Hindawi
Mobile Information Systems
Volume 2022, Article ID 3023298, 13 pages
https://doi.org/10.1155/2022/3023298

Research Article

Investigation of E-Commerce Security and Data Platform Based on the Era of Big Data of the Internet of Things

Zhiqiang Dai[1] **and Xin Guo**[2]

[1]*College of Tourism and Management Engineering, Jishou University, Zhangjiajie 427000, Hunan, China*
[2]*College Software, Jishou University, Zhangjiajie 427000, Hunan, China*

Correspondence should be addressed to Xin Guo; guoxin007788@126.com

Received 17 May 2022; Revised 30 June 2022; Accepted 8 July 2022; Published 8 August 2022

Academic Editor: Chia-Huei Wu

Copyright © 2022 Zhiqiang Dai and Xin Guo. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Internet of Things (IoT) can combine a wide range of information space with physical space and use related technologies to provide effective information interaction between objects. Nowadays, a large amount of Internet data transmitted by E-commerce communication data is vulnerable to interference, intrusion, and other attacks, posing a major threat and challenge to data security. Based on the IoT data analysis platform Hadoop, starting from the data, the problems faced by the E-commerce information security are analyzed and the E-commerce security is improved. Through the comparison of Delphi method, fuzzy comprehensive evaluation method, weighted linear evaluation method, grey cluster analysis method, analytic hierarchy process, and using the complex fuzzy evaluation method of the vague set theory, the security weights of the first and second levels are calculated according to the vague entropy value of each index attribute. It provides a useful reference for E-commerce informatization security evaluation methods. The first-level and second-level comprehensive evaluations of the vague set are used to detect and analyze E-commerce network security, transaction security, data security, and physical security. The weight of each indicator occupies a total of 100% and the final risk status is close to 0. Therefore, it can be concluded that the risk status of the E-commerce information security is "safe".

1. Introduction

With the quick growth of E-commerce and the IoT in recent days, making large digital media boom in the age of large metal devices, it has also led to the rise of big data related industries. As a rapidly developing digital platform, E-commerce carries a large amount of multimodal unstructured data. With the increase of massive data every day, if the data can be processed well according to the existing E-commerce data processing capacity, then large concurrent requests can be responded to, ensuring the security of the transaction process and the processing of structured and unstructured data. It remains to be seen whether the security management of big data storage can be guaranteed.

E-commerce information security needs to be built up on the basis of the big data platform Hadoop to establish an information security detection and evaluation model, depending on the objectives of the system of data security architecture, using a combination of technology and management to maintain information security and ensure that the status of IoT large format digital data plays a special discriminatory role to promote the growth of E-business.

The combination of big data and E-commerce security is an in-depth study of the composition of the E-commerce security system and its key security defense strategies and technologies, and some hidden dangers of the security system are analyzed. The birth of today's big data technology can solve the contradictory problem of E-commerce security. The introduction of the distributed Apache Hadoop platform, which is more popular and widely used today, describes the structure of Hadoop in detail and proposes to guide and monitor E-commerce behavior based on data to improve the E-commerce security system.

2. Related Work

At this time, there are not many achievements that can both qualitatively and quantitatively describe the E-commerce information security evaluation model. The main reason is the variability and limitations of the E-commerce construction environment, resulting in deviations in the evaluation of the system, and it is impossible to set up a uniform system of assessment in science. Ni et al. investigated the structure and properties of mist calculation and looked into the fog net's key roles, including real-time services, transient memory, data dissemination, and dispersed calculations, proposing to target threats to safety and privacy of IoT apps [1]. Yang et al. proposed a collaborative AmBC (CABC) type system in this way, in which readers can recover a message not just from A-BD, but also from RF sources. For frequency selective fading channels, a CABC system model over ambient orthogonal frequency division multiplexing (OFDM) carriers was proposed and a low-complexity optimal ML detector was derived based on it [2]. Ansari and Sun proposed a Mobile Edge Internet of Things (MEIoT) by using fiber optic wireless access technology, cloudlet concept, and software defined network framework architecture. In addition, two dynamic agent VM relocation approaches were introduced to minimize the end-to-end latency between agent VMs and their IoT devices and to minimize the total grid-connected energy consumption of small clouds, respectively. The properties of the proposed methods were verified through broad range of simulations [3]. The main findings of the Faraoni et al. study were related to the importance of website characteristics as an antecedent of E-loyalty in online grocery retailing. Although the phenomenon of originality value exploration has been extensively studied, some aspects of it remain to be fully explored, especially the effects of E-trust, E-satisfaction, and E-commitment [4]. Imtiaz et al. considered a discussion on the interpretation of customer privacy, security, and trust. The importance of privacy concerns, appropriate security measures, and trust development were also highlighted [5]. Miao et al. built a data science and big data analysis application platform based on microservice architecture for education or nonprofessional research fields. In a microservices-based environment, component updates for individual components were facilitated. The platform had a personal code experiment environment and integrated JupyterHub based on Spark and HDFS for multiuser use and a visual modeling tool that followed the modular design based on data science engine engineering [6]. Thien et al. worked on the implementation of an automatic calibration to data profiling setup and workflow for defining liquid–liquid equilibrium data using a Raman micron emission spectroscopy and a microfluidic platform. The pure fractions were premixed online using a micromixer to form a sealed system with the bonus of eliminating future losses of volatile fractions [7]. These studies are instructive to a certain extent, but in some cases the demonstrations are insufficient or inaccurate and can be further improved.

3. E-Commerce Model and Security Issues in the Era of Big Data of IoT

At present, the level of the IoT with high social acceptance is a model that divides the IoT into three layers from the bottom-up according to the process of data collection, transmission, and processing in the network. Figure 1 shows the general overall architecture of an IoT system. Different IoT application areas have different usage structures, but the overall application structure idea is the same. The information security technology of the IoT is also carried out in accordance with the multilevel requirements of the general IoT architecture [8].

At present, there are two main concepts of the IoT: narrow and broad. The narrow concept of the IoT refers to the IoT that realizes the intelligent identification, perception, positioning, and management of items. The broad meaning of IoT is the fusion of information space and physical space. Digitization connects all things, enabling the effective interaction of information between things and things, people and people, and the real environment. The complex application of computerized human society has reached a higher level by integrating various information technologies into social behavior through new service models.

As the basis for building the IoT, the perception layer is the data source for the entire network. There are various devices in the perception layer, including identification devices, such as RFID and cameras, as well as perception devices represented by sensors, such as infrared sensors [9]. The network layer is responsible for the safe, stable, and efficient interaction of data between the perception layer and the application layer. The application layer is mainly responsible for the storage and processing of data on the IoT system and is the key point for the specific operation of the IoT. If the IoT does not manage user data properly or the storage method is not rigorous, it is easy to be attacked by criminals and leak user's private data. In more serious cases, IoT applications may be exploited to install backdoors and attack the entire IoT system.

Due to the imperfection of the information security technology of the IoT and the occurrence of the high frequency of the security events of the IoT, countries all over the world have drawn high attention. Not only enterprises and research institutions, but also government agencies have issued corresponding guidelines and actively invested in the research and development of the information security protection technology of the IoT.

