Study on Access Control for Cloud Storage Security

Xinqiang Ma
Key Laboratory of Machine Vision and Intelligent Information System
Chongqing University of Arts and Sciences
Chongqing, P.R China
e-mail: xinqma@163.com

Yi Huang
Key Laboratory of Machine Vision and Intelligent Information System
Chongqing University of Arts and Sciences
Chongqing, P.R China
e-mail: cqhy@21cn.com

Mingsheng Zhang*
College of Information Engineering
Guizhou University for Nationalities
Guiyang, P.R China
*Corresponding author e-mail: gyzhangms@126.com

Youyuan Liu
Key Laboratory of Machine Vision and Intelligent Information System
Chongqing University of Arts and Sciences
Chongqing, P.R China
e-mail: 39541385@qq.com

***Abstract*—Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. At present, most of the researches on cloud storage security problems are focused on in cloud computing environment. This paper discusses storage security in cloud computing and access control of cloud storage circumstance. In order to solve the problem securely and dependably, we present some application cases such as access control based on LogicSQL database system and trusted computing. Extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure. The aim of the test was to perform sequential and random read/write accesses to the data, as well as more realistic access patterns, in order to evaluate efficiency, availability, robustness and performance of the various data-access solutions.**

Keywords—access control; cloud storage security; cloud computing; trusted computing; information security

I. INTRODUCTION

Cloud computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes [1]. It offers an innovative business model for organizations to adopt IT services without upfront investment. According to Gartner's Hype cycle, cloud computing has reached a maturity that leads it into a productive phase. This means that most of the main issues with cloud computing have been addressed to a degree that clouds have become interesting for full commercial exploitation. This however does not mean that all the problems listed above have actually been solved, only that the according risks can be tolerated to a certain degree. Cloud computing is therefore still as much a research topic, as it is a market offering [2]. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. [3].Cloud data storage is popularly used as the development of cloud technologies. We know that the network bandwidth capacity is the bottleneck in cloud and distributed systems, especially when the volume of communication is large. On the other side, cloud storage also lead to data security problems [3] as the requirements of data integrity checking. In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models. In Cloud Computing, the remotely stored electronic data might not only be accessed but also updated by the clients, e.g., through block modification, deletion, insertion, etc. To the best of our knowledge, distributed data storage and access security in wireless sensor networks (WSNs) as a fairly new area has received limited attention so far [4]. Many schemes were proposed under different systems and security models [4] [5]. Unfortunately, the state of the art in the context of remote data storage mainly focus on static data files and the importance of this dynamic data updates has received limited attention so far [6][7] and so on.

Security is about protecting information and information systems from unauthorized access and use. Nowadays, expressiveness and flexibility have become top requirements for an access control system [8]. On the one hand, in the 1970s, Bell, LaPadula, Denning and Biba developed lattice-based MLS models [9] [10] [11]. The core ideas are still valid, but systems built from these models turned out to be complex, expensive and impractical. On the other hand, role-based access control model (RBAC) [12] was accepted as an ANSI/INCITS standard in 2004[13].

In this paper, based on the storage security in cloud computing, we propose some access control models of cloud storage surroundings. First, some sample points of access control based on LogicSQL database system [14] and trusted computing to solve the problem securely and

*Corresponding author e-mail: gyzhangms@126.com

dependably[15].Then, an analysis of flexibility on RBAC model and flexible authorization architecture[16] are discussed. As a result, extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure.

II. CLOUD COMPUTING

Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques[17].The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization[17].

Cloud computing frameworks (see Figure 1) metaphor: For a user, the network elements representing the provider-rendered services are invisible, as if obscured by a cloud. Cloud computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users focus on their core business instead of being impeded by IT obstacles. It providers offer three main services models such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

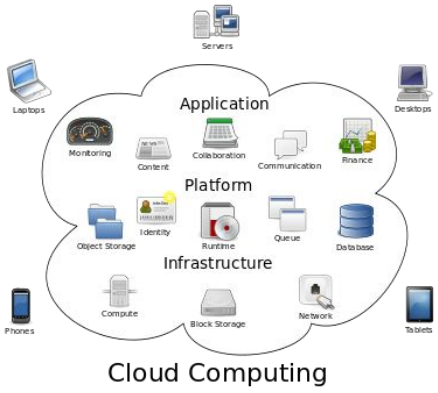

Fig. 1. Cloud computing frameworks

III. CLOUD STORAGE SECURITY

Cloud storage is based on highly virtualized infrastructure (see Figure 2) and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service (Amazon S3) or deployed on-premises (ViON Capacity Services). Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage.

