SCEHSS: Secured Cloud Based Electronic Health Record Storage System with Re-Encryption at Cloud Service Provider

R. Sumathi, *Member, IACSIT* and E. Kirubakaran

***Abstract*—An electronic health record system is a collection of health related information. Instead of collecting data from single health care centre, data could be collected from various health care centers. Collected data could be further effectively utilized by healthcare and research community. Cloud computing paradigm gives better platform for connecting various communities providing data and location independence with less maintenance. A Cloud Electronic Health Record (CEHR) integrates data to serve different needs. The goal is to collect data once and use it multiple times to adopt latest technologies in medical domain. Security for data-in-transit is one of the major issues in cloud as well as in EHR systems. Our concentration is achieving highly secure data transmission through multiple encryption and re-encryption in the cloud environment without trusting cloud service provider cent percent. Using both symmetric and asymmetric algorithms the security levels of encryption is strengthened. In 2008, Libert and Vergnaud presented the first construction of unidirectional proxy re-encryption scheme with chosen-ciphertext security in the standard model. We extended the unidirectional proxy re-encryption scheme to cloud environment by assigning the responsibility of proxy to cloud service provider for securing data-in-transit.**

***Index Terms*—Electronic health record, ciphertext security, cloud computing, cloud service provider, re-encryption.**

I. Introduction

An electronic health record (EHR) is a systematic collection of health related information about individual patients or populations in a digital format. Such records may include a whole range of data in comprehensive or summary form, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal stats like age and weight, and billing information. Though it is in digital format, these data can be utilized effectively like streamlining of the workflow in health care settings, increases safety through evidence-based decision support, developing Medical Decision support System, quality management and outcomes reporting. Among all the barriers to the implementation of EHR systems, privacy and security concerns on patients' medical records are arguably most dominating [1], [2], [3], [4]. Records stored in a central server of a healthcare provider are collected from various sources through network are subject to theft and security infringes. The health information systems literature has seen the EHR as a container holding information about the patient, and a tool for aggregating clinical data for secondary uses.

Cloud technology transforms network of computers into the largest single virtual computer. Cloud provides unlimited infrastructure to store and execute customer data with less maintenance and high scalability. Cloud is the most suitable technology for collecting medical records from various sources with less complexity and can be served for multiple purposes. Cloud Electronic Health Record (CEHR) systems may be an attractive and cost-effective solution. CEHR systems have defined some necessary data structures, vocabularies and interfaces appropriate for clinical trial research, data collection and sharing promote better clinical trials management and scientific discovery. Because of its Open System Architecture, security is the major concern in the cloud environment. Our objective is providing improved security for electronic health record in the cloud environment.

Section II describes security issues in distributed environment. Section III gives overview about unidirectional proxy re-encryption scheme. Our proposed re-encryption scheme for data-in-transit at cloud service provider is elaborated in Section IV. Result and conclusion is in Section V.

II. Security Issues in Distributed Systems

Major security concerns such as authentication, integrity and confidentiality are discussed in this section.

Authenticity and Authentication: Authenticity in general refers to the truthfulness of origins, attributions, commitments, and intentions. Authentication is the act of establishing or confirming claims made by or about the subject are true and authentic. The authentication of information can pose special problems, especially man-in-the-middle (MITM) attacks, and is often implemented with authenticating identity. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. In a healthcare system, both healthcare information offered by providers and identities of consumers should be verified at the entry of every access.

Non-repudiation: Non-repudiation implies one's intention to fulfill its obligations to a contract. It also implies that one

Manuscript received August 9, 2012; revised September 29, 2012.

R. Sumathi is with the Computer Science and Engineering Department, J.J.College of Engineering and Technology, Tiruchirappalli, TamilNadu ,India (e-mail: sumathi_rajmohan@ yahoo.com).