3.1. Influencing Factors of E-Commerce Security. As an important business activity relying on the Internet, E-commerce is very necessary to build a security architecture. According to the principles and standards of the security system, the factors affecting the information security of E-commerce are analyzed and studied, and finally a representative, comprehensive, and practical index system is

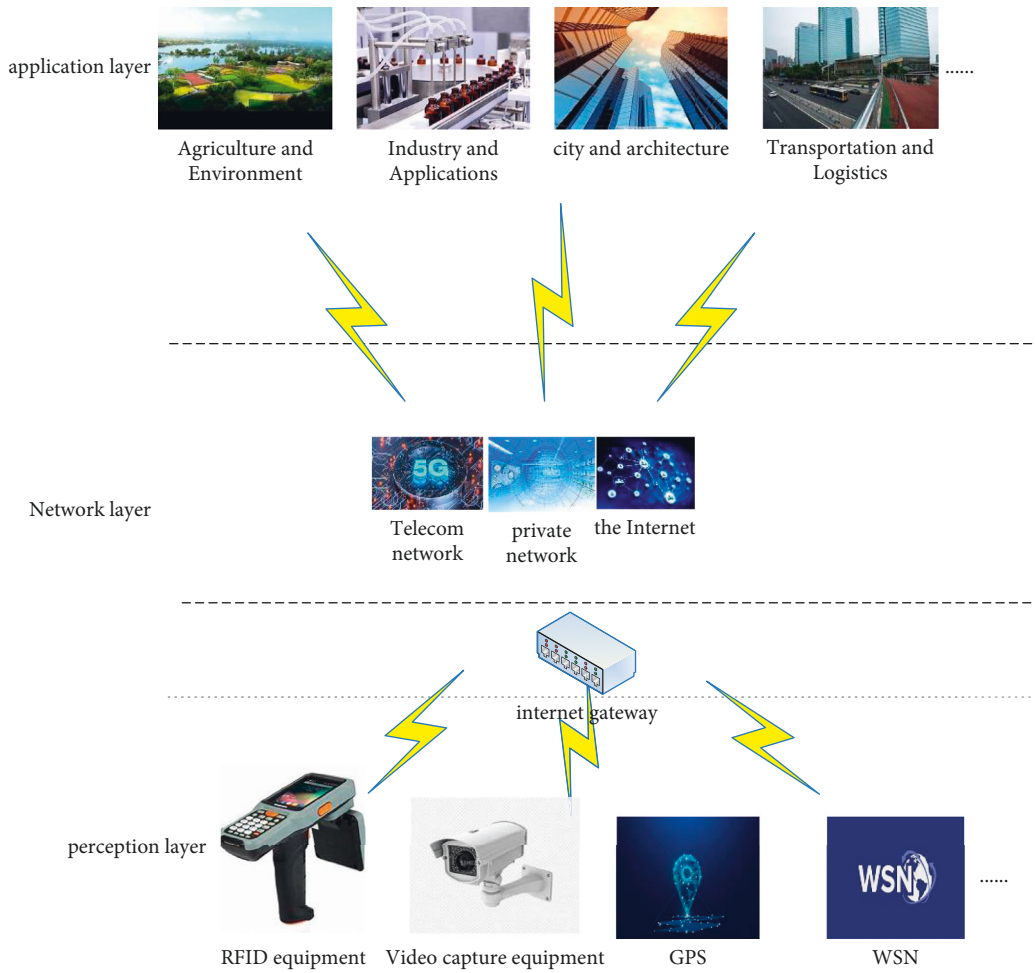

Figure 1: Schematic diagram of IoT architecture.

obtained, which is ready for the assessment of information security. The specific security hierarchy includes the following six points: (1) Network service layer: it includes access control, scanning for hidden threats, and firewalls on the network. (2) Encryption technology layer: this section includes asymmetric encryption and symmetric encryption. (3) Digital certification: it includes digital certificates and CA certification. (4) Transaction protocol layer: it includes transaction quantity, transaction time, and transaction content. (5) Business system layer: E-commerce system application layer. (6) E-commerce service requirements: it has integrity, anonymity, reliability, and validity. In E-commerce, it is the protection of these security levels and the information associated with them [10]. Then, the main threats to information security in the E-commerce environment can be simply divided into these aspects: (1) viruses, (2) natural physical threats to the platform, and (3) deterioration of the security environment, as shown in Figure 2.

The entire business chain of E-commerce consists of many parts, from suppliers to middlemen to consumers, which need to go through the continuous flow of materials. The amount of information that comes with it is also very large, and there are some uncertain hidden dangers in the transmission of information more or less [11]. Next, the security risks generated in the process of information flow and processing will be analyzed. The sources of E-commerce information security risks are mainly composed of these parts.

(1) Information security risk information brought by information transmission: to realize its value, it requires strong liquidity, and many paths need to be passed in the process of information transmission. As an important resource, in order to maximize the value of information, information must ensure the transmission time of information and control the error rate of information within a certain range [12].

(2) Risks arising from information sharing and processing: because in the process of information transmission, it is necessary to continuously process and reproduce the source information and intercept useful information. Therefore, in the process of sharing and processing information, various subjects of E-commerce will inevitably encounter risks in information conversion and other aspects. In order to ensure the normal and smooth operation of E-commerce activities, it is indispensable to ensure

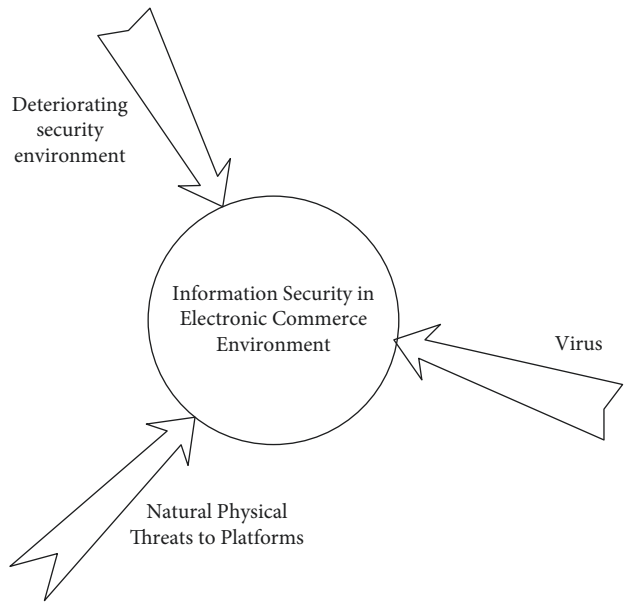

Figure 2: Information security threats in the E-commerce environment.

the relative integrity of information and the security and accuracy of storage protection to achieve the usefulness of these information.

(3) Information security risks caused by information uncertainty: since E-commerce is a complete and complex system, whether the subject is an individual, an enterprise, or other functional departments such as banks, governments, or even the Internet system platform, the information presented by them will have certain random information, fuzzy information, grey information, and other uncertain information. Therefore, the uncertainty of information in E-commerce inevitably brings security risks [13].

3.2. E-Commerce Information Security Architecture. The information environment is the social environment, political environment, and cultural environment in which the information subject is located. The information environment of privacy information disclosure refers to the consumption policy, consumption system, and group consumption culture involved in the process of consumer privacy information disclosure. To ensure the smooth progress of the evaluation work, choosing a scientific and reasonable evaluation index system is as important as choosing an appropriate evaluation model and method [14]. It can be said that the evaluation index system is the basis and premise of the evaluation work. If the indicators are not selected well, it is difficult to make the evaluation results accurate and reasonable.