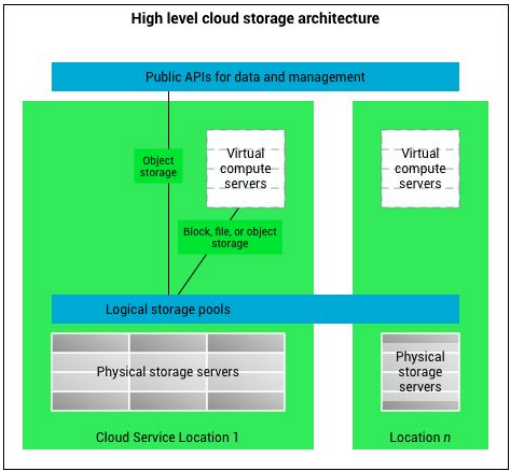

Fig. 2. High level cloud storage architecture

A. Advantages

- Companies need only pay for the storage they actually use, typically an average of consumption during a month. This does not mean that cloud storage is less expensive, only that it incurs operating expenses rather than capital expenses.
- Organizations can choose between off-premises and on-premises cloud storage options, or a mixture of the two options, depending on relevant decision criteria that is complementary to initial direct cost savings potential; for instance, continuity of operations (COOP), disaster recovery (DR), security (PII, HIPAA, SARBOX, IA/CND), and records retention laws, regulations, and policies.
- Storage availability and data protection is intrinsic to object storage architecture, so depending on the application, the additional technology, effort and cost to add availability and protection can be eliminated.
- Storage maintenance tasks, such as purchasing additional storage capacity, are offloaded to the responsibility of a service provider.
- Cloud storage provides users with immediate access to a broad range of resources and applications hosted in the infrastructure of another organization via a web service interface.
- Cloud storage can be used for copying virtual machine images from the cloud to on-premises locations or to import a virtual machine image from an on-premises location to the cloud image library. In addition, cloud storage can be used to move virtual machine images between user accounts or between data centers.

- Cloud storage can be used as natural disaster proof backup, as normally there are 2 or 3 different backup servers located in different places around the globe.
- Cloud Storage allows Word and Excel documents to be edited directly from your browser when your computer does not have them already installed or when you edit from your smartphone.
- Cloud storage can be used for hedge funds which need maximum security. Conifer cites in Hedgeweek.com that hedge funds are among the institutional investors with needs for reliable cloud storage.

B. *Security and Piracy*

- Security of stored data and data in transit may be a concern when storing sensitive data at a cloud storage provider.
- Users with specific records-keeping requirements, such as public agencies that must retain electronic records according to statute, may encounter complications with using cloud computing and storage. For instance, the U.S. Department of Defense designated the Defense Information Systems Agency (DISA) to maintain a list of records management products that meet all of the records retention, personally identifiable information (PII), and security (Information Assurance; IA) requirements.
- Cloud storage is a rich resource for both hackers and national security agencies.
- Piracy and copyright infringement may be enabled by sites that permit filesharing. For example, the CodexCloud ebook storage site has faced litigation from the owners of the intellectual property uploaded and shared there, as have the GrooveShark and YouTube sites it has been compared to.
- The legal aspect, from a regulatory compliance standpoint, is of concern when storing files domestically and especially internationally.

IV. ACCESS CONTROL MODEL AND ANALYSIS

To ensure cloud data storage security, it is critical to enable some methods or strategies to evaluate the service quality from an objective and independent perspective. Multilevel security (MLS) describes an information system which is trusted to contain information classified into different security levels and to maintain separation between the levels. In turn, these new features require new methods in order to secure the data held within. Access control is the process of mediating every request to data and services maintained by a system and determining whether the request should be granted or denied. Access control policies are security policies that govern access to resources. It can be applied to several new types of databases. LogicSQL is an object relational database management system implemented with the advanced (formula-lock based) concurrency control protocol, and the steged database architecture [18].

