Symmetry **2015**, *7*, 1028-1039; doi:10.3390/sym7021028

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

Article

Development of Patient Status-Based Dynamic Access System for Medical Information Systems

Chang Won Jeong [1,†], Vathana Ban [2,†], Kwon Ha Yoon [3,*] and Su Chong Joo [2,*]

[1] Imaging Science Based Lung and Bone Disease Research Center, Wonkwang University,
460 Iksandeaero, Iksan, Jeonbuk 570-749, Korea; E-Mail: mediblue@wku.ac.kr

[2] Department of Computer Engineering, Wonkwang University, 460 Iksandeaero, Iksan,
Jeonbuk 570-749, Korea; E-Mail: vathana11ban@wku.ac.kr

[3] Department of Radiology, Wonkwang University School of Medicine and Hospital,
460 Iksandeaero, Iksan, Jeonbuk 570-749, Korea

* Authors to whom correspondence should be addressed; E-Mails: khy1646@wku.ac.kr (K.H.Y.); scjoo@wku.ac.kr (S.C.J.); Tel.: +82-63-859-1921(K.H.Y.); +82-63-850-6750 (S.C.J.); Fax: +82-63-859-1009 (K.H.Y.).

Academic Editor: Neil Y. Yen

Received: 10 February 2015 / Accepted: 4 June 2015 / Published: 8 June 2015

Abstract: Recently, the hospital information system environment using IT communication technology and utilization of medical information has been increasing. In the medical field, the medical information system only supports the transfer of patient information to medical staff through an electronic health record, without information about patient status. Hence, it needs a method of real-time monitoring for the patient. Also, in this environment, a secure method in approaching healthcare through various smart devices is required. Therefore, in this paper, in order to classify the status of the patients, we propose a dynamic approach of the medical information system in a hospital information environment using the dynamic access control method. Also, we applied the symmetric method of AES (Advanced Encryption Standard). This was the best encryption algorithm for sending and receiving biological information. We can define usefulness as the dynamic access application service based on the final result of the proposed system. The proposed system is expected to provide a new solution for a convenient medical information system.

Keywords: medical information system; dynamic access control; patient status condition; symmetric methods; patient-centric service

1. Introduction

Currently, the trend of the hospital information system environment is to share the health records, diagnosis, and treatment information of patients by linking hospitals with cloud computing technology [1–4]. In addition, systems that provide continual medical information services in the wired and wireless communication environment of various smart devices are being studied actively [5–7].

However, security measures are required for these hospital information systems because they manage important patient private information, such as personal information, bio-signal and medical image information used for diagnosis and treatment. In particular, dynamic access control technology is necessary to access hospital information through various paths in the system environment that consists of various smart devices.

There are many studies that have applied the situation-based access control, rule/role-based access control, and situation recognition-based access control as representative security technologies of medical information systems [8–10].

The medical information access control method proposed in this study for the smart mobile environment is similar to those of the above representative studies. However, our proposed method is different because it is based on the patient's status, although client classification control and rule-based control methods are the main-stream methods. The proposed method has the advantage of being able to respond quickly to urgent on-site hospital situations because medical information is accessed through dynamic access rules based on patient status. For this, this study designs the dynamic access control system environment based on the convenient system environment of the hospitals. Also, we applied the symmetric method of AES (Advanced Encryption Standard) for security in real-time monitoring of patient status. It uses an e-health sensor platform by cooking hacks that can collect biological information through multi-sensors such as SPO2, ECG, body temperature, blood pressure, glucometer, Airflow, and EMG.

In the rest of this paper, we will explain as the following structure. In Section 2, the studies on representative medical information access methods are examined. In Section 3, the system environment and the dynamic access control of service process proposed in this paper are described. In Section 4, the result of the proposed system application is shown through examples. Lastly, in Section 5, this paper presents its conclusions and the contents of future research.

2. Literature Review

This section describes the studies related to representative access control methods, such as situation recognition-based medical information service and rule/role-based medical information access methods, and the studies related to smart device-based hospital information systems.

2.1. Studies on Role-Based Access Control Model

The role-based access control model is one of the most widely used information access methods between clients and servers. It is applied to hospital information systems to prevent patient medical information, such as medical records and various diagnostic data, from leaking to unauthorized users accessing the medical system in a ubiquitous environment. The model controls access to patient information based on user status information, such as location and time. For example, the RBAC model for U-healthcare has been studied to protect the privacy of users [11,12]. This model provides the management standards of access control for healthcare service in the ubiquitous environment. It includes a role delegation function that depends on user information, user roles, and reading scope of the role information. Furthermore, by directly setting the roles, grades, and readable range, it can control the reading rights of medical personnel for patient medical information. In particular, given the recent diversity in information access devices used by medical personnel, this model includes access control technology by device.

