A NOVEL CLOUD STORAGE SYSTEM WITH SUPPORT OF SENSITIVE DATA APPLICATION

Alireza Souri[1], Arash Salehpour[2], Saeid Pashazadeh[3]

[1, 2]Department of Computer Engineering, East Azarbaijan Science and Research Branch, Islamic Azad University, Tabriz, Iran
[3]Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

ABSTRACT

Most users are willing to store their data in the cloud storage system and use many facilities of cloud. But their sensitive data applications faces with potential serious security threats. In this paper, security requirements of sensitive data application in the cloud are analyzed and improved structure for the typical cloud storage system architecture is proposed. The hardware USB-Key is used in the proposed architecture for purpose of enhancing security of user identity and interaction security between the users and the cloud storage system. Moreover, drawn from the idea of data active protection, a data security container is introduced in the system to enhance the security of the data transmission process; by encapsulating the encrypted data, increasing appropriate access control and data management functions. The static data blocks are replaced with a dynamic executable data security container. Then, an enhanced security architecture for software of cloud storage terminal is proposed for more adaptation with the user's specific requirements, and its functions and components can be customizable. Moreover, the proposed architecture have capability of detecting whether the execution environment is according with the pre-defined environment requirements.

KEYWORDS

Sensitive data application, Hardware USB-Key; Data security, Active protection; terminal software customizable.

1. INTRODUCTION

The cloud era is coming with increasing network bandwidth and reliable and flexible network connections that allow users to access software and data resources that are distributed in the remote data centers. The Cloud Service Provider (CSP) provides us with an almost unlimited infrastructures, software services and storage space. As customers, we do not need maintain the complicated infrastructure and software services, and we just use hardware resources, software resources and application services. Moreover, we can access and process the shared or exclusive data resources.

While the users get many benefits from the cloud storage, they are also worried about the security of their data, especially for security of sensitive data storage and process applications. Although the cryptographic technologies provides some security for sensitive data storages and process applications, however, there are still many security threats and challenges in the face of cloud storage security environment, which is very different with the traditional security environment for the terminal node data. Specifically, these security challenges [1, 2, 3] mainly, include:

1.1. Security threats arose from un-trusted cloud storage service provider

Existing cloud storage architecture and security mechanism cannot guarantee that the service provider cannot access and change user's data illegally.

1.2. Users lose control over data

In the existing cloud storage architecture, once the users outsource their data into the cloud, they lose control of the data. Consequently, anyone that who can access the data can spread and modify the data illegally.

1.3. Risk of data interception

Although there are related cryptographic communication mechanisms to guarantee the security of the data transmission process, while the encrypted data is decrypted for using, the plaintext may be intercepted by attackers.

1.4. The cloud terminals lack necessary requirements for ensure the data security during the data processing procedure

Although there are considerable traditional terminal security technologies, however, these technologies tend to focus on preventing malicious attacks to the entire terminal's system. As a result, they scarcely consider the security of the data usage process.
Our goal in this paper is to study a case for the cloud storage system that supports the sensitive data application. Our approaches mainly include ensuring the user identity and behavior is trustworthy by enhanced trusted mechanism guaranteeing the sensitive data transmission security by data security container and ensuring the security of data accessing process through security enhanced cloud storage terminal software.

The key contributions of this paper are:

- **Improved cloud storage system architecture:** compared to the typical cloud storage systems, the improved structure increases hardware USB-Key to enhance the security of user identity and interaction between the users and the cloud storage system.
- **Data security container for Transmission Process**: we improve the traditional process of transmitting the encrypted data by encapsulating the encrypted data, increasing appropriate access control and data management functions, by this way, we turn the static data blocks into a dynamic executable data security container.
- **Security Enhanced Cloud Storage Terminal Software**: we distinguish the cloud storage terminal software into several security levels according to the different security requirements of users, in other words, the terminal software functions and components are customizable.

The rest of this paper is organized as follows. Section 2 presents related works. Section 3 presents system requirements and architectural design. Section 4 presents the key technologies for the system and finally section 5 presents our conclusion.

