Dual Signature based Privacy and Binding of Medical Data on Cloud

Malik Najmus Saqib, Ahmed Alghamdi

College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

Summary
It is State-of-the-art nowadays to host the Electronic Medical Record (EMR) on the cloud to get benefit from the features of cloud paradigm. Such medical records must guarantee privacy and binding of patient medical information. Access to medical data is provided by the cloud service provider to three entities. These three entities are verifier, medical doctor and researcher for integrity verification, medication, and research purpose, respectively. The level of privacy of EMR for the said three entities should be different. This work will investigate a mechanism for preparing the EMR of each patient before uploading it on the Cloud. The proposed mechanism ensures that each entity can only see the information for which it is intended. This mechanism ensures the privacy of patient medical data from verifier and researcher. Moreover, it also binds the patient identity with patient medication information.

Keywords:
Medical record, Dual Signature, Privacy, binding Security.

1. Introduction

Cloud is considered the norm nowadays to store huge amount of data that can be readily available via Internet from any part of the world. The promising features provided by the cloud attracts many huge applications and businesses. One of such application is the storage and then readily availability of medical data. With the modernization of digital world, the medical data is changed from the paper to electronic form. Nowadays, huge medical data is generated and stored on the Cloud since the Cloud provides cost effective resources and scalable infrastructures on demand that can be access via Internet [1]. It will not only save the data management cost and time of the hospital but also ensure the 24/7 availability of medical record through Internet via secure channels. The privacy issue of such record store on the third-party cloud storage is utmost important. The medical data of the patient is always considered to be a private except from the doctor and the patient him/her selves. However, storing such data on cloud also introduces many privacy issues [2]. For example, who can access the data, what is the level of access etc.

Each EMR consists of two major parts, direct identifier (the patient identity) and sensitive identifier (patient medical information) as shown in Fig. 1.The stored data on cloud can be access/used by a doctor for the medication purposes. A patient can view his/her medical data. The two entities that can access medical data are the researcher and verifier. A researcher should be allowed to access the huge amount of medical data for the research and analysis purpose only. The data on cloud needs to verify in a timely manner to ensure its integrity. For this purpose, cloud service provider give access to the trusted third party called a verifier to check the integrity of medical data. For these two entities the access to medical data should be performed in such a way that it preserves the privacy and integrity of patient record on the Cloud.

This research work proposes the mechanism for the Electronic Medical Record (EMR) of patients to be stored on cloud such that it should preserve the integrity and privacy. In this research work we have shown that how the medical record of patients is constructed and then uploaded on the Cloud so that the researcher and verifier can read only that part of record which is intended for them. The proposed mechanism also ensure that the patient identity is strongly bind with its own medical information. For example, it is detectable by the proposed mechanism if a patient A identity is used with patient B record intentionally or unintentionally.

The aim of the research is to propose a scheme to ensure the privacy of medical record of patient on cloud from the legitimate entities and with minimal overhead with respect to the computation cost. This will develop the trust of hospitals to store medical records on cloud. The proposed scheme will be implemented in java programming language and formally verified using petri nets.

2. Related Work

In [5], researcher has used fog computing environment to sure the private information and data (multimedia like x-rays etc.) in healthcare sector. They proposed authentication key agreement protocol that involve three parties in communication. It is based on bilinear pairing cryptography that is used to generate and distribute the session key among three parties. Eventually, this session key is used for secure communication. They used decoy technique to access and store the data securely.

In [6], researcher proposed access control-based privacy preserving model. It is used for the authentication of both

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.103

users of data and owner of data in a customized proposed environment. The customized environment consists of data owner and users, various entities, and key generation center. Their proposed privacy preserving model has four six phases. The initial setup phase is executed by data owner. The output of this phase is the master key and security parameters. The key generation center then generates a private key, which is saved in the server. This private key is encrypted with the session key. The private data is shred with the data user and end user using the same session key.

Yang et. al., [7] proposed a medical data sharing model for cloud computing. A vertical cross section of medical record is used to ensure various privacy concerns. It consists of four major components. They have implemented a prototype model of the proposed system on large scale medical data.

Fang et. al. [9] has proposed and developed a data access and sharing framework to protect and secure medical data on cloud. In this model data is store and process in the medical data center in the hospital. Then data are sent to trusted server for share it with various medical centers and doctors. In this whole process the privacy matter related to medical data are addressed. Before uploading the medical information about patient doctor and patient adds digital watermarks with their identification.