In the evaluation system, the evaluation indicators are often described in vague language, such as severity and quality, all of which have a strong personal subjective color, and it is difficult to quantify in the evaluation calculation, which makes the evaluation results inaccurate. Information security is implemented through the definition of various security responsibilities and provides support for the organization's security management, security operation and maintenance, and security technology. As the key link of the evaluation work, the importance of the evaluation system is self-evident. The E-commerce information security system mainly analyzes its influencing factors from the platform system of E-commerce operation and its own operating characteristics in the actual transaction process [15]. It is based on the information security management system documentation and security control mechanism in the BS7799 (ISO 17799) standard commonly used in developed countries. Based on the scientific and reasonable classification standard, the evaluation index system of E-commerce information security is constructed. From the integrity, scientificity, practicability, and relevance, four factors with greater influence are selected from the numerous influencing factors of information security in E-commerce. The four factors are cyber security, order transaction security, data security, and physical security. And taking it as the first-level indicator, the entire indicator system is formed by determining the representative subordinate indicators according to the principle of indicator selection. The set of E-commerce information security indicators is shown in Table 1.

3.3. Inspection Methods for E-Commerce Information Security in the Internet of Things Environment. Up to now, research methods at home and abroad for the evaluation and quantification of information security can be divided into three categories. One is the evaluation and quantification method based on the theoretical knowledge of probability theory. The second is to evaluate quantitative methods based on the expertise of experts in related fields, such as AHP and Delphi method. The third is fuzzy logic method, such as fuzzy complete evaluation method. By comparing the Delphi method, the diffusion complex number evaluation method, the weighted linear evaluation method, the grey cluster analysis method, and the AHP, it provides a useful reference for the E-commerce information security evaluation method [16]. Information security assessment is from the perspective of risk management and risk control, using scientific methods and technologies to identify and evaluate threats to networks and information systems.

3.3.1. Delphi Method. The Delphi method can be widely used as a qualitative and subjective analysis method in the field of forecasting. At present, this method is mainly used for the establishment of the evaluation index system and the determination process of specific indicators. The main purpose is to seek advice from experts through multiple rounds of consultation through blind selection and to conduct continuous evaluation and prediction. After many rounds of analysis and judgment, the opinions of experts tend to be consistent, and a unified and reliable conclusion and plan are obtained. As a tool for important forecasting

Table 1: E-commerce information security indicator set.

The first layer (target layer)	Risk profile														
The second layer (criteria layer)	Cyber security			Order transaction security					Data security				Physical security		
The third layer (indicator layer)	Computer network system security	Data backup and recovery	Firewall security	Intrusion detection security	Transaction confirmation security	E-commerce software quality	Digital certificate and authentication security	CA security certification	Database security	Terminal security	Information authentication security	Information encryption security	Device information protection security	I/O security	Staff safety

activities, the main steps in its implementation include: (1) Determine the forecast target and formulate a consultation table. (2) Determine the expert group. (3) Collect and process the weights of each indicator independently reported by each expert and calculate the mean and standard deviation of each indicator weight. (4) Collect and organize data multiple times until discrepancies arise. The weight of each indicator and the mean value do not exceed the default standard, and finally the prediction result is obtained [17].

3.3.2. Fuzzy Comprehensive Evaluation Method. Simple and comprehensive evaluation is done through fuzzy evaluation, while the evaluation of complex evaluation is based on the evaluation of strengths and weaknesses [18]. One of them is the vague set theory, which is used to represent uncertain things. The vague synthesis evaluation method needs to create the proper judge function and judge matrix, combine the obtained weights and the judge value obtained from the final operation, and determine the most favorable decision for the decision maker according to the principle of maximum subordination. The decision that is most beneficial to the decision maker is determined. Its main process is the following: firstly, the set of relevant factors is determined, that is, the set of relevant factors of the evaluation object is denoted as $A = \{A_1, A_2, \ldots A_n\}$, and further subdivided into $C_i = \{C_{i1}, C_{i2}, \ldots C_{\text{in}}\}$. Then, the comment set $P = \{P_1, P_2, \ldots P_m\}$ is established and the single factor of the factor set is evaluated, the membership degree V_{ij} to the evaluation level is obtained, and then the evaluation set $V_i = \{V_{i1}, V_{i2}, \ldots V_{\text{in}}\}$ is obtained, which is a fuzzy subset. Finally, the weights of the relevant evaluation factors to the comment set are determined.

3.3.3. Linear Weighted Evaluation Method. Linear weighted evaluation methods are widely used in technology-related evaluations. The main process is to first evaluate the underlying indicators, and then quantify the value of the indicators [19]. Then, the value of the top-level indicator is obtained. The specific implementation process is to multiply the value of the basic indicator by the weighting factor of the relative importance of the indicator, and then add the top-level indicator. Finally, the previous operations are repeated continuously until the upper layer is reached as an indicator, and the result of the comprehensive evaluation is finally obtained. The linear weighted sum is defined as follows:

Assuming that there are $nx_1, x_2, \ldots x_n$ of parameters, and through the corresponding weight coefficient $a_1, a_2, \ldots a_n$, the weighted sum is $P = x_1 * a_1 + x_2 * a_2 + \cdots + x_n * a_n = \sum (x_n * a_n)$. This is the generalization of expectations in probability theory.

3.3.4. Grey Cluster Analysis Method. According to the classification, grey clustering can be divided into two categories: one category is grey relational clustering. It is mainly used to merge similar factors and reduce the number of indicators. Basically, there are n observation objects, and each object has m characteristic data.

$$\begin{aligned} x_1 &= \{x1(1), x1(2), \ldots, x1(n)\}, \\ x_2 &= \{x2(1), x2(2), \ldots, x2(n)\}, \text{ and} \\ x_m &= \{xm(1), xm(2), \ldots, xm(n)\}. \end{aligned} \tag{1}$$

The absolute correlation degree with all $i \le j$, x_i, and x_j is calculated, and the characteristic variable correlation matrix A is gotten. The critical value r is given, and r is greater than or equal to 0 or less than or equal to 1. When the correlation degree is greater than or equal to a given critical value, x_i and x_j are regarded as the same class. The other category is grey variable weight clustering. There are n clustering objects, m clustering indicators, and s different grey classes. According to the sample x_{ij} of the i ($i = 1,2,\ldots, n$) object about the j ($j = 1,2,\ldots, m$) index, the i-th object is classified into the k-th grey class, which is called grey clustering. Grey cluster analysis is often used to assess geological hazards and it is also used in the assessment of air and water pollution levels. It is a method of cluster analysis based on the correlation coefficient determined by the grey system correlation analysis method, including grey correlation clustering and grey class whitening function clustering. The analysis method steps are divided into two steps: the first step is to calculate the correlation coefficient and the correlation degree. The process mainly includes: (1) Initialize the data, set the system object and characteristic parameter sequence to be evaluated, perform dimensionless processing on the original data involved in the analysis, and compress the analysis data between (0 and 1). (2) Find the difference sequence, the two-level minimum difference and the maximum difference, and determine the grey level to which each clustering index value of each clustering object belongs. (3) Find the correlation coefficient and the correlation degree. The second step is to perform cluster analysis calculation. The domain of discourse of clustering is set, and the domain of discourse is the entirety of the objects being evaluated. The size sequence of each object in the universe can be obtained, the distance of each evaluation object can be calculated, the samples with the closest distance can be clustered into one class, and so on, until all evaluation indicators are classified into one class [20].

