction factor associated with the asset and the probability that the vulnerability is exploited. The set of vulnerable points corresponding to a threat Ti ($i = 1, 2, \ldots, n$) is defined as $Vi = \{Vi1, Vi2, \ldots, Vim\}$, and the probability of any vulnerable point being utilized is an independent probability event, that is, the probability that at least one event that can be utilized in a set of vulnerable points corresponding to a threat at a certain moment occurs

$$P(V_i) = 1 - \prod_{j=1}^{m} \left(1 - P(V_{ij})\right). \tag{3}$$

Taking into account the information asset factor, the probability formula for a threat event can be written as

$$P(T_i) = P(A_i)\left(1 - \prod_{j=1}^{m} \left(1 - P(V_{ij})\right)\right). \tag{4}$$

2.4.2. Estimation of the Extent of the Threat. In the risk assessment, the quantification of the degree of impact on the system after the threat event has been a difficult problem. A threat may have different levels of impact on e-commerce systems. Common threats such as "cannot perform critical operations," "system outages," "transaction information disclosure," "loss of revenue," "damage to corporate image," and "harm the public safety" are shown. The size of a single impact attribute generated by a particular threat is not consistent, and different system platforms take different levels of attention when encountering these hazards. In order to make a better quantitative measurement of the degree of influence on Weibula, this article refers to the existing risk assessment method research and introduces the concept of multiattribute and influence degree, that is, a certain specific rib and influence on different levels of the system. It is called a certain rib and consequence attribute. Each different rib and consequence attribute is given a corresponding weight value. The weight value depends on the importance of the threat and the system's ability to withstand. Therefore, it is necessary to confirm the threats that will cause security damage to the e-commerce system based on the actual situation of the system being evaluated. When assessing the degree of influence, it weighs different consequence attributes in order to obtain the level of risk that is consistent with the actual situation.

The consequence attribute set that threatens T_i can be defined as X: $\{t = 1, 2, \ldots, s\}$, and the corresponding consequence attribute value set is D: $\{d_n | i = 1, 2, \ldots, n; t = 1, 2, \ldots, s\}$, where x_1 and d_n, respectively, represent the t-th consequence attribute of threat T_i and the possible influence value on the consequence attribute, s is the number of types of consequence attributes; the weight set corresponding to the threat consequence attribute is defined as $W\{w_1 | t = 1, 2, \ldots, s\}$, which weighs consequence attribute.

Since the impact of threats on e-commerce systems is multifaceted, different consequence attributes have different dimensions and cannot be measured directly with uniform standards. Value attribute values of each consequence are dimensionless, and the relative consequence attribute value D^*: $\{d_{it}^* | i = 1, 2, \ldots, n; t = 1, 2, \ldots, s\}$ is obtained, where d_{it}^* is the dimensionless value, indicating the relative influence value of threat T_{iw} on the consequence attribute x_t.

$$d_{it}^* = \frac{d_{it}}{\max\{d_{it}\}_{k=1}^{n}}. \tag{5}$$

According to previous section, combined with the value of the multidimensional threat consequence attribute and its weight, the formula for the degree of influence of the threat can be

$$E(T_i) = P(T_i) * \sum_{t=1}^{s} \left(w_t d_{it}^*\right). \tag{6}$$

Combine formula (4) to get

$$E(T_i) = P(A_i)\left(1 - \prod_{j=1}^{m}\left(1 - P\left(V_{ij}\right)\right)\right)\sum_{t=1}^{s}\left(w_t d_{it}^{*}\right). \tag{7}$$

2.4.3. Impact of Existing Security Policies. Regardless of the size of the enterprise, when operating an e-commerce system, a series of security controls are preconfigured to prevent potential security risks or to improve control measures against security attacks that have occurred. Existing control measures improve the results of systemic risk assessment by reducing the threat, the likelihood of occurrence, and reducing the destructive effects of the ribs and impacts. For complexity, in order to simplify the evaluation work, we consider the impact of existing security measures from each dimension. Assume that a security measure $S = \{S_1, S_2, \ldots, S_1\}$ is implemented for an asset A_{iw} enterprise, and the impact of reducing the possibility of T_i occurrence is $Sa_{ik}\,(k = 0, 1, 2, \ldots, 1)$, which reduces the damaging and destructive impact of $Sb_{ik}\,(k = 0, 1, 2, \ldots, 1)$. We define the range of Sa_{ik} and Sb_{ik} to be 0-1, 0 for complete influence and 1 for no effect.

