Hindawi
Mobile Information Systems
Volume 2022, Article ID 7501906, 11 pages
https://doi.org/10.1155/2022/7501906

Research Article

Information Disclosure of Network Platform and Corporate Social Responsibility Based on Cloud Computing

Yang Shengyong

School of Sociology and Public Administration, Guizhou University for Nationalities, Guiyang, Guizhou 550025, China

Correspondence should be addressed to Yang Shengyong; 1732261177@xzyz.edu.cn

Received 25 June 2022; Revised 11 July 2022; Accepted 21 July 2022; Published 8 August 2022

Academic Editor: Imran Shafique Ansari

With the development of information and cloud computing technology, the global data volume shows an explosive growth trend. Information has become the "circulating currency" supporting the data operation analysis of various industries, and it is the key for the website platform to obtain the core competitiveness. However, with the expansion of network transaction scale, information disclosure problems between various network platforms begin to appear. Users will continue to receive various marketing emails, SMS, and even harassing calls, which has brought great problems to users' life and led to users' refusal to disclose personal information. The network platform cannot obtain accurate information from users, so it cannot analyze and predict the bias of user behavior to provide personalized services, which undoubtedly hinders the development of the network platform. Therefore, how to promote users' information disclosure has become an urgent problem for network platform managers. Based on the multidimensional development theory, combined with the factors at the website and user level, this paper discusses its influencing factors and mechanism and develops the relevant research on privacy disclosure in a more in-depth and comprehensive way. Then, this paper studies corporate social responsibility. Stakeholders such as the government, the media, consumers, and the public all hope that enterprises will bear more social responsibility while obtaining economic benefits. Based on the analysis of relevant technologies of cloud computing network platform, this paper studies the information disclosure and corporate social responsibility of network platform so as to solve the existing problems.

1. Introduction

From the current development of cloud computing data at home and abroad, user groups are often at a disadvantage in personal information management. If users want to enjoy the shopping, communication, and consulting services of the platform, they must disclose their personal information to the platform or a third party, but there are still many deficiencies in the management of user information by the platform [1]. Firstly, this paper combs and analyzes the concepts, connotation, and related research of several variables involved in this paper, such as website trust, website reputation, and information sensitivity, defines the constituent dimensions and conceptual connotation of each variable, determines the variables of this research model based on multidimensional development theory, and deduces website trust. According to the influence relationship between variables such as privacy disclosure behavior, 20 theoretical hypotheses are proposed [2, 3]. Finally, 960 valid sample data were collected online and offline, and the research hypothesis was tested by SPSS 20.0. The results show that more than half of the supported hypotheses are 11, 7 are reverse supported, and 2 are not supported. The empirical analysis of this study draws the following four aspects. First, the trust and reputation of websites have a significant direct positive impact on privacy disclosure [4]. Second, website trust and reputation have opposite effects on users' privacy concerns, in which website trust is a positive impact, and website reputation is a negative impact. Third, the network privacy concerns of network platform users have a significant negative impact on their privacy disclosure behavior and play a partial intermediary role between website trust, website reputation, and privacy disclosure behavior [5]. Fourth, the moderating effect of information sensitivity

between website trust and network privacy concerns is not significant, and the relationship between website reputation and network privacy concerns has a significant positive moderating effect. In addition, this study also found that users' sensitivity to different types of information directly affects their privacy concerns [6]. Then, this paper analyzes corporate social responsibility. The development of corporate social responsibility information disclosure has gone from simple text information disclosure scattered in the annual report of enterprises to independent corporate social responsibility and environmental reports prepared by a large number of enterprises. The report shows that enterprises pay more and more attention to social responsibility information disclosure [7]. Is this phenomenon due to the mandatory provisions of the government and regulatory agencies, due to some needs of the company itself, or due to the pressure of social public opinion from stakeholders such as consumers, the media, and the public? There are different opinions on this issue in theory and practice, and no consistent conclusion has been reached [8]. Based on the mainstream theory of corporate voluntary social responsibility information disclosure-organizational legitimacy theory, this paper essentially analyzes the motivation of corporate voluntary social responsibility information disclosure and empirically tests the factors affecting corporate voluntary social responsibility information disclosure [9].

2. Related Work

The literature expounds the urgency of studying cloud computing data security access control mechanism, analyzes the research status of access control mechanism, discusses the benefits of attribute encryption applied to access control, and analyzes the shortcomings of existing access control solutions in solving data security problems. This paper proposes a ciphertext access control scheme based on hierarchical key management [10, 11]. The scheme encrypts the data plaintext and key hierarchically, the lower layer encrypts the plaintext, and the upper layer encrypts the key according to the data access policy to obtain two encrypted texts [12]. Only users who meet the attributes of the access policy can obtain the key by decryption and obtain the key of encrypted plaintext so as to decrypt and obtain plaintext. This method can strengthen the effective management of key, provide additional protection for plaintext, effectively avoid key leakage, ensure security, and reduce computing overhead [13]. This paper presents a data access control scheme for cloud computing based on integrity protection. In the scheme, the administrator role is added to manage the users in the group to facilitate the authorization of users. The group-oriented digital signature algorithm ElGamal is used to verify the accessibility signature of users in the group to ensure reliability and integrity [14]. The literature has solved the problems of inflexible access control and low efficiency. When the private key is generated for the user, the version number of the key is increased, and data exchange is realized between different entities by matching the version number of the key [15]. Only the latest version number can decrypt the ciphertext. When the attribute related to the user is revoked, it will no longer have the latest key version number and cannot apply for access to the data. In this way, the purpose of revoking the user attribute can be completed quickly without updating other user keys, saving the calculation cost of encryption and decryption and ensuring that the user can access the data legally [16]. A neural network model DenseNet-BiLSTM combining DenseNet and BiLSTM is proposed in the literature. DenseNet and BiLSTM are used to extract local features and temporal context information from speech, respectively.

3. Information Security and Information Disclosure of Network Platform Based on Cloud Computing

3.1. Theoretical Basis of Cloud Computing. Cloud computing platform is composed of multiple hosts, which can use the resources of each host to provide powerful storage and processing capabilities. Hadoop can integrate the storage resources of various hosts. Spark is an efficient cloud platform computing engine for iterative computing. The cloud computing platform based on Hadoop and spark can not only provide powerful storage capacity but also carry out iterative computing efficiently.