3.3.5. Analytic Hierarchy Process. The structure diagram of AHP is shown in Figure 3. The AHP approach to evaluation entails three stages: the first stage is system decomposition, the second stage is safety judgment, and the third stage is comprehensive judgment.

4. Construction and Testing of E-Commerce Data Platform

The ecosystem of the Hadoop platform is shown in Figure 4. The commonly used large scale digital data instruments include tools such as Hadoop, HPCC, Inform, Rachel Drill, and Pentaho BI. The big data security system is the infrastructure that supports the security construction and

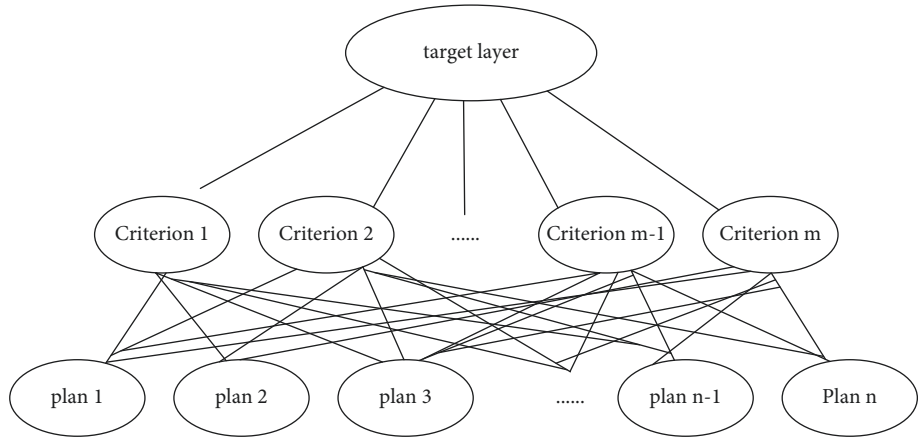

Figure 3: AHP structure diagram.

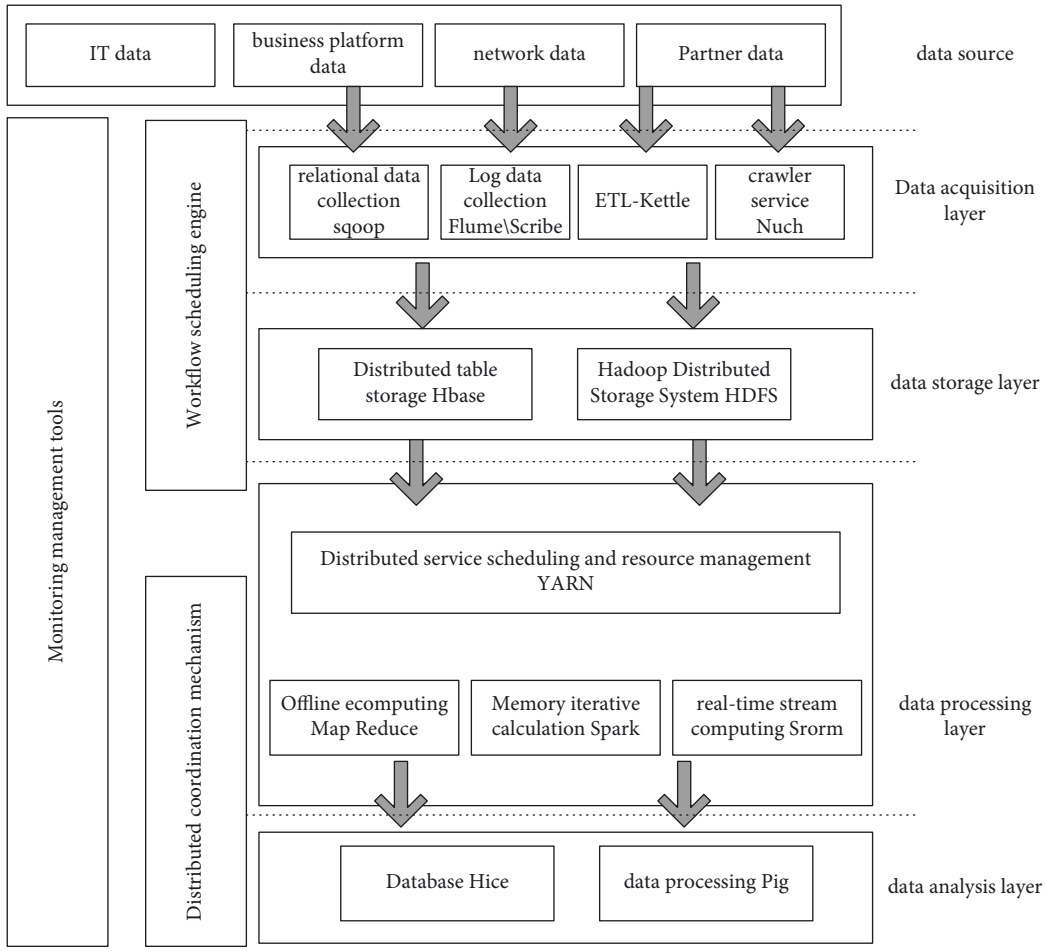

Figure 4: Hadoop platform ecosystem.

management of the big data platform system, taking into account the big data technology system and management system.

4.1. Big Data Platform Hadoop Architecture System. Initially, Hadoop was primarily used to administer huge volume of communal Internet pages, thus the security issues were not required to be considered in the design of Hadoop. The Hadoop platform includes functional modules such as file system, database, data processing, data warehouse, and big data analysis language interface. Hadoop's original vision

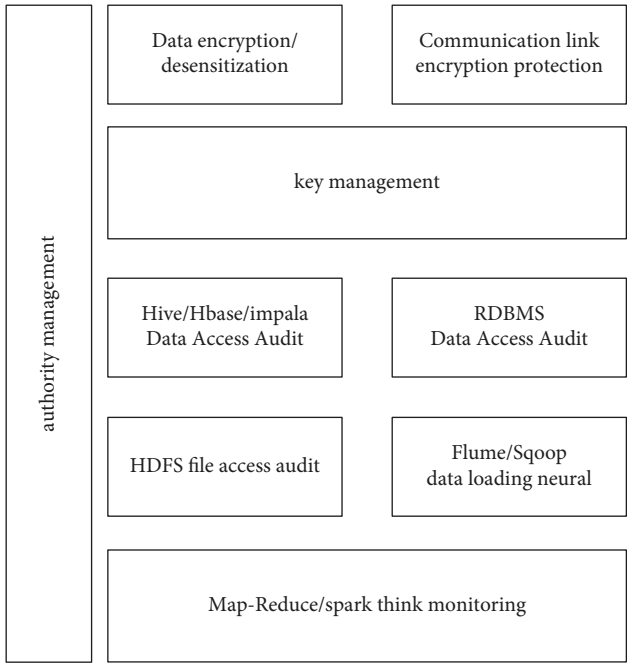

Figure 5: Key points of big data security risk assessment.

is a cluster based on a trusted environment. The main contents of the big data platform security risk assessment are as follows: protecting the boundary of the big data platform network, digitization of vulnerabilities, basic configuration inspection, weak password detection, version detection, maintenance management, deprivation, strategic data extraction and integration, comprehensive policy management, unified event analysis, full-text retrieval and data auditing, behavior for handling sensitive information, key security policies to support the management of structured and unstructured data. The evaluation points are shown in Figure 5.

