http://dx.doi.org/10.14257/ijsia.2014.8.3.25

Security System for Healthcare Data in Cloud Computing

Maya Louk[1], Hyotaek Lim[2] and Hoon Jae Lee[3]

*[1]Department of Ubiquitous IT, Graduate School of Dongseo University,
Sasang-Gu, Busan 617-716, Korea
[2]Division of Computer and Engineering Dongseo University
Sasang-Gu, Busan 617-716, Korea
[3]Division of Computer and Engineering Dongseo University
Sasang-Gu, Busan 617-716, Korea
[1]mayalouk@gmail.com, [2]htlim@gdsu.dongseo.ac.kr, [3]hjlee@dongseo.ac.kr*

Abstract

Cloud computing is a renowned computing method of sharing data resources whether publicly or privately. Cloud computing is an answer for a better computing environment. It will reduce the costs which are used efficiently. Cloud computing can be used not only for business purposes but also for medical purposes which will be used by patients, specialists, pharmacists, nurses, doctors, and hospital administrations. As an implication, security is an important issue for cloud computing. Data privacy protection and data retrieval control are security issues for cloud computing. This Paper describes security elements like monitoring, recording, tracking and notification. For the purpose of encryption-decryption, AES-256/SHA will be used. Re-encryption "tag" and "mark" for data access system will only be functional for every legal user. It suggests that the cloud computing based on encryption and decryption services. Encrypted medical data could be accessed and decrypted from anywhere and whomever with particular authentication. The writer proposed the constructive idea of Healthcare data via cloud computing and the security accessing data by authorized individuals.

Keywords: *Cloud Computing, Cryptography, Functional Re-Encryption, Medical Data, tag and Mark, Tracking*

1. Introduction

Cloud computing is a futuristic computing paradigm which has drawn extensive attention from both industrialists and scholars. By combining a set of existing and new techniques from research areas such as Service Oriented Architectures (SOA) and Virtualization, cloud computing is seen as a computing paradigm where data resources are stored over at the platonic world of Internet. Cloud computing provides consumers a new way to share data resources and services that belong to various organizations or sites. Since cloud computing shares distributed resources via the network in the open environment, thus security problems are important issues to address by developing application programs which will secure to work best for medical purposes.

Medical data is secretive and sensitive in nature. The confidentiality could only be accessed by the proper individuals, such as the particular doctor and such. This idea covers not only patients who are located in the big city with flashy high-tech hospital and abundant health-specialists, but also for every needy person who are limited to small hospital in remote regions. With this design idea, the administration staffs of the hospital or nurses will be able to record all the data they need and to upload them into the cloud computing for the health-specialists wherever they may be could analyze the data and send back his suggestion.

This design has to deal with the security system design which covers the whole of the design idea. Security system must be of the first concern because of the sensitive and private nature of the data.

- Some concern about the security for medical data in the cloud computing:
- How can the cloud provider to protect my medical data from cyber attack?
- How can the cloud provider to manage my medical data to be accessed by an authorized user?
- Cloud Provider unable to learn my medical data.
- How can the cloud provider to protect my medical data while it was being accessed by an authorized user?

2. Related Works

We note that storing the data in the cloud computing Operating System (OS) is not really new. This design idea already performed by some Microsoft researcher namely, Benaloh, Josh, *et. al.*, [6]. But processing and accessing medical data purpose using cloud computing with secure system may be new for some researchers. The re-encryption adapted from Nishanth, Chandra *et. al.*, who make a calculation with tag name for accessing the data and some simple arbitrary solution adapted from Seny Kamara and Mariana Raykova. A related works with the medical data storing into the cloud already done by Microsoft researcher. All the previous research contributes to the theory and concept of secure medical usage of cloud computing, but the most important question is: is it possible to implement it into reality? But the concern is not the theme of this paper.

3. Patient Medical Data

It will reduce the cost since there is no need to print out all the medical data for patient, and of course it will help the campaign against global warming because of excessive use of paper. The hospital has to rent or to set up an environment for cloud computing and the cloud computing environment has to be installed with all the program to read, process, access the medical data correctly and accurately. For the patient medical data that will be our concern are:

a. Authentication Medical Data

Authentication has to be done since the login process. All users need to provide the login credentials. Each user registers initially or is registered by someone else (Hospital administration), using an assigned or self-declared password. On each subsequent use, the user must know and use the declared password. The weakness in this system is that passwords can often be stolen, accidentally revealed, or forgotten. For this reason, digital activities based on the internet and many other activities require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered likely to become the standard way to perform authentication over the Internet.

b. Reliability Medical data

The medical data should be reliable because medical data is a sensitive data which need accuracy.

