CENTRALIZED AVAILABILITY ASSURANCE FOR DISTRIBUTED ELECTRONIC MEDICAL RECORD DATA

[1]YB DWI SETIANTO, [2]SHINTA ESTRI WAHYUNINGRUM
[1]Faculty of Engineering, Surakarta Christian University, INDONESIA
[2]Faculty of Computer Science, Soegijapranata Catholic University, INDONESIA
E-mail: [1]admin@uks.ac.id , [2]shinta.she@gmail.com

ABSTRACT

Many developed countries have started to adopt Electronic Medical Records (EMR) to improve their health care system. In the implementation of EMR, security and privacy factors are of great concern, and one of the main aspects of access security assurances is the assurance of data availability when they are needed. Thus, it is very important to be able to provide a valid EMR data availability assurance for the patients when it is needed. However, in our country, nationally centralized availability assurances have not been available yet. This paper proposed a system of centralized EMR data availability assurance utilizing the checksum data generated from the hash function.

Keywords: *Electronic Medical Record, Security ,Availability Assurance, Health Network*

1. INTRODUCTION

Electronic Medical Records (EMR) is a new form of Medical Records that many developed countries have adopted to improve their health care system. Although security and privacy factors are of great concern in the implementation of EMR[1,2], the majority of the patients and doctors believe that the benefits of the using of EMR are greater than the security risks that may occur[9].

The security factors being concerned in the implementation of EMR can be classified into two categories. The first category is the transmission security, and the second category is the access security [4], and one of the main aspects of access security assurances is the assurance of data availability when they are needed. Thus, providing a valid EMR data availability assurance for the patients when it is needed is very important.

In Indonesia, EMR implementations are generally centralized in health facilities or hospitals. They have not been nationally integrated [5,10]. While in some developed countries, the implementations of the national EMR generally adopt a distributed system [3,5,6,7,8] the data availability assurance are handled by each health facilities providing EMR service.

This paper proposed a system of centralized EMR data availability assurance utilizing the checksum data generated from the hash function.

2. EXISTING APPROACH

The existing concept of data availability assurance has more concentration on saving the data indirectly, by ensuring the availability of hardware and software systems where the data are stored. It has nothing to do with the data [3,5,6,7,8], and it is done locally by each health facility.

The data protection coverage existing now only includes data protection from those who are not authorized and authenticated, and those who are authorized and authenticated are generally only provided with the activity log that are stored locally [3,5,6,7,8].

The absence of the national centralized assurance, make it possible for any health care institution, a hospital or a private doctor’s office to do a massive and illegal EMR data changings.

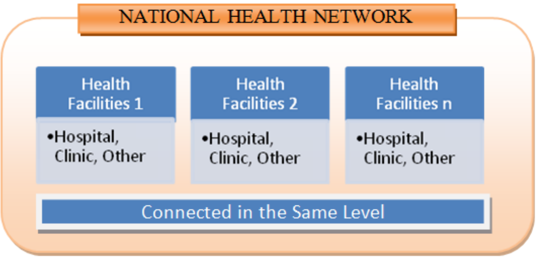

Figure 1: Existing Approach

3. PROPOSED APPROACH

Checksum is a sample of data that can represent the data. Any significant change in the data will result in a change in the checksum. The basic idea of the centralized data assurance is to utilize the checksum data as the assurance.

In this the centralized data availability assurance model, a centralized database that stores the EMR checksum of the EMR Data (EMRD) in each health facility severs is built. This centralized checksum database also serves as an index of all the EMR data existing. In addition to its function as the index server, this component will also serve as an Authentication, Authorization, and Accounting (AAA) server. The server will have a record of the EMR activity in EMRD server. It means that all doctors and patients involved in all EMR data server should be registered in this server. In this model, the server is hereinafter referred to as AAAIDX server.

AAAIDX will periodically request data changes checksum reports (insert, update, delete) that occurs at EMRD server. AAAIDX server technically also entitled to request the patients' EMR data in EMRD sever.

With this system, patients will get assurances from their AAAIDX that their EMR data won't be changed illegally in EMRD, since any illegal change would cause a mismatch data checksum, and any activity of the EMR data are recorded in AAAIDX server. Patients will also get assurances that whenever they need their EMR data, they can request it through AAAIDX, because in this system protocol EMRD server shall answer any data request from the AAIDX server. AAAIDX do not have the authority to change the patient's EMR data. It only maintains the integrity and availability of the data.

Since AAAIDX functions are strategic and vital, in this system AAAIDX server is designed to be managed by an organization/ government institutions that are independent and reliable.text

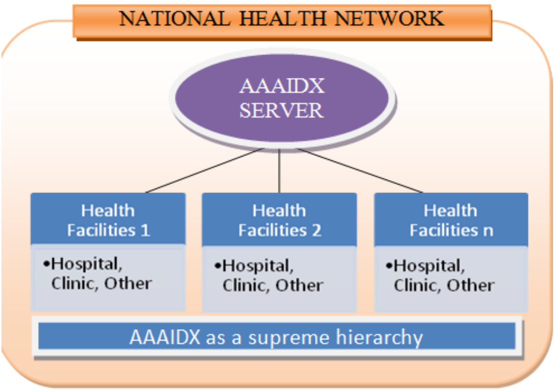

Figure 2: Proposed Approach

4. TECHNICAL IMPLEMENTATION

Basic communications protocol used in the system is the Hyper Text Transfer Protocol Secure (HTTPS), this basic communication protocol is the minimum standard in EMR implementation according to HIPAA standards [11].

The format of data objects used in communicating is the JSON format (Java Script Object Notation).This data communication format is well known for it is light and widely used.

In the centralized assurance system, there are three main activities, namely periodic checksum reporting process, the data request process, and data changes reporting process..

