International Journal of Security and Its Applications
Vol. 9, No. 5 (2015), pp. 77-84
http://dx.doi.org/10.14257/ijsia.2015.9.5.08

A Proxy-Based Data Security Solution in Mobile Cloud

Xiaojun Yu[1,2] and Qiaoyan Wen[1]

[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876 China,*
[2]*Beijing TOPSEC Network Security Technology CO., LTD. Beijing, 100085 China*
yuxiaojun@bupt.edu.cn, wqy@bupt.edu.cn

Abstract

This paper proposes a data security solution in mobile cloud, which solves the security issues in the mobile client and cloud. The proposed solution also relieves the performance limitation of mobile client when executing security technologies. The analysis about the security, feasibility, compatibility and expansibility and the experiment suggests the proposed solution is rational.

Keywords: *Mobile Cloud, Data Security, Proxy*

1. Introduction

With the development of cloud computing and smart mobile device, people begin to store data in cloud and get data by mobile device. This usage model is known as mobile cloud computing. There are many data security risks [1] in cloud. For this problem, many security technologies are proposed, such as the searchable encryption [2, 3], data deletion proving [4, 5], provable data possession [6, 7] and trusted computing [8]. However, there is the performance limitation issue of mobile client when performing above technologies, affecting on user experience. The proxy based data security solutions solved the above performance limitation [9, 10], because most of workloads in running these technologies will be migrate to the proxy, but the expansibility of these solutions and security in mobile client are not solved.

This paper proposes a proxy based data security solution. The proxy is in a virtual machine which controlled by the mobile user and deployed in the cloud computing service. We provide the detail design and analysis of the solution.

2. Assumption

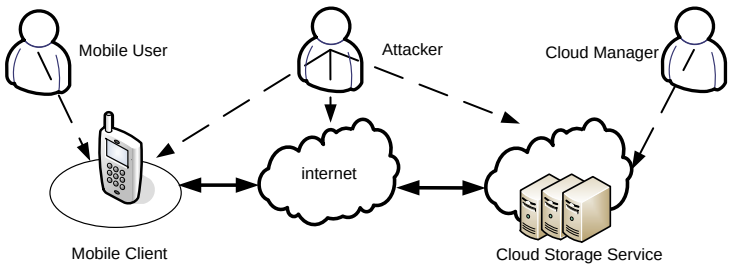


Figure 1. Security Assumption

We assume that the security risks including:

Mobile Client risk: the mobile users may install malware; result in the data leakage or tampering. The data may lost if the account stolen by the attacker.

ISSN: 1738-9984 IJSIA

Internet Risk: the attacker may monitor or tampering user's data in data transmission.

Cloud Storage Service risk: the cloud manager who has privilege may control and leak mobile user's data without permit.

3. Solution Design

3.1 Basic Ideas

The basic ideas of the solution are as following:

- **Data Confidence:** in the cloud, the data is encrypted with a searchable encryption mechanism which support ciphertext search but the encryption and decryption and the key management is under the control right of data owner. A store and the search enabled. Data is protected in transmission with a VPN technology(like SSL VPN)
- **Data Integrity:** The data integrity check will be conducted regularly after being uploaded to the cloud. Considering the limited computing performance of client, the provable data possession scheme used, because the PDP scheme doesn't need to download the original data from the cloud.
- **Performance of Client:** a security proxy entity is designed. The security proxy is a virtual machine deployed in cloud computing service. The proxy is response for performing work that belongs to the mobile client, including the data encryption, data decryption, data integrity verification and so on.
- **Security of Client:** the client is enhanced by using the trusted computing technology, which can resist on executing the malware on mobile client. The trusted computing technology supports remote attestation of mobile client platform, which can be used by the security proxy for platform identity authentication.

3.2 System Deployment Model

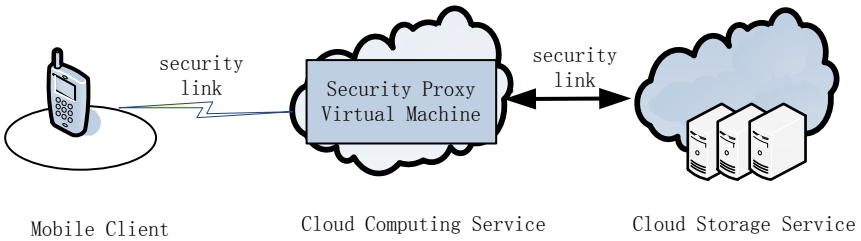


Figure 2. System Deployment Model

Figure 2 shows the system deployment; the mobile client link to the cloud storage service through the security proxy. The security proxy is a virtual machine on cloud computing service, which is different from the cloud storage service. The security proxy is managed by mobile user. With this deployment mode, the security proxy can migrate flexibly from one cloud to another. At the same time, the security proxy configuration can be adjusted according to user's needs. This architecture can improve the adaptability for different cloud storage service and different mobile client.