2.2. Hospital Information System Based on Smart Devices

The current trend is to include various smart devices, such as smartphones and tablets in the configuration of hospital systems [13–15]. A majority of studies facilitates real-time information sharing among smart devices through a medical information-sharing framework based on hybrid applications (apps) [16–18]. The hybrid apps are developed through mobile Web to overcome the constraints of platform-specific smart devices, and operate on various platforms and development environments. Furthermore, N-screen is used to support the real-time medical information sharing of medical personnel. Multiple client access of N-screen is supported through the push message on the smart devices of medical personnel whereas stable N-screen information sharing of multiple smart devices is supported through the N-screen sharing management service [19].

Because the hospital information access of multi-devices and information sharing are interlocked, security models are particularly required. The application of situation-based security technology including information access control technology has been gradually increasing. Moreover, stricter security protocols are applied to the existing security models in hospital information systems.

Therefore, this paper proposes a dynamic access control system based on patient status. Our proposed system has the advantage of patient-oriented healthcare services where the conventional security model centers on the principal agent.

3. Patient Status-Based Dynamic Access Control System

This section describes the total environment and the dynamic access method of the proposed patient status-based dynamic access control system as well as the configuration of the medical information for dynamic access support. In addition, the patient status conditions and the medical information access authentication method that are based on these are described.

3.1. Environment of Dynamic Access System for Medical Information

Figure 1 shows the environment of the dynamic access control system for medical information. The medical information server consists of the Electronic Medical Record (EMR) system of patients and Picture Archiving and Communication System (PACS), which manages Digital Imaging and Communications in Medicine (DICOM) generated from mobile X-ray imaging devices [20,21].

