Research on Privacy Protection Based on Trusted Third Party

Huijie Zhu[1,a], Chunbo Wei[1,b],Guotao Xu[1,c] and Lan Luan[1,d]

[1]Hunnan Road, Hunnan District, Shenyang City, Liaoning Province, Shenyang Jianzhu University

[a]zhuhuijie9990@163.com,[b]weichb@sjzu.edu.cn,[c]2670787599@qq.com,[d]854128356@qq.com

Keywords: Big data; Privacy Protection; Third Pparty; Framework

Abstract. With the development of big data, the data privacy of users becomes very important. In this paper, the privacy protection framework of the reliminary study, the establishment of the introduction of trusted third party privacy protection technology framework.[1] Through the introduction of credible third parties, a three-way interaction model is constructed so that the third party can authenticate the corresponding information and manage the privacy policy. This paper introduces the functions of each module of trusted third party privacy protection, which provides a new idea for further research on data privacy protection.

Research Background

With the development of cloud computing, database service DaaS (Database as a Service), as one of the most common SaaS services, is also the foundation of many other SaaS applications and is being accepted and adopted by more and more enterprises.[2] In particular, DaaS is favored by smaller companies. Because of the small size of data, small and medium-sized enterprises need to employ their own professional staff to carry out routine maintenance of the database and increase the cost of small and medium-sized enterprises.[3]

Due to the imperfect credibility of service providers and the fact that in DaAs the physical control over data is not part of the user himself but the service provider and the less than trusted service provider has all the rights to user data . In this mode, users will inevitably worry about the service provider does not operate the user's data according to the norms, and even steal the user's data privacy. [4][5]In order to prevent incomplete and credible service providers from stealing user privacy, some researchers propose introducing a trusted computing module or introducing a trusted third party.

Addressing data privacy concerns is an important prerequisite for companies to hand over data to service providers managed by service provider proxies without any worries. In the Daa S application scenario, storage and management of user-sensitive data are performed by non-fully trusted service provider agents, a process that is not user-controllable. [6]The user application needs to process the user data in various ways. [7]The user data is stored in the database in a plaintext manner, which is most conducive to the processing of data by the user application system. However, the data is stored in the cloud in a plaintext state and is easily replaced by an incompletely trusted service provider steal. In order to protect the data security and privacy of users, privacy protection measures must be taken for users' data.[8] However, in order to ensure that users' application systems are not affected by privacy protection measures, it is necessary to ensure that privacy protection measures do not significantly affect database functions and performance.[9]

Research Status

Trusted third parties, there is not a widely accepted definition. Many researchers endorse an organization as a credible third party; some also include a trusted third party that builds a secure environment with trusted computing technology. [10]Whether a trusted third party is an organization or a trusted environment, their function is the same in the cloud storage privacy protection architecture, which is to protect critical data. As trusted computing technology is still in its development stage, at present, many researchers agree that a trusted third party is still a trustworthy organization with participation.

In addition to the incomplete trustworthiness of service providers, another feature of cloud storage is multi-user. Database services can not be designed for one or a group of users. In order to reduce costs, database services must be multi-user oriented. A storage system may be multi-domain, multi-industry users to rent. In this way, privacy protection needs of different users are bound to vary greatly. How to satisfy the huge privacy protection requirements of different users is a problem that all cloud storage systems including database services must solve.

Research on the Privacy Protection Framework Based on Trusted Third Parties

According to the relevant literature, the introduction of trusted third parties, the three-party interaction model shown in Figure 1:

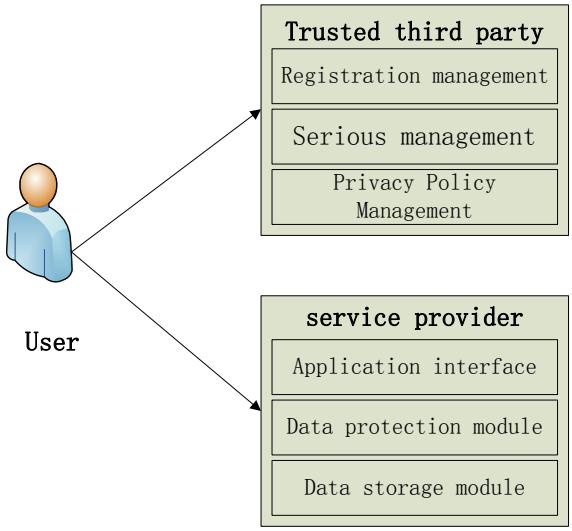

Figure 1. Three-way interaction model

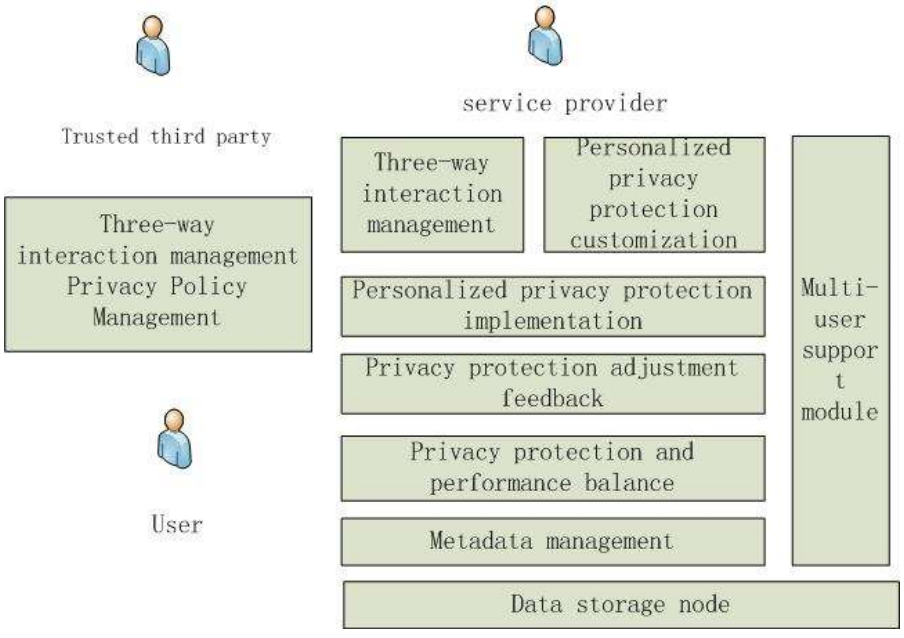

Figure 2. Trustworthy third party privacy protection architecture model diagram

As can be seen from Figure 1, in this model, a trusted third party is responsible for identity authentication and privacy policy management. The function of privacy policy management is to manage the user's privacy protection scheme. The service provider is responsible for the data protection module and data storage module. The data protection module is responsible for implementing privacy protection measures to protect user privacy. The data storage module is

responsible for data storage, management and maintenance. The focus of this work is to define the three-way interaction model, so the detailed functions of the privacy policy module and the privacy protection module are not precisely defined. This paper continues to use the three-way interaction model, designed a trusted third party based on the privacy protection structure, data protection module has been extended and defines the function of each module, the document privacy protection architecture model shown in Figure 2.

User

Users can be an individual or business, in most cases an enterprise, users rent database services over the network. In the privacy protection architecture based on trusted third parties, the users are all thin clients. The users do not need to consider and participate in the implementation of the privacy protection measures. Users only need to submit their own data and privacy protection requirements. Under the recommendation of the system, Own privacy protection strategy. In addition to the choice of privacy policy, other privacy protection efforts should be as transparent as possible to the user, as far as possible to make the user feel no difference between using the database service and using the local database.

Database Service Provider

Service providers are providers of database services, providing hardware and software for database services, while managing the dimension protect the user's data. In the privacy protection architecture shown in Figure 2, the service provider manages the personalization implicitness private custom module and privacy protection implementation module, through these two modules to provide users with personalized privacy protection service Services to meet the diverse needs of multi-user. , Privacy protection adjustment feedback is to solve the user privacy protection needs change, this article will not be considered; privacy protection and performance balancing is based on user's application requirements, the data stored separately in different storage nodes to improve the overall performance of the database .

Credible Third Party

Trusted third parties are the key to privacy protection in database services. Since service providers are not completely credible and user privacy data is not fully exposed to service providers, trusted third parties need strict control. Trusted third parties can be one A person-led agency can also be a server or a system. In the privacy protection architecture shown in FIG. 2, the main work of the trusted third party is only to protect the personalized privacy protection scheme of the user and the key data generated by the user data during the implementation of the privacy protection measure.

