Design of Data Secure Storage for Cloud Compute ring

Wenhu Yang

Information Engineering Department, Jinan 250104, China

ywh_0001@163.com

Keywords: Cloud compute ring, data security, authentication protocol, information flow control, secure accountability.

Abstract. With its great power to integrate resources, Cloud Computing can offer individuals and organizations the convenient and on-demand computing and storage service. As the increasingly influence on everyday life, its structural safety problem emerges. Due to the loss of physical control towards data, the users' data safety only relies on the cloud server unilaterally. In this paper, based on the current problems, our dissertation chooses secure cloud data storage auditing protocol as the main researching object. With the basic theory and tools of cryptography, based on provably secure theory, we analyze the existing works for detailed security, efficiency and scalability research. Meanwhile, we focus on the key technology of secure data verification, i.e. data aggregate signature algorithm.

Introduction

Cloud computing provides a large number of IT resources such as hardware and software as a service to users through the network. In cloud computing service model, users host data and application to the cloud, due to the cloud service transparency, they lose control of the data. Because it is difficult to assess cloud provider's credibility for users, data security has become the primary concern in cloud computing. [1]

Since cloud computing does related operations based on user's service request, authentication between users and cloud providers can avoid illegal access from assumed identity. Whereas, due to the large number of users, how to realize safe and efficient authentication is the main concern for users and service providers. [2] Having been authenticated, users can use the data storage and computing services. Users upload large amounts of data to the cloud and commission cloud service providers to calculate without the local copy stored. Although the cloud service provider is with strong technical strength and maintenance, it is not possible to completely prevent data damage or leakage occurs. For static storage of data, due to the mass of data, it is no longer applicable to verify integrity after downloading data to local in traditional way. [3] If users find data integrity is compromised, they can only pray the cloud service provider's disaster recovery mechanism works. Because of the characteristics of multi-tenant in the cloud, user’s access data and compute through the service process for dynamic data in computing service, the process carrier of shared access become focal point of authority. But it is difficult to achieve effective isolation and control of different users' data by shared permissions on OS level, data isolation mechanism of application solely is easily bypassed, so data confidentiality and integrity in multi-tenant environment remain to be resolved. If the data disclosure really happens, it is a key issue to charge service providers' responsibility. [4] Current accountability mechanisms need details of cloud services, which are related to cloud service providers' trade secrets, consequently it is difficult to achieve. In addition, due to the lack of trusted protection mechanism, security mechanism may be attacked, tampered or bypassed, accordingly it fails.

The essence of the cloud data security problem is the trust management between data owner and service provider, certain data constraints should be formed between them. They achieve certain data use agreement through reputation and technical means of restraint, contribute to the legitimate use of data and prevent from destroying. [5] Users can choose to rely on service provider side by reaching a mutually satisfactory security mechanism to maximize safety and security, service providers will not have a place to live in once he lost credibility. In this context, cloud service providers are willing to

cooperate with users to take data security protection technology, and never do intentional destruction of user data, but they may hide data safety accident. From this point of view, the thesis studies on the authentication, static memory data

Security issues in the environment of cloud compute ring

In the environment of public cloud, users worry about their sensitive data would be disclosed online by cloud vendors, other cloud users or hackers. And they would lost the control of data like creation; propagation amyl destruction. Scheme of storage architecture is shown in Fig. 1.

Virtualization technology and virtual machine live migration are core techniques in the cloud infrastructure. They are essential for dynamic resource re-scheduling. Virtual machine live migration brings security vulnerabilities that don't exist on non-mobile systems.

There are possibilities that cloned platforms be articled directly via physical means, like bus and memory probing, and even compromises to hardware components.