- Completeness refers to the extent that relevant records are present and the fields in each record are populated appropriately.
- Accuracy refers to the extent that recorded data reflect the actual underlying information.
- Consistency, For example, if data are entered at multiple sites, inconsistent interpretation of data entry rules can lead to data that are unreliable

c. Security Medical Data

Security of medical data is the most important issue, because somebody can modify it, or share it to another person in the internet world. The patients or all the other users who have the importance to that medical data must be free of anxiety.

d. Secure Transmitting Data (uploading/downloading)

While transmitting, the data have to be securely arrived to the cloud pool storage. There are many secure transmitting data methods used by many cloud providers or vendor to increase security, for example: Secure Sockets Layer (SSL) and AES-256 bit encryption that provided by *Dropbox.*

e. No Loss Data

It will be useless if data loss occurs while transmitting (uploading), storing, and accessing or downloading data, even if only one bit loss. Medical data is not only sensitive data but also need accuracy.

f. User Access Control

This system is designed for multiuser. The policy for accessing the medical data has to be carefully set up, and procedure for the user to access into the medical data has to be done by the cloud provider. The system could not be read or learnt by the cloud provider employee. The cloud provider employee should be prevented not to read the medical data without any permission from the hospital or the patient. Therefore to be as convenient as possible, the cloud provider should provide accurate data reading process so that the authorized doctor will be able to give the most possible accurate diagnostics available so that the patient shall receive proper medical treatment.

4. Security for Medical Data

Security system for medical data does not only to encrypt and to decrypt with public and private key, but also to monitor and to record data. all user will get notification for all activities done in the cloud computing which intruders may not know they were being monitored by the system. The system is not meant only to monitor and to give notifications but also to record data and to track intruders

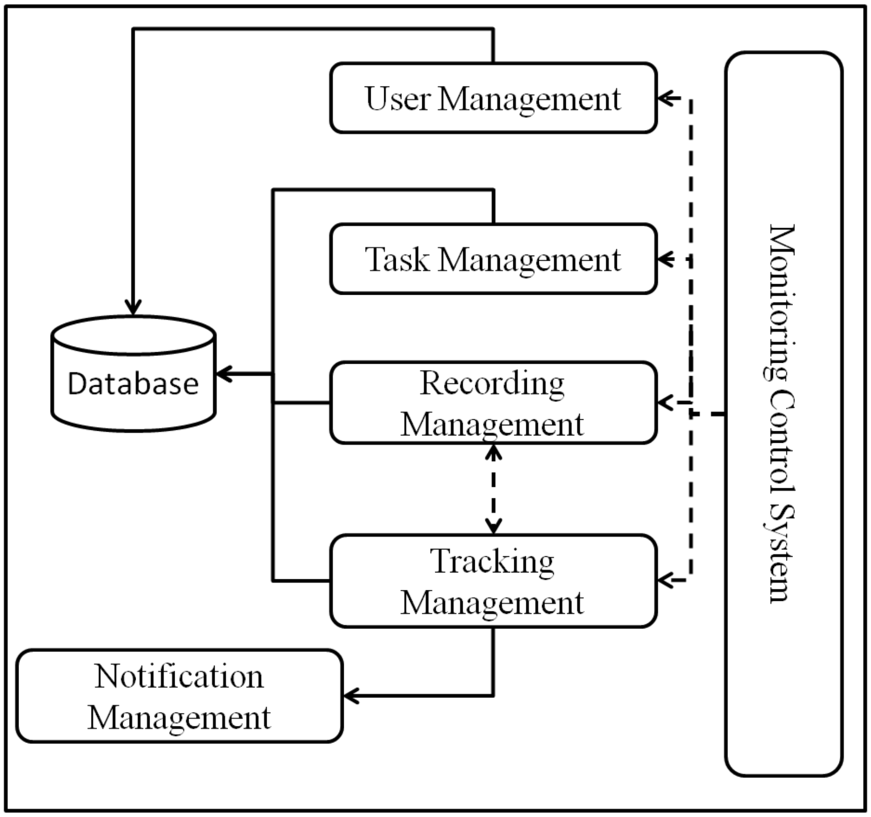

Figure 1. The Security System for Healthcare Data

According to Figure 1, when inappropriate user tries to illegally access the data, the intruder must jail breaking the security system beforehand. Thus the system will record it and track it down and send the notification to the legal user. The legal user will be able to identify the intruder and learn something about his where about.
The security system consists of:

a. User Management & Task Management: when a user wants to log into the system, a one time password will be sent into the user mobile phone via short message system (SMS). The data saved in the cloud storage will be encrypted with the proper "tag" name. It helps the nurse or hospital administrative staffs to protect the data and to forward it to the user. If the data is meant for the health-specialists, it will be saved under "doctor's" tag. The security algorithm for encryption and decryption purpose itself can be from any security schemes. For the purpose of this paper, we will use AES-256/SHA for encryption. The implementation of PBKDF2 will be used to slow down password crackers from guessing the master password in the scenario of data stolen. PBKDF2 is a key derivation function—a system that churns the master password into numbers of encryption key. With the new cloud keychain format, PBKDF2 will turn the master password into tow 256-bit keys. One is a HMAC key to integrity check the data; and the other is a key to decrypt the master key. To derive the 512-bits from the master password, HMAC-SHA512 is used within PBKDF2 in the cloud keychain format.

b. Recording and tracking: all these elements merge into one in the system. The record of all activities is ongoing progress. So every move that is made, who made it, where, and when it happened can be identified. All these progress will be reported to the proper user via mobile phone application.

