A Study on Secure Electronic Medical DB System in Hospital Environment

Yvette E. Gelogo[1] and Sungwon Park[2]*

[1]*Catholic University of Daegu, Daegu, Korea*
[2]*Department of Nursing,*
Hannam University, 133 Ojeong-dong, Daeduk-gu, Daejeon, Korea

**Correspondent Author: Sungwon Park* (sunwon@hnu.kr)*

Abstract

The medical information is very important, nowadays internet-based system deployment is used in medical field due to advantages it has to offer. All the information like patient test results, diagnosis and others are stored in the database. In this paper we discuss an internet-based medical record system and proposed a security mechanism on how to secure the retrieving of the data in the database. Here we use a cryptographic scheme to authenticate the users and give them the right to access base on their function and give the information as response to their query but limited to the scope of their privileges. In this paper we give the very simple authentication method yet, effective and easy to implement. There are two authentication methods, first is the authentication to access the system and second is the authentication to access the data.

Keywords: *Medical records, cryptography, database, Hospital Environment*

1. Introduction

Medical records are very important information that if sabotage can threat the patient health findings. For example, the intruder or Bad guy have a bad intention to the patient, so one way to execute his plan is to access the medical records of the patient and modify it, replacing the previous or existing findings/records of the patient with the different information that could harm the patient if the Physician administers the modified diagnosis. By modifying the records of the patient, the Bad guy can trick the Physician by putting different diagnosis.

The medical information is stored in the database for future referral of the patient health status or health history. The records can be used in the future medical diagnosis of the patient. The previous findings can be used to trace up the history of the health status and medication that the patient have been through. In this way the Physician has the guide in his/her medical analysis. If not secured the Bad guy can modify the medical record of the patient and this will lead to wrong diagnosis.

Who are the authorized users who can access the medical records of the patient? These people are the Physician, Nurse, Secretaries, System Administrator and Database Administrator. How to implement the security system on the records? Basically the database where the medical information is being stored needed to be secured. In this paper, we tackle the security implementation in the database where the medical records are being stored.

The content of the paper are as follows: Section 2, the Background, here we discussed the related information about the medical records and the background technology. Section 3 is the

design of the web-based medical records. Section 4 is the proposed security and discussion. And the last section is the conclusion.

2. Background

Nowadays, the used of the internet is very essential in our daily transactions. Almost everything rely on the use of the internet, like business, education, security and others are using internet as the main medium to deliver information. Now, medical field is also adopting the use of IT. We used internet-based because this is the best way to deploy the system which can be access anytime, anywhere via internet. This practice is very helpful for the Physician to access the previous medical history of the patient that they are handling. In this case they have the background, and this could help them in their analysis.

Since these medical records is stored in the database and can be access through internet, distance and time in not a consideration.

2.1 Internet-based architecture

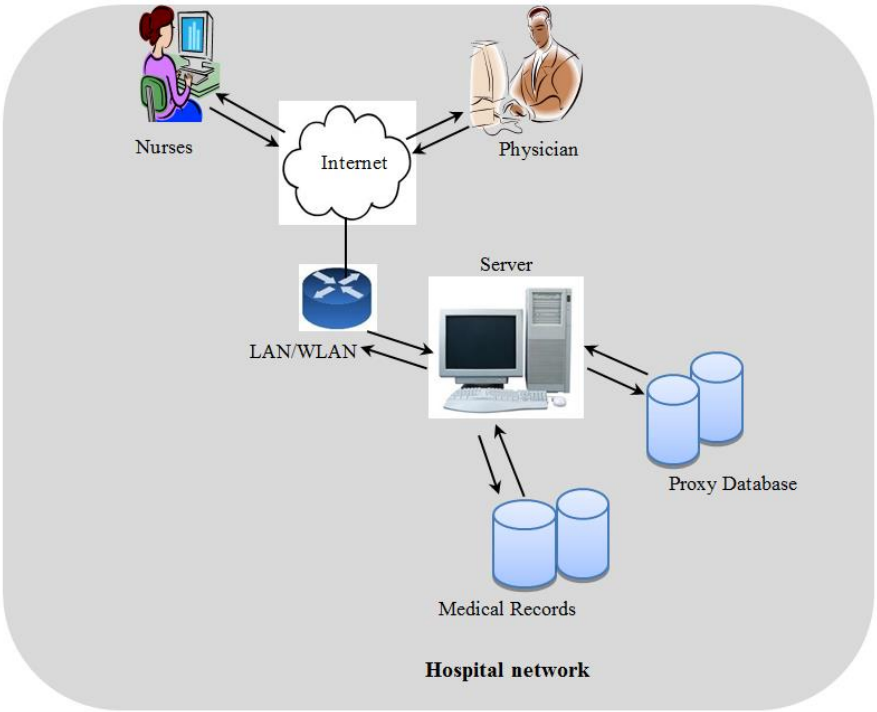

Figure 1. Internet-based medical records database overview

Figure 1 illustrates the internet-based medical record access of both patients the Physician. The information can be access through PC, mobile phone and other internet enabled devices via internet.

