A Study on Finding Emergency Conditions for Automatic Authentication Applying Big Data Processing and AI Mechanism on Medical Information Platform

Gyu-Sung Ham[1], Mingoo Kang[2], and Su-Chong Joo[3*]
[1] Department of Computer Engineering, Wonkwang University,
460 Iksandaero, Iksan, South Korea
[e-mail: ham1231@wku.ac.kr]
[2] Department of IT Contents, Hanshin University,
137 Hanshindae-Gil, Osan, South Korea
[e-mail: kangmg@hs.ac.kr]
[3] Department of Computer · Software Engineering, Wonkwang University,
460 Iksandaero, Iksan, South Korea
[e-mail: scjoo@wku.ac.kr]
[*]Corresponding author: Su-Chong Joo

Received March 18, 2022; revised April 26, 2022; accepted May 26, 2022; published August 31, 2022

Abstract

We had researched an automatic authentication-supported medical information platform[6]. The proposed automatic authentication consists of user authentication and mobile terminal authentication, and the authentications are performed simultaneously in patients' emergency conditions. In this paper, we studied on finding emergency conditions for the automatic authentication by applying big data processing and AI mechanism on the extended medical information platform with an added edge computing system. We used big data processing, SVM, and 1-Dimension CNN of AI mechanism to find emergency conditions as authentication means considering patients' underlying diseases such as hypertension, diabetes mellitus, and arrhythmia. To quickly determine a patient's emergency conditions, we placed edge computing at the end of the platform. The medical information server derives patients' emergency conditions decision values using big data processing and AI mechanism and transmits the values to an edge node. If the edge node determines the patient emergency conditions, the edge node notifies the emergency conditions to the medical information server. The medical server transmits an emergency message to the patient's charge medical staff. The medical staff performs the automatic authentication using a mobile terminal. After the automatic authentication is completed, the medical staff can access the patient's upper medical information that was not seen in the normal condition.

Keywords: AI Mechanism & Big Data Processing, Automatic Authentication, Edge Computing, Emergency Conditions, Medical Information Platform.

A preliminary version of this paper was presented at ICONI 2021, and was selected as an outstanding paper. This version includes a detail of automatic authentication and using AI mechanism and ECG data.

http://doi.org/10.3837/tiis.2022.08.017 **ISSN : 1976-7277**

1. Introduction

Medical information platform is important not only for managing medical information and personal information but also for determining the health conditions of inpatients. The medical information platforms are being developed with the recent development of IoT, network, and mobile terminal technology[1,2,3]. The medical information platforms can measure the patient's biometric data such as SpO2, NIBP, ECG, and temperature through IoT and medical devices in real-time and determine the emergency conditions of patients[4,5]. Medical staff can easily access patients' medical information through mobile terminals[2,6,7,8]. The medical staff tries simple authentication with ID and password(PWD) to access the patient's medical and personal information.

However, as medical staff inside and outside hospitals access medical information using mobile terminals, infringement and leakage of patient personal information are increasing[7,9,10]. According to IBM's "2021 cost of a data breach report" [11], the healthcare industry has topped the average total security costs for 11 years. Also, malicious insiders ranked third in terms of average total security cost and frequency of data breaches. Although the number of medical information leakage accidents has increased, the problem of simple authentication procedures centered on managers of the medical information system is not improved well[12].

Accordingly, the medical industry pays attention to the security(especially a medical information authentication model) technology of context-based medical information computing and the current authentication issues[13,14]. The medical information authentication model should require two-step authentication that consists of user authentication and user-owned mobile terminal authentication using context information to solve these problems. Also, this model should consider the subject corresponding to the user and the role according to a domain in security and context information(e.g., working hours, mobile terminal location, environment information, sensing data)[15]. Therefore, it is necessary to develop a medical information platform that provides security and transparency of medical information access rights to more enhanced and convenient user authentication and mobile terminal authentication in emergency conditions[16].

To solve these problems, we have been researching an automatic authentication-supported medical information platform[6]. The proposed automatic authentication consists of user authentication and mobile terminal authentication, and the authentications are performed simultaneously in patients' emergency conditions. The automatic authentication allows fast authentication in emergency conditions and enhances access transparency through access rights according to the patient's conditions and the role of medical staff.

In this paper, we study finding emergency conditions for the automatic authentication by applying big data processing and artificial intelligence(AI) mechanisms in the medical information platform with an added edge computing system. We use big data processing and AI mechanisms to consider the patient's underlying disease when determining the patient's emergency conditions. Also, the platform's structure is expanded by adding the edge computing system to determine emergency conditions quickly.