Influence of events and events are expressed as

$$\begin{aligned} P(T_i) &= P(A_i)\left(1 - \prod_{j=1}^{m}\left(1 - P\left(V_{ij}\right)\right)\right)\prod_{k=1}^{l} Sa_{ik}, \\ E(T_i) &= P(A_i)\left(1 - \prod_{j=1}^{m}\left(1 - P\left(V_{ij}\right)\right)\right) \\ &\quad \prod_{k=1}^{l} Sa_{ik}\sum_{t=1}^{l}\left(w_t d_{it}^{*}\right)\prod_{k=1}^{l} Sb_{ik}, \end{aligned} \tag{8}$$

$R(A_i)$ that the asset A_i faces

$$\begin{aligned} R(A_l) &= A\sum_{i=1}^{n} E(T_i) = A_l\sum_{i=1}^{n}\Bigg[P(A_l)\left(1 - \prod_{j=1}^{m}\left(1 - P\left(V_{ij}\right)\right)\right) \\ &\quad \prod_{k=1}^{l} Sa_{ik}\sum_{t=1}^{s}\left(w_t d_{it}^{*}\right)\prod_{k=1}^{l} S_{b_{ik}}\Bigg]. \end{aligned} \tag{9}$$

2.4.4. Risk Level Division. After obtaining the risk profile of a single asset, it is necessary to synthesize the risk values of all assets risk faced by. Assuming that there are N items in the asset, the risk value of each asset is dimensionlessly processed, and the risk ranking of each asset is obtained. The asset pricing strategy is based on the asset's confidentiality, integrity, and usability value of the entire system. Therefore, the weight of the assets A_i on the system can be obtained according to the value of the asset, and the value of all assets is normalized to obtain the weight of the importance of the entire system δ

$$\delta_i = \frac{V(A_i)}{\sum_{i=1}^{N} V(A_i)}. \tag{10}$$

The overall risk of the entire e-commerce system is

$$R = \sum_{i=1}^{N} \delta_i R(A_i). \tag{11}$$

3. Experiments

3.1. Experimental Design. Combined with the risk assessment framework of this article, the design of the questionnaire content for the actual investigation of enterprises needs to start from the basic security status of the system. Basic information of the enterprise includes the basic situation of the enterprise, the information assets and the overview of the e-commerce system. The information assets include hardware and software asset content, service asset content, cloud asset status, personnel assets, and document assets. The e-commerce system overview includes system network topology map, system bearer service status, system network structure, outbound lines, and network boundary conditions. Business data, data backup, and security incidents occur within one year. Security status surveys are conducted from security management organizations, security management systems, system construction and operation maintenance management, physical security, network security, equipment and host security, application and data security, emergency response and disaster recovery technologies, and personnel security management.

Using the results of the questionnaire to conduct risk assessment, experts also need to conduct statistical analysis on the collected data to determine the basic situation of the system and the main risks. These risk generation risk sets can be entered into the security knowledge base for storage to provide a reference for real-time risk monitoring. The factual data collected through the questionnaire needs to be formalized before the risk calculation, in order to make the obtained raw data meet the needs of the evaluation model. There are three types of factual data that need to be formalized: subjective indicator data, objectiveness indicator data, and objective nonindicator data.

Subjective indicator data is the subjective evaluation of some indicators by the respondents, such as the subjective cognition of the employees in the questionnaire on the overall security status of the e-commerce platform. This type of data can be evaluated by adding credibility. The degree of deviation between the score of each evaluator and the last evaluation result is the credibility of the index value, and the credibility range is between 0 and 1.