5. Re-encryption for Medical Data

Re-encyrption data is used to tag and mark data that wanted to be saved in cloud storage. Tag names will be given to all data according to all particular users. Any person that is not tagged will be unable to access the data since no authorization is given. Functional re-encryption is an expressive generalization of re-encryption. Transform ciphertext of messages or data with “tag” T with PK_A into ciphertext of data with PK determined by the F (T). Functional re encryption functionality is parameterized by a policy function F: D = [n] (*i.e.*, F has domain D and has n possible outputs) chosen from some class of functions, an input public key pk, and n output public keys. The function receives as input a ciphertext of message m with “identity” id under the input public key pk. It decrypts the ciphertext using the secret key “sk” to get m and id, and then re- encrypts m under the “appropriate” output public key cpkF(id). Following our desiderata from before, one could think of functional re-encryption as a form of fine-grained delegation of access. [1] The design of security under re- encryption security is the patient (W) who comes to the hospital. The nurse will perform medical checkup and upload the encrypted data to the pool storage.

Case 1: (there are only 2 users, the patient (W) and the specialist Doctor (P)) Patient W has $PK_A = g^a$ and $SK_A = a$ besides that Specialist Doctor P has $PK_B = g^b$ and $SK_B = b$; Data send to the cloud (uploading) X = Enc (g^a, M), which M is the plain data; Data download from the cloud (downloading) Y = Enc (g^b, M), which M is the plain data and the plain data will be decrypted under PK_B and $SK_{B.}$ Re-encryption from key g^a to key g^b can be done with the re-encryption key $g^{b/a}$

Case 2: multiuser to access one patient (W) data with different purpose and different file. Some file may not be meant to be read and accessed by another user.

Patient W has $PK_A = g^{ai}$ and $SK_A = a_i$, α_i → which i is the tag name for certain user may access the data, let assume that formula F (0) = F’ (0) and F (1) = F’ (1), so on. Then, Specialist Doctor P has $PK_0 = g^{b0}$ and $SK_0 = b_0$, Nurse O has $PK_1 = g^{b1}$ and $SK_1 = b_1$, Pharmacist T has $PK_2 = g^{b2}$ and $SK_2 = b_2$, Researcher Doctor U has $PK_3 = g^{b3}$ and $SK_3 = b_3$, and so on. Send data to the cloud (uploading) X = Enc (g^{ai}, M), which M is the plain data – encrypt message M with tag i with key $g^{a.}$ Data download from the cloud (downloading) Y = Enc ($g^{b0(i)}$, M), which M is the plain data, the data decrypted under the PK_i = and $SK_{i.}$

Advantages of Functional Re-encryption:

- Revocation of keys: changing access policy with a trusted cloud is trivial. The patient only needs to give new re-encryption key to the cloud.
- Collusion between recipients and cloud: can prove security of the scheme even when cloud colludes with some false recipients.
- Offline recipients: recipients need not be involved in the setup phase, and they can use their own public key and secret key pairs.

The input encryption scheme is as follows:

- I-Gen ($1^\lambda, 1^d$): Pick random vectors a^1, …… ,a^d from Zq^d that are linearly independent. We also generate crs, a common reference string (abbreviated CRS) for the NIZK proof system. Output pk = (crs, g, g^{a1}, ……, g^{ad}), and sk = (a^1,….,a^d). We remark that the public key pk can be viewed as being made up of d public keys pk_i = (g,g^{ai}) of a simpler scheme.

- I-Enc(pk, I, ε, [d], m): To encrypt a message *m* ε *M*, with –identity‖ i ε [d], choose random exponents r and r' from Zq, and compute:
  - ○ C = g^{rai} ; D = g^rm
  - ○ C' = $g^{r'ai}$; D' = $g^{r'}$
  - ○ π, a proof that these values are correctly formed, *i.e.*, that they correspond to one of the vectors g^{ai} contained in the public key.

