Hindawi
Mobile Information Systems
Volume 2022, Article ID 3981775, 11 pages
https://doi.org/10.1155/2022/3981775

Research Article

Information Security Countermeasures for Big Data Platforms Based on Cloud Computing

Jing He[1] **and Yu Sun**[2]

[1]*Institute for Advanced Studies in Humanities and Social Science, Beihang University, Beijing 100083, China*
[2]*CIGIS (China) Limited, Beijing 100007, China*

Correspondence should be addressed to Jing He; bhhejing@buaa.edu.cn

Received 17 March 2022; Revised 9 May 2022; Accepted 18 May 2022; Published 14 June 2022

Academic Editor: Gopal Chaudhary

Nowadays, with advanced information technology, cloud computing, big data, and other technologies are widely used in various activities, and their value has been proven and attracted people's attention. This article aims to study the challenges faced by the development of national information security in the context of big data in the new era. While the big data platform brings convenience to social life, it will also have a major impact on national information security. In order to protect information security, big data needs to be managed to improve the quality and efficiency of its use. As a result of empirical analysis, information security in this environment is a personal issue as well as an important social issue. The way to solve this problem naturally starts from increasing people's awareness of preventing personal information and increasing the protection of commercial information, but it is necessary to improve relevant government laws and regulations, improve the government's information supervision capabilities, and clean up and optimize for the government. The unique role of the information environment is more important and more fundamental. In 2018, a total of 3 billion pieces of data were leaked worldwide, an increase of 70% compared to 2017. Information leakage occurs almost all the time, so we should effectively prevent information from being stolen.

1. Introduction

1.1. Background of Topic Selection. The current network, information, 5G, and other technologies are developing with the development of society; in modern production and life, more and more people can communicate and exchange data through terminals. Big data is increasingly becoming a new type of productivity, making communication between people more convenient and faster. Now "Internet +" is the general trend, bringing more economic benefits to commercial applications and providing more financial resources for the government. One of distributed computing is called cloud computing. This means that it will be a simple distributed computing process to decompose the big data processing program into countless small programs through the "cloud" network to process and analyze it, which can quickly solve the problem of labor distribution and obtain comprehensive calculation results. At the same time, user information caused by the open network environment is stolen and used by criminals, causing widespread anxiety in various fields of society and limiting the effective application of big data. Information security is the technical and management security protection established and adopted for the data processing system, in order to protect the computer hardware, software and data from being damaged, changed, and leaked due to accidental and malicious reasons. Therefore, while protecting user privacy and information security, it is worth discussing and studying how to improve the value of applications and use big data.

1.2. Significance of the Research. As a new form of information technology, big data is evolving rapidly with a wide range of scope and has a huge impact on people's lives. The influence of big data lies not only in people's daily life but also in all aspects of the information society. Someone compared these data with coal-fired coal mines. Carbon is divided into coke, carbonate, fatty carbon, lean carbon, etc., depending on its nature. The important thing about big data

is "usefulness" rather than "big," and more importantly, capacity, cost, and value. How to use these resources is crucial. Therefore, how to protect the privacy and new performance of its information in the era of cloud computing, especially in the new environment, is a question. The current status quo has good guidance and improvement effects. It is possible to conduct a more comprehensive and objective analysis of the opportunities and challenges faced by the information security of the big data platform. It has the ability to highlight the problems faced by information protection, and is of great importance to the ability to cause problems and related countermeasures. He put forward many feasible suggestions to help analyze and solve some of the problems of domestic big data platform information security protection.

1.3. Relevant Work on Analysis of Information Security Countermeasures for Big Data Platforms. Big data has always been the research object of scholars. In related work, many scholars have analyzed the information security of big data platform. Xu et al. believe that in the era of big data, information protection is very important. Mobile cloud computing is a new example that can provide cloud computing functionality on the edge of a widespread wireless access network near mobile users. Whether it is a government agency or a commercial organization, there must be a consistent use policy when using consent information [1]. Xia et al. pointed out that in order to ensure data security, the "Cyber Security Law" must be strictly enforced, which is the most important; maintenance is a common example of cloud storage outsourcing. For privacy reasons, sensitive images such as medical images and personal images must be encrypted before outsourcing. This makes plain text domain CBIR technology useless [2]. In addition, the system requirements need to be updated. Study and formulate relevant laws and regulations. Establish a support system and strengthen the design, development, promotion, and operation of network and construction security. Hameed et al. believe that China has many information security regulations, but no regulations [3]. Yes, it is not systematic and it is difficult to guarantee data security. Therefore, expedite the legal process of information security laws. However, I believe that due to the limitations of the field of science, lack of research on computer information technology will inevitably lead to an inability to understand the root causes of information security issues.

1.4. Innovation Points of This Research

(1) Encryption algorithm for big data platform information security

(2) The cloud computing method is adopted in the analysis of information security countermeasures for research on big data platforms [4].

(3) Cloud computing can run to improve efficiency, reduce related costs, ensure data security, and has the characteristics of scalability and liquidity [5]. The application of these characteristics of cloud computing to the information security countermeasures of big data platforms is of great help, and can guarantee the security of information to a large extent [6].

2. Methods of Analysis of Information Security Countermeasures on Big Data Platforms

2.1. Theory of Cloud Computing. Cloud computing is a kind of distributed computing, which refers to the network "cloud" that decomposes huge data computing and processing programs into countless small programs, and then processes and analyzes these small programs through a system composed of multiple servers to get the results and return them to users. With the development of computer technology and the research of scholars in the field of cloud computing, it provides the definition that best meets modern needs: Cloud computing is a brand new concept at the network application level. Cloud computing is to provide related data services to individuals through Internet technology, usually using Internet virtualization technology to obtain and share related data resources. Cloud computing is one of distributed computing that can provide services related to networks, software, and communications. Its central idea is to use the network as a bridge for computing. This computing is the cloud. As shown in Figure 1, cloud computing can combine a large number of resources, and coupled with software processing, you can quickly achieve the desired effect [7]. However, after the further exploration and research of cloud computing technology by various countries, the National Institute of Standards and Technology of the United States has given a widely accepted definition at this stage: Cloud computing is the use of virtualization technology to form server clusters in different fields. According to the amount of money the user consumes and pays, the user can access and access resources anytime and anywhere.