In addition to the trusted third parties involved in the data storage phase, trusted third parties are also required during the data usage phase because service providers can not restore user data and need to authenticate users when they need to use the data, And then obtain the user's personal privacy protection programs and privacy protection measures in the implementation of the key data in order to restore the implementation of the privacy protection measures of the data.In fact this article has implemented three modules: privacy policy management, personalized privacy customization, personality Privacy protection implementation.

Privacy Policy Management Module

The privacy policy management module is responsible for storing the personalized privacy protection schemes used for managing user data and the key data information generated during the implementation of the privacy protection measures, for example, the key in the database encryption process, the random number sequence in the data block storage method, These data directly related to the user's data privacy. Due to the incomplete trustworthiness of service providers, the disclosure of these data to service providers will result in the loss of privacy protection. The privacy policy management module needs to be strictly authorized to use user privacy to protect users' personal privacy protection programs and privacy protection measures. The key data.

Personalized Custom Privacy Module

The function of personalized privacy customization module is to interact with the user, according to the user's data and privacy protection needs, recommend appropriate privacy protection method

to the user. In the actual database service, due to the characteristics of multi-users, the privacy protection needs of users vary greatly, and different privacy protection needs inevitably have different privacy protection methods. The same privacy protection needs can also be satisfied by different privacy protection methods. Different privacy protection methods have great differences in privacy protection effect and great impact on the performance of the database. The privacy policy selection module needs to refer to various factors to recommend a reasonable privacy protection method for the user and at the same time to inform the user of what kind of impact the user may choose when using different methods. As the user may not have the knowledge of privacy protection, do not understand the advantages and disadvantages of various privacy protection methods, personalized privacy customization module to show users different privacy protection methods of different effects on users in order to facilitate users to choose the most suitable for their privacy Protection method.

Personalized Privacy Protection Implementation Module

Personalized privacy protection implementation module's main function is based on the user's personalized privacy protection program, the user's data privacy protection measures. This measure can be database encryption, it can be data block storage, the specific measures based on the user's personalized privacy protection program.

Summary

Through various studies on the privacy protection framework, a trusted third party privacy protection technology has been established. The introduction of a trusted third party to achieve a three-way interaction model, so that the third party to the corresponding information authentication and privacy policy management. This article also introduces the functions of the three modules of privacy protection strategy management, personalized privacy customization and personalized privacy protection for trusted third party privacy protection, which provides a new idea for further research on data privacy protection.

References

[1] Zhen Jiang,Document-oriented Database-based Privacy Data Protection Architecture[J], WISA 2013, 2013(12): 19-22.

[2] N. P. Smart and F. Vercauteren, Fully homomorphic encryption with relatively small key and ciphertext sizes[C]//Proc 13th international conference on Practice and Theory in Public Key Cryptography, 2010:420-443.

[3] Peng L. Individual Choice and Reputation Distribution of Cooperative Behaviors among Heterogeneous Groups. Chaos, Solitons & Fractals, 2015, 77: 39-46.

[4] Macfarlane R., Buchanan W.Ekonomouet E., et al. Formal security policy implementations in network firewalls[J]. Computers & Security,2012,V 31(2): 253-270

[5] OASIS. Extensible Access Control Markup Language(XACML) Version 3.0[EB/OL]. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html, January,2013

[6] Ryan Hayward, Chia-Chu Chiang. An Architecture for Parallelizing Fully Homomorphic Cryptography on Cloud[C].//Proc 7th International Conference on Complex, Intelligent, and Software Intensive Systems,2013:72-77.

[7] Yuliang Shi,Zhen Jiang, Kun Zhang, Policy-Based Customized Privacy Preserving Mechanism for Saa S Applications[C]. GPC 2013:491-500.

[8] F.Prasser, R.bild,J,Eicher, H.Spengler, F.Kohlmayer, and K.A.Kuln. Lighting: Utility-driven anonymization of highdimensional data ,Transactions on Data Privacy,2016,9(2):161-185

[9] Dengguo Feng, Min Zhang. Yan Zhang, Zhen Xu, Study on Cloud Computing Security[J]. Journal of Software, 2011, 22(1):71-83.

[10] Yonghong Yu and Wenyang Bai. Enforcing data privacy and user privacy over outsourced database service[J]. JSW,2011.6(3):404–412.

[11] BSI.Information security management Part 2: Specification for information security management systems. BS7799-2:2012.2012