E. Kirubakaran is the Additional General Manager at Bharat Heavy Electricals Limited , Tiruchirappalli, TamilNadu, India (e-mail: ekiru@)bheltry.co.in).

party of a transaction neither denies having received a transaction nor can the other party deny having sent a transaction. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

Individual (Provider) consent and authorization: Patient can allow or deny sharing their information with other healthcare practitioners or CDOs. To implement patient consent in a healthcare system, patient may grant rights to users on the basis of a role or attributes held by the respective user. Access control mechanisms help in providing rights to various levels of users or consumers [5], [1], [4].

Integrity and confidentiality of data: Integrity means preserving the accuracy and consistency of data. In the health care system, it refers to the fact that data has not been tampered by unauthorized use. Confidentiality is one of the design goals for many crypto systems and made possible in practice by the techniques of modern cryptography [6]. Confidentiality can be achieved by access control and encryption techniques in EHR systems [7]. Our interest is maintaining integrity and confidentiality of data during transmission in the cloud environment and to keep data away from chosen ciphertext attacks.

In the next section, the basis of the Proxy re-encryption and an unidirectional proxy re-encryption scheme has been elaborated.

III. Unidirectional Proxy Re-Encryption Scheme

Two types of re-encryption schemes are Bi-directional and Unidirectional [8]. If the re-encryption key $rk_{1,2}$ necessarily allows the proxy to translate ciphertexts under pk_1 into ciphertexts under pk_2 and vice versa, the scheme is bidirectional. If the re-encryption key $rk_{1,2}$ allows the proxy to translate only from pk_1 to pk_2, then the scheme is known as unidirectional.

Proxy re-encryption scheme allows a proxy to transfer a ciphertext corresponding to sender's public key into one that can be decrypted by receiver's private key. However, the proxy in this scheme can't obtain any information on the plaintext and the private keys of both users. That gives it, strength for this technique. A Proxy re-encryption (PRE) scheme also allows a proxy to transform a ciphertext under a delegator's public-key into a delegatee's ciphertext on the same message by using some additional information [9], [10], [11].

In a proxy re-encryption (PRE) scheme, a proxy is given a piece of information that allows it to translate a ciphertext under one key into a ciphertext of the same message under a different key. The proxy cannot, however, learn anything about the messages encrypted under either key. Recently, proxy re-encryption (PRE) scheme received much attention due to its application in information storing, secure e-mail forwarding, digital rights management (DRM) or distributed storage systems, etc. Proxy re-encryption schemes are a special kind of proxy cryptosystems where delegatees only need to store their own decryption key. The goal is to securely enable the re-encryption of ciphertexts from one key to another, without fully relying on trusted parties [9].

In a uni-directional scheme is effectively one-way; messages can be re-encrypted from Alice to Bob, but not the reverse. Uni-directional schemes can be constructed such that the delegated party need not reveal its secret key. For example, Alice could delegate to Bob by combining his secret key with Bob's public key. Fig.1 shows the basic unidirectional scheme [8], [12]. This is the appropriate scheme for cloud environment to store data in the data storage. Our interest is adding security during this transaction.

The two main security notions for PRE are Message secrecy and Collusion resistance [13]. Message secrecy is the concept that the adversary cannot get the plaintext, if he is not the intended receiver (including the delegator and delegatees). Like public key encryption (PKE), there are three levels of message secrecy for PRE, i.e., chosen-plaintext secure (CPAsecure), replayable chosen-ciphertext secure (RCCAsecure), chosen-ciphertext secure (CCA-secure) (ordered by the adversary's ability). Many applications of PRE require CCA security, like encrypted email forwarding.

Another major concept of Collusion resistance is that the delegatee colluding with the proxy should be able to decrypt the ciphertexts encrypted by the delegator's public key, but cannot obtain the delegator's private key. In collusion-resistant PRE, the delegator can delegate decryption rights, while keeping signing rights for the same public key. If one value can be used to decrypt the ciphertext, but not the associated private key, the value is known as the weak private key. Hence, collusion resistance can also expressed as: although the delegatee and the proxy can get the weak private key of the delegator, they cannot get the private key of the delegator.