Therefore, it is necessary to carry out a risk assessment of the big data platform according to the security requirements and level protection requirements of the big data system based on the characteristics of big data. For specific big data applications, the big data security architecture system is constructed and the corresponding security assurance techniques are studied to solve practical security problems.

The key issues to be considered in securing a Hadoop-based big data platform are as follows: authentication mechanism, authorization mechanism, access control, data hiding and encryption, secure deployment of network edge devices, system security, device security, auditing, and event monitoring. It is used to prevent the leakage, tampering and loss of sensitive data, unauthorized access to data, leakage of secret keys, violation of user privacy and so on.

4.2. E-Commerce Information Security Assessment Based on Vague Set. The concept of fuzzy set is a complex fuzzy approach to assessment grounded in vague collection policy, which is frequently applied in many fields with complex and objective evaluation results for multilevel, multidisciplinary, and multispecies evaluation. According to various possibilities, multiple hierarchical answers are obtained, and the final evaluation results are clear and systematic. It can effectively solve vague and difficult-to-quantify problems.

The definition is: A is the domain of discourse set, and any element in it is represented by V. A vague set P on A refers to a pair of membership functions on A: t_P and f_P.

$$t_P\colon A \longrightarrow [0,1], f_P\colon A \longrightarrow [0,1], \quad 0 \le t_P(x) + f_P(x) \le 1. \tag{2}$$

Here, $t_P(x)$ and $f_P(x)$ denote the lower bound of membership of supporting evidence, which is called the true membership function of vague set A. The membership of an element x in the vague set A is defined by a subinterval $[t_P(x), f_P(x)]$ on the interval (0 and1). The interval is the vague value of element x in A, denoted as $C_P(x)$. When A is a finite universe of discourse, that is, A is discrete, then the vague set P is expressed as follows:

$$P = \frac{\sum_{i=1}^{n} [t_P(x_i)1 - f_P(x_i)]}{x_i}. \tag{3}$$

When A is an infinite universe of discourse, that is, A is continuous, then the vague set P is expressed as follows:

$$P = \frac{\int_A [t_P(x_i)1 - f_P(x_i)]}{x\ dx}. \tag{4}$$

If $t_P(x)$ and $1 - f_P(x)$ are both 1 or 0, then the information about x is very accurate, depending on whether x belongs to the set vague. The set vague has degenerated into a normal set.

Fuzzy sets are tools used to describe dispersed message, and within message law, message entry entropy is the degree of information insecurity measured in probabilistic terms, and message entropy reflects the degree of disorder in a system. As an objective weighting method, this method of entropy weighting is mainly used to determine the weights of indicators and can be used for all evaluation problems. Just in the same way as the message entropy, the entropy of the vessel set can be considered, as well as the true and false attribution datasets. Based on the entropy formula and weight formula given by the information entropy value method, and based on these formulas, the formulas of vague entropy and weights are given. The decision or evaluation matrix is given in the message entropy algorithm as follows:

$$P = \left(a_{ij}\right)_{m*n}, \quad i \in M;\ j \in N, \tag{5}$$

where, m indicates the count of units to be tested, n refers to the list of metrics to be tested, and a_{ij} represents the evaluation value of the indicators in the i-th row and j-column. a_{ij} is normalized to get the following equation:

$$v_{ij} = \frac{a_{ij}}{\sum_{i=1}^{m} a_{ij}}, \quad i \in M;\ j \in N. \tag{6}$$

When computing the entity values of the assessment of j-th index, the identity of equity is given by the following equation:

$$E_j = -\frac{1}{\ln m}\sum_{i=1}^{m} V_{ij} \ln V_{ij}, \quad i \in M;\ j \in N. \tag{7}$$

In the vague set, the introduction of fuzzy entropy is to preserve the properties describing fuzzy sets $t_P(x)$, $f_P(x)$, and $\pi_P(x)$. Then, there are the following axiomatic formulas, where$t_P(x_i)$ and $f_P(x_i)$denote the normalized values, respectively. Assuming $A = \{X_1, X_2, \ldots X_n\}$, $P \in V(A)$, then we obtain the following equation:

$$\begin{aligned} E_t &= -\frac{1}{\ln m}\sum_{i=1}^{m} t_P(x_i) \ln\ t_P(x_i), \\ E_f &= -\frac{1}{\ln m}\sum_{i=1}^{m} f_P(x_i) \ln\ f_P(x_i), \text{ and} \\ E_{1-f} &= -\frac{1}{\ln m}\sum_{i=1}^{m} (1 - f_P)(x_i) \ln (1 - f_P)(x_i). \end{aligned} \tag{8}$$

And when $A = (0,0)$ or A=(1,1), E_t, E_f, and E_{1-f} are all 0. These three formulas have been proved to be reasonable and fully consider the unknown and uncertain information of the vagueness of the vague set, which is in line with the objective reality. E_t is called the fuzzy positive entropy of vague set A. E_f is called the fuzzy negentropy of vague set A.

E_j reflects the importance of the indicator. For a given j, if the evaluation index weight is larger, the difference of the described evaluation index will be greater and the entropy value of the evaluation index will be smaller. Therefore, the weight factor of the j-th index can be represented by entropy as follows:

$$W_j = \frac{1 - E}{\sum_{i=1}^{m}\left(1 - E_j\right)}, \quad j \in N \tag{9}$$

Therefore, in the vague set theory, considering the true and false membership, the formula for calculating the weight can be obtained as follows:

$$W_j^t = \frac{1 - E_j^t}{\sum_{i=1}^{m}\left(1 - E_j^t\right)}, W_j^f = \frac{1 - E_j^f}{\sum_{i=1}^{m}\left(1 - E_j^f\right)}, \quad j \in N. \tag{10}$$

With the weight formula, the comprehensive attribute value of each scheme or evaluation can be calculated according to the vague value of each indicator and the corresponding weight.

$$Z_i(w) = \sum_{j=1}^{n} a_{ij}, w_j, \quad i \in M. \tag{11}$$

In the vague set, the vague comprehensive attribute value of each indicator can also be calculated as follows:

$$\begin{aligned} Z_i(w_t) &= \sum_{j=1}^{n} t_P\left(a_{ij}\right), w_j^t, \quad i \in M, \\ Z_i\left(w_{1-f}\right) &= \sum_{j=1}^{n}\left(1 - f_A\left(x_{ij}\right)\right) w_j^{1-f}, \quad i \in M. \end{aligned} \tag{12}$$