When a user proxy database is created, metadata for the proxy tables is imported automatically from the remote location that contains the actual tables. This metadata is then used to create proxy tables within the proxy database.

2.2 Entities

Doctor: has access to the data of his own patients, but not to the patients of another doctor.

Nurse: has access to the patient information of patients she is responsible for.

Secretary: has access to (for example) insurance information, or name and home address, of the patients of all doctors within the department.

System Administrator: responsible for taking care of the operation and/or maintenance of the system. The system administrator has access to all physical machines. He should not have access to any patient information.

Database Administrator: administers and maintains the database itself and therefore has access to the database. In a system where the database is in the hospital, this person may be the same as the system administrator. He should not have access to any patient information.

Hacker: tries to hack into the system in any way possible.

2.3 Dataset

There are primary datasets, these are datasets of patient, the doctor/nurses/ and others, the result and the diagnosis. These datasets are represented in separate tables.

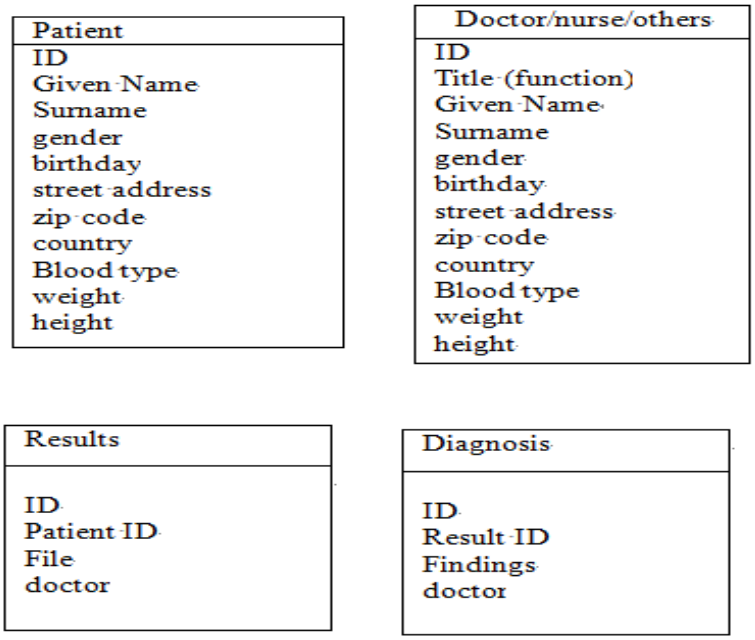

Figure 2. Main Dataset

3. Cryptography

Applying the use of cryptographic scheme is very important, since the direct access in medical records is very crucial and need to be taken care of.

3.1. Digital Signatures

To ensure that no one know the content of the message sent from database to the user, that is no modification done, digital signatures can be a good security. This will allow authentication for both sides of the communication. Digital signatures reduce amount of computation involved unlike public cryptography that computationally intensive. Digital signatures depend on hash functions. The size of the output depends on the algorithm, typically between 100 and 200 bits. It is difficult to forge; it's like a human fingerprint.
Digital Signature computed this way:

1. Compute a hash of the message.
2. Encrypt the hash with her private key, and include the encrypted hash in the message sent to the user.
3. When user receives the message, he perform step 1.
4. User decrypts the encrypted hash using patient's public key. If he gets the same value as produced by step 3, then he knows that the message was not modified en route and that it came from database.

3.2. Certificates

Public key certificate is digitally signed statement by a trusted entity. Certificate Authority (CA) is a trusted entity, the certificate is signed by the CA's private key and certificates bind an identifier to a public key. The identifier can be a person, organization, email address or an IP address. The widely used public key certificate today is X.509 standard. X.509 is being used by several protocols, including Privacy Extended Mail, Secure Socket Layer, Secure HTTP, and Public Key Cryptography Standard.

3.3. Hash Functions, Message Digest and Message Authentication Codes

Hash functions and message digest is a one-way hash function. The output of this function is random, with approximately half bits set to the opposite values of the other half. Changing one bit of an input should result in a completely different output. It is very hard to find the message that produces the same output that is what makes hash function secure.

A hash function takes a variable-size input and produces a fixed-sized output. Given this fact it is clear that there is infinity of messages that, when hashed, could produce the same output. If the size is too small, then it will be easy to try all the possible values that will produce an output. Suppose the size is 32 bits, this means that one would need to try approximately 2^{32} different messages to produce a particular output. This means that there would be 2^{32} different guesses of message in order to find the right one to produce the same output.

The most commonly used hash functions are the Secure Hash Algorithm (SHA-1) and MD5 (Message Digest), which have an output of 128 bit or more.

In this paper, we use the combination of the above mentioned cryptographic schemes.

