International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.303-310
http://dx.doi.org/10.14257/ijsia.2014.8.5.27

A Study of Key management Protocol for Secure Communication in Personal Cloud Environment

ByungWook Jin[1] and Keun-Wang Lee[2,*]

[1]*Dept. of Computer Science, Soongsil University*
Seoul, South Korea
[2] *Dept. of Multimedia Science, Chungwoon University*
113, Sukgol-ro, Nam-gu, Incheon, South Korea
[1]*Quddnr4511@naver.com,* [2]*kwlee@chungwoon.ac.kr*

Abstract

Personal cloud computing is user-oriented service to satisfy user service demand in existing cloud circumstance and personalized service is available whenever, wherever. However due to personal cloud market is growing rapidly, accidents such as unauthorized user access, leak of secret information, service invasion are occur and existing wire or wireless network communication had been threaten on security. Also the studies about user certification and data management are required. So this paper suggested key generating protocol for user certification and user authority. In addition, it designed safe contents transfer protocol for user by using generated key value. It analyzed the security with referring security service requirement of existing personal cloud service.

Keywords: *Personal Cloud Service, Key Management, Privacy Information*

1. Introduction

Personal cloud is user-oriented service for satisfy desire of existing cloud computing user. It providing user information based personalized contents to service provider and user terminal independently. It takes advantages of providing personalized services with saving/combining/managing/processing personal contents on cloud circumstance by using individual user's variable devices such as smart phone, PC, netbook, IPTV [1, 3].

With prospect, personal cloud service will started to be a target for market entering for major IT enterprises on 2013, and 50% of global enterprises will adopt hybrid computing system until 2017. Nationally, the personal cloud development by national institutes had started since 2010, and the standardization studies about cloud service and security skill are being conducted [2].

However the security vulnerability is being arise meanwhile cloud market grows rapidly, the risks levels of over-national cyber war such as hacking between virtual machine, unauthorized access, leak of personal information, privacy invasion, service invasion are predicted to affect private enterprise and national equipment. Personal cloud service has low compatibility because it depended on each cloud service provider, and the security policy about service and personal information of it is vague, and the security requirement for providing personalizing service is insufficient. In addition, the studies about personal saving

* Corresponding author

ISSN: 1738-9976 IJSIA

data managing skill are required due to the expanding of privacy invasion about stored data [4].

So this paper suggests key generating and authorizing protocol after certificate user with adding Key Server. And it also suggests the safe contents transferring method by using generated key value.

2. Related Work

2.1 Personal Clouding Service Architecture

This paragraph indicates each object's feature and role and what is the process of it with checking the basic structure of suggested personal cloud. It divided to user, client, 3rd service provider, combination service provider, service composer. The structure of personal cloud service is just like below Figure [1, 3-4, 6].