The objective indicator data is the value of an indicator that can be read directly from the system, such as the time the terminal server has been used or whether a firewall is configured (which is indicated as true). The "fuzzification" of this type of data does not need to refer to other samples, and can be directly set to a reliability of 1.

This article establishes a model-based risk assessment tool by analyzing the composition and security elements of the system. The models of information system risk factors established by these tools are usually quantified or semi-quantitatified, and the results are based on the information collected. For example, @RISK, CORA, Buddy System, etc., are risk assessment tools that combine qualitative and quantitative assessments.

3.2. Data Collection. This article analyzes the data of a part of the enterprise that deploys e-commerce in an application. Management framework and indicator system are also based on this article, the e-commerce system is investigated, and the system-related information assets and threats are identified. Risk factor such as data vulnerability is avoided. For the convenience of recording and calculation, it is used to classify the asset data under investigation. Based on the space, only some assets in the system and some threats and vulnerabilities identified are analyzed.

4. Discussion

4.1. Analysis of Security Risks of Network E-Commerce

4.1.1. Analysis of Hidden Dangers of Property Security. According to the assets, threats, and vulnerability information collected in this article, the questionnaire results are combined with the expert scores to assign corresponding risk factors, and the asset value table shown in Table 1 is obtained.

The system has set some security measures in advance when deploying the cloud-based e-commerce platform. Combined with the impact of existing security measures, the risk analysis is first performed on individual information assets. As shown in Table 2, the threats to assets are listed: the degree of vulnerability, the consequences of the threat attribute value, and the degree of impact of security measures.

As shown in Figure 3, it is a data graph of the influencing factors. According to formula (11), the comprehensive risk value of the system is $R = \sum_{i=1}^{N} \delta_i R(A_i) = 4.4$. And 9-10 is the extra high risk. According to this, the risk faced by the system is at a risk corresponding to the hardware and is most serious, indicating that the physical security of the e-commerce system, system permissions, and data backup control have urgent problems to be solved. The risks reflected by cloud data security and the configuration of security managers cannot be ignored.

4.1.2. Analysis of Hidden Dangers of Transaction Security. Transaction security refers to various insecurities in the e-commerce transaction process, including being enlarged. As shown in Figure 4, for the proportion of cases reported in the network case, it can be seen from the figure that the proportion of online shopping cases accounts for 38%. As we all know, the security risks of online e-commerce transactions cannot be underestimated. There are many transaction security issues in reality, for example, the seller uses the advantage of information to fake the buyer with inferior information; the identity of the of the to enter, and does not comply when providing the service, the fee charged is not the service or not enough services. Of course, the opposite is true.

Table 1: Asset value table.

Assets	Ava (A)	Inte (A)	Conf (A)	Reli (A)
1	3	4	5	
2	4	3	2	
3	2	4	4	
4	3	3	2	
5	4	2	1	
6	5	4	2	
7	3	3	2	
8	4	2	4	
9	2	3	5	3
10	2	6	2	5

Table 2: Single asset risk information.

Asset number	Asset value	Asset weight	Risk value
1	3.1	0.08	7.55
2	3.6	0.13	5.14
3	2.8	0.09	2.21
4	3.2	0.09	6.21
5	3.7	0.11	3.22
6	4.2	0.13	5.11
7	2.3	0.08	2.34
8	3.5	0.09	4.37
9	2.1	0.08	3.28

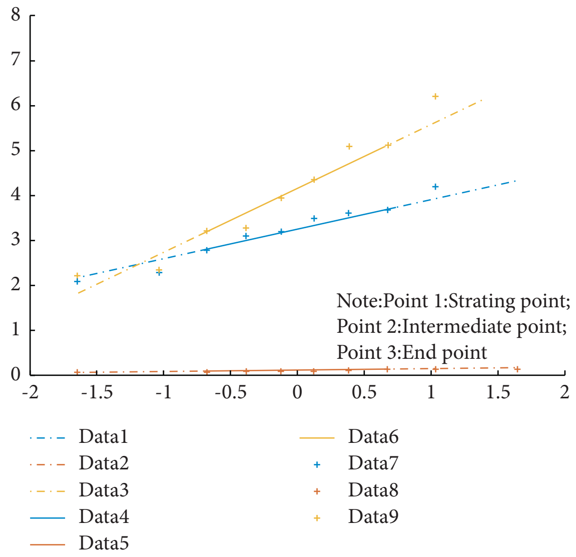

Figure 3: Single asset risk information.