4.3. Application of Vague Set Evaluation Model in E-Commerce Information Security Evaluation

4.3.1. First-Level Comprehensive Evaluation of E-Commerce Information Security Based on Vague Set. $n_y(ij)$ and $n_N(ij)$ are used to denote the number of "yes" and "no" given by n experts. Then, the degree to which indicator n_{ij} meets and does not meet the risk status in each comment can be calculated by the following formula:

$$t_{ij} = \frac{n_{Y(ij)}}{n} \ an\ d\ f_{ij} = \frac{n_{N(ij)}}{n}. \tag{13}$$

The evaluation opinions of various experts are counted, and the degree of satisfaction and dissatisfaction of the risk status in each comment can be calculated using the formula

$$\begin{aligned} W_{1j} &= (\,[0.1793, 0.1800], [0.2730, 0.2752], [0.2751, 0.2733], [0.2726, 0.2715]), \\ W_{2j} &= (\,[0.1820, 0.1739], [0.2277, 0.2148], [0.2846, 0.3019], [0.3058, 0.3095]), \\ W_{3j} &= (\,[0.2800, 0.2869], [0.2680, 0.2773], [0.2694, 0.2744], [0.1826, 0.1615]), \text{ and} \\ W_{4j} &= (\,[0.3303, 0.3360], [0.3360, 0.3280], [0.33360, 0.3336], j = 1, 2, 3, 4.). \end{aligned} \tag{14}$$

index A_{ij}, and the statistical results are expressed in vague as shown in Tables 2–5:

From the vague values given in these tables, each vague value is normalized, respectively. The calculations involved in the normalization process are all implemented with MATLAB to obtain a matrix. After a complete MATLAB calculation, the results are shown in Table 6.

According to the vague entropy value of each index attribute, the weight formula for calculating each secondary

Table 2: Vague values of each subindicator of network security.

	A_{11}	A_{12}	A_{13}	A_{14}
P_1	[0.30, 0.40]	[0.40, 0.55]	[0.60, 0.80]	[0.50, 0.70]
P_2	[0.40, 0.75]	[0.55, 0.80]	[0.45, 0.70]	[0.35, 0.60]
P_3	[0.20, 0.30]	[0.35, 0.65]	[0.35, 0.60]	[0.55, 0.70]
P_4	[0.10, 0.20]	[0, 0]	[0, 0]	[0, 0]
P_5	[0, 0]	[0, 0]	[0, 0]	[0, 0]

Table 3: Vague values of each subindicator of transaction security.

	A_{21}	A_{22}	A_{23}	A_{24}
P_1	[0.35, 0.50]	[0.25, 0.65]	[0.60, 0.80]	[0.35, 0.50]
P_2	[0.50, 0.75]	[0.60, 0.80]	[0.30, 0.50]	[0.55, 0.75]
P_3	[0.20, 0.30]	[0.20, 0.30]	[0.20, 0.40]	[0.10, 0.20]
P_4	[0.10, 0.20]	[0.10, 0.20]	[0, 0]	[0, 0]
P_5	[0, 0]	[0, 0]	[0, 0]	[0, 0]

Table 4: Vague values of each subindicator of data security.

	A_{31}	A_{32}	A_{33}	A_{34}
P_1	[0.70, 0.80]	[0.60, 0.70]	[0.65, 0.85]	[0.25, 0.55]
P_2	[0.40, 0.50]	[0.30, 0.40]	[0.35, 0.60]	[0.50, 0.60]
P_3	[0.30, 0.40]	[0.30, 0.40]	[0.45, 0.70]	[0.30, 0.50]
P_4	[0, 0]	[0, 0]	[0, 0]	[0.10, 0.20]
P_5	[0, 0]	[0, 0]	[0, 0]	[0, 0]

index attribute is obtained. The vague entropy value of each index attribute in Table 5 is substituted into the formula and the code is implemented with MATLAB, and the obtained weight of each index is as follows:

In the evaluation of e-commerce information security, in order to more clearly analyze the importance of evaluation indicators in each indicator layer, this paper decomposes the research object into actionable behavioral structures or features according to its essential properties or a certain point of the properties, and assigns weights to each element. It involves various influencing factors of the evaluation object and is also the premise of prediction and evaluation. Figure 6 can be used to express the weight composition of each indicator in network security, transaction security, data security, and physical security to make the expression more intuitive according to the weights given.

4.3.2. Second-Level Comprehensive Evaluation of E-Commerce Information Security Based on Vague Set. The second-level vague evaluation matrix of E-commerce information security is established to obtain the formula for normalizing the second-level indicators as follows:

Table 5: Vague values of each subindicator of physical security.

	A_{41}	A_{42}	A_{43}
P_1	[0.30, 0.50]	[0.55, 0.70]	[0.70, 0.80]
P_2	[0.30, 0.55]	[0.20, 0.60]	[0.40, 0.55]
P_3	[0.60, 0.80]	[0.35, 0.55]	[0.30, 0.50]
P_4	[0, 0]	[0, 0]	[0, 0]
P_5	[0, 0]	[0, 0]	[0, 0]

$$r^{t}_{A_j}\left(A_{ij}\right) = \frac{t_{A_j}\left(A_{ij}\right)}{\sum_{i=1}^{5} t_{A_j}\left(A_{ij}\right)}, \quad i = 1, 2, \ldots, 5,\ i = 1, 2, 3, 4 \text{ and}$$

$$r^{1-f}_{A_j}\left(A_{ij}\right) = \frac{1 - f_{A_j}\left(A_{ij}\right)}{\sum_{i=1}^{5} 1 - f_{A_j}\left(A_{ij}\right)}, \quad i = 1, 2, \ldots, 5,\ j = 1, 2, 3, 4. \tag{15}$$

The vague value of each second-level index in Table 6 is substituted into the formula, and the calculation process is also implemented by MATLAB, and the normalized result of the second-level index is expressed as a matrix as follows:

The entropy value formula and weight formula for calculating the index of the criterion layer are obtained from the formula, and the normalized value is brought into the corresponding formula to obtain the vague entropy value of each index of the criterion layer as follows:

$$\begin{aligned} E_1 &= [0.8056, 0.8231], \\ E_2 &= [0.7993, 0.8222], \\ E_3 &= [0.7984, 0.8153], \text{ and} \\ E_1 &= [0.6815, 0.6825]. \end{aligned} \tag{17}$$

Substituting E1, E2, E3, and E4 into the formula can get the weight of each standard layer indicator as follows:

$$\begin{aligned} W_1 &= [0.2124, 0.2064], \\ W_2 &= [0.2193, 0.2075], \\ W_3 &= [0.2203, 0.2156], \\ W_1 &= [0.3480, 0.3705]. \end{aligned} \tag{18}$$

From the weights of the indicators of the previous layer, the evaluation result of the higher layer can be calculated $P = W * \mathrm{R}$, that is, the final evaluation is as follows:

$$R = \begin{bmatrix} [0.3056, 0.2969] & [0.3056, 0.2965] & [0.3033, 0.2965] & [0.0855, 0.1105] & [0, 0] \\ [0.338, 0.3157] & [0.338, 0.3157] & [0.248, 0.2551] & [0.0840, 0.1134] & [0, 0] \\ [0.3317, 0.3039] & [0.3117, 0.3039] & [0.3117, 0.3039] & [0.0768, 0.0985] & [0, 0] \\ [0.3499, 0.3368] & [0.3062, 0.3264] & [0.3439, 0.3368] & [0, 0] & [0, 0] \end{bmatrix}. \tag{16}$$

Table 6: Vague entropy value of each indicator attribute of indicator layer.