2. RELATED WORKS

- **Cloud storage model**: wang et al [2] describes typical cloud storage architecture. And in the architecture, there are mainly three types of cloud storage entities: Users, who store their data in the cloud and operate the data depending on service provided by the cloud storage service provider, while the users include businesses, institutions and individuals; cloud storage service provider (CSP), who is responsible for building the cloud storage infrastructure, maintaining the running of services and ensuring the availability, integrity and security of the data stored on its data centers; third-party auditor (TFA), which is an optional entity, and the TPA can assess security threats of the cloud storage services. Kamara et al [4] presents a user data storage and sharing model on the public cloud infrastructure, in the model, the data requester and the data owner communicate with the token in the cryptographic manner.

- **Cloud storage data integrity:** juels et al [5] describes a proof of retrieve ability (POR) model to ensure the integrity of remote data. This model incorporates spot-checking error correction codes to ensure the property and recoverability of the files in the service system.

  Shacham et al [6] enhance the POR model, based on the POR model. They construct a random linear function on account of the homomorphism authentication code to provide unlimited queries and lower communication overhead. Bowers et al [7] summarizes the work of Juels and shacham and presents an improved framework for POR protocol, moreover, Bowers et al also extends the POR model into the distributed systems [8].
  These technologies are all needed to be preprocessed before distributed deployment, and once any changes has been made to the file, the system must broadcast the changes by the error correction code, which brings significant computation and communication complexity for the system. Schwarz et al [9] uses erasure-coding and block-level file integrity detecting methods to ensure the integrity of files across multiple distributed servers, while this method only consider the integrity of static file.

  Lillibridge et al [10] proposes a backup mechanism for the P2P system, and the mechanism partition the files into several blocks and store them in m+k nodes through (m+k, m) erasure-coding; meanwhile, each node randomly request data blocks toward its backup nodes set, the integrity of data block is ensured by the separate keyed cryptographic hashes attached on the data block, however the mechanism does not guarantee that none of the data has not been tampered.

  Filho et al [11] proposes a data integrity checking method using the RSA hash function for ens1rtirrg data property in the P2P file-sharing networks, and this method needs doing exponentiation operation on the entire data file, consequently, it is hard to put the method into practice when the file is large enough.

- **Data property assurance in cloud storage:** Ateniese et al [12] builds a Provable Data Property model (PDP) to ensure the rights of data owners in incredible environment, while the model audits the data files by the public-key mechanism based on the homomorphous tags. In a subsequent study, Ateniese et al [13] improve the PDP model using the symmetric-key mechanism to reduce computational overhead and support dynamic operations on data files. In a distributed storage system, Curtmola et al [14] extends the PDP mechanism for data property with multiple data duplicates, and this method does not require a separate coding for each copy.

3. REQUIREMENT ANALYSES AND ARCHITECTURE DESIGN

3.1. The Specific Requirements for sensitive Data Applications

There are some specific requirements for the sensitive data applications in the cloud storage system as follows:

3.1.1. The user identity is not trusted

Although this is common issue in the cloud storage system, however, for sensitive data applications, it brings even more serious security threat. Therefore, it is necessary to design a more reliable mechanism to ensure the user identity is credible.

3.1.2. The security of data transmission process

Sensitive data applications require more reliable measures to ensure data transmission security.

3.1.3. The security of data usage process

Most of the traditional methods are mainly used to ensure security while the data is encrypted, however, once the data is been decrypted and used, it will face even more serious security threat. Meanwhile, the traditional cloud storage terminal software often lacks consideration on the user's individual needs and appropriate detecting their execution environment.

3.2. Basic ideas

The main idea of the proposed architecture is:

3.2.1. A trusted hardware module

Such module is introduced to the system; by introducing a hardware trusted. Module, the system can enhance the interaction security between users and the cloud storage system. The main functions of trusted hardware module include: enhancing the security of user identity; enhancing the interaction security between users and the cloud storage system.

3.2.2. A data security container

It is introduced to the system; drawing on the idea of data active protection, we improve the traditional process of transmitting the encrypted data by encapsulating the encrypted data, increasing appropriate access control and data management functions by this way, we turn the static data blocks into a dynamic executable data security container.