2.2. Features of Cloud Computing. The value of cloud computing lies in its high flexibility, scalability, and high performance ratio. Compared with the traditional network application mode, it has the following advantages and characteristics:

2.2.1. Cloud Computing is Easy to Expand. The services provided by cloud computing are extremely scalable. Under the guidance of Internet technology, computers and servers can be easily interconnected, thereby rapidly expanding the cloud computing service platform and forming a super cloud computing service platform [8]. At the same time, users can share resources stored on the Internet through the service platform, and can also obtain the resources they want anytime, anywhere [9].

2.2.2. Cloud Computing has the Characteristics of Virtualization. Customers can enjoy rich application

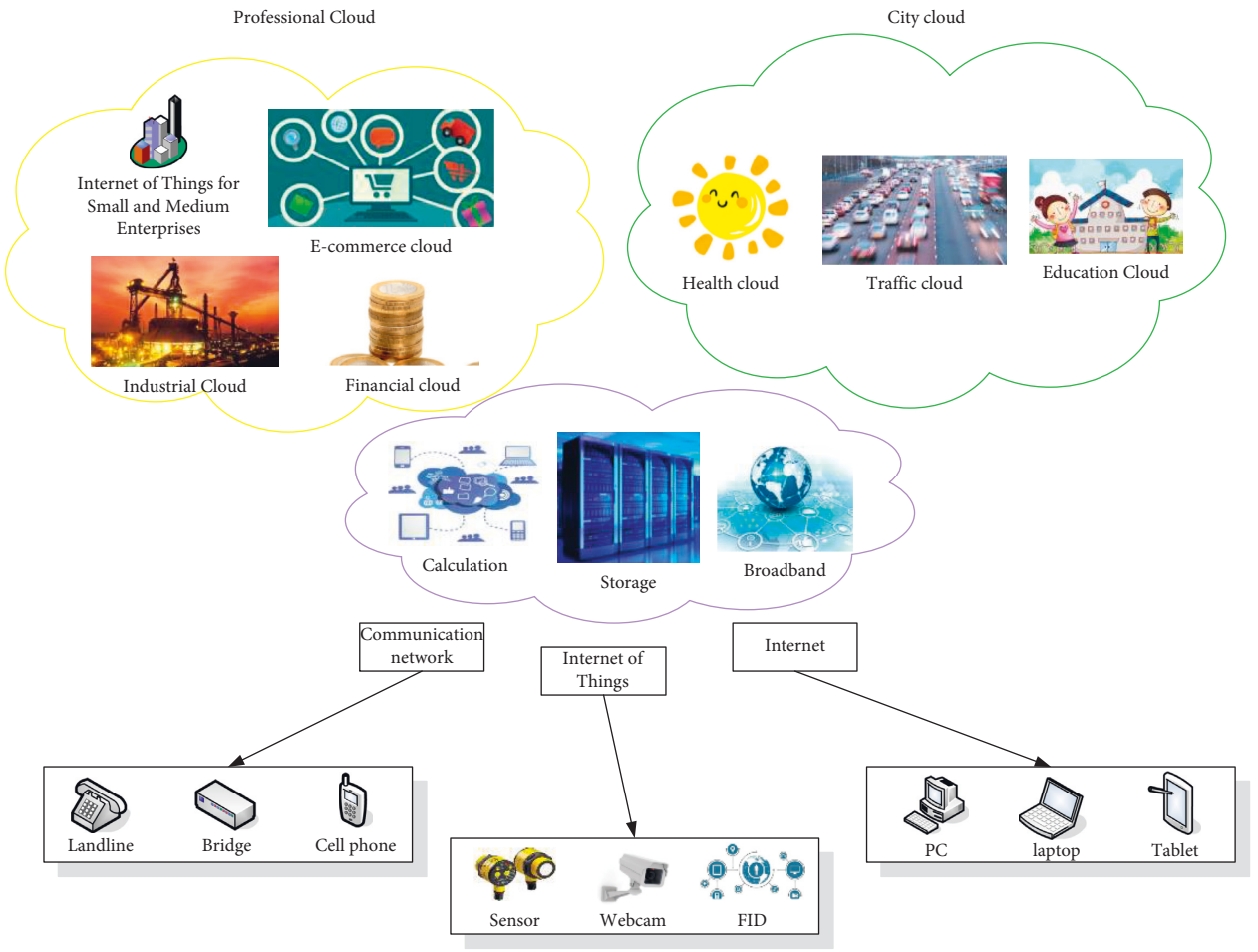

Figure 1: Schematic diagram of cloud computing.

content via the Internet at any time from any other place that can be connected to the Internet. Users do not know which server or computer these applications are running on, and they do not know the specific location of the server or computer. Only users can use Internet technology to obtain resources through mobile smart terminals.

2.2.3. Cloud Computing has the Characteristics of "Good Quality and Low Price". Its appearance is mainly due to its powerful versatility, convenient and cheap maintenance cost [10]. Cloud computing can integrate servers and computers around the world into a virtual environment through Internet technology [11]. They can access and share resources with each other, which allows many companies to centrally manage their data centers and save high maintenance costs, greatly improving resource utilization. Cloud computing not only avoids wasting a lot of server and computer resources but also achieves the national energy saving and emission reduction goal [12].