MapReduce is a programming model suitable for large-scale parallel data computing, which greatly promotes the deployment of programs in distributed systems. The main idea of MapReduce is to split the task into map and reduce processes, as shown in Figure 1. Each map runs on each node and processes the input fragments independently, so the map process is highly parallel. Reduce is the result of protocol merging map function processing. Reduce can also run independently on different nodes, so Reduce also has parallelism.

MapReduce uses JobTracker and TaskTracker master-slave models to provide high availability. JobTracker runs on the master node and is responsible for assigning each subtask to each TaskTracker. TaskTracker is a slave node, which is responsible for receiving and executing tasks. When a task executed by TaskTracker fails, it notifies JobTracker. JobTracker can list TaskTracker as an untrusted node or reschedule corresponding tasks according to the situation.

Spark can build a pseudodistributed architecture on a single machine or a distributed parallel computing framework on a cluster composed of multiple computers. At present, spark on yarn is the mainstream structure of spark distributed computing. Spark on yarn is divided into two modes: yarn cluster and yarn client. The former is suitable for production environment, and the latter is suitable for debugging and interaction. Figure 2 shows Spark's Yan cluster mode operation architecture.

First, the client sends the Application to the ResourceManager, and then the ResourceManager starts the ApplicationMaster on a NodeManager. The ApplicationMaster initializes the Spark Context and starts the application driver (Driver). Then, according to the needs of the client application, the ApplicationMaster applies for resources from the ResourceManager. Once the resource is applied for, the

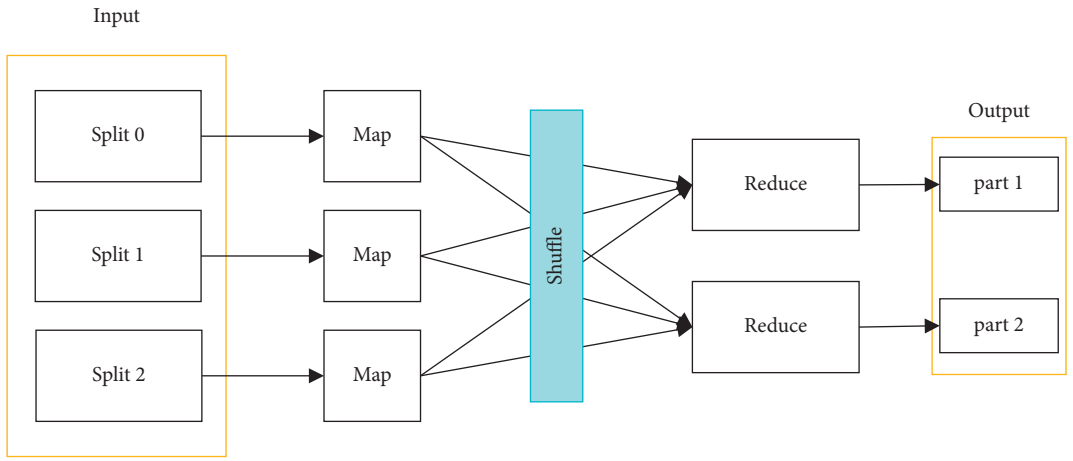

Figure 1: MapReduce processing flow.