4.1.3. Analysis of Hidden Dangers of Information Security. As shown in Figures 5 and 6, the network information is stolen and the ratio chart is taken. Illegal deletion of transaction information and the loss of transaction information may cause economic disputes and economic losses to one or more parties to the transaction. The most common information risk is the illegal theft and disclosure of information. It often causes a chain reaction and creates a follow-up risk. This is also the biggest concern for businesses and individuals. The typical manifestation of information

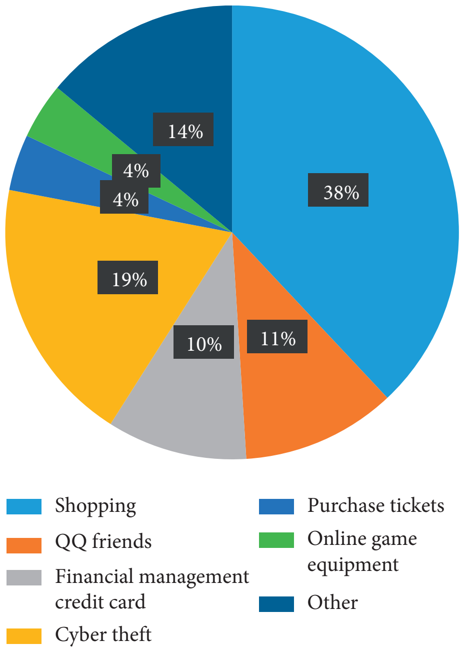

Figure 4: Proportion of network security incidents.

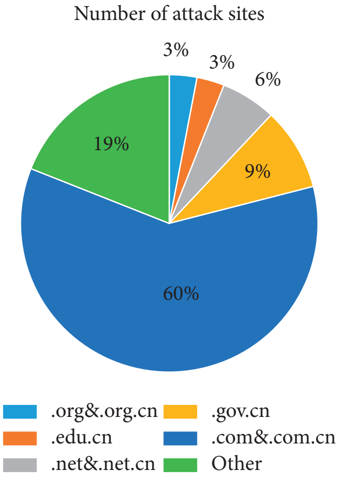

Figure 5: Statistics of website attacks.

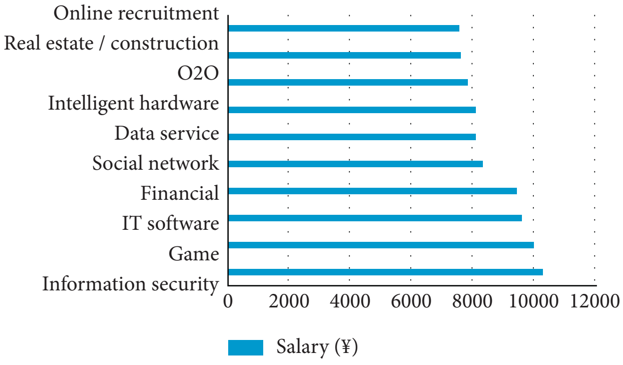

Figure 6: Industry salary treatment data map.

risk is cyber fraud. Cyber fraud brings huge economic losses to manufacturers and consumers.

4.1.4. Analysis of Hidden Dangers of Network Security. Cyber security is the measure taken to prevent the theft of such information and commercial competition.