2.2.4. Cloud Computing has one of the Most Important Security Features. Because the cloud computing system integrates computers and servers in various regions, the use of multiple security authentication mechanisms in a virtual

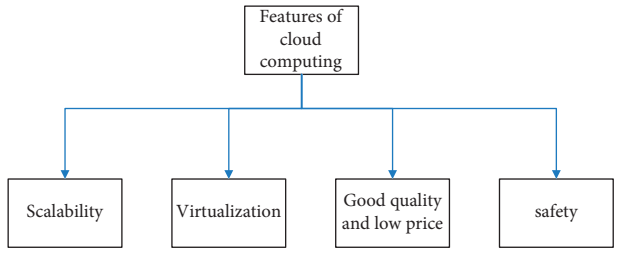

Figure 2: Features of cloud computing.

environment can greatly improve the reliability of resources and services [13]. Figure 2 shows the characteristics of cloud computing:

2.3. Security Issues Faced by Cloud Computing. Cloud computing is widely used in daily life. The subsequent data security issues in cloud computing have become more and more serious. People should have doubts about the security of data in the cloud. This incident caused an immediate loss of 10%–20% of the market share of US cloud providers, and cloud computing has transferred control of the data and storage environment. All data are in an open environment, without the protection of cloud computing platform

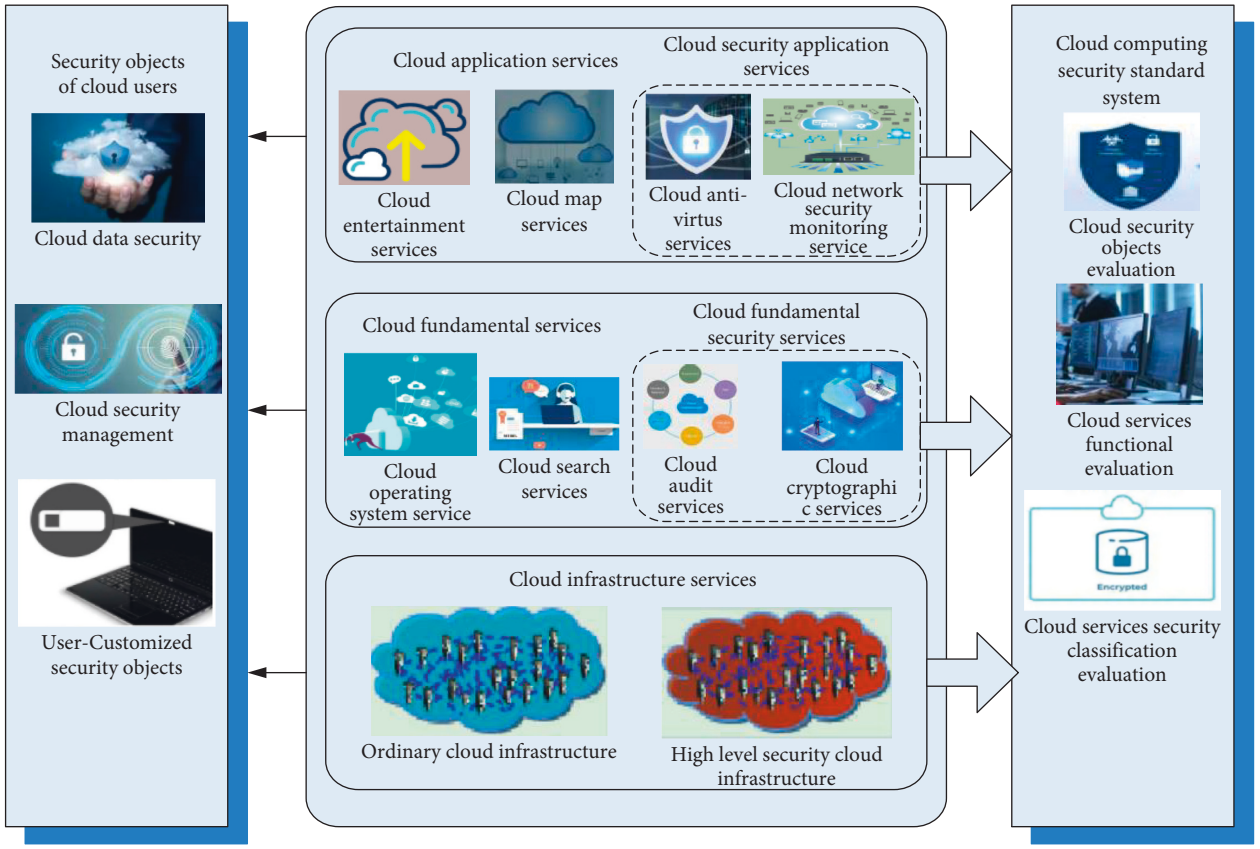

Figure 3: Cloud security reference framework.

firewalls and other isolation facilities. The data subject is excluded from the data manager. In this case, if the data are not effectively protected, it is easy to be stolen and leaked. The security of cloud data is worrying now. People have a strong sense of security about the information stored in the cloud. Figure 3 is a model diagram of the cloud security reference framework. Solving data security issues to ensure data security is an urgent issue for cloud computing. Cloud computing has high reliability, and if the server fails, it will not affect the normal operation of computing and applications. Because of the failure of single-point server, applications distributed on different physical servers can be restored by virtualization technology or new servers can be deployed for calculation by dynamic expansion function.

2.3.1. Security Issues Caused by Information Leakage. Information technology is a general term for various technologies mainly used to manage and process information. It mainly applies computer science and communication technology to design, develop, install, and implement information systems and application software. It mainly includes sensing technology, computer and intelligent technology, communication technology, and control technology. Network openness and information sharing in the network environment are data and information facing security issues [14]. In particular, when a large amount of data information is generated and the data are still transmitted through a local area network or a dedicated network, it is difficult to guarantee the quality of information transmission, which will lead to information security problems, which will be covered by certain threats, and the management and storage of data information is difficult. If the requirements are met, data information management may be destroyed, and application exceptions may also occur [15].

