A Novel Mechanism for Building an Emphatic System for Information Exchange using CDA

Mohammed aamir1, Giridharan2, Kavitha3
Student1,2, Assistant Professor3
Department of CSE
Dhaanish Ahmed College of Engineering, Chennai, India

Abstract:
Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The user pays fee depending on the amount of resources allocated, such as network, server, storage, applications and services. Successful deployment of Electronic Health Record helps improve patient safety and quality of care, but it has the prerequisite of interoperability between Health Information Exchange at different hospitals. The Clinical Document Architecture (CDA) is a core document standard to ensure such interoperability, and propagation of this document format is critical for interoperability. A problem arises even when more hospitals start using the CDA document format because the data scattered in different documents are hard to manage. Our CDA document integration system integrates multiple CDA documents per patient into a single CDA document and physicians and patients can browse the clinical data in chronological order.

Keywords: CDA, EHR.

I. INTRODUCTION

ELECTRONIC Health Record (EHR) is longitudinal collection of electronic health information for and about persons, where health information is defined as information pertaining to the health of an individual or health care provided to an individual and it can support of efficient processes for health care delivery [1]. In order to ensure successful an operation of EHR, a Health Information Exchange (HIE) system need to be implemented [2]. However, most of the HIS in service have different characteristics and are mutually incompatible [3], [4]. Hence, effective health information exchange needs to be standardized for interoperable health information exchange between hospitals. Especially, clinical document standardization lies at the core of guaranteeing interoperability. Health Level Seven has established CDA as a major standard for clinical documents [5]. CDA is a document markup standard that specifies the structure and semantics of ’clinical documents’ for the purpose of exchange. The first version of CDA was developed in 2001 and Release 2 came out in 2005 [6]. Many projects adopting CDA have been successfully completed in many countries [7], [8], [9]. Active works are being done on improving semantic interoperability based on openEHR and CEN13606 [10], [11]. To establish confidence in HIE interoperability, more HIS’s need to support CDA. However, the structure of CDA is very complex and the production of correct CDA document is hard to achieve without deep understanding of the CDA standard and sufficient experience with it. In addition, the HIS development platforms for hospitals vary so greatly that generation of CDA documents in each hospital invariably requires a separate CDA generation system. Also, hospitals are very reluctant to adopt a new system unless it is absolutely necessary for provision of care. As a result, the adoption rate of EHR is very low except for in a few handful countries such as New Zealand or Australia [12]. In the USA, the government implemented an incentive program called the Meaningful Use Program to promote EHR adoption among hospitals when a patient is diagnosed at a clinic, a CDA document recording the diagnosis is generated. The CDA document can be shared with other clinics if the patient agrees. The concept of family doctor does not exist in Korea, hence it is common for a patient to visit a number of different clinics. The exchange of CDA document is triggered in the following cases: when a physician needs to study a patient’s medical history; when referral and reply letters are drafted for a patient cared by multiple clinics; when patient is in emergency and the medical history needs to be reviewed. It takes increasing amount of time for the medical personnel as the amount of exchanged CDA document increases because more documents means that data are distributed in different documents. This significantly delays the medical personnel in making decisions. Hence, when all of the CDA documents are integrated into a single document, the medical personnel is empowered to review the patient’s clinical history conveniently in chronological order.

ILRELATED WORK

The HL7 Clinical Document Architecture Release 2 (CDA R2) was approved by American Nation Standards Institute in May 2005. It is an XML-based document markup standard that specifies the structure and semantics of clinical documents, and its primary purpose is facilitating clinical document exchanges between heterogeneous software systems. A CDA document is divided into its header and body. The header has a clearly defined structure and it includes information about the patient, hospital, physician, etc. The body is more flexible than the header and contains various clinical data. Each piece of clinical data is allocated a section and given a code as defined in the Logical Observation Identifiers Names and Codes (LOINC) [15]. Different subcategories are inserted in a CDA document.
depending on the purpose of the document, and we chose the Continuity of Care Document (CCD) [16] because it contains the health summary data for the patient and it is also widely used for interoperability.

For the integrated CDA document, we chose the Korean Standard for CDA Referral and Reply Letters (Preliminary Version) format as the number of clinical documents generated when patients are referred and replies made, is large. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services [19]. The user pays fee depending on the amount of resources allocated, such as network, server, storage, applications and services. Currently, three major types of cloud computing service exist.