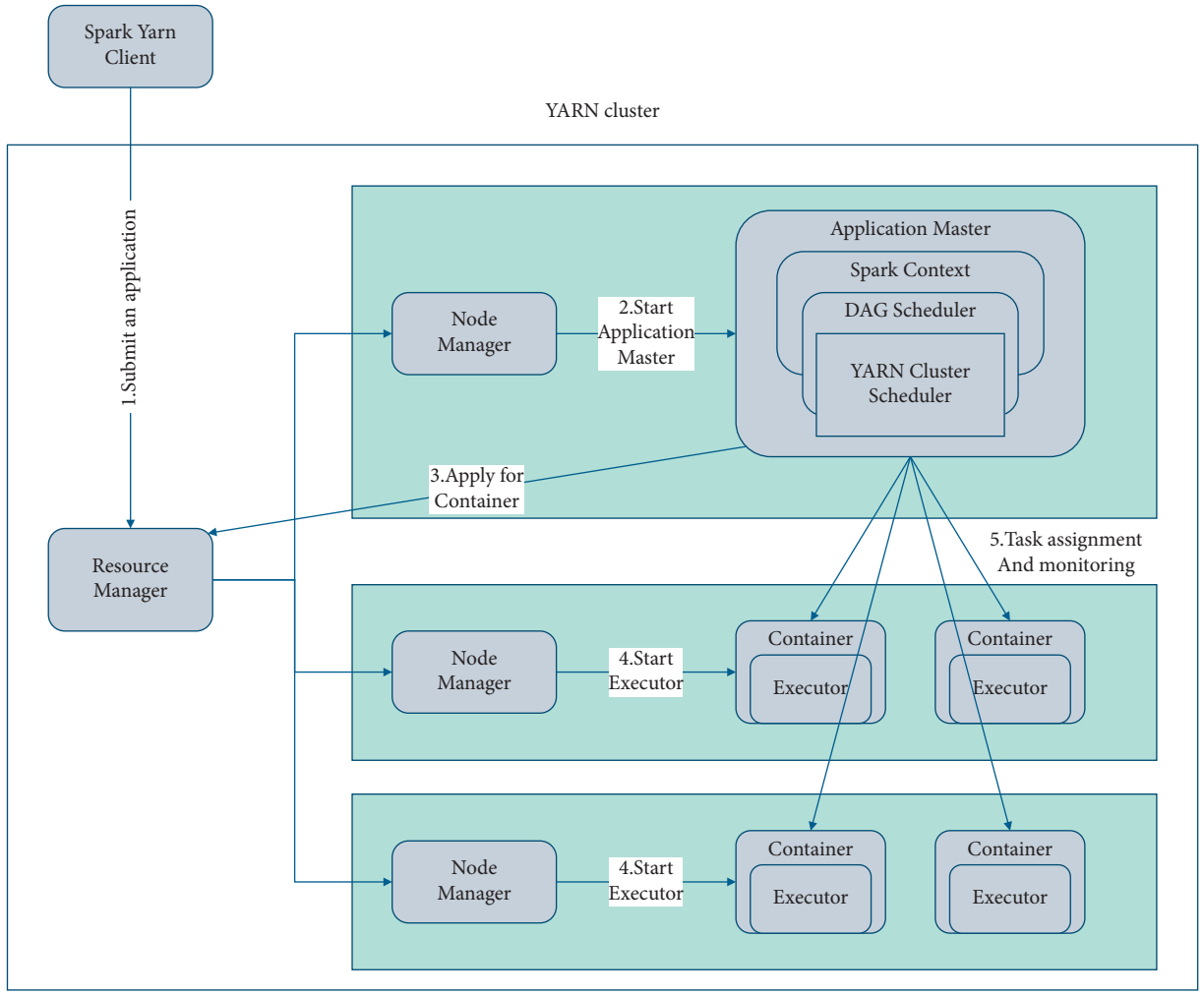

Figure 2: Operation architecture of spark in yarn cluster mode.

ApplicationMaster communicates with the corresponding NodeManager and starts the Container and Executor. Then, ApplicationMaster assigns tasks to Executors and monitors their execution status. When Application execution is complete, ApplicationMaster sends a logout request to ResourceManager and exits.

The key used for encryption and the key used for decryption in an asymmetric encryption algorithm are

different, and two keys cannot be derived from one key to the other. The RSA algorithm is a commonly used algorithm in asymmetric cryptographic algorithms. The private key is stored locally and transmitted in ciphertext. Even if it is intercepted, it is not easy to crack in terms of currently known data attacks. Theoretically, it is the most mature and complete public key cryptosystem. The high security of this encryption technology can ensure the confidentiality of data and can be applied to key distribution in cloud computing. Next, the cloud computing ciphertext access control scheme based on hierarchical key management will combine asymmetric encryption algorithms and symmetric encryption algorithms to encrypt data to ensure the security of data and keys.

The main steps of the RSA algorithm are as follows.

Choose prime numbers x, y (x, y are kept secret), and calculate the public modulus r and Euler function $\Psi(r)$:

$$r = xy; \psi(r) = (x-1)(y-1). \tag{1}$$

Choose random number z, satisfy $1 < z < \Psi(r)$, and generate parameter k:

$$k = z^{-1} \bmod (\psi(r)). \tag{2}$$

Encrypt the plaintext m to obtain the corresponding ciphertext c:

$$c = m^z \bmod r. \tag{3}$$

Decrypt the ciphertext c to obtain the corresponding plaintext m:

$$m = c^k \bmod r. \tag{4}$$

Here,

$$r = xy, \tag{5}$$

indicates the key length.

3.2. Cloud Computing Data Security Access Control Scheme Design

3.2.1. Key Generation Algorithm (KeyGen). Take the security parameter $1n$ as input, and output a pair of keys (pk, sk), which are the public key and the private key.

3.2.2. Signature Generation Algorithm (Sign). Take the private key sk and the message $m \in \{0, 1\}*$ as input, and output a signature σ, expressed as $\sigma \leftarrow \text{Signsk}(m)$.

3.2.3. Confirmed Verification Algorithm (Verify). Take the public key pk, message m, and a signature σ as input, and output a bit b. When $b = 1$, the signature is valid; when $b = 0$, the signature is invalid, which is expressed as

$$b = \text{verif}\, y_{pk}(m, \sigma). \tag{6}$$

Each user chooses a random number x (secure), $1 \le x \le p-1$, and calculates

$$y = \alpha^x \bmod p. \tag{7}$$

The signer performs hash compression on the message M to obtain the message hash code $H(M)$ and calculates

$$\begin{aligned} r &= \alpha^k \bmod p, \\ s &= (H(M) - xr)k^{-1} \bmod (p-1). \end{aligned} \tag{8}$$

Data integrity verification solutions include user administrators, cloud servers, attackers, and third-party audits. The entities and functions of the model are as follows:

(1) The user manager (Manager) is responsible for managing all users under the user manager. It is the user's controller and has the authority to grant user access rights, revoke users, and control the number of users. The user communicates with the administrator to join the group to gain access to cloud data. After receiving the request, the administrator allows the user to enter the group and provides them with a key. The user can access cloud data after verifying the digital signature, which is equivalent to the signer.

(2) The cloud service provider (CSP), the verifier in the model, has a storage computing function and can verify the user's signature and identify the user's identity.

(3) The third-party audit (AA, Automatic Auditor), after receiving the user's audit request, makes a request to the cloud service provider and then verifies the evidence returned by the cloud service provider to determine whether the data is complete.

The data integrity verification program model diagram is shown in Figure 3. The model is mainly to provide authorized users with cloud data access permissions and maintain data integrity. Any user must provide a digital signature before accessing cloud data. After the user is revoked, the third-party audit will no longer save the private key for him, and the user cannot access unauthorized data, thereby maintaining data integrity and gaining access control to cloud data.

In cloud computing, users can protect data integrity through digital signatures. In this model, the CSP stores the encrypted data uploaded by the data owner, and the user can decrypt the ciphertext after obtaining the corresponding key to obtain the data. After being verified by a third-party audit, if there is no match, the data cannot be accessed. Only after the cloud provider's signature verification is successful can the private key be used to decrypt the data, and the cloud provider can determine the user's identity based on the user's signature. When a user needs to be revoked, it is done by invalidating the user's signature or deleting his identity from the role-based user list stored by AA so that the user's attributes can be revoked easily and effectively.