2.3.2. Security Issues Caused by Data Diversification. The data sources nowadays are very large, and also generate a large amount of data. Regarding this data information, regardless of the management level or the type of management adopted, the managers will be diversified [16]. Data information is shared in an open network environment. Users' access to and use of data and information has also developed from different perspectives. However, if the administrator has insufficient work experience, faces so much data, and is diversified, it is easy to cause security problems [15].

2.3.3. Security Issues Caused by Hacker Attacks. As an open environment, data information is easy to lose, even if some data information is encrypted, it can still be found [17]. One of the main reasons is that big data has many data processing unit modules. If a hacker finds a defect in the process of detecting the data processing unit module, he or she will initiate an attack from the vulnerability [18]. The greater the amount of data, the more attackers will be attracted. If the

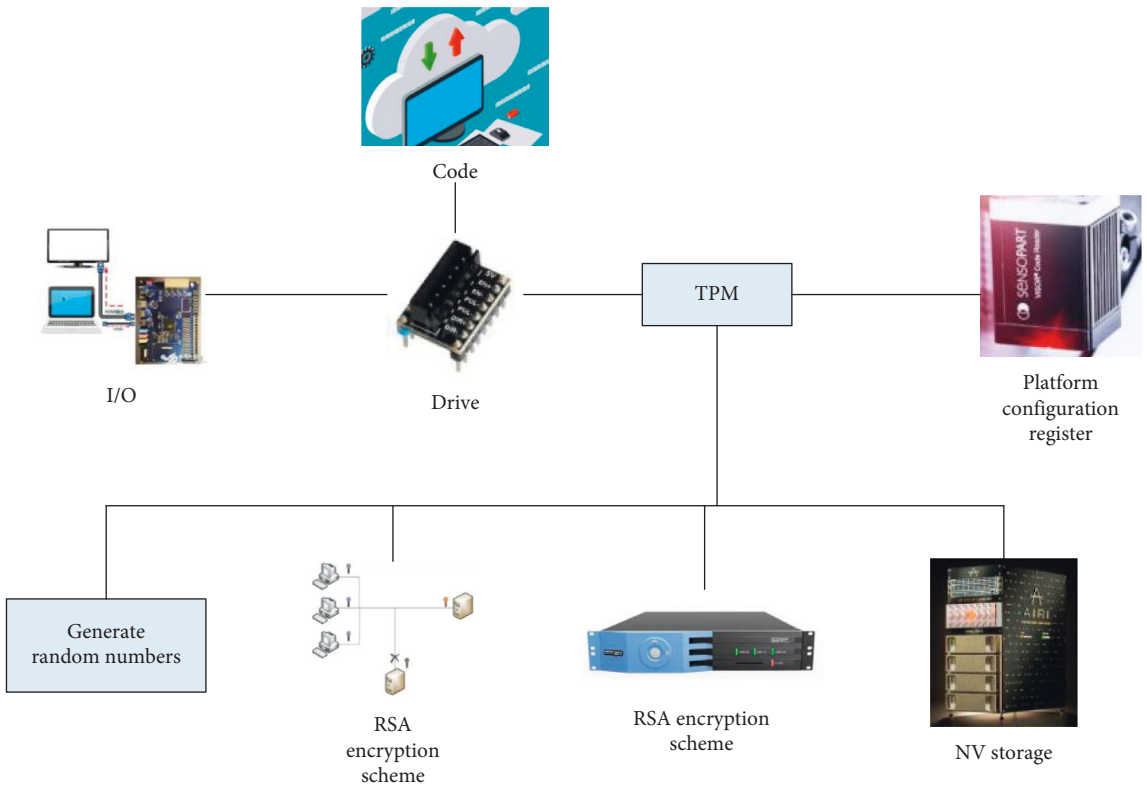

Figure 4: TPM trusted module function diagram.

hacker's attack is successful, a large amount of data and information will be leaked.

2.4. Cloud Platform Computing and Trusted Platform. According to the actual situation, each application mode adopts different security strategies. Cloud computing includes three different service models: infrastructure services, platform as a service, and software and services. The first category can have a VMM environment that provides a good host; the second category can provide a platform for computing and protection development; the third category can have software applications to protect customer data security and personal information. Ensuring the data security of the cloud computing platform requires different levels of security measures, which can meet the requirements of security standards. The reliable platform unit is a security chip installed on the computer. This is the basis of reliable processing. Each trusted platform unit has a unique identifier to indicate the reliability of the module. This unique identity is called an authentication key (EC). Although the trusted platform module is responsible for protecting data security, when hackers, Trojan horses, etc., invade, the credentials of the trusted platform module can easily be destroyed. This is why we combine other security technologies to ensure information security. Figure 4 shows the functional diagram of the trusted platform module:

TPM controls access to certain sensitive data. TPM controls issuance, authentication, and certificate storage; TPM measurement; recording of software and hardware identifiers; and provides integrity for trusted institutions. TPM security features include access control. Certificate and measurement registration and reporting TPM security report: The details of these security functions are as follows:

TCG, respectively, defines verification certificate, signature certificate, conformity certificate, platform certificate, and identity certificate. These five certificates are the TPM security certificate chain. The functions of these five certificates are:

(1) Verification certificate: The verification certificate provides sensitive information, including the types, versions, and standards of various sensitive software and hardware, and other basic information.

(2) Signature certificate: The signature certificate provides basic TPM information, including TPM version, manufacturer, EC, serial number, etc.

(3) Certificate: The certificate provides basic information such as TPM, graphics card, processor, and keyboard driver.

(4) Identity Certificate: The certificate that identifies a certificate associated with an Identity Key (AIK) pair to integrate a dedicated TPM platform. AIK is provided by trusted third parties. A trusted third party can rest assured that the TPM and platform are efficient, authentic, and if the AIK is stored in the TPM, the ID is signed.