3.2.3. Security enhanced cloud storage terminal software

In this paper, we design security enhanced cloud storage terminal software architecture. The software can be customized according to the user's requirements, and its functions and components can be changeable. Moreover, the architecture can check the execution environment; compared to the pre-defined environment requirements, ' it can determine the legitimacy of the current running environment to meet the specific security requirements for sensitive data applications.

3.3. Architecture Design

We improve the typical cloud storage architecture [2] to support the sensitive data applications. The improved cloud storage architecture supporting sensitive data applications is shown in Figure 1.

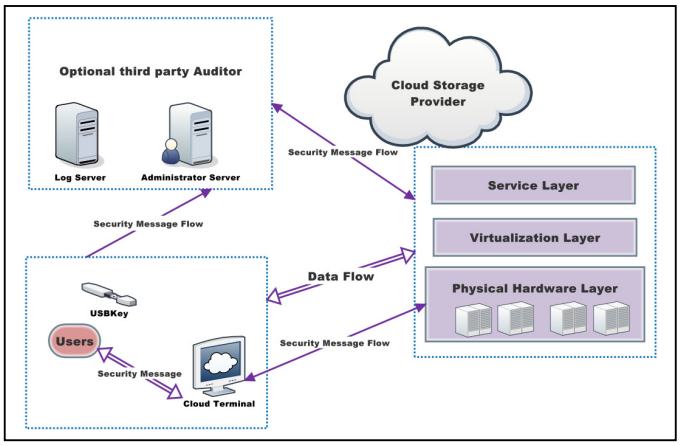

Figure 1. Improved cloud storage architecture supporting sensitive data application

In this architecture, the user interacts with the cloud storage terminal through security .enhanced software USB-Key. Furthermore, the hardware USB-Key also enhances the interaction security between cloud storage terminal and the Cloud Storage Provider.

4. KEY TECHNOLOGIES

4.1. Data Security Container for Transmission process

Through analyzing the data security threats in the sharing and transmission process, we have found some principles to guarantee the security of data transmission:

- The visitors of the data (data owners, or the users) must be legally authorized;
- The communication between the data transmitter and the data receiver is secure.

In this paper, we get some inspiration from the delivery procedure of the postman delivered the letters, while we design a trusted data transmission process. Firstly, considering a simple scenario of postman delivers the letters between the post office and the users, the basic process is shown in Figure 2.

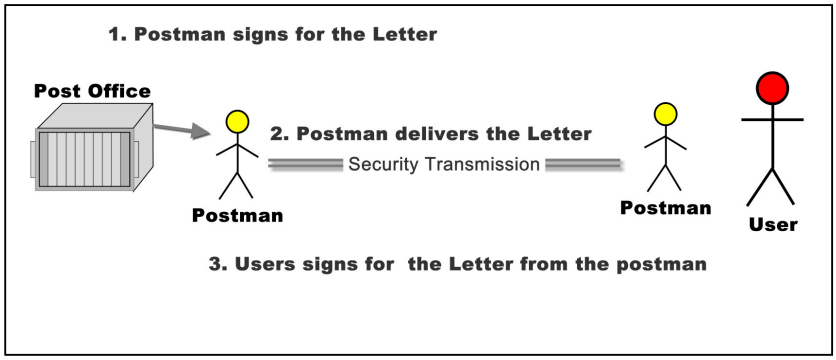

Figure 2. A simple scenario of postman delivers the letters

Drawing an inspiration from this scenario, we analogize the elements of the data transmission process and the elements of the delivery process as follows:

The data is corresponding to the letters, the post office is corresponding to the data center and the users are corresponding to the data requesters. Thus, we design a data security container to guarantee the data security during the data transmission procedure.

The security container is similar to postman. The data security container structure and interfaces are shown in Figure 3.