Keeping the Electronic Medical Record on cloud provide many benefits [4]. Few benefits are listed below

a. No need for healthcare organization to buy the hardware and software to keep the EMRs and no expense on maintaining these components. Hence reducing the cost of keeping the EMRs.
b. Keeping the Electronic Medical Records on cloud make them available 24/7 anywhere from the world.
c. Healthcare organization can transfer the management requirement for EMRs to Cloud service provider. Hence, reducing the management tasks and responsibilities.

Fig 1: Patient record

3. Preliminaries

In this section we described the entities, the requirements of the proposed system and the dual signature process. There are three entities in the proposed system. These entities are categorized based upon their level of access on electronic medical record. the level of their access to Electronic Medical Record is described in section 4. These entities are as follows:

1. Patient and Doctor
2. Verifier
3. Researchers

Patient record is called Electronic Medical Record. It consists of two parts as shown in Fig.1.

1. Direct identifier: it consists of id, name, age, gender and address
2. Sensitive identifier: it consists of medical data of patient. E.g., prescriptions, diagnostics, test reposts and etc.

3.1 Requirements

This subsection describes the requirements with their definition that are desirable in securing electronic medical record on Cloud. These requirements are as follows:

1) Security: the Electronic Medical Record is secure against any illegal attempt to read or modify it. Only the legitimate entities can access the electronic medical record
2) Privacy: the intended entities can read only that part of medical record for which they are prescribed.
3) Authenticity: only the legitimate entities can access the medical record from cloud

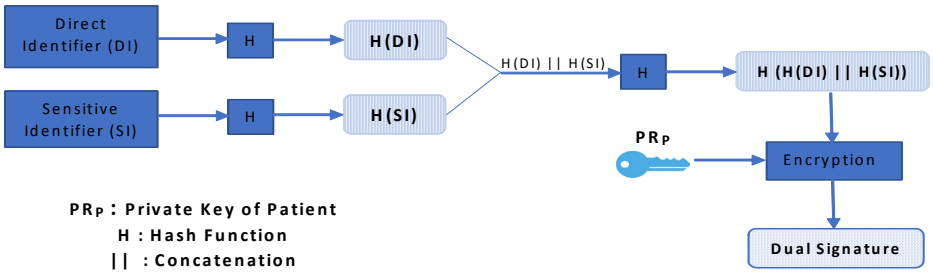

Fig 2: Dual Signature

3.2 Dual Signature

Dual signature (as shown in Fig. 2) is used in the Secure Electronic Transaction (SET) that is used to make a secure electronic credit card transaction on the Internet. This research work uses dual signature to ensure the integrity and privacy of medical record stored on cloud. Figure 1 shows various components of dual signature and its creation process.
First it calculates the hash of Direct Identifier and Sensitive Identifier separately. Then concatenate these two hashes and calculate the final hash of this concatenated hashes. In the end sign the final hash with the private key of the patient.

4. Dual Signature based Secure medical Record

This section discusses the dual signature based secure medical record construction, protocol and its implementation. The medical record can be categorized as direct identifier and sensitive identifier [3]. Direct identifier includes patient id, name, phone number, date of birth and etc. While sensitive identifier (medical data) includes sensitive attribute like patient age, tests report, diseases and codes and etc. as shown in figure 1. Such medical record of patients is uploaded on cloud.

The researcher should be able to access/read the sensitive identifier of patient without knowing direct identifier. The verifier should not be able to read the sensitive information and can access the direct identifiers.

4.1 System architecture

There are three entities in the system that are categorized based upon their level of access on medical record of patient.

1. Patient/ Doctor: can see the direct and sensitive identifiers
2. Verifier: can only see the direct identifier if require for example to ensure that a record of a patient is present and intact. It cannot see the sensitive identifier at all.
3. Researcher: can access/see the sensitive identifier only for the sake of research via legitimate access. Researcher cannot read the direct identifier. However, they can see the sensitive attributes that can be used for the research purposes.

4.2 Requirements

Following are the requirement of the proposed system for the privacy of medical record of a patient.

1. Medical doctor of a patient can see/examine the direct and sensitive identifier of patients.
2. A Patient can see his/her direct and sensitive identifier.
3. The integrity of each medical record on cloud storage should be verifiable by a trusted third party called a verifier. Verifier can only see the patient direct identifier.
4. The direct identifier of each patient record is tightly tied up with its corresponding sensitive attribute. It is not possible for any entity to merge the direct identifier of one patient record with the sensitive information of other and vice versa. Any such manipulation should be detectable.
5. The researcher all around the world via legitimate access can read the sensitive identifier but cannot read the direct identifier of patient records. The purpose of this access is to use the collection of sensitive attributes for research purposes. The identity of patient should be hidden from the researchers.
6. Data hosting service provider (cloud) or Health Administration can only see Patient ID in plaintext and his/her medical record in encrypted form.