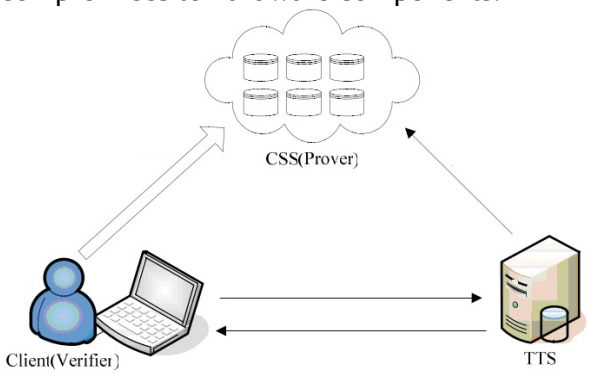

Fig. 1 Scheme of storage architecture

Password authenticated key change

A cross-cloud authentication scheme based on 3PAKE (three-party password authenticated key exchange) protocol is proposed and a provably secure authentication protocol is designed for the scheme. Users, the private cloud to which the users belong and the public cloud correspond to the three parties of the 3PAKE protocol which realizes cross-cloud authentication. The authentication scheme based on our protocol is more computation efficient than other cross-cloud authentication schemes. Traditional password authentication is vulnerable to password-guessing attacks and cannot generate a session key securely. To solve the problems of password authentication, a protocol based on elliptic curve cryptosystem is put forward. The protocol is proved to be forward securing for session keys and defeat off-line password guessing attack in the random oracle model. Compared with the PKI or IBC authentication scheme, this scheme is simple and of high security which realizes the efficiency, safety and fairness bidirectional authentication process with public cloud.

This paper promotes an accountability scheme for data integrity in cloud storage based on a TTP. In the scheme, every write operation carried out between a user and a provider is assigned with an attestation authenticated by TTP, thus holding accountable both the provider and the user. The attestations are stored in the cloud servers in order to reduce users' burdens, and this paper designs an algorithm for ensuring the integrity of the attestation chains on the basis of Merkel Hash Trees (MHTs, as shown in Fig. 2), which ensures that the providers cannot tamper or discard any of the attestations without being detected. Moreover, the paper provides designs of feasible protocols for generating attestations and auditing through them. Simulation results show that the attestation generating protocol brings little effect on the efficiency of operations.

Data storage scheme

A static data storage scheme users can very is put forward, which enables users to realize cloud data integrity verification, bug reparation and data leakage accountability. In order to enable users to recover after finding data breaches, we present a multi-copy storage preprocessing method on secret sharing and a storage method separating user identity information from available data, to prevent external attackers to collect the same user's data block to reconstruct the original file after obtaining owner's information of data. Integrity verification methods supporting above multi-copy mechanism is proposed to verify the data integrity in time, compared with existing integrity verification method, it can determine the error data block and support publicly verifiable from third-party and data dynamical update. Multi-copy integrity verification cannot guarantee data not leaked by cloud service provider, to solve this problem, a data leaked accountability method using database watermark is presented, which is based on the good characteristics of the cloud model and chaotic sequence, and help the user to investigate service provider's dereliction of duty. Compared with schemes each other is Table 1.

Table 1 Schemes

Schemes	Computation cost		Communication Steps	Security properties	
	user	Server		Password-guessing attack	Stolen-verifier attack
Huang's scheme[78]+	2	2	5	Insecure	Insecure
Lou's scheme[84]	3	4	5	Insecure	Insecure
Chang's scheme[81]+	3	4	6	Insecure	Insecure
Chien's scheme[77]+	4	7	6	Insecure	Partial
Our scheme	4	2	4	secure	secure

Dynamic Data security protection system CA-at Guarder is built based on the dispersion information flow model the CA-IFC, which provides fine-grained data isolation and control between multi tenants. In order to eliminate the ambiguity and integrity of the DIFC, we complete formal modeling for mark system and information flow rules based on propositional logic, and prove CA-IFC's safety. Then we design a distributed file system protection mechanisms, sensitive data object marking and tracking control implementation mechanism in CA Data Guarder based on the rules and privileges constraints. On the programming language level, we propose a LPE (least privilege encapsulation) mechanism to guarantee that the implementation of security strategy is easy to locate and monitor. On operating system layer, it supports upper cloud application based on a unified DIFC security policy model, transfers user information as the application context semantic to OS layer, which realizes fine-grained data control and protection.