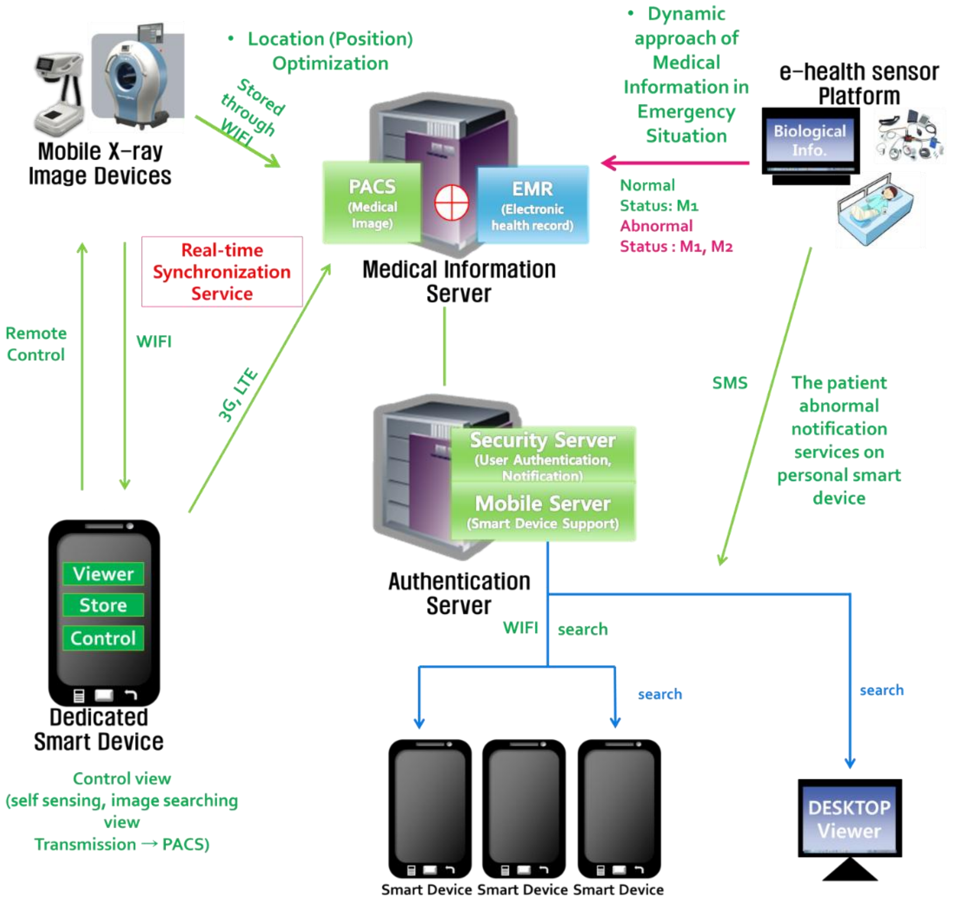

• Location (Position) Optimization
Stored through WIFI
Mobile X-ray Image Devices
• Dynamic approach of Medical Information in Emergency Situation
e-health sensor Platform
Biological Info.
Normal Status: M1
Abnormal Status : M1, M2
PACS (Medical Image)
EMR (Electronic health record)
Medical Information Server
Real-time Synchronization Service
Remote Control
WIFI
3G, LTE
SMS
The patient abnormal notification services on personal smart device
Security Server (User Authentication, Notification)
Mobile Server (Smart Device Support)
Authentication Server
WIFI
search
search
search
Viewer
Store
Control
Dedicated Smart Device
Control view (self sensing, image searching view Transmission → PACS)
Smart Device
Smart Device
Smart Device
DESKTOP Viewer

Figure 1. Dynamic access control system environment for medical information.

On the smart terminals and the checking devices of medical personnel for accessing the medical information server, information can be accessed only after receiving authentication via the authentication server that manages the authentication process of medical personnel. Patient status is determined by the sensors attached to the patient. For real-time monitoring of patients, we use the e-health sensor platform which is designed by cooking hacks in order to measure biometric sensor data for experimentation and test purposes.

The medical information access of the proposed system is controlled for normal and emergency status. In normal status, if medical personnel request to read the medical information of a patient, the information access rules of the authentication server are executed first, and when all authentication rules pass, the patient's medical information can be read. In emergency status, the change in the status information of the patient is requested to the server by recognizing the patient's emergency status based on the conditions of such a situation. Subsequently, the medical information server sends a notification message to the medical personnel responsible for the patient through the emergency status notification service. To access the medical information of patients, the information accessibility of the medical personnel is checked based on the defined authentication rules through the authentication server. If all medical information access rules are satisfied, the medical personnel can search for patient information in the medical information server; otherwise, the information access is restricted. The detailed explanation is provided in the following section.

3.2. Situation-Based Dynamic Access Method for Medical Information

Figure 2 shows the process of accessing medical information based on the changing status in the patient's situations provided by the proposed system.

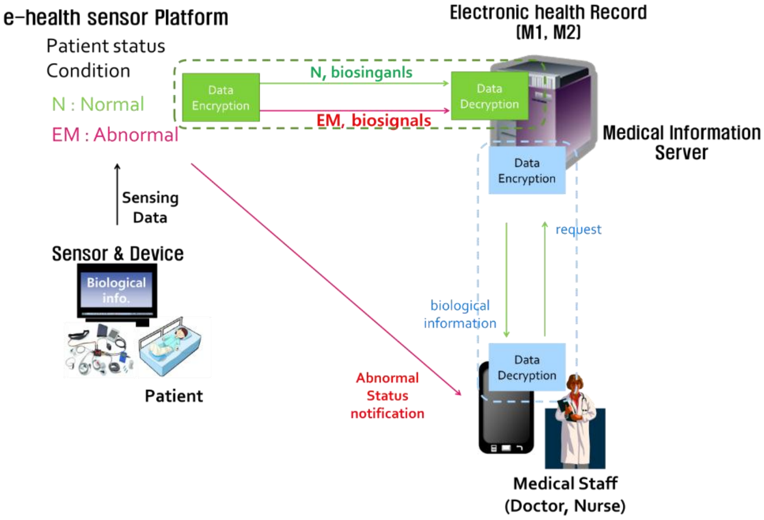


Figure 2. Method for accessing medical information of patient based on context.

To react to the patient's status in real-time, we focus on the patient status of in/out hospital, integration of medical image and biological information system. Then, we estimate a case of a patient with a brain tumor. Therefore, in this case we need both biological information and medical image to use in our proposed system.

Patient status is classified into normal situation and emergency situation based on biological information collected in real time by e-health sensor platform.

By comparing the biological information collected in real time from patients with emergency condition defined by reference values which are set to either normal (N) status or emergency (EM) status. For normal status, the medical personnel-allowed range of medical information access is restricted to the information of the EMR system. For emergency status, both the EMR and DICOM can be accessed.

Furthermore, to respond quickly in emergency status, the emergency status notification service is provided with the system sends a Short Message Service (SMS) to the mobile phones of medical personnel who are responsible for the patient. The grade for reading medical information of an emergency patient is dynamically upgraded by a change in the access right of the medical personnel who receive the notification message, so that they can read all medical information pertaining to the patient regardless of roles and grades.

