Basic and Applied Research
(ISSN:2688-4097)

The Protection Strategies of User Privacy in Cloud Computing

Shaohui Zhang

School of Network Engineering, Zhoukou Normal University, Zhoukou 466001, China.

ABSTRACT

Cloud computing attracts a large number of users by its good scalability, low cost, on-demand payment and other advantages, but due to the related technology is not mature enough, imperfect legal supervision and so on, the privacy and security problems of cloud computing are serious at present. This paper proposes a privacy data protection model based on the analysis of the security and privacy problems in cloud computing, which classifies data into private data and non-private data according to the privacy attributes of data, and considers encryption, decryption technology and data partitioning technology to protect privacy data in data transmission and data storage. Experiments indicate that this model can improve the security of privacy data to a certain degree.

Keywords: Cloud Computing; Privacy Security; Encryption; Decryption; Data Block

***Correspondence to Author:**
Shaohui Zhang
School of Network Engineering, Zhoukou Normal University, Zhoukou 466001, China.

How to cite this article:
Shaohui Zhang. The Protection Strategies of User Privacy in Cloud Computing. Basic and Applied Research 2019, 1:6

AePub LLC, Houston, TX USA.
Website: https://aepub.com/

1. Introduction

The concept of Cloud Computing was first put forward by Google in 2006. [1] It has been developing rapidly since then. As a new service mode, cloud computing has attracted the attention of all parties in the Internet industry when it is integrated into our life. [2] Now known well-known IT companies all focus on cloud computing and devote themselves to service applications based on cloud computing platform. Cloud computing provides information to users according to their needs by sharing hardware and software resources and information. [3] Because cloud computing technology requires a large number of users to participate in sharing or collecting some information, which creates new privacy security risks, and users also worry about their privacy security while enjoying cloud technology services. This problem also determines the future development trend of cloud computing, and is also related to the vital interests of users. [4]

2. Development of Cloud Computing

2.1 Background of Cloud Security Research

The development of cloud computing in China started with the "cloud computing" service business launched by IBM, Microsoft, Google, etc., which started late and developed immature. However, cloud computing in China has its own unique features. It was put forward and expounded "cloud security" very early, making it enter a more healthy development level. [5] Cloud security is to monitor and test the anomalies of software behavior in the Internet through intensive clients, so as to get the latest information of malicious virus development in the Internet. [6] The information is sent to the server, analyzed and processed, and then fed back to each client's virus solution. Because a large number of users can be said to penetrate all levels of the network, even if a small number of individual websites find new malicious viruses, they can also be intercepted and analyzed to deal with, so as to achieve the purpose of prevention. In our country, most of the solutions to the security and privacy problems of cloud computing still focus on technical countermeasures, while neglecting the role of internal management and government intervention, which need to be strengthened. [7]

2.2 Research Status of Privacy Security in Cloud Environment

Parakh first proposed the concept of implicit data security, which does not require encryption and decryption. Chiang also has many achievements in implicit data security, and has made breakthroughs. For privacy protection in cloud computing environment, the concept of PaaS is proposed in the literature [8]. In order to protect users' privacy data, the security protocol is explained and implemented in this paper. The literature [9] proposes a privacy protection system, which integrates information flow control and differential privacy protection technology. By applying this technology in MapReduce computing process, it proves that the system can effectively prevent the leakage of privacy data. The literature [10] proposes a privacy manager which can effectively manage user data. The manager packages user data and introduces a new data segmentation technology. It can also protect user privacy data without encryption and decryption. In addition, a third-party isolated storage architecture based on trusted platform is proposed. Based on this third-party architecture, data can be uploaded, downloaded and managed effectively, and privacy data can be effectively protected.