TCG defines four types of security messages, namely: packet, signature, sealed bundle, and sealed signature. The usage rules for these four message types are as follows:

(1) Grouping: The public key TPM in the message is associated with the private key stored in the TPM to ensure that the message is only exposed to the designated TPM. And make sure that the TPM on the platform cannot decrypt the message.

(2) Signature: The signature text is similar to the traditional password method. Many TPM keys can only be used for signing. Cannot be used for encryption

(3) Sealed bundle: TPM uses sealed centralized messages to transmit sensitive external entity data to the platform. Platforms that comply with the security configuration can view the data sent by the TPM.

(4) Sealed signature: Using the sealed signature text in TPM, external entities can receive platform configuration information.

According to the definition of TCG, the keys in TMP can be divided into seven types. These seven types can be divided into four groups:

(1) The signature key and root storage key can only be found in the TPM and cannot be moved.

(2) Keys that cannot be moved, such as closed keys and closed keys. It can be stored outside of the encrypted TPM format.

(3) The signature key and storage key are multi-platform mobile keys.

(4) Some signatures and storage keys will be moved appropriately between platforms.

3. Experiments on the Analysis of Information Security Countermeasures on the Big Data Platform

3.1. Application Mode of Cloud Computing. A kind of cloud computing distributed computing technology, its most basic concept is to automatically split a huge computing processing program into countless smaller subroutines through the network, and then hand it over to a huge system composed of multiple servers. After searching, calculating, and analyzing, the processing results are sent back to the user. The system structure of cloud computing is used differently in different industries, it can be divided into public clouds open to everyone, private clouds for enterprises or campuses, and hybrid clouds that take both into account. Cloud standards must have three meanings: (1) Clear cloud computing standards, (2) Cloud computing performance standards, (3) Implied meaning of standard cloud computing [19]. Cloud computing standardization initially presents the following development trends: Inheritance and development of existing technologies and standards: Cloud computing is a further development of existing IT technologies. Existing technologies and standards must be inherited and used as much as possible. You do not need to develop a complete collection from top to bottom. A new standard. Focus on the formulation of IaaS standards: In terms of cloud computing standards, IaaS has the most stringent standardization requirements, followed by PaaS and SaaS related to specific applications. Interoperability and interoperability are key issues: Looking to the future, there will be many providers at all levels of the three major cloud computing models of IaaS, PaaS, and SaaS. There is no doubt that the common goal of cloud computing standards work is openness, cooperation, and win-win. Win: Communication and cooperation between standards bodies. Getting closer and closer, any specific content in the field of cloud computing is completed by many standards organizations. Full participation in the industry chain: All links in the cloud computing industry chain will actively contribute to the formulation of cloud computing standards.

3.1.1. Public Cloud. Public clouds are models based on standard cloud computing where service providers create resources such as applications and storage and people can access these resources via the Internet. It is currently the most widely used, that is, users only need to pay a certain fee to enjoy cloud services [20]. These services include hardware equipment, data resources, application software, and data storage from cloud service providers. On the other hand, users do not need to maintain resources and focus on equipment. This kind of cloud service can be enjoyed quickly and conveniently through on-demand payment [21].

3.1.2. Private Cloud. What is built for private customers is a private cloud, which has very safe and effective services and data protection, and the company can also use some infrastructure for development. The most important thing about a private cloud is resources. It can protect data on the enterprise's firewall and control growth in the position of security protection. It is not a platform for the general public; it only provides services for the company's free employees [22]. Because of this, it can not only improve the security of company data but also save a lot of server equipment and resources. However, the private cloud must be managed and maintained by the company itself, which poses challenges in terms of technology and cost [23].

3.1.3. Hybrid Cloud. Hybrid cloud combines public cloud and private cloud. It is the main mode and direction of cloud computing growth in recent years. We already know that private clouds are mainly for enterprise users. For security reasons, companies prefer to store data in their personal cloud. But at the same time, they hope to obtain computing resources from public clouds. In this case, hybrid clouds are becoming more and more popular. More uses will combine and match public and private clouds to obtain the best results. This personalized solution achieves the goal of saving money and safety. Hybrid cloud combines the convenience

of public cloud with the security of private cloud. The hybrid cloud architecture is more complicated than the other two cloud architectures while enjoying public resources and ensuring the security of resource services [24].

3.2. Encryption Algorithm for Big Data Platform Information Security. A typical cloud service is outsourcing data. Data subjects obtain large amounts of data for storage on cloud servers. Generally, in order to protect data security, the data source can perform some encryption operations on private data before uploading it. Naive Bayes classification is a powerful classification algorithm. It is widely used in various high-dimensional data classifications such as reference systems. Message classification and analysis of medical data have proposed many projects for safe and harmless Bayesian classification protocols in the past few years. These projects assume that the data set is horizontally or vertically distributed between two or more parts. And, all participants hope to realize harmless Bayesian classification together without disclosing their own information. Unlike their model, each participant can access part of the data set. Compared with previous works, the Bayesian encryption data sorting on the cloud platform faces different privacy issues and is more difficult. In terms of protecting data privacy in external processing environments, cloud servers can only access encrypted data sets, and all processing must be performed in the cloud.

The secure comparison protocol is used in many encrypted secure data processing protocols, such as secure kNN query and secure keyword query, classification, security SVM, and other SERQ security range query protocol. With the continuous development of cloud computing services, more and more individuals and organizations apply their own databases and database services to cloud servers, and complete database searches through the powerful computing resources of cloud servers. This usually saves processing. At the same time, users who protect the privacy of their information usually encrypt the database and upload it to a cloud server.