3.3. Configuration of Medical Information for Dynamic Access Support

Figure 3 shows the medical information for dynamic access support. It is based on the Patient, Staff, R_PS, Medi_Info, and Staff_time tables. The Patient table stores the basic information of patients; the Staff table stores information regarding the hospital medical personnel; the R_PS table contains the relationships between the patient and the medical personnel responsible for the patient; and the Medi_Info table contains the relationship between the patient and the medical information accessible by situation. The Patient table consists of a unique number, name, and personal information of the patient. The Staff table contains the ID of doctors, personal information of doctors, and mobile phone information for the emergency status notification service, values of attribute for storing the roles and grades of medical personnel, and an attribute for working hours in the Staff_time table. The R_PS table connects the relationship between the patients and the doctors, and stores the members of the medical personnel responsible for each patient.

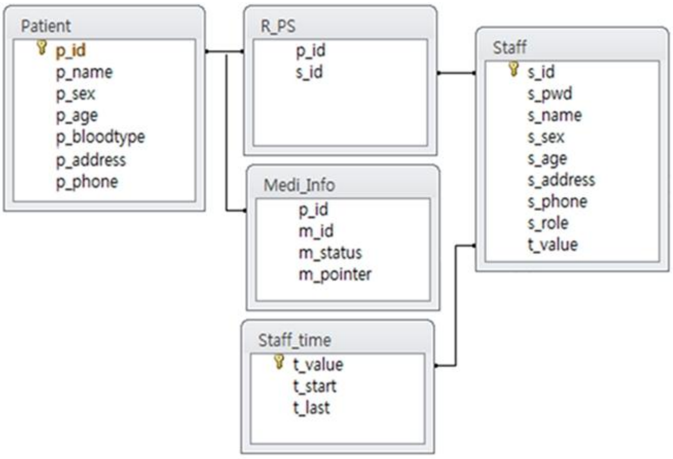


Figure 3. Medical information Entity-Relationship diagram for supporting dynamic access.

3.4. Emergency Status Criteria and Medical Information Access Authentication Method

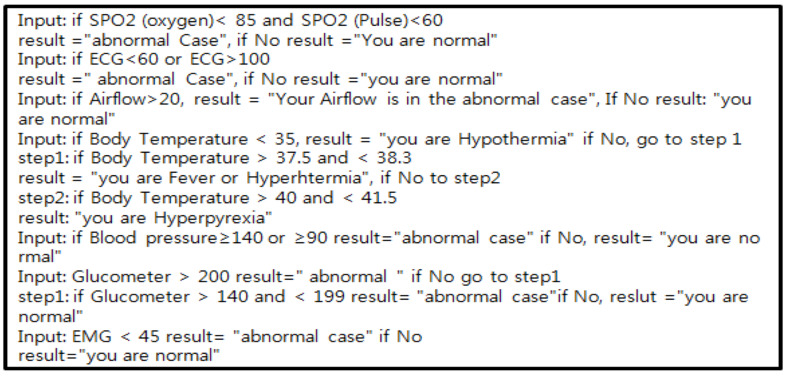
Based on the biological information obtained from the patient, status of the patient is identified according to the seven identification criteria listed in Table 1.

Table 1. Criteria for identifying patient status.

Identification Condition	Patient Status Classification	
	Normal	**Abnormal**
SPO2	95% to 100% (Oxygen in blood) 60–100 bpm (Pulse)	<85% (Oxygen in blood) <60 bpm (Pulse)
ECG	60–100 bpm	<60 bpm >100 bpm
Airflow	16–20 bpm	<16 bpm >20 bpm
Body Temperature	36.5–37.5 OC	<35 OC (Hypothermia) >37.5–38.3 (Fever or Hyperthermia) >40.0–41.5 OC (Hyperpyrexia)
Blood Pressure	60–100	≥140 or ≥90
Glucometer	70 to 99 mg/dL (no food for 8 h) <140 mg/dL (2 h after eating)	>200 mg/dL <140 mg/dL to 199 mg/dL
EMG	55–70 mV	<45 mV

Table 1 indicates the numeric status of sensor value which is divided into normal and emergency, based on patient's situation. Moreover, in this study we include seven biological information kinds of attachable sensors, with values determined by the different types of sensor. To be more accurate, SPO2 is defined as the measurement of the amount of oxygen in the blood, and ECG represents the electrical and muscular function of the heart. Airflow refers to measurement of the breathing rate of patient in need of respiratory help; body temperature is measurement about body temperature, blood pressure in the arteries, Glucometer determines the approximate concentration of glucose in the blood while EMG is the measurement of the electrical activity of muscles at rest and during contraction.