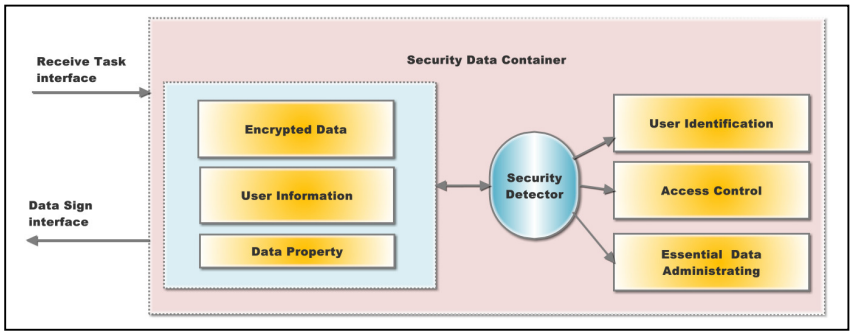

Figure 3. Architecture of the security data container

The encrypted data, essential user information and data accessing authorities are encapsulated in the data security container.

Meanwhile, a security detector is designed to identify the user's identification, access control for the data and manage the data yet the user information.

4.2. Security Enhanced cloud storage Terminal software

In this paper, we distinguish the cloud storage terminal software into several security levels according to the different security requirements of users, in other words, the terminal software functions and components are customizable.

According to the user types and the different execution environment, the cloud storage terminal software can distinguish that whether the user's identification is legal and whether the execution environment is accord with the predefined requirements. Specifically, there are two kinds of users who can use the terminal software:

- Anyone can use this terminal software;
- Only specific users or group of users with common features can use the terminal software.

Similarly, in order to adapt the specific requirements for sensitive data application, it is also need to distinguish the software execution environment as follows:

- The terminal software can run on any computer terminal;
- The terminal software can only run on a specific computer terminal;

The components and cooperating progress between the users and the terminal software are shown in Figure 4. The user holds his proprietary hardware USB-Key, and only a legitimate user to holding his legal USB-Key can use the cloud storage terminal software. The communication process between users and terminal software is shown as follows:

- Identification authentication between users and the terminal software;
- Customizing the terminal software depending on the identity of the user and configure the corresponding components.
- The terminal software detects its execution environment to determine whether the current environment is accord with the Pre-configured requirements;
- Security communication between users and the terminal software;
- Data requesting and data Processing operations between users and the terminal software.

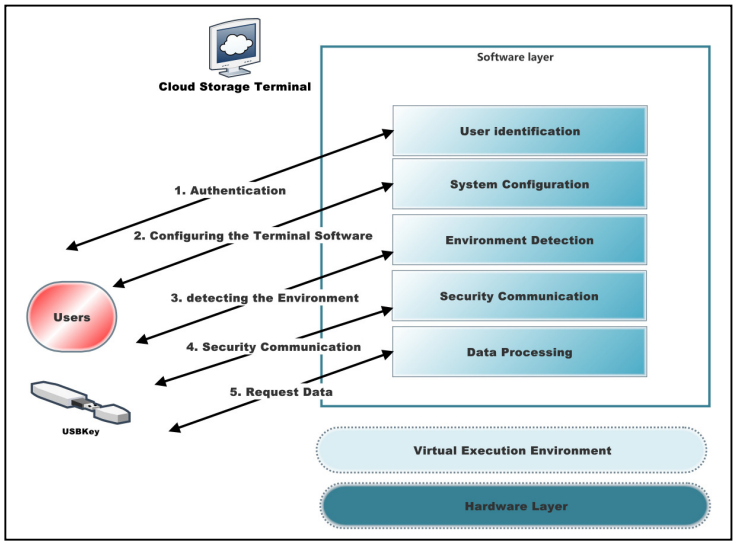

Figure. 4 The components of cloud Storage Terminal Software

5. CONCLUSIONS

In this paper, improved architecture for the typical cloud storage architecture to support sensitive data application is proposed. We have argued that multiple security enhanced metrics must be introduced to the system to accommodate the specific security requirements and user's personal demands. Therefore, related trust enhancement technologies are designed to meet the system requirements. Clearly, much work remains to be done to realize the entire system. We believe that, sensitive data application is important fields in the future cloud storage systems. Meanwhile, the users are willing to regard their personal privacy information as sensitive data.

