Journal of Applied Science and Engineering Innovation, Vol.2 No.1, 2016, pp.157-160
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Education Big Data Information Security Policy Analysis and Research in Cloud Computing Environment

Nie Jun, Zhang Dongbo, Zhang Xu
Guangdong University of Science & Technology, Dongguan,523083,China

Abstract: Our country's education area's development and revolution is facing unprecedented challenges. The combination of big data and education is the inevitable demand of time developing. The combination of big data and education plays a more and more important role in teaching practice. However, the security and privacy problem of education big data has become a noticeable problem in cloud computing environment and attracted more and more people's attention. This article analyzed the problem of big data information security in cloud computing environment and probed into establishing education big data security policy in cloud computing environment and offer reference to guarantee safe access to education big data.

Keywords Cloud computing; Education big data; Security policy

INTRODUCTION

As education develops, the combination of big data and education plays a more and more important role. However, the security and privacy problem of education big data has become a noticeable problem in cloud computing environment and attracted more and more people's attention. As a result, constructing education big data security guard in cloud computing environment is more and more important.

EXISTING PROBLEMS OF EDUCATION BIG DATA SECURITY IN CLOUD COMPUTING ENVIRONMENT

The security problem of education big data facing in cloud computing environment mainly reflects in the immaturity of security technology, barbarism of security standard and unsoundness of regulatory system and so on sides.

Immaturity of security technology

Under the background of cloud computing rapidly developing, education big data suppliers also develop quickly. Vast education big data service providers appeared. Every service provider offers different big data cloud platform. Every service provider has his or her own big data security standard. As a result, every service provider has different big data safety performance. Users' information and education resources can not be protected better, concretely reflected in data storage, purview division and so on sides. As for data storage, it's asked to guarantee reasonable and lawful search and usage. As for purview division, education big data should guarantee data supplier, users, cloud service provider these three can only delete and alter after authorization, which is related with the problem of purview division.

The barbarism of safety standard

As internet develops at high speeds, cloud service platform kinds are various, safety standard are not regular, education big data safety aims are not clear, each education big data safety guard core is different. To understand the safety needs of education big data, make targeted safety aims, quantify each kinds of education resources' safety index. Through the third party to make test evaluation to offer different safety strategies to different safety categories and improve education big data service providers' service level and quality and increase users' use times.

Short of regular safety evaluation methods is another reflect of unhealthy safety standard. Short of regular safety evaluation methods is hard to make big data service provider security reach related safety standard and users can not believe service provider can protect their secrets from leak. As a result, only launch related education big data safety evaluation methods, can every education big data service providers test its security through the third party, can users use it at ease, can education big data developing be pushed. Divide safety levels of different education resources in education big data and take different safety standards to different level's education big data, allow different safety standard's user visit different level's education big data, let different people receive needed education data.

Unsoundness of regulatory system

Cloud platform is open, shareable, real time and dynamic. Traditional supervision method can not adapt to new challenges any more. Under the background of globalization, cloud platform offer service according to users' needs. The education resources stored in cloud environment can not be supervised by the same government. Law differences also make it harder to supervise. As a result, normal

Corresponding Author: Nie Jun, Guangdong University of Science & Technology, Dongguan, 523083, China

and unified, formal and complete safety supervision system is needed to guarantee education data. Guarantee education resources are used legally and safeguard the legitimate rights and interests of education resources.

EDUCATION BIG DATA INFORMATION SAFETY POLICY'S CONSTRUCTION IN CLOUD ENVIRONMENT

Guarantee of the construction of system technical framework

Although in cloud environment, education big data satisfied different people's needs, the insecurity and potentially sensitive data leakage risk cause the danger of leaking users' information and users' data. As a result, a safe education big data environment is needed to be constructed to guarantee the safety of education big data. From the previous analysis, we can know that our country's education big data security policy in cloud computing environment mainly involve safety technology frame, safety use standard and supervision system three aspects.

Safety technology frame construction

(1) Data secret protection policy

The major of constructing security technology framework is data encryption and cloud access control storage encryption technology, property encryption algorithm including keypad policy and CP - ABE. Decryption rules involve keypad policy to avoid rapid cost, and when visiting cipher text，control secret key distribution. When access control strategy dynamically changes, data owners should re-encrypt the data. In cloud computing environment, education big data privacy data process is shown as Fig. 1.