Function definition:

(1) $P_j = PKeyGen(0)$: This function is used to generate a public parameter P_j function. At the initial stage, a bilinear group G with a prime number p and a generator g will be selected, and the bilinear pairing operation e: $G \times G \longrightarrow G_l$ will be performed. Attribute space $V = \{V_1, V_2, \ldots . V\}_n, V_i \in V\,(1 \le i \le n)$, $y_i, c, d \in Z_p$ is randomly selected. The function *PkeyGen* is shown in formula (1):

$$\left\{G_l, g, g_d, e(g,g)^c, \left\{T_i = g_{y_i}\right\}_{i=1}^{n}\right\}. \tag{1}$$

(2) $M_j = MKeyGen(0)$: This function is used to generate the master key M_j. Among them, g, c, d are defined as the above function *MKeyGen* as shown in formula (2):

$$\{g^c, d, \{y_i\}_{i=1}^{n}\}. \tag{2}$$

(3) $A = Encrypt(P_j, N, L)$: This function uses the public parameter P_j and the access control structure L to encrypt the plaintext N, and obtains the ciphertext A. Γ is to meet the authorization set collection requirements of the corresponding access control structure. Among them, $\mathrm{att}(y)$ returns the attribute information of node y.

$$\left(\Gamma, \tilde{A} = Ne(g,g)^{cs}, A = g^{ds}, \forall y \in Y\colon A_x = g^{q_{y(0)}}, A_x' = L_{att(y)}{}^{q_{y(0)}}\right). \tag{3}$$

(4) $S_j = SKeyGen(N_j, B)$: This function uses master key N_j and user attribute set B to generate user private key S_j. As the attribute set associated with the user's private key, B is a nonempty subset of the data file attribute set V. Choose random number $\gamma \in Z_p$, individual attribute $s \in B$, random number $\gamma_s \in Z_p$. The function $\mathrm{SKeyGen}(N_j, B)$ is shown in formula (4):

$$\left(E = g^{(c+\gamma)/d}, \forall s \in B\colon E_s = g^{\gamma} T_s^{\gamma_s}, E_s' = g^{\gamma_s}\right). \tag{4}$$

(5) $N = \mathrm{Decrypt}(D, S_j)$: This function uses the user's private key S_j to decrypt the ciphertext CT to obtain the plaintext N. Before defining this function, first define the recursive operation $\mathrm{Decrypt}(D, S_j, z)$, let $i = \mathrm{att}(y)$, each leaf node z can calculate the recursive function $\mathrm{Decrypt}(D, S_j, z)$ as shown in formulas (5) and (6):

$$\frac{e(E_i, A_z)}{e(E_i{}', A_z')} = e(g,g)^{\gamma q_z(0)}, i \in B, \tag{5}$$

$$\frac{1}{e(E_i, A_z)} = e(g,g)^{r q_z(0)}, i \in B. \tag{6}$$

(6) For each nonleaf node z, at least j_z $e(g,g)^{\gamma q_z(0)}$ can be used as Lagrangian polynomial interpolation nodes. After calculation, $e(g,g)^{\lambda q_{Z_s}(0)}$ can be obtained, and $e(g,g)^{\gamma q_z(0)}$ can be calculated by the child node $\{Z_s\}$ of node z. Assuming $U = e(g,g)^{\gamma q_R(0)} = e(g,g)\lambda_s$, $\mathrm{Decrypt}(D, S_j)$ is as shown in formula (7):

$$\frac{\tilde{D}}{(e(D,E)/U)}. \tag{7}$$

The realization of computer cloud computing needs to create certain environment and conditions, especially the architecture must have the following key features. First, it is required that the system must be intelligent and autonomous, and the automatic processing platform should respond intelligently on the premise of reducing manual work, so the cloud system should be embedded with automation technology; secondly, the cloud system should have agile response ability in the face of changing signals or

Table 1: Gender distribution of investigator.

Gender	Male	Female	Total
Number of people	151	149	300
Percentage (%)	50.33	49.67	100

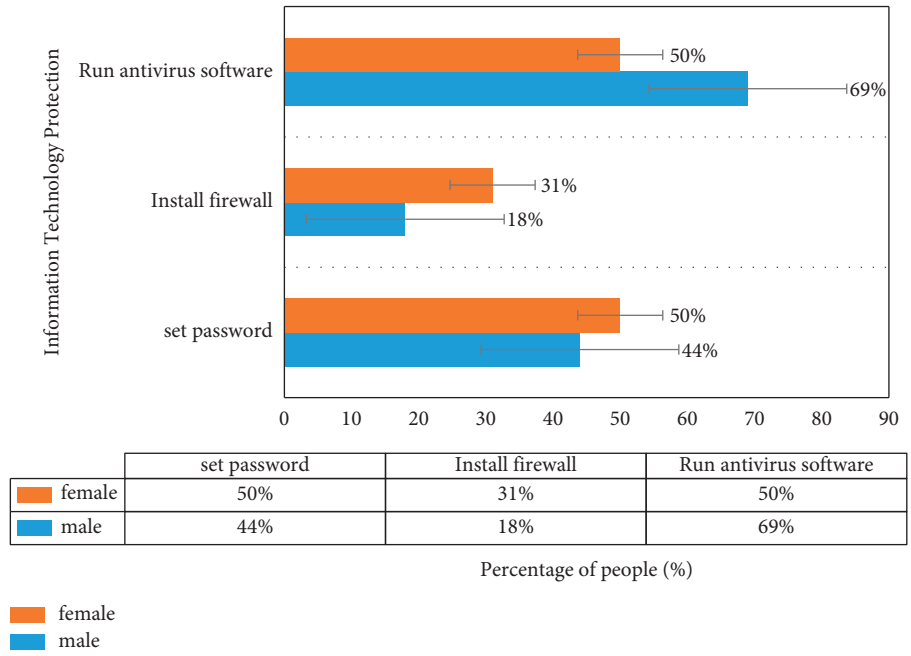

Figure 5: Information technology protection of people of different genders is different.

demand signals, so it has certain agile requirements for the architecture of cloud computing. At the same time, with the rapid changes of service level and growth rate, cloud computing is also facing great challenges, and embedded clustering technology and virtualization technology can cope with such changes.