Table 1: Tables of Symbols

Symbols	***Meaning***
DS	Dual Signature
DI	Direct identifier
SI	Sensitive Identifier
H, Hash	Hash
PU_V, PR_V	public and private key of verifier
PU_R, PR_R	public and private key of researcher
PU_P, PR_P	public and private key of doctor
K_V	Symmetric key share between cloud and verifier
K_R	Symmetric key share between cloud and researcher

4.3 Dual Signature based medical record

Dual signature is a simple process that is used to provide the privacy and security of medical record. The patient when visit the hospital for the first time is required to perform the registration process. In this process the direct identifier (id, name, phone number, date of birth) related information about the patient is collected. Fig. 3 shows the complete process of creating, storing and verifying the medical record.
Let DI and SI are the direct and sensitive information respectively see Fig. 2. The Dual Signature (DS) can be calculated as

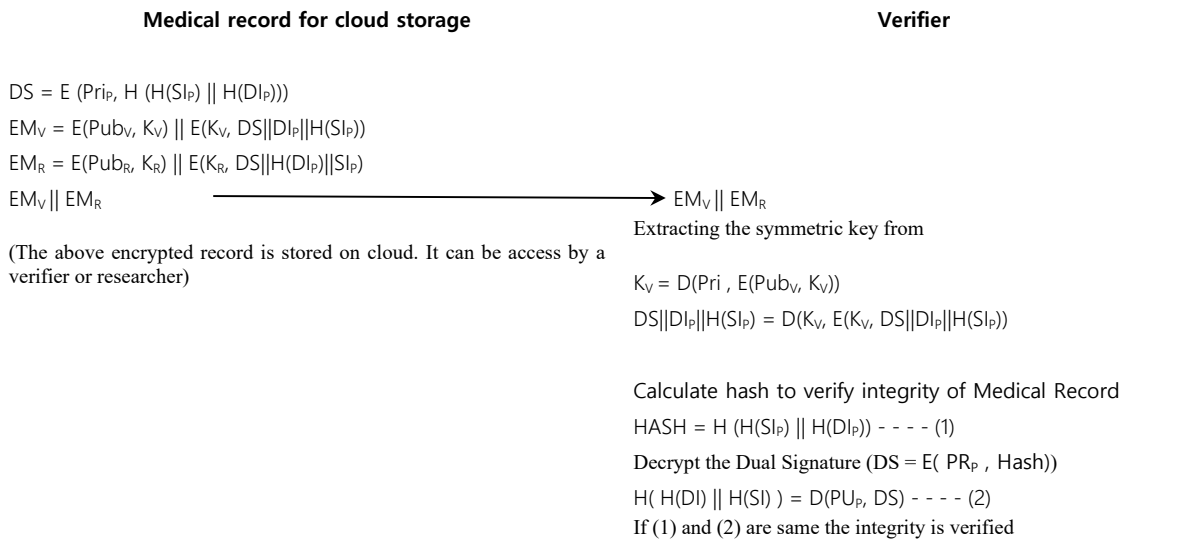

Fig.3: Process of creating, storing, and verifying medical record

$$Hash = H(H(DI) \| H(SI))$$
$$DS = E(PR_P , Hash)$$

where H is the hash function, PR_P is the private key of patient and E is the encryption function. Dual Signature is generated by encrypting the concatenated hash of DI and SI with the private key of patient.

Preparing Medical Record for cloud storage

Following encrypted information is a medical record of one patient on the cloud

$$DS||DI_P||SI_P$$

From the above stored record, the cloud will prepare the following messages for the verifier to verify the integrity of medical data of patient.

$$EM_V = E(PU_V, K_V) \| E(K_V, DS||DI_P||H(SI_P))$$

K_V is the symmetric key that is encrypted by the public key of verifier. The other data in the message is encrypted with the symmetric key K_V.
Similarly, from the stored record, the cloud will prepare the following message for the researcher to use medical data for research purpose without knowing the identify of patient.

$$EM_R = E(PU_R, K_R) \| E(K_R, DS||H(DI_P)||SI_P)$$

The patient record Sensitive identifier can be update/modify any time when a patient visits the hospital. So EM_V and EM_R will be prepare by the cloud as needed by verifier and researcher. K_R is the symmetric key that is encrypted by the public key of researcher. The other data in the message is encrypted with the symmetric key K_R.