4. Security Architecture

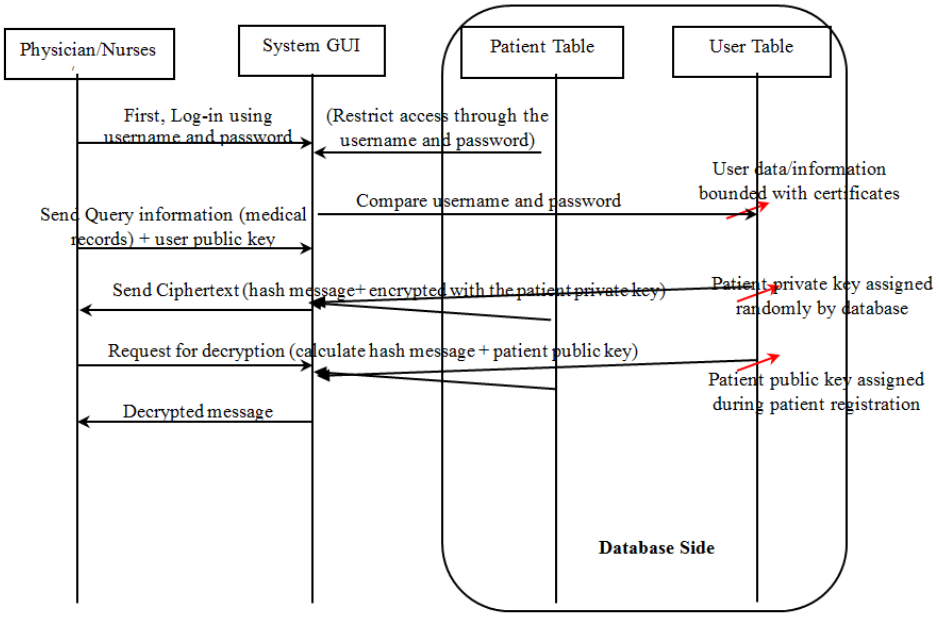

Figure 3. Flow of the proposed security

Figure 3 illustrates the flow of how the User (physicians, nurses, secretaries, database administrator) accesses the medical records of the patient and the process of the authentication.

At start the User access the system by logging in with the username and password. This means that before the User can log-in in the system, he/she must register first in the system. In the registration process, this is the time where all the information about the User is being stored in the system. The User information is stored in different table separate from the patient's information. This means that during the registration process, the restriction and the access rights on the user are already set. So every time they access the system, the database automatically return the only possible data that they can access.

Plus of course, to verify the identity on the user, there is a secret key that need to be used to authenticate. When the entity sends a query message, the database will send the ciphertext to the User. This ciphertext was encrypted by the patient private key. The message is decrypted through the patient private key. The patient private key was pre-assigned, which was randomly generated when the patient account was created. The User Public key was pre-assigned through certified authority (CA). As you can see, the User that want to access the data will have to undergo two authentication processes, first the use of the username and password to access the system and next is the use of the key to decrypt the encrypted information.

To simplify, this is the encryption and decryption process:

1. Compute the hash message
2. Encrypt the hash message with the private key of the patient and send it to the User through the system.

3. When user receives the message, he perform step 1.
4. The User will request for decryption using the system.
5. The system will compute the hash message using the patient public key. If it returns the same value with the step one, it means the data was not modified en route.

5. Conclusion

There is a need to secure the medical records of the patient with the internet based system. The use of Internet technologies for remote access to medical records is undoubtedly a convenient way of sharing patient information within and between healthcare facilities. The security measures, in our opinion, are adequate for permitting access only to authorized users without compromising the confidentiality of medical records.

In this paper we proposed a secured medical record system. In order to have verify the user and give them the right permission to access the records, used the two authentication method. First is the permission to access the system then the permission to access the medical records. The restrictions on the access of the medical records are based on the specified rights of the user. For example, physician can access this kind of information and the nurses can only access limited information. The physician access rights are depending on the patient's key. Patients key signify the patients identity and the physician that is allowed to access the patient's information. This physician could be the one who is treating the patient and of course the nurse in charge.

Acknowledgements

This paper has been supported by the 2013 Hannam University Research Fund.

References

[1] E. Lastdrager, "Securing Patient Information in Medical Databases", MS Thesis, **(2011)** August.
[2] S. Mohammed and J. Fiaidhi, "Ubiquitous Health and Medical Informatics: The Ubiquity 2.0 Trend and Beyond", Medical Information Science Reference, ISBN 978-1-61520-777-0, **(2010)**.
[3] T. D. Gunter and N. P. Terry, "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions", in J. Med Internet Res., vol. 7, no. 1, **(2005)**.
[4] S. Silverstein, "2009 a pivotal year in healthcare IT", Drexel University, **(2009)**.
[5] L. Dunlop, "Electronic Health Records: Interoperability Challenges and Patient's Right for Privacy", Shidler Journal of Computer and Technology, vol. 3, no. 16, **(2007)**, http://www.law.washington.edu/WJLTA/Issues/3/3/8.