User-friendly Application for operability with HL7 in mobile agent of Ubiquitous Health Environment

이정훈, 곽동엽, 문강남, 토니 사하마, 김정태*
퀸즈랜드공과대학교, 목원대학교*

User-friendly Application for operability with HL7 in mobile agent of Ubiquitous Health Environment

JeongHoon Lee, DongYeup Kwock, KangNam Moon, Tony sahama, Jung-Tae Kim*
Queensland University of Technology, Mokwon University*
E-mail : jeonghoon.lee@connect.qut.edu.au

ABSTRACT

Mobile Health (M-Health) system is a recent term for medical and public health practice supported by mobile devices, such as mobile phones, PDAs, and other wireless devices. Mobile Health system has been successfully establishing at few general hospital in Korea. However, to use diverse devices manufactured by various company cause inoperability, and lack of security disappoints customers often. Although the outstanding health environment, most of hospitals are unavailable to share electronic patient records due to lack of standard protocol to handle the interoperability each other. Health Level 7 (HL7) is the best solution for the problem. In this paper, we will analyse a current M-Health service in terms of security and mobile device, and suggest iPhone for the best device against hospital environment. Also, for keep confidentiality of health information and patient privacy, enhanced security mechanism is introduced. As a consequence, interoperable standard, and most appropriate device for supporting staffs and M-Health performance, and enhanced securirty mechanism will be integrated in order to propose improved M-health model.

Keyword
Mobile Health, HL7, iPhone, Ubiqutous Health, EAP-TLS

Ⅰ. Introduction

The development of information technology has eased the medical services and provided the Electronic Health (E-Health) service. Furthermore, for the last few years, the mobile devices are combined with E-Health in order to respond faster from emergency call and provide a better medical care system. In addition, smart phone enable users to do more things than a laptop computer did, so medical stakeholders such as doctors, nurses and other staffs have recently demanded for more convenient and efficient handheld devices. Especially, we focus on iPhone, the one of the most popular smart phone for business, because iPhone supports many essential functions. The health system using mobile device is called M-Health, and amount of market volume of M-Health is estimated to be over one thousand million won in 2012 as following Samsung Economic Research Institute [1]. According to a survey, more than 90% of the medics and staffs mark satisfactory in function, but complainers point a mobility of mobile device and a length of message for communication [2]. The aforementioned problems can be caused by misunderstand of Health Information System (HIS) and a lack of study about the most sufficient mobile device for hospital

environment. Moreover, various medical and healthcare devices manufactured by various companies offer their own data communication protocol. In the event, interoperability collision occurs while data-exchange between devices let alone between hospitals and nations. The collision can be solved by HL7 standard. ISO/IEEE 11073 is a group of standards for medical device communication. It is an integration format from ENV13734 (represent of vital signs information), ENV13735 (the model for access to the data), and MIB/IEEE 107(services and communication protocols for interoperability between medical devices.) which managed by the TC251 of European Committee for standardization (CEN) [3]. Also, HL7 V3 message based the HL7 Clinical Document Architecture (CDA) is a standard for markup of document, and it specifies the structure and format of a clinical document for exchange. A CDA document is a defined the data object that can contain text, and multimedia contents.

With the components as above, the rest of paper discussed a design of HL7-oriented M-Health system model using iPhone. Firstly, this paper specifies the features of HL7 methodology that can facilitate the consensus in health informatics standards in section 2. Then, section 3 describes architecture of the model and considerations of this system each part of it. In 4th section, the proposed model is compared with conventional health system, and the improved factors and expected effects on hospital environment are shown.

II. Health Level 7

HL7 is a International Organization for Standardization (ISO) approved standard for inter-exchange health information. The paper outlines the HL7 methodology is using in developing HL7 version 3. Four features are worthy of note in order to be interoperable between inter-organization and international health informatics standards [4]. Firstly, Communication adaptability is the ability to comprehend or transmit messaging into diverse forms in order to meet the specific protocol. Secondly, Collaborative standards development is a methodology designed to support cooperation between disparate interests. Thirdly, Adoption of various codes and vocabularies is for maintaining a coded vocabulary which can be used in conjunction with HL7 and relevant principles and that enable the communication of information in such a way so that sending and receiving systems have a shared, well defined, and unambiguous knowledge of the meaning of the data being exchanged. Lastly, Specialization to meet region- or nation-specific requirements is for region or nation that needs unique requirement. It supports opportunities to define solution for the requirement. Technically, the information model can be adapted to meet these needs by adding new classes or by creating specializations of existing classes.