3.3 Components Architecture

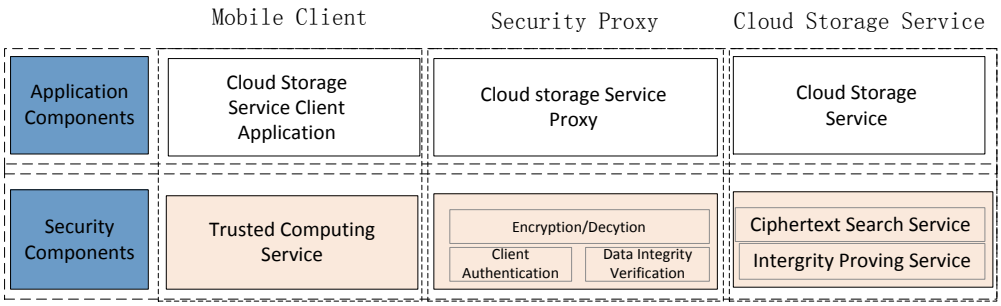


Figure 3. Component Architecture

Figure 3 show the solution component consists of application components and security components, these components are distributed in the mobile client, security proxy and cloud storage service.

- **The Mobile Client Components**
  - Application component: refers to client software of cloud storage service, the functions are data upload, data download, data deletion, data query and so on.
  - The security component: refers to the trusted computing service, this component provide client platform authentication information. And platform to integrity check of client software of cloud storage service
- **The Security Proxy Component**
  - Application component: refers to the proxy service for cloud storage service, the functions are user data upload, data download, data deletion, data query preprocessing, data format conversion, plaintext query conversion and so on.
  - Security components: including: (1) encryption and decryption. Data encryption when user uploads data to cloud and data decryption when user downloads ciphertext from cloud (2) identity authentication. Verifies the validity of the mobile client identity and the integrity of the mobile client platform. (3) Data integrity verification.
- **The Cloud Storage Service Component**
  - Application components: refers to the cloud storage service components, which realize basic functions such as data upload, data download, data deletion, data query and so on.
  - Security components: including data integrity proving and ciphertext search. The data integrity proving is a tool used to prove that the data is integrity in cloud to the user .The ciphertext search component is used to ensure the confidentiality of data and provider query function of the encrypted data.

3.4 System Flow

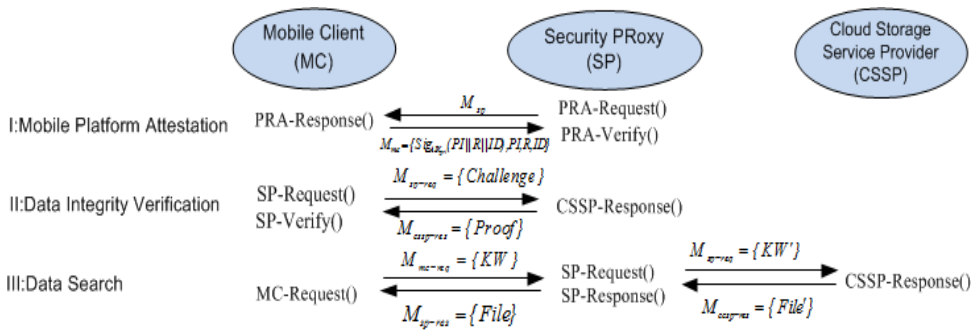


Figure 4. System Flow

I: Mobile Platform Attestation:

(1) PRA-Request(): The SP sends authentication request M_{sp} to the MC.

(2) PRA-Response(): The MC measures the state information of mobile platform PI, then signs $Sig_{AIK_{pri}}()$ the platform information with the private key of client platform AIK_{pri}, at last, the signature information , a random number R, user identity information ID all together $M_{mc} = \{Sig_{AIK_{pri}}(PI \| R \| ID), PI, R, ID\}$ return to the SP.