Suppose there is a group containing multiple users in the cloud, and there is a group user administrator in the group, who has the authority to grant user access rights, revoke users, control the number of users, etc., and can assign roles

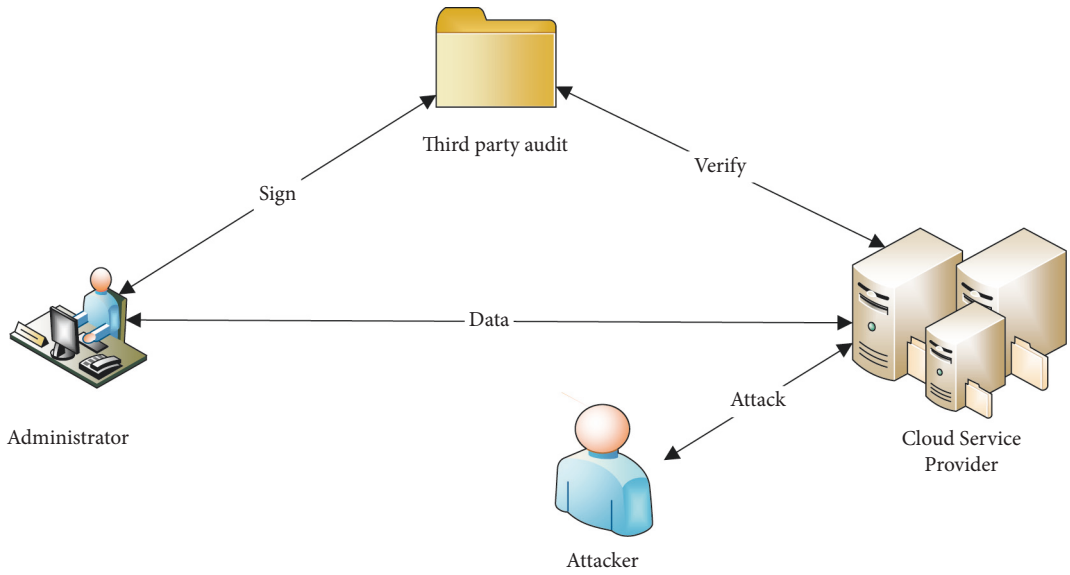

Figure 3: Model diagram of data integrity verification scheme.

according to the request of each user or revoke users in the group. Three users X, Y, and Z request to join the group. The administrator processes the request, distributes roles $R1$, $R2$, and $R3$ to the three users, generates digital signatures DS1, DS2, and DS3, and stores them in AA. Using the master key KM and the public key KP, combined with the user's identity, generate each user's private keys $K1$, $K2$, and $K3$. Users can access cloud data through digital signatures and private keys. Since private keys are differentiated based on the user's role and identity, the private keys are also completely different, and the data that can be accessed is also different. The user administrator can also delete a user from the user group and invalidate its signature and key so that the user cannot access the data again. The data exchange in the system is shown in Figure 4. When the user needs to verify the integrity of the cloud data, the data verification negotiation information should be sent to a third-party audit. After receiving the user's verification request, it will send a message to the cloud server. After the verification inquiry is received, the cloud server calculates the verification conclusion based on the information and submits it to a third party for audit. Then, a third-party audit monitors the accuracy of the verification conclusion, and if it is correct, it indicates that the cloud data is complete. Otherwise, it means that the integrity of the data may have been destroyed.

The user sends an application to the group manager. When applying to join the group, the user manager obtains the user's identity, calculates the user's ID Ai, and stores it in the RL role list in the group. When Ai is a newly set value, the group administrator generates a role for it. The user will have the same permissions as other users and can share data for data access processing.

$$A_i = x^{(\alpha+H_1)} \prod_{j=1}^{n} (\alpha + H_1),$$
$$A_i \longrightarrow \text{rolesset}(\alpha + H_1). \tag{9}$$

3.2.4. Delete User. When the user attribute changes or leaves the group, CSP will mark the user key for special processing and calculate RI. The signer's private key and the group user's public key are used to calculate the digital signature. Therefore, it is impossible to infer which user in the group has generated the signature through key verification. CSP gives RI to the group administrator. When the group administrator receives the user role RI, it determines the user's identity through calculation and deletes the user from the RL role list. When the user logs in again, even if he has the key, you do not have permission to access, continue to view, and modify data, and you can complete the user attribute revocation operation.

$$R_i = x^{\prod_{j=1}^{n} (\alpha+H1).} \tag{10}$$

The user administrator sends the user ID Ai to AA, and I used the ElGamal encryption algorithm to generate a digital signature for the user according to the master key. IDU represents the identity of each role. DS is a digital signature generated by the user.

$$\begin{aligned} &\text{DS} \leftarrow \text{SignGen}(\text{IDU}, K_M, B(s)), \\ &B(s) = \text{rand}(k_1, k_2, \ldots, k_n), \\ &\text{DS} = \exp(g, \text{mult}(d, f)). \end{aligned} \tag{11}$$

The meaning of the symbols is shown in Table 1.

3.2.5. Data Integrity Analysis. After obtaining reasonable permissions, the cloud user submits an audit request to AA, conducts data integrity audit and disclosure, and obtains user data integrity audit results. If the data verification is complete, the result returns success; otherwise, it returns failure. If the result of the data integrity verification is correct, then the following equation holds true, and the left and right sides are equal.

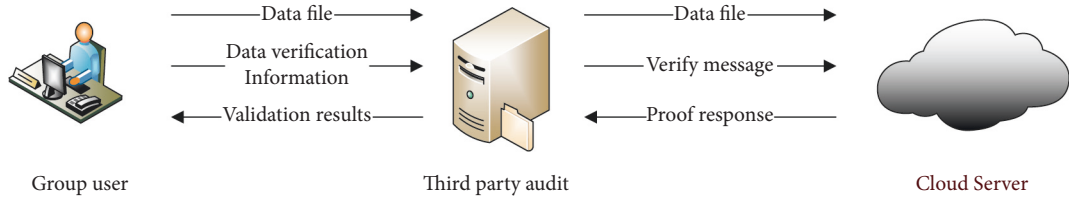

Figure 4: Data integrity verification process.

Table 1: Meaning of symbols.