	$j=1$	$j=2$	$j=3$	$j=4$
E_{1j}	[0.6865,0.6887]	[0.6749,0.6771]	[0.6725,0.57945]	[0.6755,0.6815]
E_{2j}	[0.7553,0.850]	[0.7130,0.7640]	[0.6435,0.6630]	[0.6250,0.6640]
E_{3j}	[0.6350,0.6640]	[0.6340,0.6740]	[0.6645,0.6270]	[0.7350,0.6450]
E_{4j}	[0.6590,0.6725]	[0.6531,0.6803]	[0.6656,0.7614]	

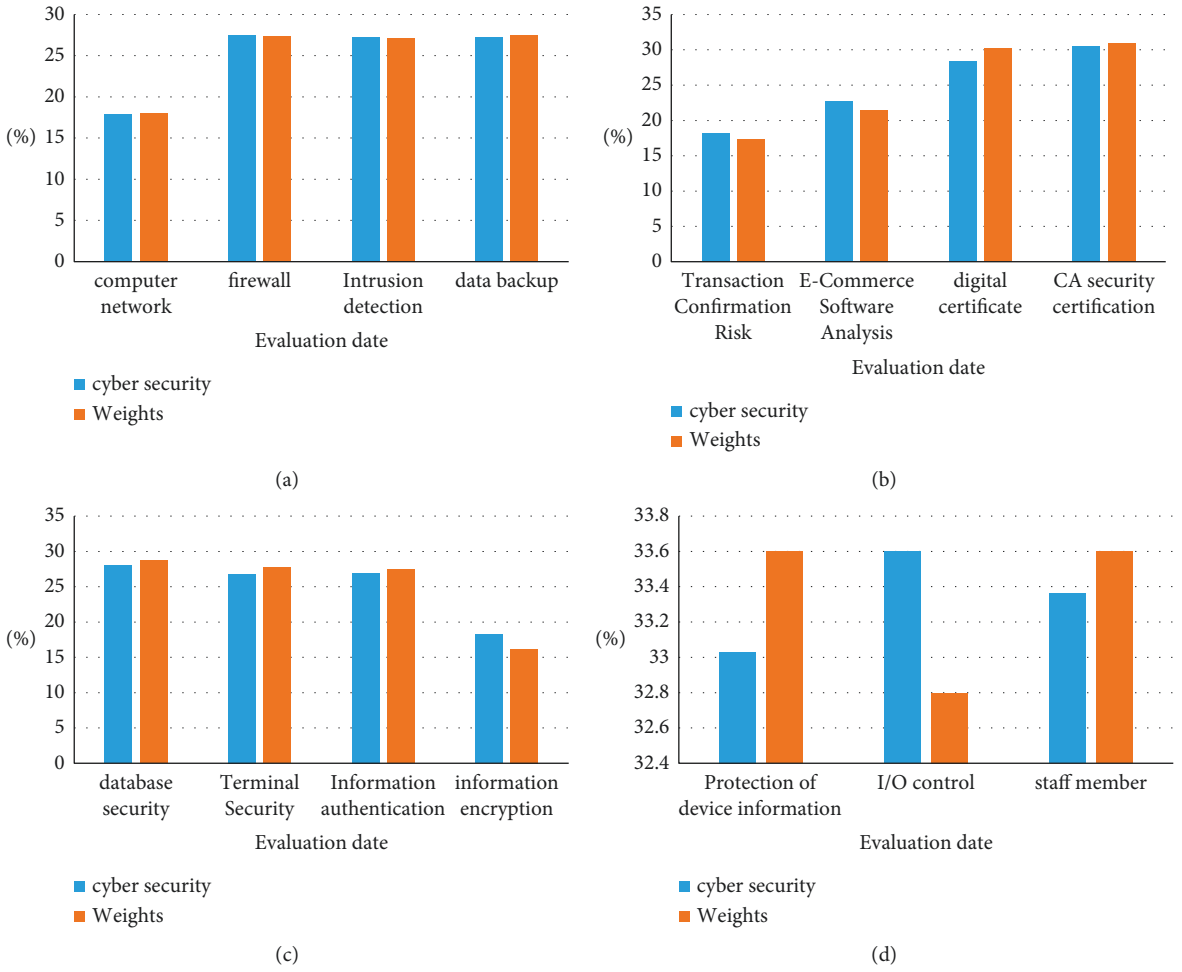

Figure 6: Indicator weight composition of network security, transaction security, data security, and physical security.

$$P = ([0.3480, 0.3368], [0.3062, 0.3264], [0.3439, 0.3368], [0.855, 0.1134], [0, 0]). \tag{19}$$

The final weight and final evaluation can be graphically represented as shown in Figure 7.

$$\begin{aligned} &S(E(P_1)) = -0.3152, S(E(P_2)) = -0.3674, \\ &S(E(P_3)) = -0.3193, S(E(P_4)) \\ &\quad = -0.8011, S(E(P_5)) = -1. \end{aligned} \tag{20}$$

As a result, the final sorting result is shown in Figure 8.

$$S(E(P_1)) > S(E(P_3)) > S(E(P_2)) > S(E(P_4)) > S(E(P_5)). \tag{21}$$

It can be seen from the chart that the comprehensive evaluation of the first and second level of E-commerce information security in the vague set, the weight of each indicator in network security, transaction security, data security, and physical security occupies a total of 100%. The final risk status is close to 0, so it can be concluded that the risk status of the E-commerce information security is "safe".

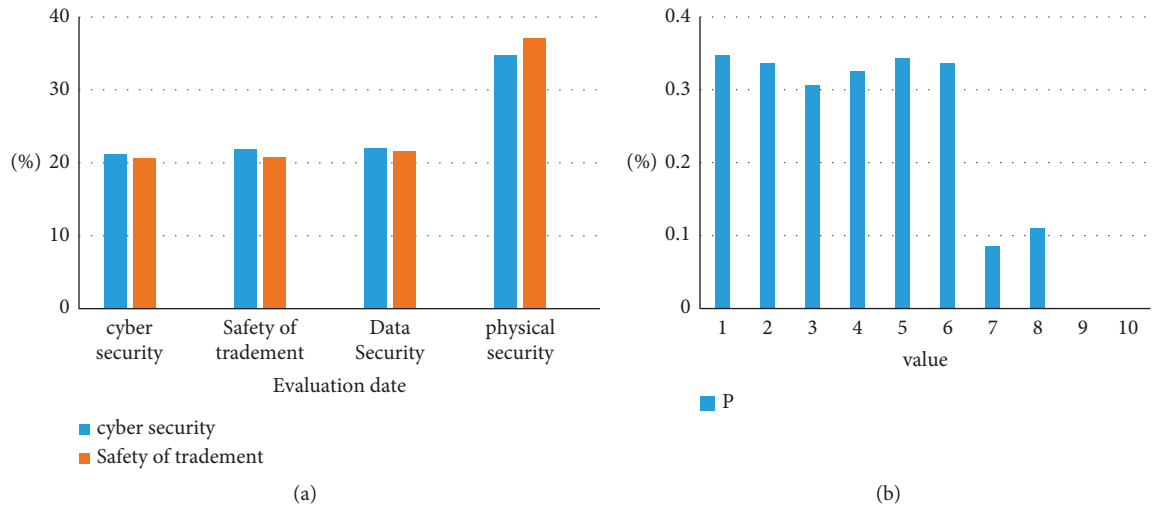

Figure 7: Analysis chart of criterion layer weight and final risk status evaluation result. Finally, according to the sorting function $S(E(A_i)) = t_{A_i} - f_{A_i}$, it can be gotten.

