Research on the Key Technology of the Cloud Platform Data Security

Xuefeng Jiang[1, a], Zhengmin Wang[1,b], Huiliang Dong[1, c], Xuan Du[1, d]

[1] China Tobacco Zhejiang Industrial Co., LTD, Hangzhou, 310009, China

[a]jxf@zjtobacco.com, [a]wangzm@zjtobacco.com, [a]donghl@zjtobacco.com,[a]duxuan@zjtobacco.com

Keywords: Cloud Platform; Data Security; Data Storage; Storage Service

Abstract. Since the establishment of the relationship of trust exists between transparency, cloud computing services platform providers and data users, the integrity of the cloud computing service provider platform to the data stored in the user data information to prove, at the time of data information sharing to ensure that confidential data information interaction and so are the need for further research to solve problems. Based on the in-depth analysis to protect the integrity of data security issues cloud platform computing environment based on the presence of current, mainly on the cloud platform computing environment data stored information, confidentiality protection and data storage carrier when the underlying data information sharing Security protection facilities of these three aspects studied.

Introduction

Cloud computing platform is the most worth looking forward to worldwide technological revolution, with its dynamic resource allocation, design-demand service at a lower cost to solve the unique charm of the massive data processing, creating hope for the technological revolution. Cloud computing technology platform emerged an objective necessity [1]. With the promotion and application of cloud computing platform services, data storage and data processing pressures continue to grow, and thus also led to the rapid development of the storage market, cloud storage has become typical of cloud computing services platform, which foreshadowed for next-generation storage service ideal choice [2].

But feeling good momentum of development at the same time, we must also recognize that the development of new matters is the fact that both opportunities and challenges, will store data in the cloud platform might cause information security problems. Including cloud computing services platform both own security risks, but also involves security risks cloud computing platform to provide services for data users and their specific applications when, for example, the composition of its transparency feature makes internal cloud infrastructure and service platform computing systems offer form completely transparent to users of the data, the data users need only have a legal identity and authorization to access manner anywhere network access and access to services through cloud computing system platform, and precisely because of this transparency, cloud computing service providers and data platform establish a trust relationship between the user, the cloud computing service provider platform to prove the integrity of the data users store data information and other data to ensure the confidentiality of information, further studies are needed to solve the problem when the data exchange information sharing [3-4]. Existing security technology is difficult to deal with these issues, making a number of characteristics of cloud computing platform is not fully, so to promote the comprehensive development of cloud computing technology platform to address the many data security issues cloud platform computing environments that exist imperative .

Cloud data storage service analysis

Data storage volume growth to bring pressure storage services, at the same time it is also driving forward the rapid development of storage service, which is also an ideal choice for cloud storage next-generation storage services. But feeling good momentum, but also must recognize that storing data in a cloud environment may bring problems [5]. In this paper, on the whole cloud

computing services described and to explore cloud computing services for issues related to data security, and cloud data storage service structure shown in Figure 1.

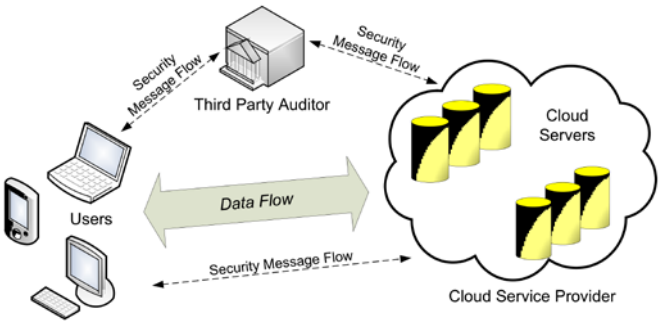

Figure 1. The architecture of cloud data storage service

Cloud storage is a cloud platform technology in the storage area of a typical application services. From the perspective of routine use of the situation, when the data users their personal data is stored in the device (such as: desktops, laptops, etc.), the data the user is responsible for data processing, while the user's own data must also store data on their own security protection, so in this type of case data users with the highest privileges to manipulate the data. In contrast, once the user selects the cloud data storage service for data storage, operation and safety monitoring data users store data are mainly from the cloud platform service providers responsible for data users at all will not have control over the data [6].