Symbol	Meaning
Z_q^*	A prime field with nonzero elements
i	The data block number
id_i	The identity of the user
Vi	Random select from Z;
x_j	The group member s secret key
x_j'	The group member^s partial secret key

$$\hat{e}\left(\prod_{i\in I} H(id_i)^{v_i}\cdot u^{\mu}, PK\right) = \hat{e}(g,\sigma). \tag{12}$$

First, simplify the equation:

$$\begin{aligned}
\sigma_i &= \sigma_i'\cdot (PK/g^{x_j})^{-r_j}\left(H(id_i)\cdot\mu^{\delta_i}\right)^{x_j},\\
\sigma_i &= \left(H(id_i)\cdot\mu^{\delta_i}\cdot g^{r_j}\right)^{x_j\prime}\cdot\left(\frac{g^x}{g^{x_j}}\right)^{-r_j}\left(H(id_i)\cdot\mu^{\delta_i}\right)^{x_j},\\
\sigma_i &= \left(H(id_i)\cdot\mu^{\delta_i}\right)^{x}.
\end{aligned} \tag{13}$$

The second step is to audit data integrity:

$$\begin{aligned}
\hat{e}(g,\sigma) &= \hat{e}\left(g,\prod_{i\in I}\sigma_i^{v_i}\right),\\
\hat{e}(g,\sigma) &= \hat{e}\left(g,\prod_{i\in I}\left(\left(H(id_i)\cdot\mu^{\delta_i}\right)^{x}\right)^{v_i}\right),\\
\hat{e}(g,\sigma) &= \hat{e}\left(g,\prod_{i\in I}\sigma_i^{v_i}\right),\\
\hat{e}(\mathrm{g},\sigma) &= \hat{e}\left(\mathrm{g},\prod_{\mathrm{i}\in \mathrm{I}}\left(\mathrm{H}(\mathrm{id_i})\cdot\mu^{\delta_i}\right)^{\mathrm{x}}\right)^{\mathrm{v_i}},\\
\hat{e}(\mathrm{g},\sigma) &= \hat{e}\left(\mathrm{g}^{\mathrm{x}},\prod_{\mathrm{i}\in\mathrm{I}}\left(\mathrm{H}(\mathrm{id_i})^{\mathrm{v_i}}\cdot\mu^{\sum_{\mathrm{i}\in\mathrm{I}}\delta_{\mathrm{i}}\mathrm{v_i}}\right)\right),\\
\hat{e}(\mathrm{g},\sigma) &= \hat{e}\left(\prod_{\mathrm{i}\in\mathrm{I}}(\mathrm{H}(\mathrm{id_i})^{\mathrm{v_i}}\cdot\mu^{\mathrm{u}},\mathrm{PK}\right).
\end{aligned} \tag{14}$$

3.3. Analysis of the Status Quo of Information Disclosure on Online Platforms. Generally speaking, the results obtained when the sample size is 10–20 times the number of items have good reliability and validity. In this study, a total of 960 valid sample data were collected, which was 18 times the item items. The actual questionnaire effective rate was 90.38%. The SPSS 20.0 program was used for descriptive statistical analysis. The results are shown in Table 2.

It can be seen from Table 3 that the CITC values of all items of the privacy disclosure behavior are above 0.5, which are all greater than 0.4, and Cronbach's α is 0.758, indicating good reliability.

The exploratory factor analysis results of privacy disclosure behavior are shown in Table 4.

It can be seen from Table 5 that the standardized factor loads of each variable element in this study are all greater than 0.5, all at the level of 0.001, which is significant. The combined reliability (CR) of each variable is greater than 0.6, and the extraction of the average variance (AVE) of each variable is greater than 0.5. The above data results show that the scale has high convergent validity and discriminative validity.

Before hypothesis testing, statistical analysis is performed on the standard deviation, average value, and correlation between variables. Table 6 shows that there is a significant correlation between the variables, so the next step hypothesis testing analysis can be performed.

In general, this paper contains two hypotheses. One is the mediating role of network privacy concerns, and the other is the regulatory role of information sensitivity.

The first part is the intermediary effect test. Based on the viewpoint of data, this paper first investigates the relationship between website trust, website reputation, and network privacy concerns, that is, whether there is a significant influence relationship between independent variables and intermediary variables. Finally, the independent variables and intermediate variables are added to the model at the same time to observe whether the influence of independent variables and dependent variables changes. In addition, on the basis of referring to previous studies, combined with the research objects and situations of this study, age, education level, Internet age, and times of distress are taken as variables.

The second part is inspection. Test the moderating effect of information sensitivity between website trust, website reputation, and privacy disclosure behavior, namely, hypothesis 4 and hypothesis 5. This paper uses age, education, Internet age, and the number of privacy problems as control variables to verify that information sensitivity plays an intermediary role in the relationship between website trust, website reputation, and network privacy concerns.

Table 2: Descriptive statistics of the sample ($N = 960$).

Feature	Classification	Sample size	Proportion %	Feature	Classification	Sample size	Proportion %
Gender	Male	645	67.2	Frequency of privacy distress	Very frequently	107	11.1
	Female	315	32.8		More often	327	34.1
Number of online purchases	At least once a day	27	2.8		Generally	387	40.3
	At least once a week	294	30.6		Less	134	14.0
	At least once a month	431	44.9		Never	5	0.5
	At least once a quarter	133	13.9	Use computer to surf the Internet	More than 8 hours	155	16.1
	At least once a year	56	5.8		4–8 hours	373	38.9
	Never	19	2.0		1–3 hours	386	40.2
Exposure to information abuse report frequency	Very frequently	79	8.2		0 hours	46	4.8
	More often	345	35.9	Use mobile phone to surf the Internet	More than 8 hours	193	20.1
	Generally	402	41.9		4–8 hours	393	40.9
	Less	117	12.2		1–3 hours	367	38.3
	Never	17	1.8		0 hours	7	0.7

Table 3: Reliability analysis of privacy disclosure behavior.

Dimension	Question	CITC value (>0.4)	Cronbach's alpha (>0.7)
Privacy disclosure	Q1	0.672	0.758
	Q2	0.553	
	Q3	0.565	

Table 4: Exploratory factor analysis results of privacy disclosure behavior.

Variable	Question	F1
Privacy disclosure	Q1	0.873
	Q2	0.798
	Q3	0.802
The KMO value is 0.700, and the chi-square value of Bartlett's sphere test is sig < 0.000		

Table 5: Scale convergent validity test.

Variable	Question	Normalized factor load	Combined reliability (CR)	AVE	Variable	Question	Normalized factor load	Combined reliability (CR)	AVE
Control	Q1	0.89	0.91	0.77	Secondary use	Q1	0.61	0.91	0.71
	Q2	0.92				Q2	0.87		
	Q3	0.83				Q3	0.94		
Collect	Q1	0.83	0.88	0.71		Q4	0.93		
	Q2	0.91			Website trust	Q1	0.73	0.86	0.58
	Q3	0.78				Q2	0.89		
Mistake	Q1	0.68	0.84	0.64		Q3	0.76		
	Q2	0.88				Q4	0.72		
	Q3	0.83			Website reputation	Q1	0.86	0.88	0.75
Improper access and remedy	Q1	0.67	0.91	0.61		Q2	0.92		
	Q2	0.82				Q3	0.83		

Table 6: Descriptive statistical analysis and correlation coefficients between variables.