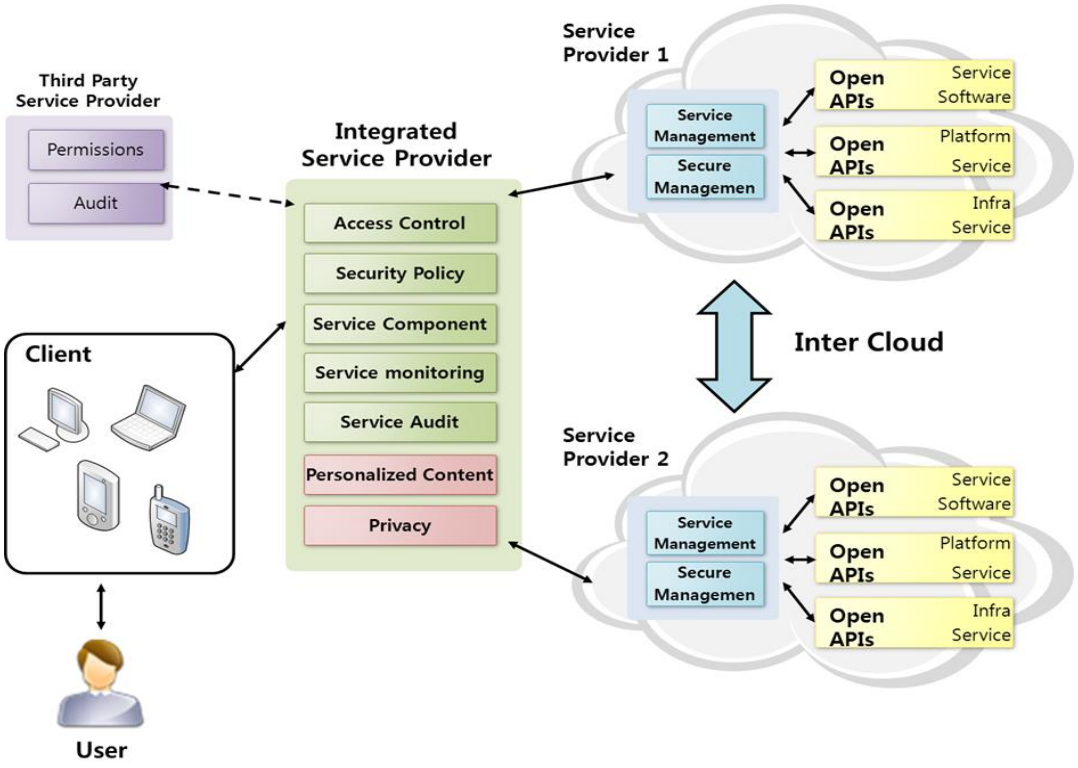

Figure 1. Personal Cloud Service Communication Architecture

- User

User provided service with cloud device through inputting user information.

- Client

Client provided personal cloud service through user identification after input ID and PW on client display.

- 3rd party service provider

The 3rd party service provider provides user identification service such as user identifying and authority permission. The examples of them are public institutions or authorized identification institution [8].

- Combination service provider

Combination service provider provided services after requiring each personalized contents with concerning user information. Afterward, combination service provider provides service with composing to make usable for user.

- Service provider

Service provider obtaining personalized contents and variable contents and service according to the requirement of combination service provider. All of the services are composed by open API.

2.2 Personal Clouding Service Security Requirements

Basic security model of personal cloud is same as existing cloud computing however, additional security solution for user privacy is required. This paragraph explains about security requirement about personal clout security risk and domain [1-3, 5, 7].

- Asset Management

Asset Management should manage hardware composing cloud infra, network and software asset (physical or virtual). Asset management must include accessible account to physical or network base of asset to inspect and observing regulation.

- Cryptography: Key and Certificate Management

Security systems require infra for manage encryption key and certification. And the systems include standard encryption and service for information security.

- Data/Storage Security

Data must be encrypted for security. In addition, some of the users might require separate saving of their data for protection.

- End-Point Security

Users must provide terminal point security in cloud service. Terminal point security must provide limited terminal point security according to the type of network protocol and device.

- Event Auditing and Reporting

User must be accessible to data about events on cloud, particularly system error and security.

- Identity, Roles, Access Control and At

On cloud-based resources, the definition about properties following user and services; distinguish, regulation, authorizing is must be available.

- Network Security

Switch, router, packet unit network traffic must be protect, and IP stack also requires security.

- Security Policies

Access control, resource allocation, and policy decisions consistent definitions, and security policy decisions capability must be available. Policy defining method must be carried out automatically according to SLA and license.

- Service Automation

Security control process and analysis should be automated. In addition, service automation should notice user security policy or license violation to manager.

- Workload and Service Management

Circumstance setting, operating, surveillance service should available according to defined security policy and user license agreement.

3. Proposed System

The system configuration suggested in this paper for key managing protocol about user identification is just like below Figure 2.