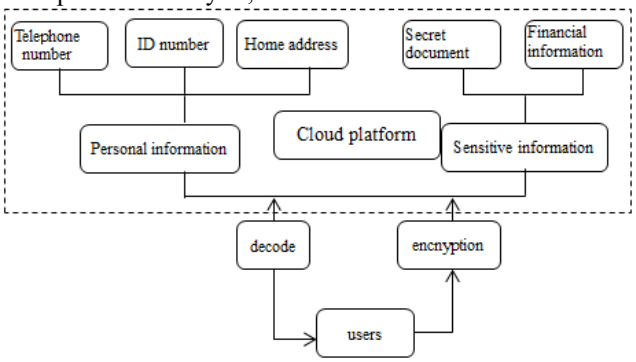

Fig. 1 Cloud computing protection privacy data work flow

(2) Access control policy

As the core service content of cloud safety technology, cloud access control mechanism plays an important role. In such an open internet environment, traditional access control method cannot meet the requirement of protecting data content. As a result, we need to establish feasible fusion data access control mechanism in cloud environment. Authentication and control are not controlled by client-side any more, but by cloud to realize digital content authentication and access control to stop illegal access and download and ensure the security of overall access control mechanism.

Through safety access control policy of cryptology, these problems can be avoided effectively. This policy is based on open internet system. When conducting this policy, "read" and "write" rights of data stored in system will be allocated to users. When data is under reading condition, symmetric key is allocated to users.

Users decode the data received from server to get needed data information. "Decryption key" is used to check data integrity; when data is in written condition, "decryption key" also will be configured to users. Users will encrypt the data that is going to be written and send into server. "Encryption key" is used to calculate data integrity. At the same time, "decryption key" is configured to the server to check the integrity of data. Cryptography access control policy is shown as Fig. 2.

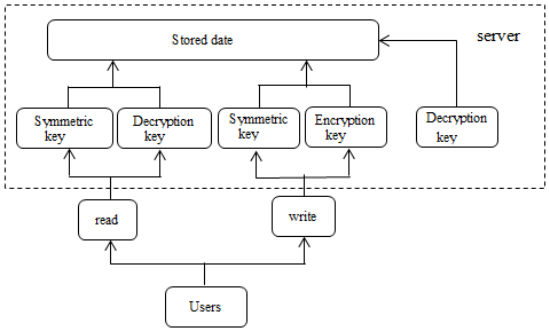

Fig. 2 Cryptography access control policy

Through constructing the cryptography access control policy shown in picture 2, establishing safety encryption database, data will not be decoded in cloud service provider. But to legal users, related decoding right of data content can be awarded to them. As a result, the protection of database privacy and data content can be strengthened effectively and avoid

hacker attack outside the internet to ensure the safety of access control mechanism.

(3) Identity authentication policy

Unified identity authentication strategy can effectively reduce duplication of authenticating users, improve work efficiency and the convenience of cloud service and enhance use efficiency of users using the education big data.

Adopting unified identity authentication method reduces the possibility of users' personal information leakage and being stolen and ensure the safety of user information transmission. By way of single sign-on, users can use all application system with appropriate permissions after system certification only by using key or login information set when registering, so as to avoid repeat login.

(4) Data backup strategy

Classifying protecting education big data is the basic principle of safety protection measures in a cloud computing environment. According to different security levels, implement different levels of protection. As for core data, we need to take absolute protection. Data backup should be stored according to the principle of multiple copies and long-distance storage, perform daily backup in strict accordance with the system and record the backup management; as for important data, we need to take emphasized protection and data should adopt redundant backup; as for key data, we need to take special protect. Key data has very high use value or secret nature and should be stored according to redundant backup and long-distance storage; as for common data, this kind of data have common use value, we should make focus backup regularly; as for open data, we should make regular daily backup.

Construction of safe use standard

Establishing education big data security standard in a cloud environment has positive significance to the safe usage of education data in a cloud environment.

(1) Safety evaluation framework

On the basis of the policies, laws and regulations, according to the importance degree, classify safety evaluation system, evaluate every level from the level of management and technology. Management level mainly includes the management institutions and personnel, management system and daily operation; Technology mainly includes the hardware security, network security, system security, data security, etc. Among which measured security mechanism mainly include identification, access control, security audit, etc. In the management level, bring security management organization, personnel post settings and so on into the management class assessment indicator; in the technical level, the education big data safety evaluation methods in cloud environment is divided into six aspects, such as platform security, data security. Cloud computing data safety test framework is shown as Fig. 3.