When the user's information is stored in the cloud, we need to consider whether the supplier has a comprehensive security rights management measures, whether through encryption of stored data security management, and storage in the form of stored data is reasonable. For the processing of data in the cloud, we can consider two aspects: the equipment is a service environment and the Simple Storage Service, or software as a service platform that is applied under reserve Services. Data stored in the cloud to consider reliability, confidentiality and integrity. The general solution is to encrypt the data by operation, so reliable encryption algorithm to encrypt data for the effect it is very important. Modern cloud computing need to deal with large amounts of data communications, storage and applications. In the process, taking into account the speed and efficiency of computing, symmetric encryption algorithm is more in line with the data processing needs of cloud computing. In addition, also we need to consider the management of data encryption algorithm, theoretically should be the creator of data to be managed, but not every user can encrypt data on their operations, so that they will work to the cloud service providers.

Data security analysis under the cloud platform

The preceding analysis of security risks and problems of cloud computing, but not to say that these problems in traditional IT systems does not exist, but that, because of the cloud of its own characteristics, some issues become more apparent or critical. Cloud computing in ensuring the efficiency, we must also pay attention to transmission security work is perfect, the integrity of the data and whether it meets the requirements related to the confidential documents [7]. To solve the primary task of the cloud for threats, establish an overall composition contains from bottom

Physical structure to the top-level application security framework, which can have a destination for different levels of security into the cloud

Line research. Combining cloud computing security offer practical level framework based on a hierarchical security architecture cloud platform, as shown in Figure 2.

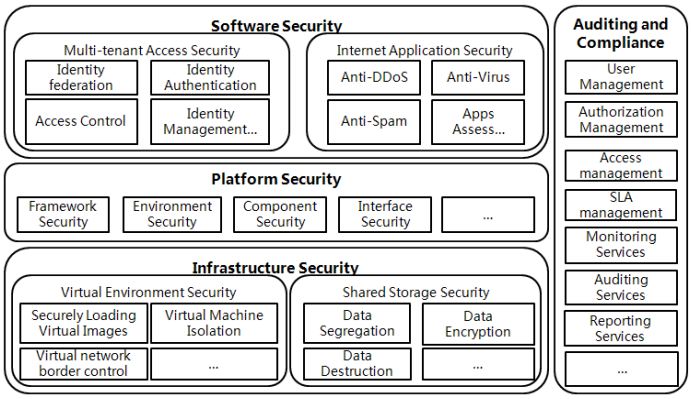

Figure 2. Cloud platform data security architecture

This architecture includes cloud computing and cloud computing security service system safety standards and evaluation system in two parts, in order to achieve security objectives cloud users to provide technical support. The primary safety objective cloud users about data security and privacy protection services. Cloud computing security service system is an important technological means to achieve security objectives cloud users, cloud computing environment combining different levels of cloud computing security service is further divided into a trusted cloud infrastructure services, infrastructure services cloud security and cloud security applications. Cloud computing security standards and evaluation system for cloud computing security service system provides an important technical and management support. In this framework, the research on this topic cloud content security service system involved is worth learning.

Our Proposed Scheme

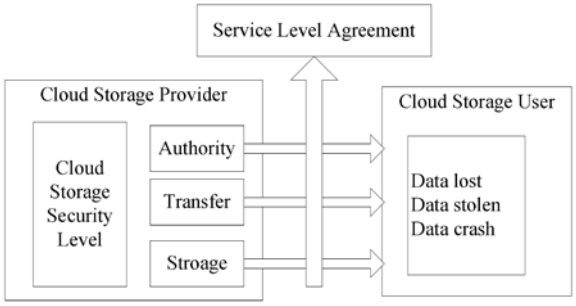

Figure 3. Framework to ensure data security

In this paper, we propose a framework for unified cloud storage providers and users, as shown in Figure 4. Service Level Agreement is an agreement between the service providers and users. It defines the type of service, service quality and customer payment terms. Users are often concerned if it is possible data loss (not restored), data theft, and crash. SLA can define the probability of occurrence of all these data disaster, the storage vendors use different techniques to obtain SLA. .