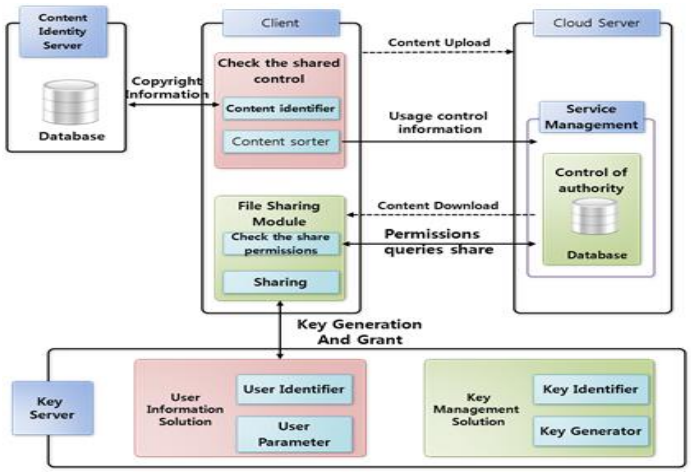

Figure 2. Proposed Key Management System

User identify login with client device. Afterward, client accesses key management solution before get authority identification. And assign each appropriate key for user authority generating key with user information and key information module. Also by using key, personal cloud service is available through down/uploading contents for user area.

3.1. Key Generation and Grant Protocol

This paragraph suggesting client key generating and assigning protocol process. Key generating and assigning protocol is just like below Figure 3.

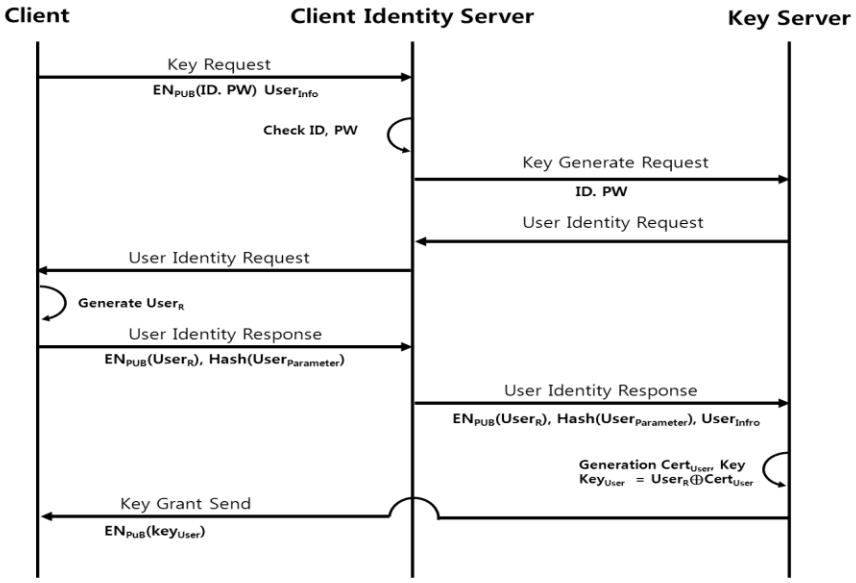

Figure 3. Key Generate and Grant Protocol

1. Client encrypt open key in Client Identity Server and transfer ID, PW and user information.

EN_{Pub}(ID, PW), $User_{Inoo}$

2. Client Identity Server check ID and PW and transfer to Key.

3. Key Server receives data and requires user identification data to client in Client Identity Server.

4. Generate USER and encrypt user to Client and generate USER as hash function and transfer it.

$EN_{PUB}(User_R)$, $Hash(USER_{Parameter)}$

5. . Client Identity Server transfers received message and UserInfo to Key Server.

$EN_{PUB}(User_R)$, $Hash(USER_{Parameter)}$, $User_{Infor}$

6. Key Server generates identification value and key value and transfer to the Client to assign each appropriate key value to user authority.

$Key = Cert(User_R, Key)$, $EN_{PUB}(Key_{user})$

3.2. Communication Protocol

This paragraph suggests communication protocol requiring contents data from Client to Cloud Server. Client transfer user authority and user parameter with Client Identity Server and Key Server to Cloud Server. Afterward Cloud Server generate session key and encrypt contents data with transferring session key and identification value to Client. Designed communication protocol is just like below Figure 4.

1. Client transfer ID and User Information to Client Server and require Content Data.

2. Cloud Server require user identification value with transferring received ID and User Information to Client Identity Server.