To identify data that is obtained from the sensor whether it is a normal or emergency case, we use the information which is shown in Table 1 which contains the values of seven kinds of sensors. This is the condition for comparison with the real-time data that is obtained from the sensors. Based on that information, we create an algorithm which can identify the status of patients that are shown in Figure 4.



```
Input: if SPO2 (oxygen)< 85 and SPO2 (Pulse)<60
result ="abnormal Case", if No result ="You are normal"
Input: if ECG<60 or ECG>100
result =" abnormal Case", if No result ="you are normal"
Input: if Airflow>20, result = "Your Airflow is in the abnormal case", If No result: "you
are normal"
Input: if Body Temperature < 35, result = "you are Hypothermia" if No, go to step 1
step1: if Body Temperature > 37.5 and < 38.3
result = "you are Fever or Hyperhtermia", if No to step2
step2: if Body Temperature > 40 and < 41.5
result: "you are Hyperpyrexia"
Input: if Blood pressure≥140 or ≥90 result="abnormal case" if No, result= "you are no
rmal"
Input: Glucometer > 200 result=" abnormal " if No go to step1
step1: if Glucometer > 140 and < 199 result= "abnormal case"if No, reslut ="you are
normal"
Input: EMG < 45 result= "abnormal case" if No
result="you are normal"
```

Figure 4. The algorithm for patient status.

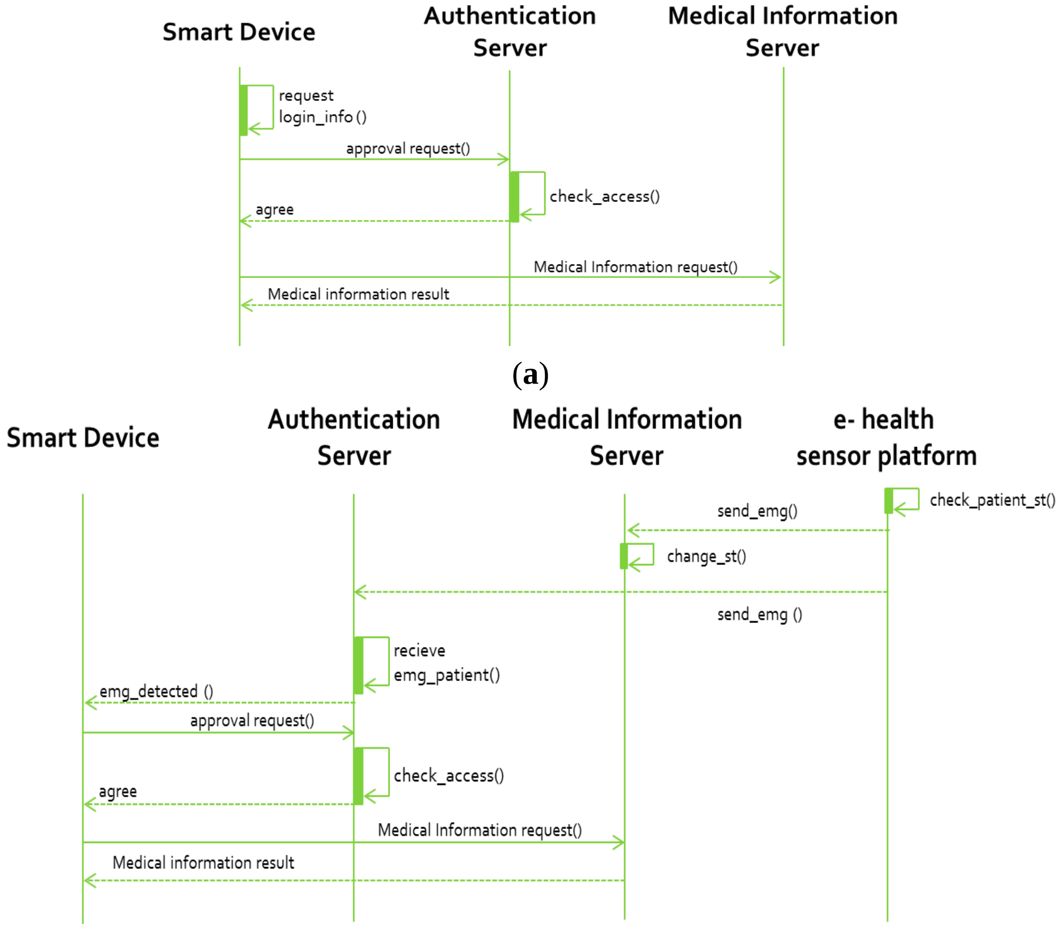
3.5. Authentication Rules for Accessing Medical Information System

Table 2 lists the items required to access medical information based on the proposed dynamic access information system.