Our proposed Unidirectional CSP based Re-encryption scheme also fulfill the above mentioned security notions.

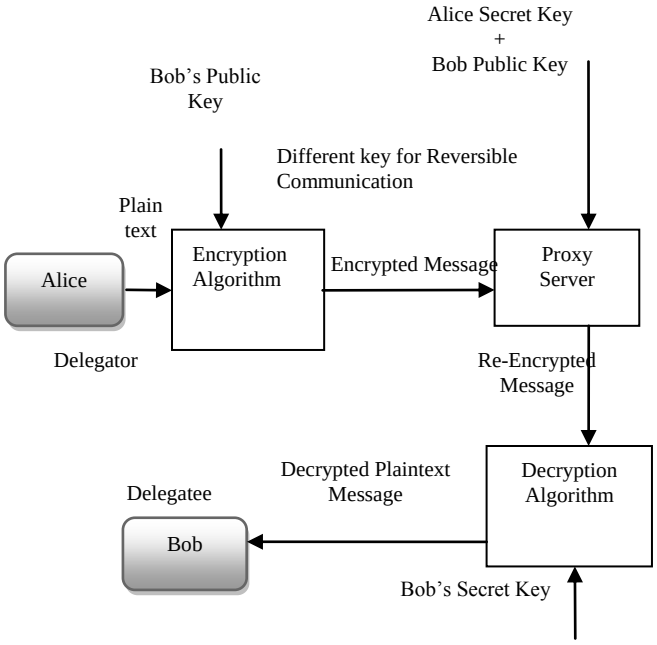


Fig. 1. Basic unidirectional proxy re-encryption scheme.

IV. Proposed Re-Encryption Scheme for Data-in-Transit at Cloud Service Provider

We elaborated an improved unidirectional CSP based re-encryption scheme in this section. Figure 2 shows the

proposed system architecture for secured EHR data transmission in the cloud.

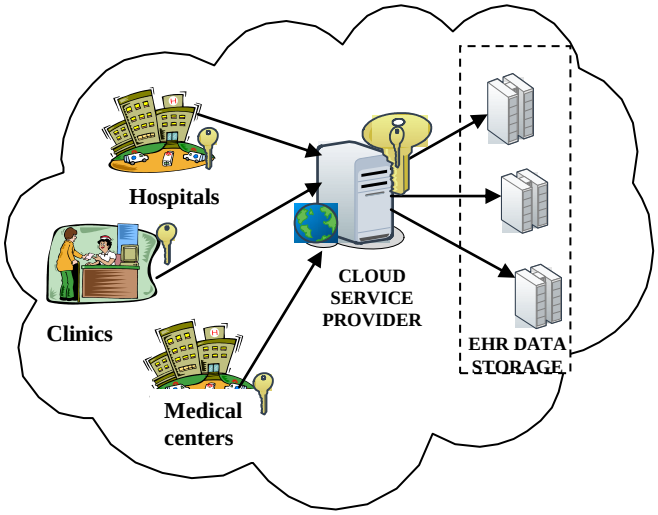


Fig. 2. Proposed system architecture

The proposed system flow includes Client – CSP – Data Storage Transaction. This transaction process contains two sub parts. They are Client to CSP transaction and CSP to Data Storage transaction. The following sub sections contain notations used in this transaction, secured Client to Cloud Service Provider communication and the secured communication between CSP and Data storage.

A. Notations

Notations used in the proposed unidirectional CSP based re-encryption scheme are given below.:

GSetup(λ)→pp: The GlobalSetup algorithm is run by a trusted party that, takes as input a security parameters λ. It generates the global parameters pp which used by all parties in the scheme.

KeyGen(a, b, pp)→(pk,sk,mc,sc): The key generation algorithms generates the public key pka, the private key ska, the master code mca and the secret code sca for user a.

RKeyGen(λ)→rk: The re-encryption key generation algorithm, run by trusted party, takes as input as security parameters λ. It outputs a re-encryption key rk.