3. Client Identity Server require user parameter after check ID and User Information.

4. Client transfers user parameter and hash value to Client Identity Server with KeyUSER after generates USERParameter.

$Key_{USER}(User_{Value})$, $Hash(User_{Parameter})$

5. Cloud Identity receives User Value after transfer received message to Key Server and encrypt as open key to Cloud Identity Server.

$EN_{PUB}(User_{Value})$

6. Cloud Identity Server generates SK after transfer and encrypts user value to Cloud Server.

$SK = (UserValue \oplus Cert_{CS})$

7. Cloud Server transfer contents data with encrypting SK and CertCS to Cloud Server.

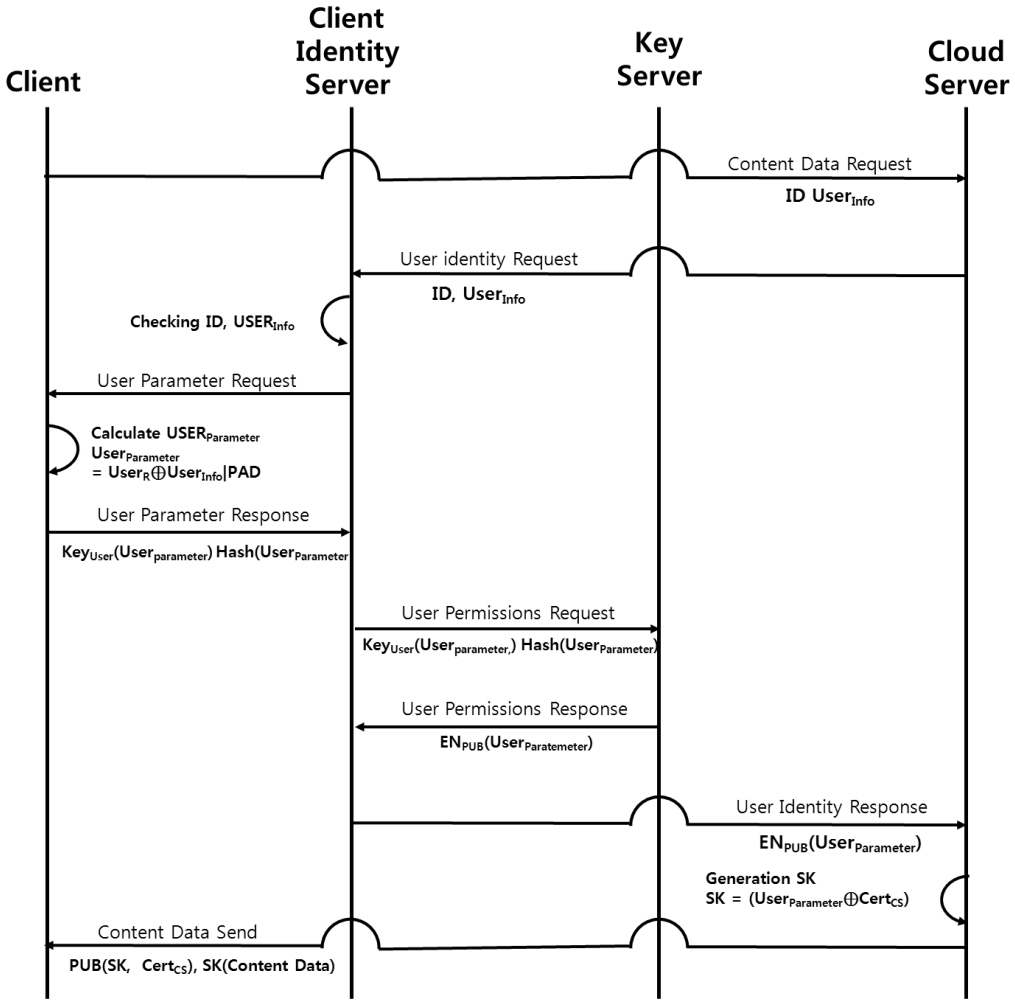

Figure 4. Communication Protocol

4. Safety Analysis

This paper analyzes the security about designing method about key generating and assigning after user identification in personal cloud computing circumstance. Suggested key managing protocol analyzed about 4 significant factor for user private information management on personal cloud circumstance; user-oriented risk analysis, circumstance setting, double encryption, feedback. And it designed to guarantee the safety about user identification and authentication, permission, security/privacy and key management. The explanation about safety is like below paragraph.