3. Advantages of Cloud Computing

3.1 Safety Storage Guarantee for Enterprise Users

Some data is very important for enterprise users, which may cause an inestimable loss if lost. Most people think that storing data in memory-enabled devices can guarantee its security, but this is not the case. Personal computers may be damaged (e.g. hard disks that store data are damaged so that data can't be read), or viruses that infect downloads cause data loss and can't be read, or illegal data access may invade computers and steal data, resulting in personal privacy disclosure. If the data is uploaded to the server provided by cloud computing for data storage, the most advanced and reliable data storage center and complete and secure hardware facilities can perfect avoid most problems related to information security, and ensure the integrity of data to a great extent. [11]

3.2 Low Cost and Easy to Use

The original way of software maintenance is mainly through the continuous upgrade of new versions, which is very troublesome, and consumes time and energy. Some software is difficult to run because of compatibility problems on some systems. In addition, in order to adapt to the replacement of operating system and software, we need to constantly upgrade the hardware to match it. In order to open a different file or video format, you must use software that matches different downloads. In order to avoid virus infection, download software, you need to install anti-virus software, anti-virus software will cause some programs can’t run. [12] Such a bad cycle increases the user's use cost and has a negative impact on the user's sense of experience. Cloud computing has a very low requirement for users' equipment, and because of its internal network sharing; it can save unnecessary trouble in maintaining software, which is very convenient and fast.

3.3 Short Product Development Cycle and Low Investment Cost

Cloud computing service providers provide infrastructure usage services, which enable customers to find and use the required related resources through communication devices, reduce the time required by customers and saves the user's investment in resources and facilities. Only this link of network operation can achieve the goal, greatly shortening the product development cycle. The shortening of product development cycle will result in cost reduction and great benefit return for some companies, especially in IT industry.

4. Privacy Security in Cloud Environment

Cloud computing is developing vigorously and has a bright future, but it is not perfect either. Especially in the aspect of protecting users' privacy, regulatory measures are weak, insufficient and lagging behind in dealing with problems. Users of cloud services can be divided into three categories: individuals, enterprises and governments. The industry involved can be said to be all-inclusive, and some of its user data is also of great significance, its security is self-evident. Nowadays, cloud computing service providers and large Internet companies are only doing a trick in security and privacy. The loopholes invisibly threaten the normal operation of the system and lead to the leakage of privacy.

4.1 Privacy Security for Client User

Cloud computing relies on today's network, and any device connected to the network is an integral part of it. When devices are connected to the network, they have become a node of the Internet. If there is no effective protection, cloud computing can enter other nodes through related channels. It can be said that any operation of the user will leave an indelible trace on the computer, and can be obtained by other computers through a certain way. In cloud computing mode, the process of data centralized storage and data preservation and processing is unknown to users. Without perfect supervision system and rules, users' data will inevitably be in an unsafe state, which may lead to large-scale privacy leakage and theft. Therefore, information security is the primary issue to be considered and solved in the large-scale promotion of cloud computing. People will be assured that it is not blind to deposit money in financial institutions, most of which are state-owned and strictly regulated and protected by national laws. Therefore, only by dispelling users'security concerns can people be more assured to store data in. In the process of providing data to service providers for processing when users use cloud computing, the following user privacy issues generally arise:

(1) Access: Users have the right to know which user's personal information, such as the user's birthday, age, family status, contact information, is stored and acquired by the service provider while using cloud computing services, and users have the right to request the service provider to delete personal information.

(2) Compliance: Users have the right to understand the requirements and rules of information privacy regulations in compliance, and how the migration of user data in cloud computing services will affect the rules of personal information privacy in compliance.

(3) Storage: Where is cloud computing data stored? Is it transmitted to another physical address? Is it mixed with data from other users?

(4) Retention and destruction: When users cancel services, do cloud computing service providers retain user information? How long will it last if it is retained? How do cloud computing service providers destroy personal information after the retention phase? How to ensure that information is destroyed and that it is properly destroyed and not used by other users?

(5) How to know that the privacy of users is infringed, how to ensure that when the privacy is infringed, cloud computing service providers will inform users and how to determine whose fault is causing the privacy infringement?

4.2 Privacy Security in Network Transmission

Cloud computing generally has the following services at present: practical computing, network services, IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), SaaS (Software-as-a-S -ervice), MSP (Management Service Provider); business service platform and internet integration service. Cloud computing service providers are committed to more convenient, fast and handy access to the required data, but in any case, data transmission is an indispensable part of it. It can be seen that the security and reliability of data in the process of network transmission is one of the key issues of cloud services can be promoted widely.