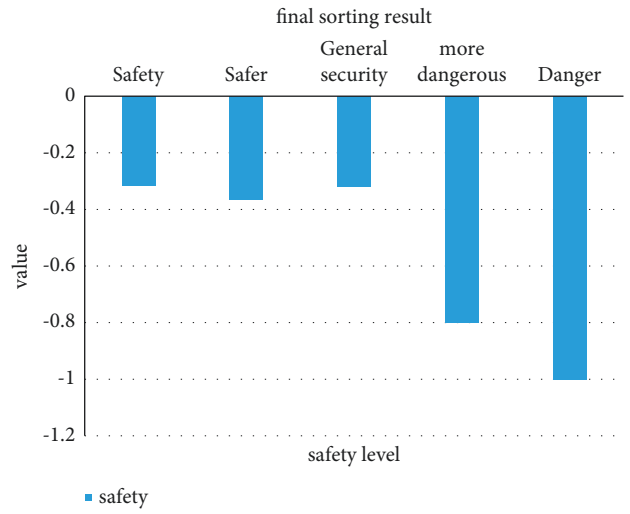

Figure 8: Final sorting result.

5. Discussion

E-commerce is a commercial activity that is based on the business theme, based on computer networks, and conducts business electronically under legal authorization. With the development of E-commerce, the amount of E-commerce data continues to grow, which poses an immeasurable threat to information security. Through the network layer of the IoT, the data interaction security evaluation of the sensing layer and the application layer, according to the influencing factors of E-commerce security, Delphi method, fuzzy comprehensive evaluation method, linear weighted evaluation method, grey cluster analysis method, analytic hierarchy process, and other related detection methods are mainly used in Hadoop environment to detect electronic information security.

The solution to the information security risks faced by E-commerce in the big data environment of the IoT is of great significance to promoting the development of E-commerce and even the national economy. It is hoped that there will be an effective security risk assessment model, which can solve the risk assessment problem of E-commerce information dynamics in the IoT environment and promote the safe, stable, and sustainable development of E-commerce and IoT data.

6. Conclusions

Through the Hadoop data analysis platform, this paper used the vague set method combined with the Delphi method, the fuzzy comprehensive evaluation method, the linear weighted evaluation method, the grey cluster analysis method, and the analytic hierarchy process to collect the predicted information security indicators and evaluate the E-commerce information security. The index system was divided into safe, relatively safe, general security, relatively dangerous, and dangerous grades, and expressed by the weight of each index in network security, transaction security, data security, and physical security so that the E-commerce information security issues could be expressed more intuitively. The application of vague set-based models and methods to E-commerce information security assessment is a research field that keeps pace with the times and meets urgent needs. E-commerce users should also pay attention to personal privacy protection, do not download files from unknown sources, and ensure that personal information is not stolen by others and cause unnecessary losses.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Key Laboratory of Eco-tourism in Hunan (STLV2003).

References

[1] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[2] G. Yang, Q. Zhang, and Y. C. Liang, "Cooperative ambient backscatter communications for green internet-of-things," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1116–1130, 2018.

[3] N. Ansari and X. Sun, "Mobile edge computing empowers internet of things," *IEICE - Transactions on Communications*, vol. E101.B, no. 3, pp. 604–619, 2018.

[4] M. Faraoni, R. Rialti, L. Zollo, and A. C. Pellicelli, "Exploring e-Loyalty Antecedents in B2C e-Commerce:empirical results from italian grocery retailers," *British Food Journal*, vol. 121, no. 2, pp. 574–589, 2019.

[5] S. Imtiaz, S. H. Ali, and J. K. Dong, "E-commerce growth in Pakistan: privacy securit and trust as potential issues," *Culinary Science&Hospitality Research*, vol. 26, no. 2, pp. 10–18, 2020.

[6] K. Miao, J. Li, W. Hong, and M. Chen, "A microservice-based big data analysis platform for online educational applications," *Scientific Programming*, vol. 2020, no. 239, 13 pages, Article ID 6929750, 2020.

[7] J. Thien, L. Reinpold, T. Brands, H. J. Koß, and A Bardow, "Automated physical property measurements from calibration to data analysis: microfluidic platform for liquid-liquid equilibrium using Raman microspectroscopy," *Journal of Chemical & Engineering Data*, vol. 65, no. 2, pp. 319–327, 2020.

[8] W. Yu, F. Liang, X. He et al., "A survey on the edge computing for the internet of things," *IEEE Access*, vol. 6, no. 99, pp. 6900–6919, 2018.

[9] T. Listyorini and R. Rahim, "A prototype fire detection implemented using the Internet of Things and fuzzy logic," *World Transactions on Engineering and Technology Education*, vol. 16, no. 1, pp. 42–46, 2018.

[10] T. Xu and I. Darwazeh, "Non-orthogonal narrowband internet of things: a design for saving bandwidth and doubling the number of connected devices," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2120–2129, 2018.

[11] H. Atlam, A. Alenezi, R. Khalid Hussein, and G. Wills, "Validation of an adaptive risk-based access control model for the internet of things," *International Journal of Computer Network and Information Security*, vol. 10, no. 1, pp. 26–35, 2018.

[12] L. Du, Y. Du, Y. Li et al., "A reconfigurable streaming deep convolutional neural network accelerator for internet of things," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 1, pp. 198–208, 2018.

[13] M. Papert and A. Pflaum, "Development of an ecosystem model for the realization of internet of things (IoT) services in supply chain management," *Electronic Markets*, vol. 27, no. 2, pp. 175–189, 2017.

[14] X. Lyu, H. Tian, L. Jiang et al., "Selective offloading in mobile edge computing for the green internet of things," *IEEE Network*, vol. 32, no. 1, pp. 54–60, 2018.

[15] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: establishing trust in the internet of things ecosystem using blockchain," *IEEE Cloud Computing*, vol. 5, no. 4, pp. 12–23, 2018.

[16] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Internet of things forensics: the need, process models, and open issues," *IT Professional*, vol. 20, no. 3, pp. 40–49, 2018.

[17] Y. Liu, P. Furth, and W. Tang, "Hardware-efficient delta sigma-based digital signal processing circuits for the internet-of-things," *Journal of Low Power Electronics and Applications*, vol. 5, no. 4, pp. 234–256, 2015.

[18] K. Zhang, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Mobile edge computing and networking for green and low-latency internet of things," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 39–45, 2018.

[19] M. Saad and M. Shahid, "The internet of things architecture, feasible applications and fundamental challenges," *International Journal of Computer Applications*, vol. 179, no. 39, pp. 52–55, 2018.

[20] H. Hallikainen and T. Laukkanen, "National culture and consumer trust in e-commerce," *International Journal of Information Management*, vol. 38, no. 1, pp. 97–106, 2018.