HL7 are encoded in Extensible Markup Language (XML). In this paper, we describe two HL7 messages between devices and database server, and between organizations. In the former message, the XML is encrypted after converting user inputs to HL7 message (XML format), and forwarded to database server. The entities for user input in the application observe the standard as below Figure 1.

Figure 1. Interface for M-Health Application

The latter HL7 message is based on HL7 CDA. Major components of a prototypic CDA are shown in Figure 2. Many required components are skipped for simple example.

```
<ClinicalDocument>
  ... CDA Header ...
  <structuredBody>
    <section>
      <text>(a.k.a. "narrative block")</text>
      <observation>...</observation>
      <substanceAdministration>
        <supply>...</supply>
      </substanceAdministration>
      <observation>
        <externalObservation>...
        </externalObservation>
      </observation>
    </section>
    <section>
        <section>...</section>
    </section>
  </structuredBody>
</ClinicalDocument>
```

Figure 2. Major component of CDA

CDA documents can be exchanged in HL7 messages. All components in CDA document that are essential part of wholeness (such as attested multimedia) can be exchanged as a unit, and to modify any of the references (e.g., a reference for multimedia in a exclusive file) is no needed within the base CDA document when creating or extracting the exchange package (indeed, they cannot be changed). There are no restrictions on the directory structure used by receivers. It means receivers can place the components of the CDA document into any directories of their choosing.

The transmitted HL7 messages are monitored by CDA standard (XML format), and stored in hospital database. As shown in the figure 3, the sections of database is originated by HL7-standard includes Practitioner license or other ID number (PLN), patient identification (PID), patient allergy information (AL1), and numerous tables

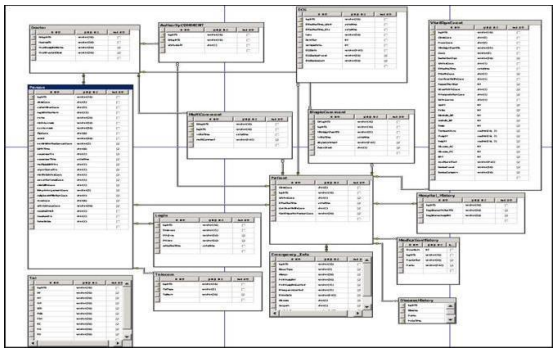

Figure 3. Tables in DB for HL7 standard

III. enhanced security of M-Health model

There are still numerous issue even though interoperability problem is solved by HL7 standard. The other big issue in M-Health is maintenance of security [5]. M-health system is designed as an enhancement of E-health supported by wireless access, so not only software vulnerability, but also wireless network vulnerability can cause critical security problems. For more secure M-Health security, wireless security architecture should be designed as an essential requirement for wireless EMR access. Especially, patient privacy concerns take on one more importance in HIS environment. In fact, leakage of patient privacy in hospital has been reproved for a last few years. For mitigating aforementioned problem, we propose a security mechanism that protects EMR and fit to the M-Health system. The mechanism consists of numerous security measures such as authentication and cryptographic algorithm for more flexible, rapid, and secure performance.