  Output the ciphertext (E, E', π) where E = (C, D) and E' = (C', D'). Looking ahead, we remark that E looks like an encryption of message m under pk_i, while E' looks like an encryption of 1_G under pk_i. E' is primarily used by the re-encryption program for input re-randomization, and is not required if he encryption scheme is used stand-alone without the functional re-encryption program.
- I-Dec (sk, (E, E')): If any of the components of the ciphertext E' is 1_G or if the proof π does not verify, output τ. Ignore E', π subsequently, and parse E as (C,D). Check that for some *i* ε [d] and *m* ε *M*, D $(C^{1/ai})^{-1}$ = (*m*, ….. ,*m*). If yes, output (*i*,*m*). [1]

The Output Encryption Scheme is as Follows:

- O-Gen (1^{λ}): Pick â ⟵ Zq. Let pk‖ = $h^{â}$ and sk‖ = â.
- O-Enc(pk, *m*): To encrypt a message *m* ε *M* Ċ G,
  - ○ Choose random n umber r ⟵ Zq.
  - ○ Compute Ŷ = $(h^{â})^r$ and Ŵ = h^r.
  - ○ Output the ciphertext as [Ŝ,Ĝ] : = [e(g, Ŷ), e(g, Ŵ) · e(*m*, *h*)]
- O-Dec(sk = â, (Ŝ,Ĝ)): The decryption algorithm does the following:
  - ○ Compute Ő = Ĝ · $Ŝ^{-1/â}$
  - ○ For each *m* ε *M*, test if *e(m,h)* = Ő. If so, output *m* and halt. (Note that if *e(m,h)* are precomputed for all *m* ε *M*, then this step can be implemented with a table lookup.) [1]

6. Conclusion & Future Work

This idea provides more secure data transmitting for medical purpose. The re - encryption formula will help the multiuser to use and trust the cloud computing, encryption and decryption under a certain tag name that put together with the file. It will thrive to control the user access to the medical data. Several questions that imply this project are: (1.) Can access policy be applicable to lower class of access policies? (2.) Is that possible to access and to make limitless access policies? (3.) Can we construct smaller esoteric texts? All questions must be reviewed to improve the security system. In future work we are going to implement it and calculate the possibility to outsource arbitrary multi-party computations securely to the cloud. Arbitrary Code Execution is a technique to execute any task of computations into the targeted computer, which in this context is Cloud Computing. Furthermore, it is important that every process is done without the cloud provider employee could learn anything about the content of the data. Future project from this is paper is the implementation project using EC2 and the improvement of quality performance from the mobile application using android device.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (grant number: 2013-071188). And it also supported by the BB21 project of Busan Metropolitan City.

References

[1] N. Chandran, M. Chase and V. Vaikuntanathan, “Functional re-encryption and collusion-resistant obfuscation”, Theory of Cryptography. Springer Berlin Heidelberg, **(2012)**, pp. 404-421.

[2] J. Benaloh, “Patient controlled encryption: ensuring privacy of electronic medical records”, Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, **(2009)**.

[3] G. Kulkarni, “A security aspects in cloud computing”, Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on. IEEE, **(2012)**.

[4] W. Liu, “Research on cloud computing security problem and strategy”, Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference IEEE, **(2012)**.

[5] International Organization for Standardization and International Electrotechnical Commission. “Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary.” Iso/IEC 27000, <<http://webstore.iec.ch/preview/info_isoiec27000%7Bed2.0%7De n.pdf>, accessed in June 2013, **(2009)**.

[6] S. Kamara and M. Raykova, “Secure Outsourced Computation in a Multi-Tenant Cloud”, IBM Workshop on Cryptography and Security in Clouds, **(2011)**.

[7] J. Benaloh, “Patient controlled encryption: ensuring privacy of electronic medical records”, Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, **(2009)**.

[8] P. Kumar, “Effective Ways of Secure, Private and Trusted Cloud Computing”, arXiv preprint arXiv:1111.3165, **(2011)**.

[9] S. Ramgovind, M. E. Mariki and E. Smith, “The management of security in cloud computing”, Information Security for South Africa (ISSA), 2010. IEEE, **(2010)**.

[10] Z. Shen, “Cloud computing system based on trusted computing platform”, Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference, IEEE, vol. 1, **(2010)**.

[11] G. Seroussi, “Elliptic curve cryptography”, Information Theory and Networking Workshop, 1999, IEEE, **(1999)**.

[12] V. Paxson, “Bro: a system for detecting network intruders in real-time”, Computer networks, vol. 31, no. 23, **(1999)**, pp. 2435-2463.

[13] A. Omerovic, V. Muntés Mulero and P. Matthews, “Risk and Quality Analysis in Multi-Cloud Environments”, **(2013)**.

[14] M. Ben-Yehuda, “The nonkernel: a kernel designed for the cloud”, Proceedings of the 4th Asia-Pacific Workshop on Systems. ACM, **(2013)**.

[15] N. Santos, K. P. Gummadi and R. Rodrigues, “Towards trusted cloud computing”, Proceedings of the 2009 conference on Hot topics in cloud computing, **(2009)**.