4.3 Privacy Security for Server

Google has sent notifications to some online document and spreadsheet users that it mistakenly shared some of the user's documents without the user's confirmation permission. Even though less than 0.05% of user documents have been affected by the false haring event, it reminds customers to carefully consider privacy and security issues related to cloud computing. If there are serious technical problems in cloud computing, the disclosure of personal privacy will result in an incalculable social crisis. Up to now, cloud computing still lacks a safe and reliable standard to measure it. This brings a great challenge to the management of cloud-based customer data, and with the progress of network technology and the overflow of applications, the form of security will only become more and more severe.

5. Solutions to Privacy Security Problems in Cloud Environment

Cloud computing generally divides into private cloud, public cloud and hybrid cloud. Private cloud is the infrastructure that users can freely control to realize cloud function. Data storage and operation are all implemented under their own control. So private cloud is more secure than public cloud. Public cloud is a common storage and operation facility for all users. The storage of data is totally uncontrolled. How to store and where to store the data are unknown, so that users' privacy data security will be threatened and there is no way to do it. In fact, the data of users or organizations can’t be stored entirely in private clouds, only a large number of non-private data can be stored in public clouds. Enterprises with large amount of private data will also put private data on the public cloud, which can save some of the economic expenses. Therefore, in order to achieve the security of data on the public cloud, encryption measures must be taken. When users read these data, they should decrypt it accordingly.

5.1 Privacy Security Protection Model in Cloud Environment

In the cloud computing environment, in order to improve the efficiency of data use, save time and economic expenses, users' privacy data and non-privacy data should be stored separately. That is to say, private data should be stored in private cloud and non-privacy data in public cloud. However, this storage method also has new problems: public cloud. Applications may request the application of private data on private clouds, either internally or externally. However, if a large number of data are stored in the public cloud, the security of the data should be taken into account. For example, the data on the public cloud can be encrypted and stored by using data encryption method. Only the corresponding decryption processing is needed to obtain these data for example.

The user authentication module is proposed in this paper. The requests for private data on private cloud may be private cloud insiders or private data through public cloud. The authentication module is used to distinguish requesters of private data and restrict access to private data through this mechanism. Do and protect private data. Some operations may not be executed in the private cloud and have to migrate to the public cloud, which may involve private data on the private cloud. Therefore, the encryption/decryption module is applied to encrypt data transmission in the model to ensure the security of data transmission between the public cloud and the private cloud.

The public cloud part of this model is mainly used to protect the data security on the public cloud, mainly using data partitioning and data encryption to protect data. The figure is the specific process of data protection, in which the privacy level division module mainly decides the privacy of user data and takes corresponding level of security protection measures. Data partitioning module is to use data partitioning technology to decompose the data to be stored into several data blocks, and then store them in different memory with a certain mechanism. This can greatly improve the security of data. We need these data, just read and decrypt from these memory in the future.

5.2 User Authentication Module

In order to ensure the security of privacy data in cloud environment, this paper divides requests for data into different types and treats them differently. One is requests for access to privacy data, called privacy requests, and the other is requests for non-privacy data, called public requests. This classification is based on the privacy of the data. It can also be divided according to the source of the data request. The internal access to data belongs to the internal request, and the external access to data belongs to the external request.

When introducing the privacy data protection model, this paper classifies the data into two categories: private data and non-private data, because the privacy data is stored in the private cloud of the enterprise itself, so the privacy data is completely controlled by users. Non-privacy data generally has a large amount of data and should be stored in the public cloud. Therefore, no matter where the requests for access to non-privacy data come from, they will be transferred to the public cloud. The public cloud will respond to the requests and process them. The requests for access to privacy data will be processed entirely within the private cloud, so that the security of privacy data can be guaranteed. The authentication module is deployed in the private cloud. When there are requests for access to private data in the private cloud, the module verifies the identity of the requester. If it is an internal request, it responds directly. Otherwise, it may refuse to respond.

5.3 Key Management Module

If applications on public clouds need to use private data on private clouds, private clouds need to transfer private data to public clouds, but for the security of the transmission process, data need to be encrypted before transmission. In the model proposed in this paper, both private and public clouds have a key management module, which is designed to protect the security of data transmission between private and public clouds. In this model, we adopt different encryption methods from other methods; the specific process is as follows:

Step1: Private cloud generates a public key randomly and sends it to the public cloud. Private cloud keeps the private key corresponding to the public key at the same time.