Virtualization-based architecture

A trusted cloud computing platform is constructed based on virtualization-based architecture, which provides a trusted execution environment to execute above data security protection mechanisms. First of all, we realize formal modeling and safety proving for the transfer of platform trust chain and afford theoretical support. Given the openness of OS, in order not to increase the user's security overhead, we enhance credibility in VMM (a virtual machine monitor) layer, and propose a unordered trust chain transfer mode, which provides integrity measurement and isolation protection for executable program for the upper VMs against malicious code tampering and destroy data security mechanism destroying. To reduce the security overhead of cloud service providers, it is assumed that only part of the host cloud infrastructure is enhanced, then we propose a credibility binding plan of virtual machine images and cloud computing environment.

From the applicable point of view to the data stored in the cloud, it tries to cope with the problems of confidentiality protection during data interaction in Cloud Storage. Inspired by the identity-based encryption mechanism, it makes use of fuzzy identity-based encryption mechanism where the

identities are extended to deal with the data information, and then extract the selection of identities to the problem of attribute relevance analysis in data mining for keeping the confidentiality of those identities.

Finally, focusing on the infrastructures used for data storage in the cloud, it considers the security of host system. Based on the requirement of establishing trust relationship between data user and cloud service provider, which is proposed due to the transparency of service provision, it conducts a comprehensive investigation about the works on combination of Trusted Computing and Cloud Computing. The conception of virtual machine migration with its corresponding virtual trusted platform module between trusted environments is proposed in order to protect the sect- ritzy of those infrastructures used for storage.

Multi-dimensional protection system

In the discussion of the mufti-dimensional system model, each dimension has its focused. The user-dimensional use the trust management technology as the focus, and had put forward the identity authentication and authorization system which based on trust management. The data-dimensional use the data encryption technology as the focus. And a cloud storage encryption solution is proposed and implemented. The service-dimensional use the security audit and monitoring as the focus, a service-oriented cloud security monitoring system is proposed. The basic-dimension focuses on network and host security. In addition, aiming at the problem of cloud security standardization, a cloud security standardized assessment system which based on cloud implementation is purposed.

Aiming at the security issues such as data leakage and data tampering in cloud storage technology, combined with the characteristics of HDFS data integrity verification mechanism, a kind of data security technical solution which bases on data transmission and data storage of HDFS is designed and implemented. The data uploaded to HDFS is encrypted by AES algorithm and stored in cipher, and the AES secret key is encrypted by RSA algorithm. This solution can effectively avoid the leakage of data transmission and storage. The tile stored in two kinds of form, cipher’—form or plaintext—form. The user can choose whether or not to encrypt the file. On the basis of the security analysis and experimental data of the performance test, tile security and viability of this solution is verified.

Conclusions

Aiming at the confidentiality, integrity and availability of the data, and combining with the characteristics of cloud computing architecture, this thesis propose one kind of multidimensional protection system which based on user-dimension, data-dimension, application-dimension and basic-dimension. According to this classification, the safety technologies and strategies were proposed specifically. Simultaneously, the subjects which use and manage "cloud" (cloud computing users and service providers) and the environment (network hardware environment and the social system environment) were accepted into cloud security system. The destination of this system is to gasp the problems of all aspects in the process of application and promotion of cloud computing as far as possible, so as to set up a thorough and comprehensive "trusted cloud" system.

References

[1] Armbrust M, Fox A, Griffith R, et al. Above the clouds: A berkeley view of cloud computing. Technical ReportNo.UCB/EECS-2009-28. Berkeley, USA: University of California at Berkeley, 2009.

[2] Information on http://blogs.forrester.com/stefanried/11-04-21-sizing the cloud.

[3] Decandia G, Hastorun D, Jampani M, et al. Dynamo: amazon's highly available key-value store. SOSP'07. Stevenson, Washington, USA: ACM, 2013: 205-220.

[4] M. Naor, G. N. Rothblum. The complexity of online memory checking. Journal of ACM, 2011, 56(1): 21-46.

[5] M. Li, S. Yu, K. Ren. Securing personal health records in cloud computing: patientcentric and fine-grained data access control in multi-owner settings. Proceedings of ICST Security and Privacy in Communication Networks, Singapore, 2010: 89-106.