Traditional and classical access control policies/models, i.e., discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC), have been formulated to meet different application requirements in the cloud computing. An access control policy specifies access rights, which regulate whether requests made by principals should be permitted or denied [19]. In access control, we refine the notion of a principal to be one of a:

- User: a human
- Subject: a process executing on behalf of a user
- Object: a piece of data or a resource.

The enterprise cloud information search management tools based on LogicSQL security database is consistent with the security functions of database. The core functions of the system as follows: Archiving that replaces the traditional backup functions is completed in the system; Information on the enterprise server and personal computers are protected and managed; The latest search technology is used to realize the rapid and accurate searching for the backup information, including keyword, semantics, the integrated use of intelligent search technology; Search results are consistent with the security level of users. The cloud system architecture graph of the search system is shown as " Figure 3".

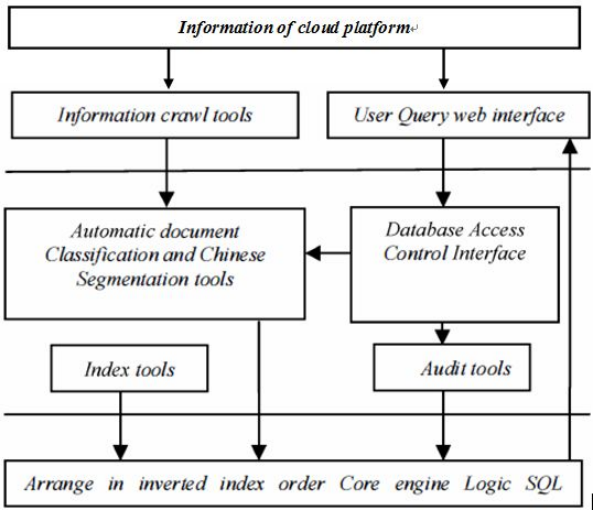

Fig. 3. Cloud system architecture based on LogicSQL

In the cloud search system, the following mandatory access control is adopted in the search process. Access control label is used in specific designer, and it is divided into two parts: security classification and group sets. Security level can be expressed as: L= (C, G), and C is security grade, and G is the group of set. Two security level: L_1= (C_1, G_1), L_2= (C_2, G_2) .If and only if $C_1 \geqslant C_2$ and G_1 include G_2, $L_1 \geqslant L_2$ is correct.

All operation of subject to object are abided by simple-security property and * -property principle:

1) When Ls ⩾Lo, subject S can read object O, and it is called down-read.

2) When Ls ⩽Lo, subject S can write object O, and it is called up-write.

Audit function is enhanced in the search system based on database. All operation related events are audited, and they increase the security of the cloud search system.

V. FLEXIBILITY ON RBAC MODEL

We should also notice that RBAC is a "flexible" model[16]. Although the administration of users and access privileges in large enterprises is a complex and challenging task, RABC has powerful functions for simplifying access control. RBAC models regulate the access of users to the information resources on the basis of the organizational activities and responsibility that users have in a system. In RBAC, permissions are assigned to roles, where roles can be defined as sets of actions and responsibilities associated with a particular working activity, and users are associated with appropriate roles to acquire the roles' permissions. Users can obtain authorizations through roles. This mechanism can greatly simplify management of permissions. Moreover, roles may be created for the various job functions in an organization, and users can be assigned roles in terms of their responsibilities and qualifications. Also, users can be easily reassigned from one role to another, and roles can be granted new permissions in a new application environment. These functions make RBAC very flexible.

In fact, RBAC can not only be a promising alternative to traditional discretionary and mandatory access controls, but also articulate different policies by means of precise configurations and interactions of various RBAC components. Since RBAC have those flexibilities above, there are many literatures extending and utilizing RBAC. For instance, Barker and Stuckey extended the standard RBAC, and enable security administrators to define a range of access polices with the features like denials of access and temporal authorizations. These features are often useful in practice, but are not widely supported in existing access control models. It is more important that representing access policies as constraint logic programs makes it possible to support constraint checks and administrator queries, and also enables access requests and constraint checks to be efficiently evaluated. Therefore, we think that RBAC should be an appropriate framework that supports flexible policies. In the same time, flexible authorization framework based on logic programs is applied to cloud computing environment.