Table 2. Items for access authentication of medical personnel.

Rule Item	Rule Description
ID and password	ID of medical personnel for differentiating users
Current location information of user	Location information when requesting medical information (e.g., GPS reception range: in/outside of hospital)
Role information	Role information of medical staff (e.g., doctor, nurse, *etc.*)
Access hours depending on role	Working hours and allowed information access hours of medical staff (e.g., 09:00–18:00)
Emergency code	Authentication number sent for patient emergency (e.g., 0000000, combination of number and letters)

There are five conditions: personnel IDs for medical staff to verify their access clearance to the medical information system; role information to verify the position and role of medical staff; current location information of the user requesting medical information; the allowed access hours to the information according to the working hours of the medical staff; and emergency code sending for patient emergency. The first step in the authentication rules of the authentication server is a process of logging in by storing user ID and password in order to identify the medical staff. Once the member authentication is completed, the current location of the device requesting the medical information is verified in order to identify whether the information request is made from inside or outside the hospital. By identifying the location information, the medical information of the patient is prevented from leaking outside the hospital. In addition, the role position of the user device is identified. Because the accessed EMR information varies by medical staff at the hospital, the proposed system supports access to different types of EMR based on role. The access hours, depending on role, are the information that is used to change the allowed access hours for doctors and nurses on duty in the hospital for checking patient status. When all pertinent conditions are satisfied through the authentication server, medical staff can access the medical information server to read medical information. When a patient emergency situation occurs, the medical information of the emergency patient is verified by entering the emergency code obtained through the emergency notification service. Figure 5 shows the authentication process divide into two parts, normal situation and emergency situation.



(**a**)

(**b**)

Figure 5. Event Trace Diagram for authorization process. (**a**) Normal situation; (**b**) Emergency situation.

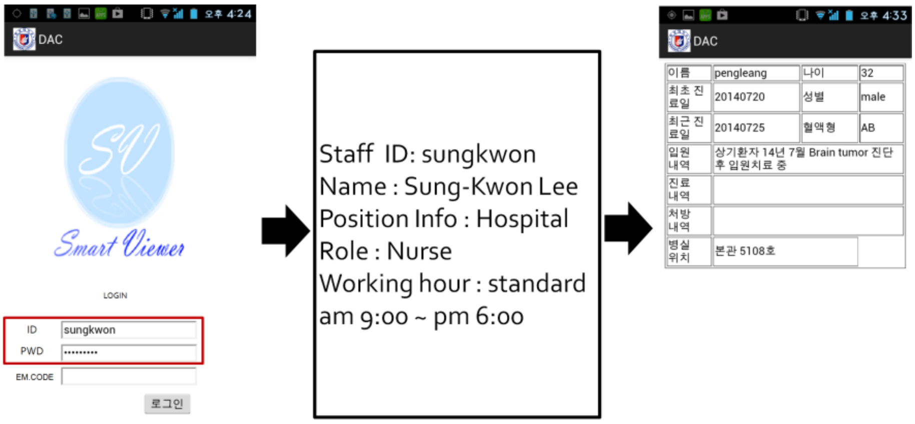
In the normal situation, medical staff do not need notification from authentication server. In this case, medical staff request patient information for checking the patient status generally. They follow procedures such as login, check location information, role verification, current time, and then medical information requesting and result receiving.

For the emergency situation, firstly medical staff receives notification message from the authentication server through an e-health sensor platform. Then, they execute authorization processing which is similar to a normal situation process.

4. Result of Performing Emergency Notification and Dynamic Access of Medical Information Services

This section shows the performance of the notification service provided in the proposed system for normal and emergency situations according to the emergency criteria of the patient and the authentication process defined in the previous section.

When the patient status information indicates a normal situation, medical staff are authorized to access the medical information system based on their IDs and passwords, their location information, and the role and working hour information of each individual according to the defined information access rules. Figure 6 shows an example of a normal situation where nurse "Sung-Kwon Lee" can access the general information of a patient by satisfying the rule conditions.