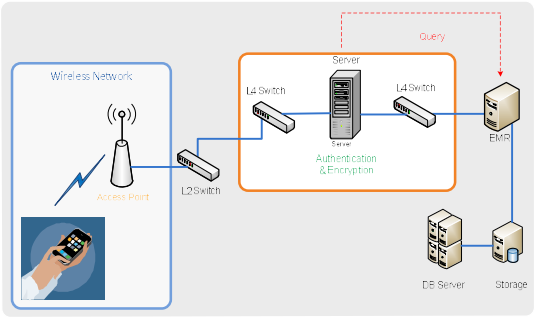

Figure 4. Configuration of system

Mobile devices may assist the medical services with its portable, user-friendly and multi-functional feature. In this paper, iPhone is used due to the special reason that it supports essential functions in hospital and satisfies requirement, such as barcode read, availability of multi-function, and RFID communication (Plug device required). Especially, for the purpose of security, iPhone supports passcode requirement for physical security, latest wireless security protocol, a function to find lost device, remote data protection, and self-data-encryption for storage. In cryptology, iPhone provides AES-128 algorithm which is the best for achieving compromise between security and performance at speed [6]. For finding the best network environment for M-Health, the organisational characteristics of the hospital should be analysed. With mobile devices in hospital, the staff will be able to access database to view or update patient's medical records. The staffs are usually permanent users. It means they are suitable to use a digital certificate rather than using an ID and Password. To utilize Digital certificate, the Extensible Authentication Protocol (EAP) can be selected, and there is one suitable EAP authentication methods in order to satisfy the conditions as mentioned before. It is EAP-TLS. EAP-TLS, in which servers and clients concurrently use the certificate-based authentication, can be the best protocol for the secure hospital wireless environment. To apply EAP-TLS for a wireless network, implementation of WLAN standard is required. Wi-Fi Protected Access2 (WPA2) is one of the

standards in which EAP-TLS can be implemented. Also, WPA2 employs AES-CCMP to overcome vulnerabilities of other wireless communication standards. [9].

In the network, RADIUS server acts as authentication server and private Certificate Authority (CA). Private CA means that it is used only for intra-network. It requires large budgets to be built at first, but hospitals need to pay no extra charge for the certificates, while public CA usually demands for a payment regularly. Moreover, vulnerability of personal information leakage may be mitigated because it does not need to send data to networks outside. Also, private CA has good scalability because it is possible to control the certificate standard based on the requirements.

Ⅳ. Assessment

As a last step, the proposed M-Health system is assessed by comparison to fragile security and non-HL7 system which can often be used in real industries.

Table 1. Security Assessment

Item	Conventional Health System	Proposed M-Health Model
Data-exchange in inter-organization	No interoperability	Clearly operable, even international data-exchange
Authentication Method	ID & Password authentication	Digital Certificate, ID & Password double authentication,
Data Encryption in transmission	weak encryption prior to transmission	strong encryption prior to transmission (AES-128)

As shown in table 1, in terms of data-exchange in inter-organization, conventional hospital neglect the importance of same semantic interpretation of the data elements. If they need data sharing, interface may require many weeks of analyst time to implement due to the principal limitation. However, in proposed M-Health system, every organization, even international information is easier implemented, and develop coexistence and co-prosperity together. In terms of mutual security, the use of ID and password for access to EMR database can be vulnerable. While, authentication using the digital certificate will prevent illegal access even if hackers obtain the user's ID and password in the proposed model.

On the other hand, the proposed security model has an issue with compatibility. The latest wireless device may be required because some of old wireless router cannot support WPA2, but it could be worth to invest in new devices because it may provide mutual security to the wireless hospital system.

Ⅴ. Conclusion

The integrated M-Health system with HL7, iPhone, and security mechanism is proposed and assessed. The HL7 Version 3 is a worthy candidate as a methodology to use in generating collaboration and consensus between multiple standards developers in an international effort. Also, enhanced security mechanism keeps confidentiality and contribute reliable hospital environment. iPhone not only supports both process with high performance, but encourages medics and staffs with fantastic user-interface. The mix of the three components will make the hospital environment closer to perfect HIS, and system must be secured permanently, either when being just transmitted or stored in databases.. Following development, more security measurement will be demanded. It was also implemented with consideration the characteristics of the hospital in the real world, so that optimized security protocols and mechanisms are employed for the higher performance and security. Finally, a challenge in the near future will be the integration of Ubiquitous Sensor Network (USN) with the three components to the hospital environment.

References

[1] Samsung Economics Research Institude. (2004). *Issue Paper : Economic effection and Growing Strategy of u-Health*

[2] NewsWire. (2004). *Satisfaction survey of KT Mobile Hospita*l. (accessed in 29th Sep : http://www.newswire.co.kr/irnews/?job=newsView&no=207)

[3] Miguel Galarraga, Luis Serrano, Ignacio Martínez, Paula de Toledo. (2006). *Review of the ISO/IEEE 11073- PoCMDC standard for medical device interoperability and its applicability in home and ambulatory telemonitoring scenario, Electrical and Electronic Engineering.* University of Zaragoza.

[4] Beeler. W. G. (1998). HL7 Version 3－*An*

object-oriented methodology for collaborative standards development. International Journal of Medical Informatics.

[5] Digital Daily. (2009). *Unsecure wireless envirnments generalted zombie-PC.* (accessed in 27th Sep: http://www.daily.co.kr/news/news_view.php?uid=52825

[6] Snyder, A. M., & Weaver, A. C. (2006). *The e-Logistics of Securing Distributed Medical Data. Department of Computer Science*, University of Virginia.