VI. CONCLUSION

The paper is organized as follows. In the next section, we propose the cloud computing concept, and some cloud frameworks and service models are given. In Section 3, the high level cloud storage architecture is presented. Section 4 presents the access control based on LogicSQL database system in cloud computing. In Section 5, an analysis of flexibility on RBAC model is made to illustrate the efficiency of the cloud storage security.

ACKNOWLEDGMENT

The research work was supported by Natural Science Foundation of CQ CSTC under Grant No. cstc2014jcyjA40056 and cstc2013jcyjA40053, and Science and Technology Foundation of Guizhou Province under Grant No. J [2014]2092, and Scientific and Technological Research Program of Chongqing Municipal Education Commission under Grant No. KJ1401112, KJ1401117 and KJ111218, and Natural Science Foundation of Ycstc under Grant No. 2013nb8001, 2014bf2001 and 2013ad2002.

REFERENCES

[1] Borko Furht, Armando Escalante, Handbook of Cloud Computing, Springer, 2011.

[2] Smith, David Mitchell. Hype Cycle for Cloud Computing, Gartner. 2013.

[3] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, Enabling public auditability and data dynamics for storage security in cloud computing, IEEE Trans. Parallel Distrib. Syst. 2011,22 (5) pp.847-859.

[4] Qian Wang, Kui Ren, Wenjing Lou, Yanchao Zhang, Dependable and secure sensor data storage with dynamic integrity assurance, ACM Transactions on Sensor Networks, 2011,8(1), pp.9-24.

[5] Alina Oprea, Michael K. Reiter, Ke Yang, Space efficient block storage integrity, in: Proc. 12th Ann. Network and Distributed System Security Symp (NDSS 05),2005.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, Provable Data Possession at UntrustedStores, Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07) , 2007,pp.598-609,.

[7] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08) , 2008, pp.1-10.

[8] S.Vimercati, P.Samarati and S.Jajodia. Access control policies and languages. Int. J. Computational Science and Engineering, 2007,3(2).

[9] D.E. Bell. Secure computer systems: A refinement of the mathematical model. Technical Report ESD-TR-278, vol. 3, The Mitre Corp., Bedford, MA, 1973.

[10] D.E. Denning. A lattice model of secure information flow. Communications of the ACM,19(5), 1976,pp.236–243.

[11] K.J. Biba. Integrity considerations for secure computer systems. Technical Report TR-3153, The Mitre Corporation, Bedford, MA, 1977.

[12] R.Sandhu, E.Coyne, H.Feinstein, and C. Youman. Role- based access control models. IEEE Computer, 29(2), 1996,pp.38–47.

[13] R.Sandhu, D.Ferraiolo, and R.Kuhn. The NIST model for rolebased access control: Towards a unified standard. In Proceedings of 4th ACM Workshop on Role-Based Access Control, 2000,pp.47–61.

[14] Ma Xinqiang, Huang Yi, Bo Lv. Study on Access Control Based on Trusted Computing. Applied Mechanics and Materials ,441, 2014,pp .980-98.

[15] Yi. Huang,Xinqiang Ma. An access control model based on Trusted Computing, Journal of Chongqing University of Arts and Sciences, 29(3) 2010, pp.54-57.

[16] Mingsheng Zhang, Yuanpu Wang, Xinqiang Ma. Specifying Flexible Features in Authorization Using Logic Program. 2010 Second International workshop on Education Technology and Computer Science (ETCS 2010) ,IEEE Computer Society, 2010,pp.578-581.

[17] HAMDAQA, Mohammad. Cloud Computing Uncovered: A Research Landscape (PDF). Elsevier Press. 2012, pp. 41–85. ISBN 0-12-396535-7.

[18] Li Danning, Li Qi, Ma Xinqiang. Research of security mechanisms based on LogicSQL database. 2012nd International Conference on Mechanical Engineering and Green Manufacturing, MEGM 2012, pp352-356.

[19] P.Samartini,S.D.Capitani di Vimercati. Access Control:Policies, Models, and Mechanisms. In Foundations of Security Analysis and Design: Tutorial Lectures, Lecture Notes in Computer Science, 2001.(2171), pp. 137—193.