E1(m, mcb, pp)→C1: on input of public parameters pp, a receiver's master code and a plaintext m, this probabilistic algorithm outputs a first level ciphertext that cannot be re-encrypted by another party.

E2(C1, pkb, pp)→C2: given public parameters pp, receiver's public key pkb and a first level ciphertext C1, this randomized algorithm outputs a second level ciphertext that can be re-encrypted by another authorized user using the suitable re-encryption key.

ReEnc(C2, rk, pp)→CT: The re-encryption algorithm, run by the proxy, takes as input a original ciphertext C1 and public parameters pp. It is further encrypted under a re-encryption key rk and outputs a re-encrypted ciphertext CT.

ReDec(CT, rk, pp)→C1: The re-decryption algorithm, run by the receiver, takes as input as a re-encrypted ciphertext CT and public parameters pp. It is further decrypted under a re-encryption key rk and outputs a original ciphertext C1.

D1(C2, S[skb], pp)→C1: The level 1 decryption randomized algorithm takes as input a onetime private key S[skb], public parameters pp and a cipertext C2. It outputs a message m. One time key is the combination of client's key, date, time and random number.

D2(C1, mcb, pp)→m: The level 2 decryption probabilistic algorithm takes as input a receiver master code mcb and a original ciphertext C1 and public parameters pp. It outputs a message m.

Fig. 3 elucidates the entire proposed system flow with appropriate notations used in every stage.

B. Client – CSP – Data Storage Transaction

Major drawback of the cloud environment is trusting CSP cent percent. Here we introduced trusted third party for key generation and key distribution. At CSP, re-encryption takes place for getting ciphertext as input.

At the client side the first level encryption is done using the master code of the data storage system. Then a second level encryption using the public key of the CSP is done. This multiple encrypted message is received by the semi trusted CSP, which does the first level decryption with its own key. Now the CSP does another encryption using the re-encryption key given by the receiver. The receiver that is data storage now decrypts the message using the re-encryption key, followed by a decryption using the master code. Then the receiver finally gets the original message. The original data sent from the healthcare providers are stored at the data storage. Other healthcare professionals utilize the data stored at data storage. Fig. 4 shows the Pseudocode for our proposed secured CSP based unidirectional re-encryption scheme.

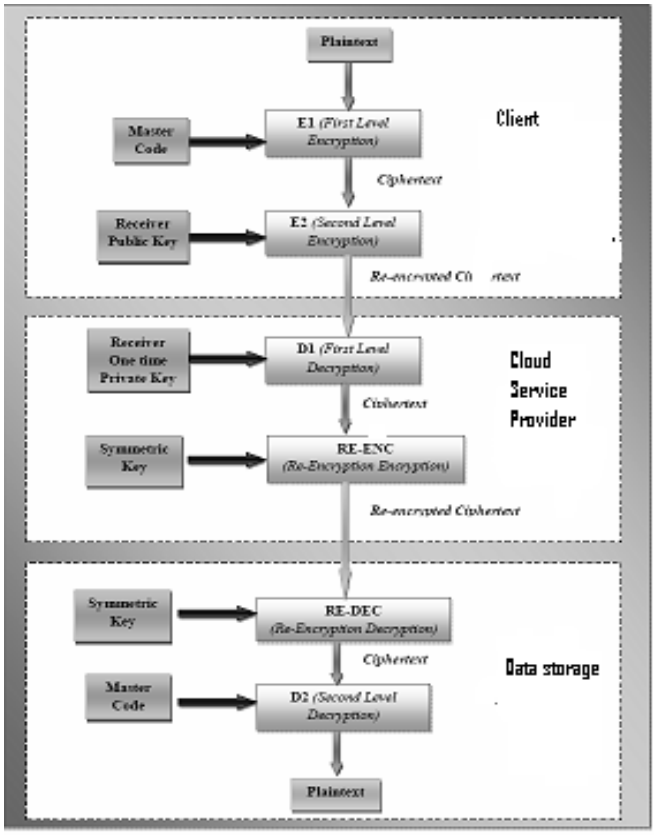


Fig. 3. Transaction process.