(1) User-oriented risk analysis

Cloud computing should managed securely about service availability and user contents. Suggested protocol generates and assign appropriate key for user authority, to make accessible to the contents.

(2) Circumstance setting

Circumstance setting is the function that manager's assignment appropriate authority for each users. It should set user authority according to each policy mechanism in personal cloud.

So suggested protocol set user's access authority by generating appropriate key after analyze user's parameter and user information.

(3) Double encryption

Double encryption should be designed for counteract to risk of leaking private data and etc. By open key way encryption, the user information is confirmed. Afterward, appropriate key for each personal authority is generated with user parameter value. When transfer contents data in client server, secure communication is available through encryption after generate SK.

(4) Feedback

The feedback should be provided to personal cloud service user through reports about privacy providing. So the protocol suggested in this paper provided feedback to the user with received hash value and user information.

(5) Key management

Key management makes secure communication with assigning personal cloud computing user as each authority of them. And it supported to manage all of key management for encrypted services.

5. Conclusion

This paper suggested key management generates and contents communication method to enhance security and supplement vulnerability about personal information management on personal cloud circumstance. It enables the service for user through generating each user authority key after transferring ID and PW to Key Server by client. After, the protocol for safe user contents transfer that generate SK after identify and transfer use ID, PW, Hash through Client server is suggested on communication process.

In addition, this paper analyzed about vulnerability of personal cloud computing circumstance and important factor on servicing existing cloud computer circumstance such as user-oriented risk analysis, setting, double encrypting, feedback, key management.

After, suggested protocol required for studies about secure communication method that adoptable on expanded communication circumstances such as contents data management, existing wire/wireless network security risks, not about existing user identification management system. In addition, the studies about quantitative efficiency analysis for suggested protocol above.

References

[1] M.-S. Song, S.-K. Ko, J.-H. Lee and D.-H. Seo, "Mobile cloud virtual terminal collaboration technologies and provisioning", **(2012),** pp. 77-86.
[2] H.-S. Kim and C.-S. Kim, "Cloud Comput and Privacy Authentication", Korea institute of information security & crpyology, **(2010),** pp. 11-19.
[3] "TTAK.KO", Privacy Protection Refernce Model for Personal Coud, **(2012)**.
[4] "TTAK.KO", Definition and Requirement Analsis of Personal Cloud Service, **(2011)**.
[5] M. K. Yusof, A. F. A. Abidin and M. A. M. Amin, "An Architecture for Securing a Private Instant Messenger",vol. 2, no. 1, **(2012),** pp. 60 -70.
[6] C. Xiao, Z. Huang and D. Li, "A Tutorial for Key Problems in the Design of Hybrid Hierarchical NoC Architectures with Wireless/RF", vol. 3, no. 6, **(2013),** pp. 425-436.
[7] M. Jang, M. Yoon and J.-W. Chang, "A k-Nearest Neighbor Search Algorithm for Enhancing", IJSH,vol. 7, no. 3, **(2013),** pp. 239-248.
[8] K.-K. Seo, "An Explorative Model for B2B Cloud Service Adoption in Korea -Focusing on IaaS Adoption", IJSH, vol. 7, no. 5, **(2013),** pp. 155-164.

Authors

Byung Wook Jin, he received his B.S. degree in Multimedia Science from ChungWoon University, Chungnam, Korea. in 2010, and M.S. degree in Computer Science from Soongsil University, Seoul, Korea, in 2013. He is Currently a Ph.D Course in the Computer Science, Soongsil University. His research interests include Personal Cloud Service, Authentication System, Network Security.

Keunwang Lee, he received his B.S. degree in Computer Science from Hanbat National University, Daejeon, Korea, in 1993, and M.S. and Ph.D. degrees in Computer Science from Soongsil University, Seoul, Korea, in 1996 and 2000, respectively. He is currently an Associate Professor in Chungwoon University, Chungnam, Korea. His research interests include multimedia communications, multimedia applications, mobile communications, and multimedia security.