Step2: The public cloud receives the public key from the private cloud, produces a symmetric key, encrypts the symmetric key with the public key, and then sends the encrypted symmetric key to the private cloud.

Step3: Private clouds use previously reserved private keys to decrypt symmetric keys from public clouds. At this time, both private clouds and public clouds have symmetric keys.

Step4: Data that needs to be transmitted can be encrypted with symmetric keys and sent to the other party. The other party can use the symmetric keys to decrypt.

The advantages of this method are as follows: firstly, the public key is generated by the private cloud because the public cloud is multi-user shared, which avoids the influence of too many private keys handled by the public cloud on efficiency; secondly, symmetric keys are encrypted by the public key, so that even if intercepted, symmetric keys can’t be obtained because there is no private key, thus the privacy data will not be leaked.

6. Summarize

In fact, in addition to strengthening investment in the field of technology and preventing the leakage of privacy data from data storage and data transmission, the protection of privacy security has a certain relationship with users' own security awareness, national laws and regulations, and the supervision functions of relevant departments. Privacy data should be protected. Safety should be considered from many aspects. We should not unilaterally emphasize the importance of one aspect. We must integrate and complement each other in many aspects, angles and levels. To protect the security of privacy data, besides the security of privacy data transmission and storage, the following points should be done:

(1) To strengthen their own security awareness, users should first strengthen their privacy protection awareness in the use of cloud services to prevent the leakage of privacy data. User's own security protection mainly includes password setting, login encryption, password management, authentication mode, data backup, software selection, fixed login location and so on. For example, if a user's password is set to his or her birthday, the password is unsafe, because many of his or her friends may know the user's birthday, which can easily lead to the leakage of privacy data.

(2) The management of access rights to privacy data must not grant access rights to untrustworthy users to prevent users from stealing and spreading.

(3) Establish and improve the regulatory mechanism, besides users and cloud service providers, we should establish and improve the third-party regulatory bodies, mainly for the supervision and management of cloud service providers, and conduct a comprehensive evaluation of cloud services to ensure the safety, health and sustainable development of cloud services.

References

[1] Wang Qingfeng. A Preliminary Study on Cloud Computing and Cloud Data Management Technology[J]. Computer Software and Applications, 2013 (04): 252-255.

[2] He Ming, Chen Guohua et al. Research on Cloud Data Storage Security and Privacy Protection Strategies in the Internet of Things [J], Computer Science, 2011 (05): 62-66.

[3] [3]Mao Jian, Li Kun et al. Privacy Protection Scheme in Cloud Computing Environment [J]. Journal of Tsinghua University (Natural Science Edition), 2011 (10): 1357-1362.

[4] He Wenna. Geological Informatization Research Based on Internet of Things and Cloud Computing in Big Data Era [D]. Jilin: Jilin University, 2013.

[5] Chen Guoying. Analysis of Data Security and Privacy Protection in Cloud Computing Environment [J]. Network Security Technology and Applications, 2019 (02): 40-41.

[6] ChiangC, LinC, ChangR. A New Scheme of Key Distribution Using Implicit Security in Wireless Sensor Networks[C]//Proceedings of the 12th International Conference on Advanced Communication Technology. Gangwon-Do, Korea: IEEE Advanced Communication Technology, 2010:151-155.

[7] Parakh A, KakS. Space Efficient Secret Sharing for Implicit Data Security[J].Information Sciences,2011,181(2):335-341

[8] Mell P, Grance T. The NIST Definition of Cloud Computing [J]. NIST special publication, 2011, 07.

[9] Arnold S. The Issue of Privacy in Cloud Computing [J]. KM World, 2012:14-22.

[10] Friedman AA, West D M. Privacy and Security in Cloud Computing[M]. Center for Technology Innovation at Brookings, 2010.

[11] Wang Haitao, Song Lihua. Security Management of Cloud Computing [J]. Data Communication, 2019 (04): 44-46.

[12] Cheng Guangde. Research on Big Data Security and Privacy Protection Strategy in Cloud Computing Environment [J]. Computer Products and Circulation, 2019 (07):145.