4. Information Security Countermeasures on the Big Data Platform

4.1. Big Data Information Security Countermeasures on Cloud Platform. Through the application of cloud computing to establish big data platform information security measures, big data information can be collected, processed, and stored, and big data management can be realized. In order to ensure the security of big data information, corresponding security measures need to be taken.

4.1.1. Build a Big Data Information Security System. By building large-scale data platforms and cloud computing applications to achieve centralized data information management, data information can play a role in scaling, and the value of data information within the scope will increase exponentially. It is necessary to conduct good supervision and management of data and information to improve the protection of data and information. Pay attention to the training of relevant professional and technical personnel, and continuously improve the big data information security system from the perspective of application.

4.1.2. Strengthen the Research and Development of Big Data Security Technology. The information network has become an important driving force for social development. With the emergence of large amounts of data, it is obviously difficult to implement data management using existing security technologies. And, the application of computer and network technology has penetrated into all aspects of government, military, culture, education, and daily life. It is very necessary to strengthen the supervision of information network data. There is a lot of important information in social and economic life, including government macro-control decision-making, financial data, commercial banks, bank stocks, securities, energy resources, and scientific research data, which are mainly sensitive information, even state secrets. These data must be stored, transmitted, and exchanged, so it often attracts human attacks from all over the world, including data theft, falsification, deletion and addition of data, computer viruses, and so on. They must also withstand the test of natural disasters. Therefore, how to protect computer information security has become a hot topic in computer information security research, and has attracted more and more attention from all walks of life. To ensure the security

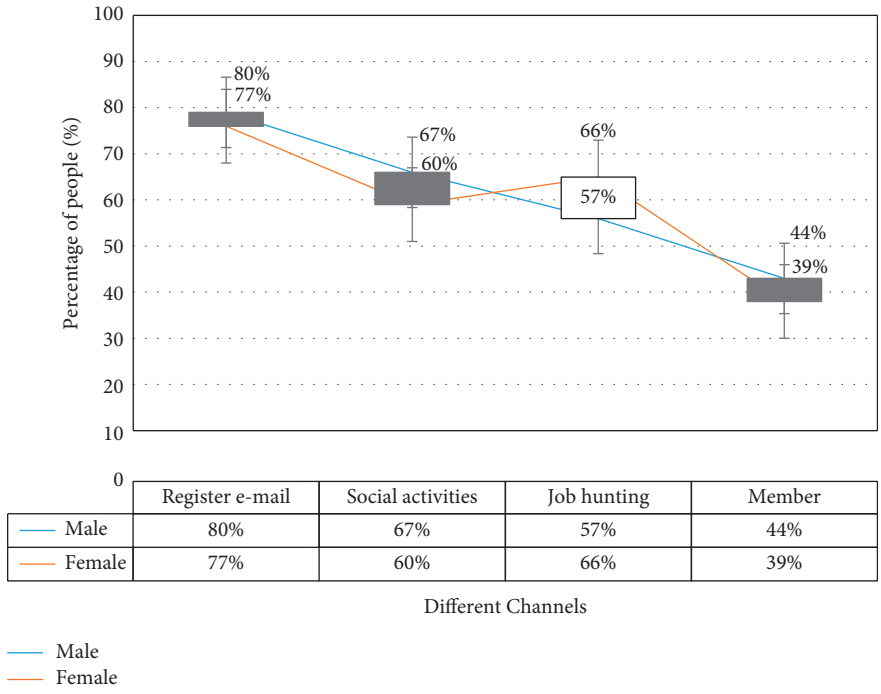

Figure 6: Information leakage of people of different genders through different channels.

of big data, it is necessary to improve the level of information and information security technology by investing in research and development of information and information security.

4.1.3. Strengthen the Supervision and Management of Highly Sensitive Data and Information. Because a large amount of data is collected on the cloud platform, data with high sensitivity is bound to leak. When using big data, if big data is not used in accordance with regulations, data may be stolen. In order to maintain the security of highly sensitive data, it is necessary to divide the data into different levels, to clarify the scope of the main database, and to manage the confidentiality of the data well, and to strengthen the supervision and management of the data.

4.2. Survey Data Analysis. After investigation and analysis, we conducted investigations in two aspects: the channels of our main information provision and the protection of information technology.

4.2.1. Gender Distribution of Survey Respondents. Among them, the number of boys is 151 and the number of girls is 149. The gender structure is shown in Table 1:

4.2.2. Information Technology Protection of the Investigator. The result is the password setting, firewall installation, and operation of related anti-virus software.

The difference in information technology protection of people of different genders is shown in Figure 5:

As shown in Figure 5, for gender, men's willingness to protect information technology is higher than that of women, because men's preference for computer types will be deeper.

4.2.3. Channels for Providing Main Information. Basically, most people use different channels, such as registered emails, social activities, job search, and membership, which lead to information leakage.

The information leakage of people of different genders through different channels is shown in Figure 6:

The wanton spread of personal information on the Internet and endless telemarketing have occurred from time to time. From its root, this is closely related to citizens' lack of sufficient awareness of information protection. Citizens' awareness of personal information protection is relatively weak, which creates conditions for information theft. For example, if you click on the website, you need to fill in relevant information, and some websites even require accurate information such as ID number. Many citizens do not realize that the above behavior is a violation of information security. In addition, some websites openly disclose or sell related information based on the characteristics of weak civic awareness. Furthermore, there is also the risk that information will be used illegally by filling out leaflets and other materials casually in daily life.