(3) PRA-Verify (): The SP verifies the validity of signature and the integrity of mobile platform. If passed, the MC is permit to perform further operation, otherwise, the link between the MC and the SP is closed.

II: Data Integrity Verification:

(1) SP-Request(): The SP send challenge $M_{Sp-req} = \{Challenge\}$ to the CSSP. The M_{Sp-req} includes a random factor for verification data block choice.

(2) CSSP-Response(): The CSSP send back the data integrity proof $M_{cssp-res} = \{Proof\}$ to the SP.

(3) SP-Verify(): The SP verifies the valid of integrity proof $M_{cssp-res}$. if passed, that meaning the user data is integrity, otherwise the user data may be tampered .

III: Data Search:

(1) MC-Request():The MC sends a data search request $M_{mc-req} = \{KW\}$ to the SP, KW stands for the query keywords.

(2) SP-Request():The SP forwarding requests $M_{sp-req} = \{KW'\}$ to the CSSP, KW' stands for the encrypted version of keyword..

(3) CSSP-Response(): the CSSP performance ciphertext search according to the encrypted keywords KW', then returns the query results $M_{ccsp-res} = \{File'\}$, $File'$ means the encrypted data file.

(4) SP-Response(): the SP return the search results $M_{sp-res} = \{File\}$ to the MC after decrypting the ciphertext, $File$ means the decrypted files.

4. Solution Analysis

The solution can be analyzed from the security, feasibility, compatibility and expansibility as flowing:

- **Security**
  - in the mobile client, the security service based on trusted computing can verify the integrity of cloud storage service client software and reject the tampered one to execution. The security service can also ensure the legitimacy of mobile platform, preventing the illegal user from connecting to the security proxy.
  - in the cloud storage service , the data is encrypted, thus it is invisible to illegal users or cloud manager. If the ciphertext is leaked out, it is also difficult to crack or decrypted without the encryption key. At the same time, the provable data possession technique can examine whether the data be tampered or damaged.
  - In the security proxy, the virtual machine is managed by the mobile user and the virtual machine image is encrypted.
  - the communication links among the mobile client, security proxy, cloud storage service are protected by using the VPN technology, such as SSL..

- **Feasibility**
  - In the mobile client, the trusted computing technology has been widely deployed in mobile devices. At the same time, the mobile cloud storage service client application is in user mode, thus the maintain and update work are relatively easy
  - In cloud storage service, the security services are implemented using the web service standard, which is a mature technology and the ciphertext search technology and the data integrity verification technology are relatively mature scheme.
  - the security proxy is deployed in the virtual machine, which is relatively mature application in cloud service market..
- **Compatibility**
  - the mobile client components are running in user space of operation system ,thus it is easy to migrate the components to different mobile platforms.
  - the cloud storage security service components are implemented in standard web service and the modification to the cloud storage system was slight. thus, these services are convenient for migration to the other cloud storage service providers
  - the proxy is easy to migrate to other cloud platform as virtual machine image format is easy to convert into other virtual machine format of different virtualization platform.
- **Expansibility**
  - in the mobile client, in addition to the remote platform authentication function ,other security functions can also explored based on the trusted computing services, such as mobile user's key storage, access control and so on
  - in the cloud storage service, cloud storage security service uses the standard web service to realize, therefore, it is ease to add the new security services, such as data deletion proving.
  - the security proxy is hosted on a virtual machine cloud service, which is elastic extension and can configuration dynamic adjustment..

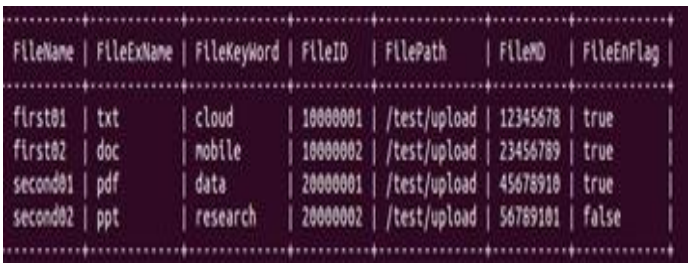
5. Emulation

The emulation environment: PC with configuration: CPU 3.2GHz , 4 cores, 4Gbit memory, Three virtual machines with the same configuration: CPU 3.2GHz, 4 cores,1Gbit memory, which are used for the simulation of mobile client, security proxy and the cloud storage server. The experiment are implemented with the open source software, including ftp4, Trouser [11], TPM_emulator [12] cryptDB [13], MySQL. See Table 1.