II. PROBLEM FORMULATION

Hospitals have to purchase propriety software to generate and integrate CDA documents and bear the cost as before. Service is not applicable to various developer platforms. CDA template is available in existing then in existing we are going to parse the CDA document in future from one hospital to another hospital in sequential order.

IV. EXISTING SYSTEM

The concept of family doctor does not exist in existing system, hence it is common for a patient to visit a number of different clinics. The exchange of CDA document is triggered in the following cases, when a physician needs to study a patient’s medical history, when referral and reply letters are drafted for a patient cared by multiple clinics, when a patient is in emergency and the medical history needs to be reviewed. It takes increasing amount of time for the medical personnel as the amount of exchanged CDA document increases because more documents means that data are distributed in different documents. This significantly delays the medical personnel in making decisions. Hospitals have to purchase propriety software to generate and integrate CDA documents and bear the cost as before. Service is not applicable to various developer platforms.

V. PROPOSED SYSTEM

In our proposed system all of the CDA documents are integrated into a single document, the medical personnel is empowered to review the patient’s clinical history conveniently in chronological order per clinical section and the follow up care service can be delivered more effectively. In our proposed method a CDA document generation system that generates CDA documents on different developing platforms and a CDA document integration system that integrates multiple CDA documents scattered in different hospitals for each patient. Our cloud computing based CDA generation and integration system has a few pronounced advantages over other existing projects. First, hospitals do not have to purchase propriety software to generate and integrate CDA documents and bear the cost as before. Second, our service is readily applicable to various developer platforms because an Open API is to drive our CDA document generation and integration system. Regardless of the type of the platform, CDA documents can be easily generated to support interoperability.

VI. ARCHITECTURE

Figure 1: User registration

Figure 2: Architecture

VII. ALGORITHM

HASH BASED MESSAGE AUTHENTICATION CODE

It is a specific type message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. It may be used to verify both the data integrity, and the message authentication. Cryptographic hash function such as MD5 and SHA-1 and may be used as a HMAC the resulting algorithm such as MD5 or HMAC. The strength of HMAC based on underlying cryptographic strength based on size of key. The iterative hash function breaks up a message into a blocks of a fixed size and a compression function. For example, MD5 and SHA-1 operate on 512 bit blocks. The output of the HMAC same as the underlying hash function.

\[
\text{HMAC}(K,m) = H((K^1 \oplus \text{opad}) \Vert H((K^2 \oplus \text{opad}) \Vert m))
\]

Where H is a cryptographic hash function then K is the secret key M is the message authentication, K^1 is the secret key opad is the outer padding.
IMPLEMENTATION

```c
function hmac (key, message) {  
if (length(key) > blocksize) {  
    key = hash(key) // keys longer than blocksize are shortened  
}  
if (length(key) < blocksize) {  
    // keys shorter than blocksize are zero-padded (where || is concatenation)  
    key = key || [0x00 * (blocksize - length(key))] // Where * is repetition.  
}  
  
o_key_pad = [0x5c * blocksize] ⊕ key // Where blocksize is that of the underlying hash function  
i_key_pad = [0x36 * blocksize] ⊕ key // Where ⊕ is exclusive or (XOR)  
return hash(o_key_pad || hash(i_key_pad || message)) // Where || is concatenation
```

To distinguish about the HMAC with the reduced version of MD5 with SHA-1 carrying functionalities to give the unique. Random functions to distinguish to allow to attach the differential equations and rectangular second premiage attacks. these attack do not contradict the security proof but provide existing hash functions. The system compares the HMAC attached to the received message using the constant time comparison digit by digit to arbitrary message.

EXAMPLES

Here is the some UTF-8 encoding assuming the 8-bit ASCII values then there are some non empty HMAC values 8-bit ASCII and utf-8 encoding

```
HMAC_MD5(“key”,”the quick brown fox jumps over the lazy dog”) = 0x8007071346e7749b90c2dc24911e275e1e275
```

VIII. CONCLUSION

In this module patient health information are send to the cloud server. Now the cloud server will generate unique id for every users based on patient name, father name and date of birth using PJW Hash Algorithm. If already id exist then the patient details will be appended with patients clinical history else new CDA document will be generated. In this module the new patient enter into hospital no need to give details about the disease and symptoms. The patient history already maintained in cloud server so we can get the patient histories by using key it is retrieve from patient personal details. The patient histories maintained in document which is contains patient clinical histories (hospital name, disease, prescription).

IX. REFERENCES