	Mean value	Standard deviation	XI	X2	X3	X4	X5
Online privacy concerns	4.2886	0.48517	1	—	—	—	—
Privacy disclosure	2.8907	0.79826	0.128	1	—	—	—
Website reputation	3.7148	0.74908	288	0.202	1	—	—
Website trust	3.0058	0.80508	0.129	0.364	0.087	1	—
Information sensitivity	2.6396	0.69834	0.178	0.372	−0.005	0.303	1

4. Research on Corporate Social Responsibility Information Disclosure

4.1. Data Sources. In recent years, the number of private listed companies in China has increased year by year, gradually changing from the vulnerable group in China's capital market to almost the same as the state-owned listed companies in the market. As of December 31, 2020, there were 2342 listed companies in the two cities, including 1162 private listed companies, accounting for 49.6% of the total number of listed companies in the market. From the perspective of plate structure, the SME board has been an important part of private listed companies since it was listed and established in a stock exchange on June 25, 2013. As of December 31, 2020, a stock exchange has 1411 listed companies, including 484 on the main board, 646 on the small and medium-sized board, and 281 on the GEM board. According to statistics, of the 1411 companies listed in a city, 964 are private listed companies, accounting for 68.32%. These 964 private listed companies are specifically distributed in 190 main boards, 515 small and medium-sized boards, and 259 GEM boards, accounting for 39.26%, 79.72%, and 92.17%, respectively. Considering the short listing time of GEM, as of this survey, listed companies have only disclosed 2019 annual report and 2020 annual report at most, the operation is still not mature, and the threshold of listing conditions is low. Firstly, the basic data is obtained from the database of a private listed company and then manually checked one by one according to the 2020 annual report. In the process of checking, it is found that the basic data obtained from a company has some errors and is incomplete. After checking the ownership structure of its 2020 annual report, 26 listed companies found that their controlling shareholders are overseas legal persons, but their actual controllers are one or more natural persons holding Chinese or foreign passports. Based on the definition of the concept in this paper, these companies should not be regarded as foreign shares but should be regarded as private and included in the scope of this paper.

Consider that, in recent years, a stock exchange requires the component companies of "Shenzhen 100 index" to disclose the social responsibility report at the same time as the annual report and disclose it separately. Therefore, this paper excluded 12 private listed companies on the small and medium-sized board from the list of Shenzhen 100 index published on the website of Shenzhen Stock Exchange on February 1, 2012, and obtained 529 voluntary disclosure of listed companies on the small and medium-sized board. Next, The authors selected 265 listed companies with odd securities codes. After excluding st securities code 002113 in the current year, the sample is 264 companies. In addition, the sample number of empirical analyses on the influencing factors of voluntary social responsibility information disclosure of listed companies with securities code 002551 is 263. The Tobin Q value of listed companies with securities code 002645 is missing, which is eliminated, and the number of samples finally entering the empirical analysis of voluntary social responsibility information disclosure effect of private listed companies is also 263. The 2020 annual report and 2020 social responsibility report of each listed company were obtained from the website of Shenzhen Stock Exchange, and a total of 263 annual reports and 30 independent social responsibility reports were obtained. In addition to the annual report information and social responsibility report of listed companies obtained on the website of a stock exchange, the Tobin Q value of listed companies comes from a China Economic and financial database, and the data of other private listed companies comes from a financial database.

4.2. Research Assumptions and Model Construction. The factors affecting corporate social responsibility information disclosure come from two aspects: external driving factors and internal driving factors. External factors determine the social pressure faced by enterprises, including laws and regulations, regional distribution, industry type, media attention, customer and competitor behavior, and requirements of nonprofit organizations such as industry associations. Internal factors determine how enterprises deal with social pressure, including corporate characteristic variables, such as corporate size, corporate profitability, corporate debt level, and equity concentration, and corporate governance structure variables, such as the size of the board of directors, whether the chairman and the general manager are one. According to the legitimacy theory, enterprises with great social pressure should seek legitimacy to ensure the normal operation and development of enterprises and are more inclined to disclose more social responsibility information to obtain legitimacy. Enterprises with large scale, good profitability, and high debt ratio also need to maintain legitimacy to ensure that enterprises expand operation, continue to make profits and obtain loans, and tend to disclose more social responsibility information. Enterprises with good corporate governance structure and high equity dispersion tend to actively respond to social pressure and disclose more social responsibility information.

There is no doubt that corporate voluntary social responsibility information disclosure will bring costs to enterprises. Regardless of whether the disclosure of social

responsibility information can benefit enterprises, not all enterprises can and are willing to bear the cost of disclosure. The data show that there is a significant positive correlation between voluntary information disclosure and company size because large enterprises increase costs due to the increase of voluntary information disclosure, large enterprises can hire professional technicians and adopt complex reporting systems, and the public and institutional analysts' demand for large enterprise information is increasing. According to the legitimacy theory, large enterprises have broader objectives, are more likely to become the focus of attention from all walks of life, and face higher political costs and wider information needs from investors and stakeholders. Large enterprises tend to disclose more social responsibility information in terms of disclosure costs and reasons so as to establish a good market image and corporate reputation, reduce government control and public pressure, and enhance their legitimacy.

In China, especially the voluntary disclosure of corporate social responsibility information, the nonmandatory requirements of the regulatory authorities will certainly produce disclosure costs. Therefore, according to the reporting theory, the more profitable the company is, the more it can bear the costs of performing social responsibility and information disclosure. The performance of social responsibility and information disclosure can bring greater economic benefits to the company by displaying a good corporate image to stakeholders. After obtaining benefits, the company has more motivation to perform social responsibility and corresponding information disclosure. This forms a virtuous circle.