A. Main Idea. In order to achieve secure, scalable, and fine-grained access control outsourced data in the cloud, we use the following three and a unique combination of advanced encryption technology: KP-ABE, PRE and lazy re-encryption specifically, we will each. Data files and a set of attributes, and assign each user an access structure to define these properties expression. Access to perform this type of control, we use KP-ABE escort the data encryption key data file. This structure allows us to enjoy good access control dignitaries immediately. However, this architecture, if deployed separately, will introduce large computational overhead and burden of tedious data network owner, he is responsible for all data / user management operations. Specifically, this problem is caused by the user undone, which inevitably requires the owner of all of the data leaving the user to access data files, or even data owners need to keep online for users to update the key. Solve challenging problems, make construction suitable for cloud computing, our unique and KP-ABE to enable the data owners and before most of the compute-intensive operations entrusted to the cloud server did not disclose the underlying file content. Such construction allows data

owners to control access to data files and minimal overhead computing efforts and online time, so for cloud computing environments. Data confidentiality also reached from the cloud server cannot understand any of the plaintext data file in our building.

Notation	Description
PK, MK	system public key and master key
T_i	public key component for attribute i
t_i	master key component for attribute i
SK	user secret key
sk_i	user secret key component for attribute i
E_i	ciphertext component for attribute i
I	attribute set assigned to a data file
DEK	symmetric data encryption key of a data file
P	user access structure
L_P	set of attributes attached to leaf nodes of P
Att_D	the dummy attribute
UL	the system user list
AHL_i	attribute history list for attribute i
$rk_{i \hookrightarrow i'}$	proxy re-encryption key for attribute i from its current version to the updated version i'
$\delta_{O,X}$	the data owner's signature on message X

Figure 4. Notation used in our scheme description

B. Definition and Notation. A meaningful attributes necessary for access control is assigned to each data file owner. Different data files can have a common subset of attributes. Attribute update each property and the version number for the purpose of later we will discuss. Cloud server maintains a list of attributes for each attribute version AHL history of evolutionary history and PRE key. In addition to these interesting properties, we also define a virtual property, denoted by symbol Att_D for the purpose of key management. Att_D is required to be included in every data file's attribute set and will never be updated.. Allocate an owner for each data file Group meaningful attributes necessary for access control. Different data files can have a common subset of attributes. Attribute update each property and the version number for the purpose of later we will discuss. Cloud server maintains a list of attributes for each attribute version AHL history of evolutionary history and PRE key. In addition to these interesting properties, we also define a virtual property, Figure 4 shows the description of symbols using our program.

For clarity, we will present our program at two levels: system-level and algorithm level. At the system level, we have achieved a high level description of the operation, that the system settings, a new file to create a new user Grant and revoke user, file access, file deletion, the interaction between the relevant parties. On the algorithm level, we focus on low-level operating system-level algorithm called.

Conclusion

In this paper, a comprehensive, in-depth study of data security infrastructure cloud platform storage services that exist in the current environment, respectively data integrity protection, security protection and the protection of confidentiality of data stored in a data carrier infrastructure information sharing when a study . Our own security problems began to study information from the data stored in the cloud environment, analysis of existing storage data integrity protection research work proposes a framework for unified cloud storage providers and users, and to explore how to use a unique combination of advanced encryption technology KP-ABE, PRE and lazy re-encryption, to implement secure, scalable, and fine-grained access control outsourced data in the cloud. This article only is in some preliminary attempt, there are many issues that need further study and improvement.

Reference

[1] Wang Q, Wang C, Li J, et al. Enabling public verifiability and data dynamics for storage security in cloud computing[M]//Computer Security–ESORICS 2009. Springer Berlin Heidelberg, 2009: 355-370.

[2] Wang C, Wang Q, Ren K, et al. Privacy-preserving public auditing for data storage security in cloud computing[C]//INFOCOM, 2010 Proceedings IEEE. Ieee, 2010: 1-9.

[3] Wang Q, Wang C, Li J, et al. Enabling public verifiability and data dynamics for storage security in cloud computing[M]//Computer Security–ESORICS 2009. Springer Berlin Heidelberg, 2009: 355-370.

[4] Wang C, Ren K, Lou W, et al. Toward publicly auditable secure cloud data storage services[J]. Network, IEEE, 2010, 24(4): 19-24.

[5] Chen D, Zhao H. Data security and privacy protection issues in cloud computing[C]//Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. IEEE, 2012, 1: 647-651.

[6] Wang Q, Wang C, Ren K, et al. Enabling public auditability and data dynamics for storage security in cloud computing[J]. Parallel and Distributed Systems, IEEE Transactions on, 2011, 22(5): 847-859.

[7] Chow R, Golle P, Jakobsson M, et al. Controlling data in the cloud: outsourcing computation without outsourcing control[C]//Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009: 85-90.