ID sungkwon
PWD ••••••••••
EM.CODE

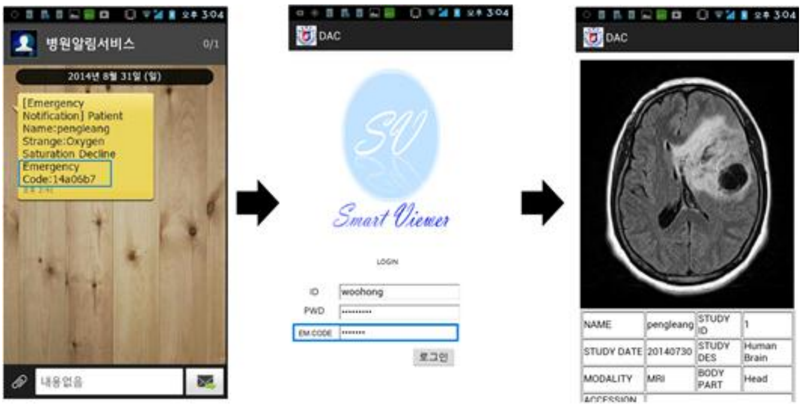
Staff ID: sungkwon
Name : Sung-Kwon Lee
Position Info : Hospital
Role : Nurse
Working hour : standard
am 9:00 ~ pm 6:00

이름	pengleang	나이	32
최초 진료일	20140720	성별	male
최근 진료일	20140725	혈액형	AB
입원내역	상기환자 14년 7월 Brain tumor 진단 후 입원치료 중		
진료내역			
처방내역			
병실위치	본관 5108호		

Figure 6. Result of performing medical information access in normal situation.

In the emergency case, based on the patient whose status changes to an emergency situation in the relationship table of patients and doctors (the R_PS table), an SMS is sent to the smart device number of the hospital medical staff who is responsible for the patient to notify an emergency. The corresponding emergency code is sent as an attachment to the emergency notification message in order to minimize additional authentication of the medical staff and access rules of medical information. The medical staff that receives the emergency notification message can enter the emergency code to access the medical information system, thus bypassing all authentication items, other than ID. The emergency code minimizes the authentication process for accessing medical information in order to support fast medical treatment and emergency measures by the medical staff in an emergency situation.

Figure 7 shows the medical image information (DICOM) on a smart device when an emergency occurs confirmed by the medical staff after the doctor receives an emergency message.



병원알림서비스 0/1

2014년 8월 31일 (일)

[Emergency Notification] Patient Name:pengleang Strange:Oxygen Saturation Decline Emergency Code:14a06b7

DAC

Smart Viewer

LOGIN

ID woohong

PWD ••••••••••

EM CODE ••••••••

로그인

DAC

NAME	pengleang	STUDY ID	1
STUDY DATE	20140730	STUDY DES	Human Brain
MODALITY	MRI	BODY PART	Head
ACCESSION			

Figure 7. Result of performing emergency notification service and dynamic access service of medical information.

Based on the proposed dynamic access control system, conventional medical information and medical image information (DICOM) for normal and emergency situations are shown by the notification service.

As a result, we confirmed the proper accessibility of relevant patient information in the medical information server depending on normal and emergency situations based on the patient status proposed in this paper. Through this, the proposed system is expected to provide a new solution for conventional medical information access.

5. Conclusions

With advancements in information technology, the medical services of hospitals is changing. In particular, with the development of smart devices, doctors and nurses in hospitals and individuals as well as general users can use various types of smart devices. As a result, they can access medical records and medical information of patients in the hospital information system under the cloud environment. Thus, the security technology for medical information and private information has become an extremely important issue.

In this paper, we proposed a medical information access control system that targets various smart devices for the medical information system according to patient status in a hospital environment. For the data managed with the proposed system, the access restrictions on the smart devices of medical staff were defined through information access rules based on the medical image information (DICOM) of patients stored in PACS and the medical records and information of patients stored in the EMR system. Furthermore, the implementation of the proposed system was confirmed through applications based on dynamic access rules, such as the minimization of access rules for medical information of patients and changes in the readable range of medical information by medical staff for normal and emergency situations of patients. Consequently, the proposed system proved its ability to access medical information dynamically and to respond to an emergency quickly depending on patient status.

Future studies will include an optimization of the dynamic security rules and performance assessments of the conventional security models. In addition, a clinical utilization study is planned through field tests.

Acknowledgments

This study was supported by a grant of the Korean Health Technology R&D Project, Ministry of Health & Welfare, Korea (A120152).