Thus the proposed system of unidirectional re-encryption

scheme at CSP with chosen-cipher text security in the standard model is introduced and messages have been secured from chosen-ciphertext attacks while keeping them efficient and robust. We also used symmetric and asymmetric algorithms for encrypting data at different levels.

```
class Unidirectional_Cloud_Secure_Scheme {

Key_Generation(CSP a, Cloud_Client b, Storage_Server d, Public parameter pp)
Re-encrypted_Key_Generation(Security parameter λ)
First_Level_Encryption(Message m, Master code mc, Public parameter pp)
Second_Level_Encryption(Ciphertext C1, public key pk, Public parameter pp)
First_Level_Decryption(Ciphertext C2, Private key sk, Public parameter pp)
Re-Encryption(Ciphertext C2, re-encrypted key rk, Public parameter pp)
Re-Decryption(Ciphertext CT, re-encrypted key rk, Public parameter pp)
Second_Level_Decryption(Ciphertext C1, Mastercode mc, Public
```

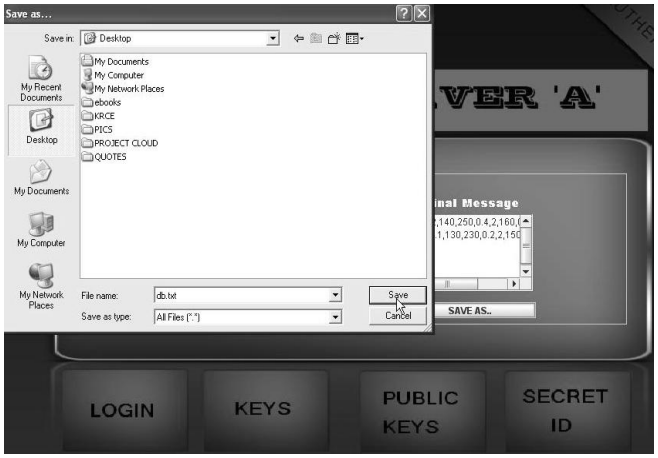
Fig. 4. Pseudocode for unidirectional cloud secure scheme.

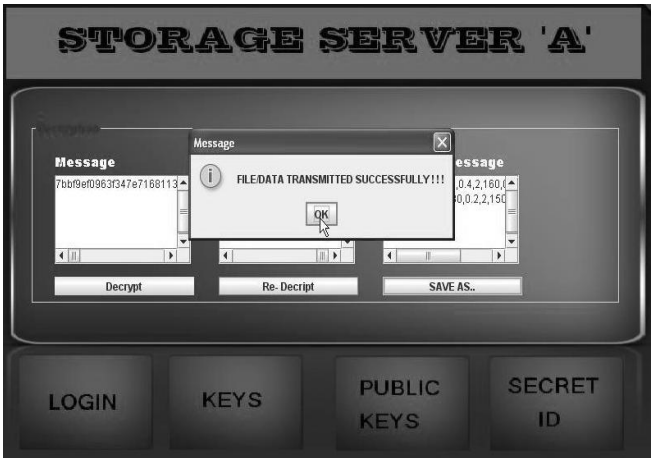
a. Input data file for first level encryption.

b. Input encrypted data file for second level encryption.

c. Encrypted data sent to CSP.

d. One level decryption and re-encryption at CSP.





e. Original data stored at data storage after decryption.

Fig. 5. Screen shots show level by level encryption.