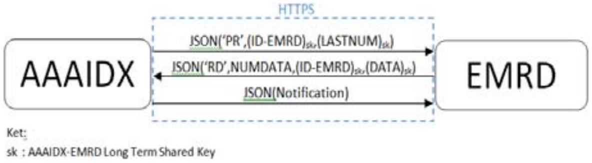
HTTPS
AAAIDX
EMRD
JSON('PR',(ID-EMRD)sk,(LASTNUM)sk)
JSON('RD',NUMDATA,(ID-EMRD)sk,(DATA)sk)
JSON(Notification)
Ket:
sk : AAAIDX-EMRD Long Term Shared Key

Figure 3: Push Index & Checksum Report

Push Index & Checksums Report Process is a procedure that will be performed regularly by AAAIDX, this process is an order the EMRD to give latest data checksum (if any) with the data number after LASTNUM. EMRD will respond by providing the latest data checksum (if any) according to the specified format

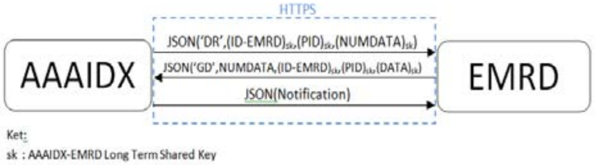
HTTPS
AAAIDX
EMRD
JSON('DR',$(ID\text{-}EMRD)_{sk}$,$(PID)_{sk}$,$(NUMDATA)_{sk}$)
JSON('GD',NUMDATA,$(ID\text{-}EMRD)_{sk}$,$(PID)_{sk}$,$(DATA)_{sk}$)
JSON(Notification)
Ket:
sk : AAAIDX-EMRD Long Term Shared Key

Figure 4: Data Request

Data Request Process is a data request procedure performed by AAAIDX, this process is a command to EMRD to provide the latest EMR data as many as the NUMDATA of the patient with ID = PID. EMRD will respond by providing the latest data as many as the NUMDATA according to the format specified.

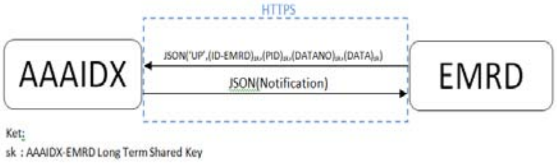
HTTPS
AAAIDX
EMRD
JSON('UP',$(ID\text{-}EMRD)_{sk}$,$(PID)_{sk}$,$(DATANO)_{sk}$,$(DATA)_{sk}$)
JSON(Notification)
Ket:
sk : AAAIDX-EMRD Long Term Shared Key

Figure 5: Update Data Report

Update Data Report process is a data changing notification procedure made by EMRD. This process is a notification to the AAAIDX to change the EMR data of the PID patients with the number DATANO. AAAIDX will respond by changing the requested data.

5. FUTURE WORK

The future work that will be done to the centralized EMR data availability assurance model is to design the implementations protocol in more details to accommodate the variety of system platforms that are already exist in EMRD and also to design the regulation to protect the implementation.

6. ACKNOWLEGMENT

This research was funded by the General Directorate of Higher Education, Indonesian Ministry of Education, on the scheme of Competitive Grants Research 2015.

REFRENCES:

[1] Benaloh, Josh., Chase, Melissa., Horvitz, Eric., Lauter, Kristin. "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Record". CCSW'09, Chicago, Illinois, USA. 2009. ACM 978-1-60558-784-4.

[2] Carman, David and Britten, Nicky. "Confidentiality of Medical Records: The Patient's Perspective". British Journal of General Practise. 1995, 45, 485-488.

[3] Cimino, James J., Patel, Vimla L., Kushniruk, Andre W. "The Patient Clinical Information System (PatCIS) : Technical Solution for and Experience With Giving Patients Access to Their Electronic Medical Records". International Journal of Medical Informatics 68. 2002. 113-127.

[4] Khan, Stasia and Sheshadri, Vikram. "Medical Record Privacy and Security in a Digital Environment". IT Professional Vol. 10, No. 2 March/April 2008. IEEE Computer Society 1520-9209.

[5] Kurniati, Angelina Prima. "Indonesian e-Health Management System Prototype". Competitive Grants Research's Final Report. 2012. Telkom Institue of Technology. Bandung

[6] Ludwick, D.A. dan Doucette, Jhon. "Adopting electronic medical records in primary care: Lessons learned from health information systems implementation experience in seven countries". International Journal of Medical Informatics 78 (2009) 22–31.

[7] Protti, Denis and Bowden, Tom. "Electronic Medical Record Adoption in New Zealand Primary Care Physician Offices". Issues in International Health Policy, Commonwealth Fun Pub 1434. 2010. Vol 36.

[8] Ralston, James D., Carrell, David., Reid, Robert., Anderson, Melissa., Moran, Maureena., Hereford, James. "Patient Web Service Integrated With a Shared Medical Record : Patient Use and Satisfaction". Journal of American Medical Informatics Association Volume 14 Number 6 Nov / Dec 2007.

[9] Perera G, Holbrook A, Thabane L, Foster G, Willison DJ. "Views On Health Information Sharing And Privacy From Primary Care Practices Using Electronic Medical Records". International Journal of Medical Informatics, 2011 Feb;80(2):94-101. doi: 10.1016/j.ijmedinf.2010.11.005. Epub 2010 Dec 16

[10] Setianto, Y. B Dwi., Utami, YRW. "A new patients' rights oriented model of EMR access security". International Conference on Advanced Computer Science and Information Systems (ICACSIS), 18-19 Oct. 2014, 19 – 24

[11] Departement of Health & Human Service - USA. "HIPAA Security Guidance" .http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf on 10 Jun 2015