In order to test the above assumptions, the following two regression models are established in this section:

$$\begin{aligned}\text{CSDquan} &= \beta_0 + \beta_1 MPin + \beta_2 MPpn + \beta_3 IN\ D + \beta_4 PREd \\ &\quad + \beta_5 SIZEmplo + \beta_6 SIZEta + \beta_7 ROE + \beta_8 LEV \\ &\quad + \beta_9 SS + \beta_{10} BS + \beta_{11} RD + \beta_{12} CRC + \varepsilon, \\ \%\quad \text{CSDqual} &= \beta_0 + \beta_1 MPin + \beta_2 MPpn + \beta_5 IN\ D + \beta_4 PREd \\ &\quad + \beta_5 SIZEmplo + \beta_6 SIZEta + \beta_r ROE + \beta_8 LEV \\ &\quad + \beta_9 SS + \beta_{10} BS + \beta_{11} RD + \beta_{12} CRC + \varepsilon. \end{aligned} \tag{15}$$

4.3. Descriptive Statistics of Influencing Factors of Corporate Social Responsibility Information Disclosure. The descriptive statistics of variables are shown in Table 7. The highest score of CSR information disclosure quantity of sample companies is 62, the lowest is 1, the mean value is 19.23, and the standard deviation is 9.18.

4.4. Regression Analysis of Factors Affecting Corporate Social Responsibility Information Disclosure. First, perform a normal PP diagram test on model 1 (see Figure 5). The results show that the fitting value of the dependent variable corporate social responsibility information disclosure quantity (CSDquan) is approximately on a straight line, conforms to a normal distribution, and satisfies the prerequisites for using the least square method.

Using the stepwise regression method, the variables that enter model 1 are the major shareholder's shareholding ratio (SS), the combination of chairman and general manager (RD), and the corporate social responsibility committee (CRC). The variance inflation factor (VIF) of each variable is close to 1, indicating that there is no multicollinearity problem. The Durbin-Watson value is 1.667, which means that there is no autocorrelation problem. After the model is adjusted, R^2 is 0.078; that is, the overall explanation of the independent variable to the dependent variable in the model is 7.8%, $F = 8.405$, and sig. = 0.000, indicating that the F value is significant at the 1% significance level, which indicates that regression model 1 is statistically valid.

Judging from the coefficients of the regression equation in Table 8, the standardized coefficient of the independent variable's major shareholder's shareholding ratio (SS) is 0.223, and the significance is 0.000, indicating that it is at the 1% significance level, and the information disclosure of the dependent variable corporate social responsibility (CSDquan) is significantly positively correlated, which is in line with the expected direction of the hypothetical H6a. It indicats that the higher the estimated stock concentration, the more corporate social responsibility information disclosure. The standardized coefficient of the independent variable chairman and general manager's integration (RD) is −0.168, and the significance is 0.006, indicating a significant negative correlation with the number of dependent variable social responsibility information disclosures (CSDquan) at the 1% significance level. It is consistent with the expected direction of Hypothesis H8a, indicating that the number of social responsibility information disclosures of a company whose chairman and general manager are the same person is lower than that of a company whose chairman and general manager are not the same person. The independent variable corporate social responsibility committee (CRC) has a standardized coefficient of 0.146 and a significant degree of 0.017, indicating that it is significantly positively correlated with the number of dependent variable corporate social responsibility information disclosures (CSDquan) at the 5% significance level and is in line with the expected direction of hypothesis H9a Consistent, indicating that the number of corporate social responsibility information disclosures that have established a social responsibility committee is higher than that of companies that do not have such a department. Other variables did not pass the significance test.

First, perform a normal P–P chart test on model 2 (see Figure 6). The results show that the fitted value of the dependent variable corporate social responsibility information disclosure quality (CSDqual) is approximately on a straight line, conforms to a normal distribution, and satisfies the prerequisites for using the least square method.

Using the stepwise regression method, the only variable that enters model 2 is the asset-liability ratio (LEV). The variance inflation factor (VIF) of each variable is close to 1, indicating that there is no multicollinearity problem. The Durbin-Watson value is 1.382, which means that there is no autocorrelation problem. After the model is adjusted, R^2 is

Table 7: Descriptive statistics of influencing factors model variables of voluntary social responsibility information disclosure.

	CSDquan	CSDqual	MPin	MPpn	SIZEmpIo	SIZEta	ROE	LEV	SS	BS
Sample	263	263	263	263	263	263	263	263	263	263
Minimum	1	1	405	0	4.94	18	−50.45	0.76	11.77	6
Max	62	38	1500000	278	9.93	23.58	29.24	89.47	89.98	14
Mean	19.23	10.77	32737	7.46	7.32	21.27	8.68	31.04	59.74	8.69
Standard deviation	9.18	5.78	105551	18.05	0.91	0.68	6.45	18.64	13.82	1.59
Variable	IND	—	RD	—	CRC	—	—	—	—	—
Minimum	0	—	0	—	0	—	—	—	—	—
Max	1	—	1	—	1	—	—	—	—	—
Frequency 0	62	23.1%	159	60%	263	99.6%	—	—	—	—
Frequency 1	203	76.9%	106	40%	1	0.4%	—	—	—	—
Number of samples	264	100%	263	100%	263	100%	—	—	—	—

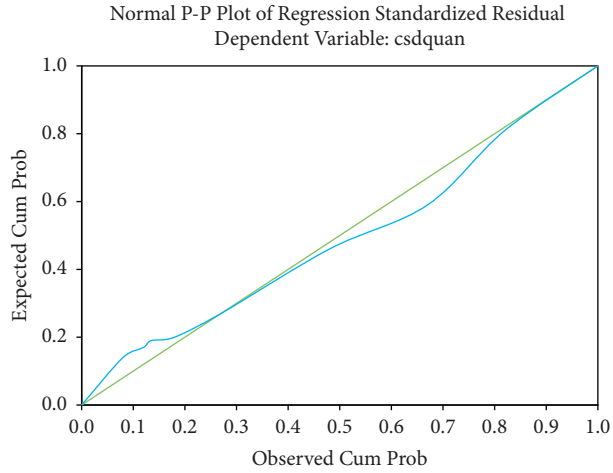

Figure 5: *P–P* chart test for the normality of the number of corporate social responsibility information disclosures.

Table 8: Regression estimation results of the number of voluntary social responsibility information disclosures.