Author Contributions

Chang Won Jeong, Su Chong Joo designed the overall system and wrote the manuscript. Vathana Ban implemented symmetric method and helped the experiments. Kwon Ha Yoon carried out research direction and contributed to manuscript critical reading. All authors read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Xu, B.Y.; Xu, L.D.; Cai, H.M.; Xie, C.; Hu, J.Y.; Bu, F.L. Ubiquitous data accessing method in iot-based information system for emergency medical services. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1578–1586.
2. Tamassia, R.; Yao, D.F.; Winsborough, W.H. Independently verifiable decentralized role-based delegation. *IEEE Trans. Syst. Man Cybern. A* **2010**, *40*, 1206–1219.
3. Hanson, S.L.; Davis, M.; Altevogt, B.M. Institute of Medicine Forum on Neuroscience and Nervous System Disorders. In *CNS Clinical Trials: Suicidality and Data Collection: Workshop Summary*; National Academies Press: Washington, DC, USA, 2010; p. 75.
4. Pan, Y.; Zhang, J. Parallel programming on cloud computing platforms—Challenges and solutions. *J. Converg.* **2012**, *3*, 23–28.
5. Hii, P.C.; Chung, W.Y. A comprehensive ubiquitous healthcare solution on an android™ mobile device. *Sens.Basel* **2011**, *11*, 6799–6815.
6. Siddiqui, Z.; Abdullah, A.H.; Khan, M.K.; Alghamdi, A.S. Smart environment as a service: Three factor cloud based user authentication for telecare medical information system. *J Med. Syst.* **2014**, *38*, doi:10.1007/s10916-013-9997-5.
7. Park, D.K.; Jung, E.Y.; Jung, B.H.; Moon, B.C.; Kang, H.W. Smart medical information service for chronic disease patients. *Eur. J. Public Health* **2012**, *22*, 144–144.
8. Beimel, D.; Peleg, M. The context and the sitbac models for privacy preservation-an experimental comparison of model comprehension and synthesis. *IEEE Trans. Knowl. Data Eng.* **2010**, *22*, 1475–1488.
9. Duncan, R.G.; Shabot, M.M. Secure remote access to a clinical data repository using a wireless personal digital assistant (PDA). *J. Am. Med. Inform. Assoc.* **2000**, 210–214.
10. Gupta, P.; Stoller, S.D.; Xu, Z.Y. Abductive analysis of administrative policies in rule-based access control. *IEEE Trans. Dependable Secur. Comput.* **2014**, *11*, 412–424.
11. Ni, Q.; Bertino, E.; Lobo, J.; Brodie, C.; Karat, C.M.; Karat, J.; Trombetta, A. Privacy-aware role-based access control. *ACM Trans. Inf. Syst Secur.* **2010**, *13*, 41–50.

12. Zhou, L.; Varadharajan, V.; Hitchens, M. Enforcing role-based access control for secure data storage in the cloud. *Comput. J.* **2011**, *54*, 1675–1687.
13. Lee, B.G.; Lee, B.L.; Chung, W.Y. Mobile healthcare for automatic driving sleep-onset detection using wavelet-based eeg and respiration signals. *Sensors* **2014**, *14*, 17915–17936.
14. Calliess, T.; Bocklage, R.; Karkosch, R.; Marschollek, M.; Windhagen, H.; Schulze, M. Clinical evaluation of a mobile sensor-based gait analysis method for outcome measurement after knee arthroplasty. *Sensors* **2014**, *14*, 15953–15964.
15. Fong, E.M.; Chung, W.Y. Mobile cloud-computing-based healthcare service by noncontact ECG monitoring. *Sensors* **2013**, *13*, 16451–16473.
16. Baig, M.M.; Gholamhosseini, H. Smart health monitoring systems: An overview of design and modeling. *J. Med. Syst.* **2013**, *37*, doi:10.1007/s10916-012-9898-z.
17. Tan, J.K.H. *New Technologies for Advancing Healthcare and Clinical Practices*; Medical Information Science Reference: Hershey, PA, USA, 2011; p. 436.
18. Matta, M.B.B.A.N. Dynamic knowledge mapping guided by data mining: Application on healthcare. *J. Inf. Process. Syst.* **2013**, *9*, 1–30.
19. Lomotey, R.K.; Deters, R. Supporting n-screen medical data access in mhealth. In Proceedings of the 2013 IEEE International Conference on Healthcare Informatics (ICHI), Philadelphia, PA, USA, 9–11 September 2013; pp. 229–238.
20. Alvarez, L.R.; Solis, R.C.V. DICOM RIS/PACS telemedicine network implementation using free open source software. *IEEE Lat. Am. Trans* **2013**, *11*, 168–171.
21. Jeong, C.W.; Joo, S.C.; Ryu, J.H.; Lee, J.; Kim, K.W.; Yoon, K.H. Development of a mini-mobile digital radiography system by using wireless smart devices. *J. Digit. Imaging* **2014**, *27*, 443–448.