5. Conclusions

Cloud computing is a computing method based on the Internet. In this way, shared hardware and software resources and information can be provided to computers and other devices on demand. Users no longer need to know the details of the infrastructure in the "cloud," nor do they have the corresponding expertise, nor do they need direct control. Whether it is e-commerce, in era economic networking information, it has a pivotal position. The combination of the three is the mainstream in the future. In the process of combining the three, how to avoid various risks and create a safe and stable network environment is a new topic facing enterprises and scholars. It is also based on this purpose, the author of the "risk assessment as a service" idea integrate big data security, cloud computing security, e-commerce security, risk assessment four major content, and research in the enterprise to deploy e-commerce system in cloud computing in the environment; in order to solve various security problems faced, a security risk assessment model needs to be established.

The article analyzes the patterns of e-commerce in big data and cloud environments and the specific practical problems such as the reliability of supplier services, storage risks, service continuity, and the concealment of viruses and hacker attacks, establishing a cyclical risk. In the cycle of risk assessment, information such as information assets, threats, risks, and security policies are continuously enriched to form a security knowledge base. By migrating the security knowledge base to the cloud, a risk management cloud can be generated. When the e-commerce enterprise operates the system platform, the risk management cloud can dynamically monitor and manage the system security in real time, and realize the idea of "security as a service." The framework theoretically realizes the dynamic in systems under and cloud environments.

The product of the fusion of traditional computer and network technology development such as load balancing, by distributing computing on a large number of distributed computers, rather than wooden computers or remote servers, the operation of enterprise data centers will be more similar to the Internet. This enables businesses to switch resources to the applications they need, accessing computers and storage systems on demand. Typical cloud computing providers often provide general network business applications, allowing us to access software and data stored on servers through software such as browsers or other Web services. In this article, the risk assessment model established for realizing the dynamic management of e-commerce system security risk under big data and cloud environment has not been tested by the actual network environment. The validity and practicability of the model need to be tested by practice and continuously improved and strengthened. At the same time, the model established in this article needs to be further strengthened in the quantification of the system after the threat event occurs and the improvement of the security knowledge base. Solving the security risks faced by e-commerce under big data and cloud environment to promoting the even national economy. It is hoped that there will be an effective model with dynamics under big data and cloud environment. The risk assessment problem promotes the consistent and steady development of big data, cloud computing, and e-commerce. However, due to the limitations of time and technology, we have not conducted in-depth research on e-commerce network security under the combination of cloud computing and big data.

Data Availability

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Conflicts of Interest

The author states that this article have no conflicts of interest.

Acknowledgments

This work was supported by the Scientific Research Foundation of Hunan Provincial Education Department (Grant nos. 21A0535, 20B060, and 19B321), Natural Science Foundation of Hunan Province, China (Grant nos. 2021JJ40635 and 2020JJ5623), and Changsha Municipal Natural Science Foundation (KQ2007084).

References

[1] Z. Li, Z. Tang, and Y. Yang, "Research on architecture of security video surveillance network cascade system with big data," *World Journal of Engineering*, vol. 13, no. 1, pp. 77–81, 2016.

[2] M. Yuan and H. Sheng, "Research on the fusion method of spatial data and multimedia information of multimedia sensor networks in cloud computing environment," *Multimedia Tools and Applications*, vol. 76, no. 16, pp. 1–18, 2017.

[3] L. F. Hsu, "E-commerce model based on the Internet of Things," *Advanced Science Letters*, vol. 22, no. 10, pp. 3089–3091, 2016.

[4] S. Garg, A. Singh, K. Kaur, and Aujla, "Edge computing-based security framework for big data analytics in VANETs," *IEEE Network*, vol. 33, no. 2, pp. 72–81, 2019.

[5] F. Akhbar, V. Chang, Y. Yao, and Méndez Muñoz, "Outlook on moving of computing services towards the data sources," *International Journal of Information Management*, vol. 36, no. 4, pp. 645–652, 2016.

[6] E. Loukis, N. Kyriakou, K. Pazalos, and Popa, "Inter-organizational innovation and cloud computing," *Electronic Commerce Research*, vol. 17, no. 3, pp. 379–401, 2017.

[7] I. S. Razo-Zapata, A. J. Gordijn, P. D. de Leenheer, and Wieringa, "e 3 service: a critical reflection and future research," *Business & Information Systems Engineering*, vol. 57, no. 1, pp. 51–59, 2015.