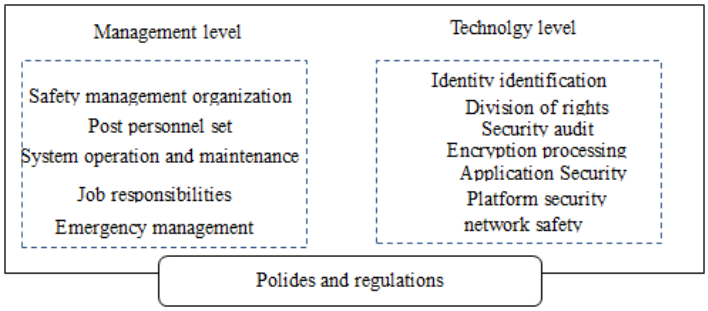

Fig. 3 Cloud computing data safety test framework

(2) Safety performance index strategy

Cloud platform safety performance index involves functionality, usability, efficiency, reliability, maintainability and portability. Functionality refers to whether cloud platform has the characteristic of satisfying education data providers' using; Usability refers to whether a cloud platform meets the characteristic of that education data providers and users can operate easily; reliability refers to whether the cloud platform owns the characteristic of education data providers; efficiency refers to whether the cloud platform have the characteristics of the education data can be effectively used; maintainability refers to whether cloud platform have the features of cloud service providers' maintaining; portability means whether a cloud platform has the characteristic of transplanting to other data management system.

(3) Safe use standard strategy

Make cloud platform rating scale according to safety performance six indicators, divide related security level, help users understand the safety of cloud service providers providing services, provide a reference for the user to select a suitable cloud services.

Table 1 safety level rating scale

score	G≥90	80≤G<90	70≤G<80	60≤G<70	G<60
level	1 level safety	2 level safety	3 level safety	4 level safety	unsafe

The construction of security supervision system

According to the particularity of education big data, build security supervision system which should include offline and online supervision system, offline supervision system mainly includes education department, the cloud service provider and the third party safety regulators, in order to test whether the safety measures of cloud service providers is up to the standard. At the same time, adopt safety certification to cloud computing service providers that passed assessment, data providers and users get certification from cloud service providers' name list that have already got certification and choose suitable service according to their own requirements and establish cooperation and rental relationship. The form of offline supervision system could strengthen applying effect of education big data effectively and ensure the use safety of education big data. On-line supervision system mainly includes the artificial regulation and regulation of computer security software, ensure that safety and reliability of education data that users uploaded and downloaded. Safety supervision system is shown in Fig. 4.

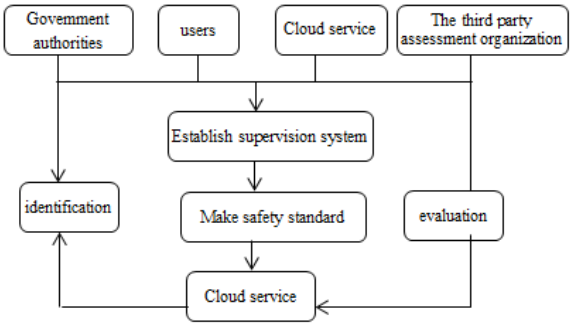

Fig. 4 Safety supervision system

CONCLUSION

Through analyzing the safety problems education big data facing in cloud education environment, mainly the immaturity of security technology, barbarism of security standard and unsoundness of regulatory system three sides, this article constructed technology framework strategy, safe use standard strategy and safety supervision system strategy according to these three sides' problems, offering reference to realizing education big data safety in cloud computing environment.

FOUNDATION PROJECT

This paper is funded by the subject:Permanent magnet synchronous motor servo system design and algorithm study,The youth projects for creative talents in Guangdong province,Num(2015KQNCX191)

REFERENCES

Chen Quan，Deng Qianni. Cloud computing and its key technology[J].Computer application， 2009， 29(9): 2562-2567

Chen Xiaoyan. Probe into defense measures of data safety in cloud computing times[J].Electronic technology and software engineering, 2013 (16):245-246

Feng Dengguo， Zhang Min,etc. Research on cloud computing safety[J]. Journal of Software ,2011,22(1)

Han Ying.Network copyright protection problems and coping strategies in cloud computing environment [J]. China Publishing Journal，2012 (10): 54-56

Li Guojie.Scientific value of big data research[J]. China computer federation communication,2012,8(9): 8-15

Li Yuan.Cloud services security policy in cloud computing[J].Computer developing and applying，2013 (11)

Li Zhanbao, Zhang Wengui. Cloud computing and its security analysis[J]. Information internet safety, 2011

Nie Jun. UAP cloud platform SPC extension algorithm based on intellectual group identification[J].Scientific communication ,2015(2):125