5. Conclusion

When the concept of cloud computing was first proposed, it was still run through some distributed computing. Cloud computing is also called network computing to a certain extent. It can perform functions such as assigning work, calculating results, and analyzing data. In the current information technology environment, various emerging

technologies are developing rapidly and are accepted by more and more ordinary people. A type of distributed computing is called cloud computing, which decomposes big data into small programs through a cloud network, and then collects, analyzes, and records information through the cloud network. Operate. Many back-end servers receive the processed information, and finally feedback all the results to the user for the user to perform the required operation. Using this technology, it can process and feedback tens of millions of data in a short time, so that it can be very effective. Network services. The other kind of technology is big data. It does not end with the acquisition of a large amount of data, but on the basis of obtaining a large amount of data, the data are processed and fed back in a very professional manner, which is similar to a certain degree. The importance of these industries is to improve the profitability of the industry. In daily life, the relationship between big data and cloud computing is not just two technologies. They are more like the pros and cons of a coin, and the two are interrelated and interdependent. However, the development of the two technologies is still in the preliminary exploration stage, and certain applications have many hidden dangers, which will lead to major data and information security issues. This requires large-scale data platforms to take necessary information security measures to ensure the quality of data information and its value within the scope.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

Ningxia Natural Science Foundation, No. 2021AAC03060.

References

[1] C. Xu, J. Lei, W. Li, and Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Transactions on Networking*, vol. 24, no. 5, pp. 2795–2808, 2016.

[2] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2594–2608, 2017.

[3] A. Hameed, A. Khoshkbarforoushha, R. Ranjan et al., "A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems," *Computing*, vol. 98, no. 7, pp. 751–774, 2016.

[4] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (sdn) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[5] O. Awodele, A. A. Izang, S. O. Kuyoro, and F. Y. Osisanwo, "Big data and cloud computing issues," *Applied Radiology*, vol. 3, no. 12, pp. 1647-1648, 2016.

[6] A. Paranjothi, M. S. Khan, and M. Nijim, "Survey on three components of mobile cloud computing: offloading, distribution and privacy," *Journal of Computer and Communications*, vol. 5, no. 6, pp. 1–31, 2017.

[7] M. Mesbahi, A. M. Rahmani, and A. Masoud Rahmani, "Load balancing in cloud computing: a state of the art survey," *International Journal of Modern Education and Computer Science*, vol. 8, no. 3, pp. 64–78, 2016.

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

[9] M. B. Karimi, A. Isazadeh, and A. M. Rahmani, "QoS-aware service composition in cloud computing using data mining techniques and genetic algorithm," *The Journal of Supercomputing*, vol. 73, no. 4, pp. 1–29, 2017.

[10] S. Namasudra and P. Roy, "Secure and efficient data access control in cloud computing environment: a survey," *Multiagent and Grid Systems*, vol. 12, no. 2, pp. 69–90, 2016.

[11] A. A. l-Shuwaili, O. Simeone, A. Bagheri, and G. Scutari, "Joint uplink/downlink optimization for backhaul-limited mobile cloud computing with user scheduling," *IEEE Transactions on Signal & Information Processing Over Networks*, vol. 3, no. 4, pp. 787–802, 2016.

[12] G. Fan, H. Yu, and L. Chen, "A formal aspect-oriented method for modeling and analyzing adaptive resource scheduling in cloud computing," *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, pp. 281–294, 2016.

[13] J. Huang, "Patent portfolio analysis of the cloud computing industry," *Journal of Engineering and Technology Management*, vol. 39, no. 9, pp. 45–64, 2016.

[14] M. Jouini and L. B. A. Rabai, "A security Framework for secure cloud computing environments," *International Journal of Cloud Applications and Computing*, vol. 6, no. 3, pp. 32–44, 2016.

[15] Y. Wang, S. Meng, Y. Chen, R. Sun, X. Wang, and K. Sun, "Multi-leader multi-follower stackelberg game based dynamic resource allocation for mobile cloud computing environment," *Wireless Personal Communications*, vol. 93, no. 2, pp. 1–20, 2017.

[16] R. S. Padilla, S. K. Milton, L. W. Johnson, and M. W. Nyadzayo, "Impact of service value on satisfaction and repurchase intentions in business-to-business cloud computing," *Service Science*, vol. 9, no. 1, pp. 5–13, 2017.

[17] Q. Alam, S. U. R. Malik, A. Akhunzada, K.-K. R. Choo, S. Tabbasum, and M. Alam, "A cross tenant access control (CTAC) model for cloud computing: formal specification and verification," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1259–1268, 2017.

[18] M. Ibtihal, E. O. Driss, and N. Hassan, "Homomorphic encryption as a service for outsourced images in mobile cloud computing environment," *International Journal of Cloud Applications and Computing*, vol. 7, no. 2, pp. 27–40, 2017.

[19] H. Aziza and S. Krichen, "Bi-objective decision support system for task-scheduling based on genetic algorithm in cloud computing," *Computing*, vol. 100, no. 2, pp. 65–91, 2018.

[20] H. Rezaei, B. Karimi, Karimi, and S. J. Hosseini, "Effect of cloud computing systems in terms of service quality of knowledge management systems," *Lecture Notes on Software Engineering*, vol. 4, no. 1, pp. 73–76, 2016.

[21] J. Thaman and M. Singh, "Current perspective in task scheduling techniques in cloud computing: a review," *International Journal in Foundations of Computer Science & Technology*, vol. 6, no. 1, pp. 65–85, 2016.

[22] C. Napoli, G. Pappalardo, G. M. Tina, and E. Tramontana, "Cooperative strategy for optimal management of smart grids by wavelet RNNs and cloud computing," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1672–1685, 2016.

[23] C. Zhang, Y. Yang, Z. Du, and C. Ma, "Particle swarm optimization algorithm based on ontology model to support cloud computing applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 7, no. 5, pp. 633–638, 2016.

[24] A. C. Caminero, S. Ros, R. Hernandez, A. Robles-Gomez, L. Tobarra, and P. J. T. Granjo, "VirTUal remoTe labORatories managEment System (TUTORES): using cloud computing to acquire university practical skills," *IEEE Transactions on Learning Technologies*, vol. 9, no. 2, pp. 133–145, 2016.