Verification by verifier

The verifier receives the following message from the cloud to verify the integrity of patient records.

$$EM_V = E(PU_V, K_V) \| E(K_V, DS||DI_P||H(SI_P))$$

It will decrypt the first part of the message using its private key, to obtain a symmetric key K_V.

$$K_V = D(PR_V, E(PU_V, K_V))$$

Then it will use that symmetric key K_V to decrypt the second part of the received message.

$$DS||DI_P||H(SI_P) = D (K_V, E(K_V, DS||DI_P||H(SI_P))$$

Now the verifier starts the verification process to ensure the integrity of the patient record. It will calculate the hash of DI_P. Then combined hash as follow:

$$Hash' = H (H(SI_P) \| H(DI_P))$$

Now, it will decrypt the Dual Signature DS

$$Hash = D (PU_P , DS)$$

Now a comparison is performed between Hash and Hash' values. If both are same patient record integrity is intact otherwise not.

Researcher

A researcher uses medical data only for the research purpose. Before using the sensitive identifier of a patient for research purposes, the researcher will ensure the integrity of patient record without knowing the direct identifier. Researcher receives the following message from the cloud.

$$EM_R = E(PU_R, K_R) \,||\, E(K_R, DS||H(DI_P)||SI_P)$$

After receiving the above message, the researcher first decrypts the first part of message, using its private key, to get the symmetric key as follow:

$$K_R = D(PR_R, E(PU_R, K_R))$$

the symmetric key K_R is used to decrypt the second part of received message as follows

$$DS||H(DI_P)||SI_P = D\,(K_R, E(K_R, DS||H(DI_P)||SI_P)$$

The verification process is as follow

1. Compute the hash of SI_P.
2. Compute the hash of both $H(DI_P)$ and $H(SI_P)$ as follows

$$Hash' = H\,(H(DI_P) \,||\, H(SI_P))$$

Now the Dual signature will be decrypted

$$Hash = D\,(\,PU_P\,,\,DS)$$

Now the two hashes are compared. If they are same the integrity is intact otherwise not.

5. Discussion

The verifier and researcher both are given access to medical records. Following type of attack can be launches by malicious user (which can be researcher and verifier)

1. Changing the bits of DI or SI randomly with intention to manipulate the record unintelligently.
2. Trying to exchange the DI or SI with some other patient medical record.

In both above cases the malicious user has to produce the dual signature such that the changes by the malicious user will be undetectable. And this is not possible as malicious user cannot access private key that is used to produced dual signatures.

Its optional for researcher to verify the integrity of the medical record before using sensitive information. This research proposed to use the dual signature on Patient ID (PID) and its Medical Data (MD). The use of dual signature addresses the requirements no 3, 4 and 5 in section 4.2.

6. Conclusion

This research work focuses on the privacy of the medical record for each patient that is store on the cloud. It proposes a model that ensure the privacy of patient medical record at different level from various entities. A dual signature-based approach is used to ensure the integrity of medical record of patient. It not only ensures that any modification is detectable but also it tightly bound the patient information with its medical record. With this approach it is not possible to attach direct identifier of one patient with another patient.

Acknowledgments

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-08-18-DR). The authors, therefore, acknowledge with thanks the University of Jeddah technical and financial support.

References

[1] M. Peter and G. Tim, The NIST Definition of Cloud Computing, NIST 2009

[2] Q. Lin, A. Srinivasan, J. Hu and G. Wang, “Preface: Security and Privacy in big data cloud”, Future Generation Computer System, Elsevier, vol. 72, July 2017, pp 206-207

[3] A. G. Divanis, G. Loukides, “Publishing data from electronic health records while preserving privacy: A survey of algorithms”, Journal of Biomedical Informatics, Elsevier, Vol 50, 2017, pp 4-19

[4] Abbas, Assad. (2016). e-Health Cloud: Privacy Concerns and Mitigation Strategies. 10.1007/978-3-319-23633-9_15.

[5] Thilakanathan, D., Chen, S., Nepal, S., Calvo, R., Alem, L.: A platform for secure monitoring and sharing of generic health data in the cloud. Future Gener. Comput. Syst. 35, 102–113 (2014)

[6] Hadeal Abdulaziz, Mizanur Rahman, et. al., A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography, IEEE Access, Sept 23 2017.

[7] K. Anand, A. Vijayaraj, M. Vijay Anand, "Privacy preserving framework using Gaussian mutation based firebug optimization in cloud computing", The Journal of Supercomputing, 2022.

[8] Yang, J., Li, J., Nui Y., A hybrid solution for privacy preserving medical data sharing in the cloud environment, Future Generation Computing, Vol 43-44, pp 74-86, Feb 2015.

[9] Fang, L., Yin, C., et. al., Privacy Protection for Medical Data Sharing in Smart Healthcare, ACM Transaction on Multimedia Computing, Communication and Applications, Volume 16, Issue 3s Oct 2020