V. Result and Conclusion

We extended the concept named Proxy Re-Encryption (PRE) scheme. PRE allows turning a cipher text encrypted under a given public key into an encryption of the same message under a different key. The obvious problem with this strategy is that the proxy learns the plaintext and sender's private key. Another problem in this scheme is the proxy key which can be used for both sender to receiver and receiver to sender, which may be undesirable in situations where trust relationships are not symmetric. In the cloud environment, cloud limits the freedom of users and ranks them dependent on the cloud service provider. To overcome the aforementioned three problems, our CSP based unidirectional re-encryption scheme allows CSP to encrypt the ciphertext without knowing the plaintext sent by the client. Thus the proposed work of unidirectional re-encryption scheme at CSP in the standard model has been successfully emulated using java and messages have been secured from chosen-ciphertext attacks while keeping them efficient and robust. Screen shots of our proposed system in each level are given in fig.5. We also used both symmetric and asymmetric algorithms at different levels. It further strengthens the security of this model. In the medical domain, our cloud based proposed system provides efficient, robust and secure e-health data storage system. This stored data would be helpful for other healthcare professions and allied healthcare professions to further investigation.

References

[1] K. Mand and A. Simpson, "Delegation in a distributed healthcare context: A survey of current approaches," in *Proc. of Information Security Conf. (ISC '06),* S. K. Katsikas et al., eds.(CN '08). 2006.

[2] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," in *Proc. of 14th Int'l Workshop Database and Expert Systems Applications (DEXA).* 2003.

[3] P. Ray and J. Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR," in *Proc. of 28th IEEE EMBS Ann. Int'l Conf*., pp. 4686-4689, 2006.

[4] L. Zhang, G. J. Ahn, and. B. T. Chu, "A rule-based framework for role-based delegation and revocation," *ACM Trans. Information and System Security*, vol. 6, no. 3, pp. 404-441, 2003.

[5] M. Abdalla, E. Kiltz, and G. Neven, "Generalized key delegation for hierarchical identity-based encryption," in *ESORICS'07, LNCS 4734*. New York: Springer, pp. 139–154, 2007.

[6] J. H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," in *Eurocrypt'02, LNCS 2332*. New York: Springer, pp. 83–107, 2002.

[7] A. Boldyrea, A. Palacio, and B. Warinschi. (2003). Secure Proxy signature schemes for delegation of signing rights. Cryptology ePrint Archive, Report. [Online]. Available: http://eprint.iacr.org/2003/096.pdf.

[8] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Eurocrypt '98*, vol. 1403, pp. 127–144, 1998.

[9] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in *IEEE Transaction on Information Theory*, vol. 57, no. 3, pp. 1786–1802, 2011.

[10] S. Hohenberger, G. N. Rothblum, A. Shelat, and V. Vaikuntanathan, "Securely obfuscating re-encryption," in *TCC'07, LNCS 4392*. New York: Springer, pp. 233–252, 2007.

[11] J. Shao, P. Lu, Z. Cao, and G. Wei, "Multi- use unidirectional proxy re-encryption," in *ICC 2011*, Kyoto, Japan, pp. 5-9, 2011.

[12] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *ACM CCS'07*. New York: ACM, pp. 185–194, 2007.

[13] Wiki. (2011). Proxy Re-Encryption Techniques with the security notions protocols and attacks. [Online]. Available: http://en.wikipedia.org/wiki/Proxy_re-encryption.

R. Sumathi received her B.E in Computer Science and Engineering from Regional Engineering college Tiruchirappalli and M.Tech from M.S University, Tirunalveli. She is pursuing her research under Anna University. She is having more than 15 years of teaching experience. Currently she is serving as a professor. She has published nearly 50 research papers in various national/ international conferences /journals. Her research area includes Data mining, Cloud Computing and Network security.

Dr. E. Kirubakaran obtained B.E (Hons.) degree in Mechanical Engineering, M.E. in Computer Science and Ph.D. in Computer from Regional Engineering College, Tiruchirappalli. He has obtained his M.B.A. degree from IGNOU. He has more than 30 years of Industrial experience at Bharat Heavy Electricals Ltd. Tiruchirappalli and presently he is employed as an Additional General Manager at BHEL. He has been a visiting faculty to a number of educational institutions. He had held the posts of Secretary,Vice-Chairman and Chairman of Computer Society of India, Tiruchirappalli. He is a Member of the Syndicate of Bharathidasan University, Member in the Academic Council Anna University, Trichy and Academic Council Anna University, Chennai.