Table 1. Technology Detail

Component	Technology detail
Mobile client component	(1) cloud storage service client applications is implemented based on the open-source ftp4 project transformation(2) the trusted computing service is built based on the open source Trouser software. (3) cloud storage service client and trusted computing services are run in user space.
Security proxy components	(1) cloud storage service is build based on ftp4 open source software and cryptDB. The ftp4 software was used to realize the plaintext storage proxy. the front end of cryptDB implements the encrypted storage proxy. (2) the SSL is used to protecting the links among the mobile client, security proxy virtual machine and cloud storage service
Cloud storage service component	(1) The cloud storage service is emulated with MySQL(2) The data integrity service is build based on the idea of provable data possession from paper [6]. (3) the ciphertext search is implemented with the cryptDB..

Figure 5. Data in Cloud Storage Service



FileName	FileExName	FileKeyWord	FileID	FilePath	FileMD	FileEnFlag
first01	txt	cloud	10000001	/test/upload	12345678	true
first02	doc	mobile	10000002	/test/upload	23456789	true
second01	pdf	data	20000001	/test/upload	45678910	true
second02	ppt	research	20000002	/test/upload	56789101	false

Figure 6. Output of Security Proxy

Figure 5 shows the output when select data directly from the cloud storage service, Figure 6 shows the output of security proxy. With the solution, the administrator or cloud service provider is preventing from seeing the user's data without the decryption key.

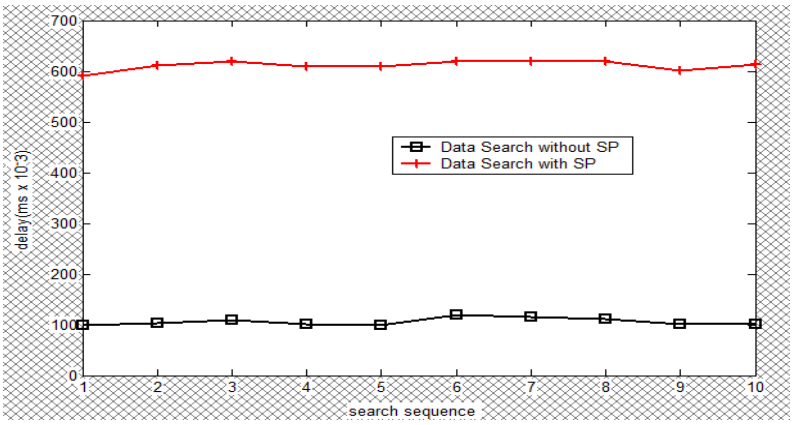


Figure 7. Data Search Delay with SP and without SP

Figure 7 shows the delay of the data search with or without security proxy. The delay of data search with security proxy is longer than the one without security proxy. We argue that the delay variation is stable and not related to the client platform. Thus our solution can hold the user experiment by improving the SP only.

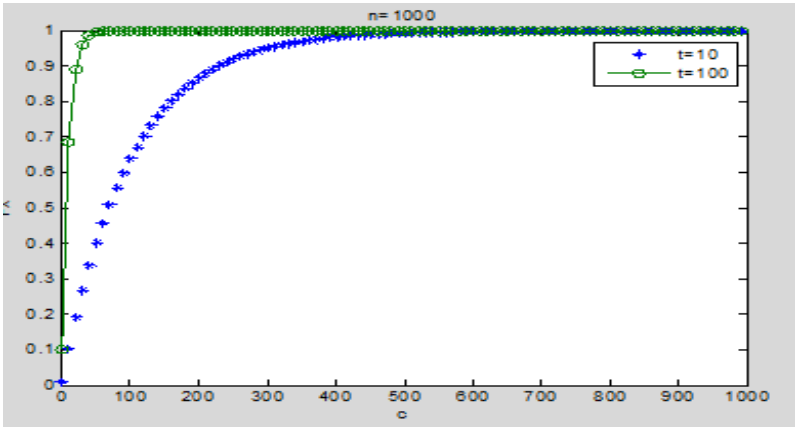


Figure 8. Broken Data Detection Probability

If the data volume is huge, it is hard to directly verify the integrity of all data. Thus, our solution use the integrity detection mechanism based on probability. Figure 8 indicates the relation between the probability of broken data detection P_x and the number of challenged data blocks c .Let X the variable of the tampered data block number. n Represents the total number of data blocks, t stand for the tampered data block number, then:

$$P_x = P\{X \geq 1\} = 1 - P\{X = 0\} = 1 - \frac{n-t}{n} \times \frac{n-1-t}{n-1} \times \ldots \times \frac{n-c+1-t}{n-c+1},$$

because $\frac{n-i-t}{n-i} \geq \frac{n-i-1-t}{n-i-1}, 0 \leq i \leq c-1,$

thus, $1 - \left(\frac{n-t}{n}\right)^c \leq P_x \leq 1 - \left(\frac{n-c+1-t}{n-c-1}\right)^c$; as example, when the condition is n =1000, t =10, c =458 or n =1000, t =100, c =43, then P_x will be 99%。

6. Conclusion

The most existing technologies or solutions focus on data security or performance issues in cloud side that may not suite for the mobile client. We proposed the data security solution based on proxy architecture. The solution solves the data security issue and the performance limit in mobile client. The analysis from security, feasibility, compatibility and expansibility suggests the rational of our solution.

The future work includes: (1) the security proxy architecture optimization. One work is to improve the availability of security proxy which is also importance aspect. This work may be completed by using the host-slave architecture or virtual machine cluster (2). The cloud security service optimization. The searchable encryption scheme used in this paper causes some modification to the cloud storage service. Thus, the next work is to reduce this change.

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (Grant Nos. 61300181, 61272057, 61202434, 61170270, 61100203, 61121061), the Fundamental Research Funds for the Central Universities (Grant No. 2012RC0612, 2011YB01).

References

[1] "Top Threats Working Group", The Notorious Nine Cloud Computing Top Threats in, **(2013)** https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.
[2] J. Li, Q. Wang and C. Wang, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing", In Proceedings of INFOCOM, **(2010)** March 14-19, pp. 1-5.
[3] H.-A. Park, J. H. Park and D. H. Lee, "PKIS: practical keyword index search on cloud datacenter", EURASIP Journal on Wireless Communications and Networking, vol. 64, **(2011)**, pp. 1-16.
[4] M. Paul and A. Saxena, "Proof Of Erasability For Ensuring Comprehensive Data Deletion In Cloud Computing", Recent Trends in Network Security and Applications Communications in Computer and Information Science, Springer, vol.89, **(2010)**, pp. 340-348.
[5] M. Paul and A. Saxena, "Zero Data Reminance Proof in Cloud Storage", International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 4, **(2010)** October, pp. 256-265.
[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Pe-terson and D. Song, "Provable data possession at untrusted stores", In Proceedings of the 14th ACM conference on Computer and communications security, New York, USA, **(2007)**, pp. 598–609.
[7] P. S. Kumar and R. Subramanian, "RSA-based dynamic public audit service for integrity verification of data storage in cloud computing using Sobol sequence", International Journal of Cloud Computing, vol. 1, no. 2/3, **(2012)**, pp. 167-200.
[8] "TCG Mobile Trusted Module Specification Specification", version 1.0 Revision 6, vol. 26, **(2008)** June.
[9] R. Seiger, S. Groß and A. Schill, "SecCSIE: A Secure Cloud Storage Integrator for Enterprises", In Proc. 2011 IEEE 13th Conference on Commerce and Enterprise Computing, **(2011)**, pp. 252-255.
[10] A. M. Talib, R. Atan, R. Abdullah, M. A. A. Murad, "Towards a Comprehensive Security Framework of Cloud Data Storage Based on Multi-Agent System Architecture", Journal of Information Security, vol. 3, **(2012)**, pp. 295-306.
[11] "TrouSerS", The open-source TCG Software Stack, http://trousers.sourceforge.net/.
[12] "TPM_emulator", http://sourceforge.net/projects/tpm-emulator/.
[13] "CryptDB", http://css.csail.mit.edu/cryptdb/.

Authors

Xiaojun Yu, He is a Ph. D candidate of Beijing University of Posts and communications. His interesting research fields including cryptography, cloud computing security.

Qiaoyan Wen, She is a Professor of Beijing University of Posts and communications, her interesting research fields including modern cryptography, quantum cryptography and network security.