[8] A. K. Kar and A. Rakshit, "Flexible pricing models for cloud computing based on group decision making under consensus," *Global Journal of Flexible Systems Management*, vol. 16, no. 2, pp. 191–204, 2015.

[9] M. S. M. Dhar and R. Manimegalai, "A policy-oriented secured service for the e-commerce applications in cloud," *Personal and Ubiquitous Computing*, vol. 22, no. 5-6, pp. 911–919, 2018.

[10] A. Mukherjee and D. De, "Low power offloading strategy for femto-cloud mobile network," *Engineering Science and Technology, an International Journal*, vol. 19, no. 1, pp. 260–270, 2016.

[11] D. Samant and U. Bellur, "Handling boot storms in virtualized data centers-A survey," *ACM Computing Surveys*, vol. 49, no. 1, pp. 1–36, 2016.

[12] G. L. Santos, P. T. Takako Endo, L. G. F. D. Ferreira da Silva Lisboa Tigre, and Ferreira da Silva, "Analyzing the availability and performance of an e-health system integrated with edge, fog and cloud infrastructures," *Journal of Cloud Computing*, vol. 7, no. 1, p. 16, 2018.

[13] Y. Liu, S. Sheng, and S. R. Marston, "The impact of client-side security restrictions on the competition of cloud computing services," *International Journal of Electronic Commerce*, vol. 19, no. 3, pp. 90–117, 2015.

[14] W. Xie, "Research on big data processing model of multi objective genetic algorithm based on static bayesian game in cloud computing," *Journal of Computational and Theoretical Nanoscience*, vol. 13, no. 12, pp. 9633–9637, 2016.

[15] C. Bing, C. Tan, and Z. Xiang, "Cloud service platform of electronic identity in cyberspace," *Cluster Computing*, vol. 20, no. 1, pp. 413–425, 2017.

[16] J. Chen, J. Peng, X. Zhi, and M. Qiu, "Research on application classification method in cloud computing environment," *The Journal of Supercomputing*, vol. 73, no. 8, pp. 3488–3507, 2017.

[17] F. Pop, C. Dobre, B. C. Mocanu, and Citoteanu, "Trust models for efficient communication in Mobile Cloud Computing and their applications to e-Commerce," *Enterprise Information Systems*, vol. 10, no. 9, pp. 982–1000, 2015.

[18] R. Chaudhary, N. Kumar, and S. Zeadally, "Network service chaining in fog and cloud computing for the 5G environment: data management and security challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 114–122, 2017.

[19] Z. Chen, G. Xu, V. Mahalingam, L. Ge, and Nguyen, "A cloud computing based network monitoring and threat detection system for critical infrastructures☆," *Big Data Research*, vol. 3, no. 33, pp. 10–23, 2016.

[20] H. Long, L. Kai, M. M. Hassan, A. Alamri, and A. Alelaiwi, "CFSF:On cloud-based recommendation for large-scale E-commerce," *Mobile Networks and Applications*, vol. 20, no. 3, pp. 380–390, 2015.

[21] X. Li, H. Jianmin, B. Hou, and P. Zhang, "Exploring the innovation modes and evolution of the cloud-based service using the activity theory on the basis of big data," *Cluster Computing*, vol. 21, no. 1, pp. 907–922, 2018.

[22] Y. Zhang, X. Xiao, L. X. Yang, Y. Xiang, and S. Zhong, "Secure and efficient outsourcing of PCA-based face recognition," *IEEE Transactions on Information Forensics and Security*, vol. 15, 2019.

[23] Z. Lv, X. Li, W. Wang, B. Zhang, J. Hu, and S. Feng, "Government affairs service platform for smart city," *Future Generation Computer Systems*, vol. 81, pp. 443–451, 2018.

[24] N. Chen, B. Rong, X. Zhang, and M. Kadoch, "Scalable and flexible massive MIMO precoding for 5G H-cran," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 46–52, 2017.