REFERENCES

[1] J. Heiser, M. Nicolett, "Assessing the Security Risks of Cloud Computing," Gartner Inc, 2008.

[2] C. Wang, Q. Wang, K. Ren, et al., "Ensuring Data Storage Security in Cloud Computing," Charleston, SC, United states, 2009.

[3] R. Geambasu S. D. Gribble, H. M. Levy, "Cloud Views: Communal Data Sharing in Public Clouds," in HotCloud'09 Workshop on Hot Topics in Cloud Computing, 2009.

[4] S. Kamara, k. Lauter, "Cryptographic Cloud Storage," in Proceedings of Financial Cryptographic: Workshop on Real-Life Cryptographic Protocols and Standardization 2010, pp. 1-14.

[5] Juels, B. S. Kaliski Jr, "Pors: Proofs of Retrievability for Large Files," Alexandria, VA, United states, pp. 584-597, 2007.

[6] H. Shacham, B. Waters, "Compact Proofs of Petrievability," in Advances in Cryptology - Asiacrypt 2008. vol. 5350, 2008, pp. 90-107.

[7] K. D. Bowers, A. Juels, A. Oprea, "Proofs of Retrievabilify: Theory and Implementation," 2008.

[8] K. D. Bowers, A. Juels, A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Chicago, IL, United states, pp. 187-198, 2009.

[9] S. J. Thomas Schwarz, E.L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Lisboa, Portugal, 2006.

[10] M. Lillibridge, S, Elnikety, A.Birrell, et al., "A Cooperative Internet Backup Scheme," in Usenix Association Proceedings of the General Track, ed, 2003, PP. 29-41.

[11] D. L. G. Filho, P. S. L. M. Barreto, "Demonstrating Data Possession and Un-Cheatable Data Transfer," 2006.

[12] G. Ateniese, R. Bums, R. curtmola, et al., "Provable Data Possession at Untrusted Stores," in Ccs'07: Proceedings of the 14th ACM Conference on Computer and Communications Security, 2007, pp. 598-609.

[13] G. Ateniese, R. D. Pietro, L. V Maacini, et Bl., "Scalable and Efficient Provable Data Possession," Istanbul; Turkey, 2008.

[14] R. Curtmola, O. Khan, R. Burns, et al., "MR-PDP: Multiple-Replica Provable Data Possession," Beijing, China, pp. 411-420, 2008.

Authors

Alireza Souri received his B.Sc. in Computer Engineering University College of Nabi Akram, Ira n in 2011. Currently, he is receiving M.Sc. in Software Engineering from East Azarbaijan Science and Research Branch, Islamic Azad University in Iran. His main interest is in the formal verification, modeling and analyzing Network systems, Multilayer systems, Antivirus systems, Grid computing, and Real-time systems. He is member of The Society of Digital Information and Wireless Communications.

Arash Salehpour, He is M.Sc. (computer engineering -software - He has worked as Progra m Committees, reviewer at numerous international conferences such as : The International Conference on Informatics Engineering & Information Science (ICIEIS2011), University Technology Malaysia, Malaysia, The World Congress on E-Commerce and Business on the Web (WCEBW2012), United Kingdom and …,The areas of his Research and Interests include: Examines both automatic systems and collaborative systems as well as computational models of human software Engineering activities, Presents knowledge representations and artificial intelligence techniques as well as, he is already acts as member in numerous international organizations such as: The Society of Digital Information and Wireless Communications (SDIWC).

Saeid Pashazadeh is Assistant Professor of Software Engineering and chair of Info rmation Technology Department at Faculty of Electrical and Computer Engineering in University of Tabriz in Iran. He received his B.Sc. in Computer Engineering from Sharif Technical University of Iran in 1995. He obtained M.Sc. and Ph.D. in Computer Engineering from Iran University of Science and Technology in 1998 and 2010 respectively. He was Lecturer in Faculty of Electrical Engineering in Sahand University of Technology in Iran from 1999 until 2004. His main interests are modelling and formal verification of distributed systems, computer security, and wireless sensor/actor networks. He is member of IEEE and senior member of IACSIT and member of editorial board of journal of electrical engineering at University of Tabriz in Iran.