Variable	Regression coefficient	Standard deviation	T value	Significance level	Expansion factor
Constant	11.584	2.459	4.713	0.000	—
SS	0.223	0.041	3.732	0.000	1.009
RD	−0.168	1.113	−2.835	0.006	1.004
CRC	0.146	8.882	2.432	0.017	1.014
AdjR^2 = 0.078 F = 8.405 (sig = 0.000) D–W = 1.667					

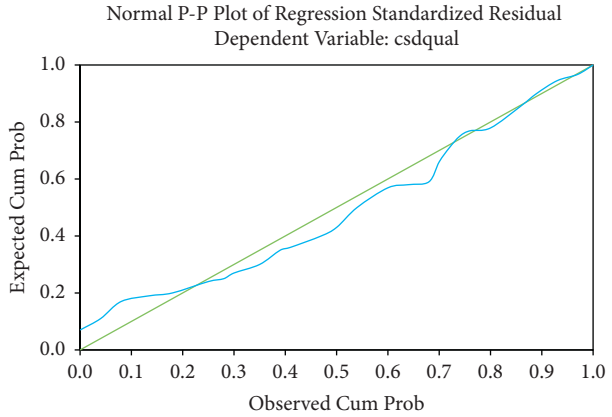

Figure 6: *P–P* diagram test of the normality of corporate social responsibility information disclosure quality.

0.034; that is, the overall explanatory degree of the independent variable to the dependent variable in the model is 3.4%, F = 10.146, and sig. = 0.002, indicating that the F value is significant at the 1% significance level, indicating that regression model 2 is statistically valid.

5. Conclusion

With the continuous expansion of Internet users, the transaction scale of online shopping market is also growing. With the help of the Internet, the network platform can obtain user data, business data, and competitive data from the website through various methods and channels for analysis and processing and extract and analyze user behavior habits. In recent years, user information disclosure events have occurred on many large network platforms,

including Facebook. After information disclosure, the platform has almost no compensation measures for users, but users are likely to be harassed by continuous information such as email, SMS, and telephone. These possible privacy risks and insecurity will prevent users from disclosing their personal information in the process of purchasing products or services. In order to answer the above questions, this study collected 960 sample data through a questionnaire survey for theoretical hypothesis verification and analysis. Then, this paper studies corporate social responsibility. Based on a systematic review of the literature on the motivation, influencing factors, and effects of corporate social responsibility information disclosure at home and abroad, this paper focuses on the institutional background and organizational legitimacy theoretical framework of corporate social responsibility information disclosure, investigates and analyzes the current situation and motivation of corporate social responsibility performance and information disclosure in China, and empirically verifies the factors and effects of voluntary social responsibility information disclosure of private listed companies.

Data Availability

The data used to support the findings of this study are available from the author upon request.

Conflicts of Interest

The author does not have any possible conflicts of interest.

References

[1] Y. Qu, S. Yu, L. Gao, W. Zhou, and S. Peng, "A hybrid privacy protection scheme in cyber-physical social networks," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 773–784, 2018.

[2] J. Liu, F. Zhang, X. Song, Y.-I. Song, C.-Y. Lin, and H.-W. Hon, "What's in a name? an unsupervised approach to link users across communities," in *Proceedings of the 6th ACM International Conference on Web Search and Data Mining*, pp. 495–504, Rome, Italy, 2013.

[3] Y. Li, Z. Zhang, Y. Peng, H. Yin, and Q. Xu, "Matching user accounts based on user generated content across social networks," *Future Generation Computer Systems*, vol. 83, pp. 104–115, 2018.

[4] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: anonymous location- based queries in distributed mobile systems," in *Proceedings of the 16th International Conference on World Wide Web*, pp. 371–380, Banff Alberta Canada, 2007.

[5] Y. He and J. Chen, "User location privacy protection mechanism for location-based services," *Digital Communications and Networks*, vol. 7, no. 2, pp. 264–276, 2021.

[6] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2034–2048, 2020.

[7] X. He, T. Xiao, and X. Chen, "CSR disclosure and corporate finance constraints," *Financial Research*, vol. 8, pp. 61–72, 2012.

[8] Y. Guo, C. Su, and Y. Zhang, "Does corporate social responsibility disclosure improve the company's market performance?" *Systems Engineering-Theory & Practice*, vol. 39, no. 4, pp. 881–892, 2019.

[9] C. Leuz and R. E. Verrecchia, "The economic consequences of increased disclosure," *Journal of Accounting Research*, vol. 38, no. 1, pp. 91–124, 2000.

[10] X. Du, Y. Xiao, S. Ci, M. Guizani, and H.-H. Chen, "A routing-driven key management scheme for heterogeneous sensor networks," in *Proceedings of the IEEE International Conference on Communications*, pp. 3407–3412, Glasgow, UK, June 2007.

[11] S. Hussain, F. Kausar, and A. Masood, "An efficient key distribution scheme for heterogeneous sensor networks," in *Proceedings of the International Wireless Communications and Mobile Computing Conference*, pp. 388–392, IWCMC '07, New York, NY, U S A, August 2007.

[12] P. Traynor, H. Choi, G. Cao, S. Zhu, and T. La Porta, "Establishing pair-wise keys in heterogeneous sensor networks," in *Proceedings of the 25th IEEE International Conference on Computer Communications*, pp. 1–12, INFOCOM '06, Athens, Greece, April 2006.

[13] A. Durresi, V. Bulusu, V. Paruchuri, M. Durresi, and R. Jain, "WSN09-4: key distribution in mobile heterogeneous sensor networks," in *Proceedings of the IEEE Global Telecommunications Conference*, pp. 1–5, GLOBECOM '06, Francisco, CA, USA, December 2006.

[14] Q. Shi, N. Zhang, M. Merabti, and K. Kifayat, "Resource-efficient authentic key establishment in heterogeneous wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 73, no. 2, pp. 235–249, 2013.

[15] S. U. Khan, L. Lavagno, and C. Pastrone, "A key management scheme supporting node mobility in heterogeneous sensor networks," in *Proceedings of the 6th International Conference on Emerging Technologies* ,vol. 10, pp. 364–369, ICET, October 2010.

[16] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu, and T. La Porta, "Efficient hybrid security mechanisms for heterogeneous sensor networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 6, pp. 663–677, 2007.