The remainder of this paper is structured as follows. Section 2 briefly examines medical information platform studies using big data processing, AI mechanism, and edge computing. Section 3 describes the proposed platform's structure, the proposed automatic authentication, and finding emergency conditions for automatic authentication. Section 4 describes the implementation result of the proposed platform. Section 5 describes a structural comparison of the proposed platform with other existing authentication studies. Finally, Section 6 closes

with conclusions and future research.

2. Related Works

The biometric data measured by medical devices is accumulated in a big data database of medical information platforms[17,18]. The big data processing and AI mechanisms benefit in predicting diagnosis, patient care, and making emergency conditions decisions[17,19,20]. Nishita Mehta et al.[19] surveyed big data analytics and AI technologies in the healthcare system. The big data sources include prescription records, medical records from the EMR of hospitals and clinics, and biometric data from wearables and sensors attached to the patient. As big data processing and AI technologies, correlation analysis, cluster analysis, data mining, machine learning, deep learning, and pattern recognition are used[20,21,22,23]. Ultimately, it is important to provide services to users by using which data sources and which processing and analysis techniques are appropriate. So, we focused on finding the emergency condition decision value of the patient as authentication means using underlying disease data and electrocardiogram(ECG) data.

Types of the underlying diseases include hypertension, diabetes, asthma, etc. These underlying diseases are recorded in the hospital DB with biometric data such as age, sex, blood pressure, fasting blood sugar, ECG, and living habits(e.g., smoking or not, etc.). Machine learning of AI mechanisms can detect patients' underlying diseases[24]. Types of machine learning using healthcare data are typically Bayesian classifier, decision tree, K-Nearest Neighbors(KNN), and Support Vector Machine(SVM) methods. The input data is biometric data and is denoted by $x = (x_1, x_2, \dots, x_n)$. The label is the underlying diseases and is denoted by y. The machine learning models predict the underlying disease through each function $y = f(x)$. The SVM can handle high-dimensional and unusual data and generally have high accuracy[25]. In this paper, we detect the patient's underlying disease through the SVM and use it as authentication means.

The ECG data is used in various medical diagnoses, such as diagnosing a patient's heart disease, detecting heartbeat, etc. With the recent development of AI, ECG and AI mechanisms are used for cardiovascular diseases prediction, emotion recognition, arrhythmia detection, and sleep recognition[20,25]. One of the characteristics of ECG data is time-series data that includes changes over time. Representative deep learning models that use ECG as training data include 1-Demansional Convolution Neural Network(1-D CNN) and Long Short-Term Memory(LSTM). The 1-D CNN can perform a 1-D convolution operation using multiple filters to extract effective and representative 1D time-series sequence data features. Also, the 1-D CNN is very effective in processing fixed-length data. The LSTM is a Recurrent Neural Network (RNN) mainly used to process time-series data. LSTM differs from 1-D CNN in learning long-term dependencies to obtain temporal features of sequential data. In this paper, we use ECG data with 1-D CNN to detect arrhythmias in patients and use this to determine emergency conditions.

On the other hand, recently, medical information platforms applying edge computing systems have been studied to control various IoT sensors(biometric sensor, medical device, environment sensor, etc.) and provide patient context-based services[4,5,18,26]. The edge computing system is located between the medical devices and the medical information server. The edge computing system performs device management, monitoring of patient's biometric information, preprocessing biometric data, transmitting data to the medical information server, and determining patient's emergency conditions. Md. Abdur Rahman et al.[5] designed a medical cloud service applying edge computing to download the necessary COVID-19

prediction model for each region and tested COVID-19 via camera. Min Chen et al.[4] studied a platform to focus edge computing hardware resources on emergency patients by hand-over smart devices connected to edge computing to other edge computing in emergency conditions. Applying edge computing systems have advantages such as support for quick decision-making by medical staff, localization, and flexible system operation according to patient conditions. However, when a staff accesses patient information, the authentication and authorization have a problem with excessive access rights compared to simple authentication. In addition, the patient's condition was not considered as context authentication information. Therefore, in this paper, we apply edge computing to determine the patient's emergency conditions quickly and then aim for a study on authentication based on the patient's conditions.

3. Design of Our Researched Platform

3.1 Structure of Our Platform

The structure of the extended automatic authentication-supported medical information platform using big data processing, AI mechanism, and edge computing is shown in **Fig. 1**. The smart space device part consists of medical devices and IoT. It transmits a patient's biometric data such as ECG, SpO2, NIBP, and environmental data such as temperature and humidity to an edge node in the edge computing part. The edge node preprocesses the received data and determines the patient's emergency conditions. The edge node uses the patient's condition decision value and model from the medical information server. The medical information server stores the biometric data into a biometric big data database and performs modules of big data processing and AI to derive conditions decision value and model considering patient's underlying diseases such as hypertension, diabetes mellitus, and arrhythmia. The authentication server performs the automatic authentication when the patient is in emergency conditions. The details of the automatic authentication in emergency conditions are explained in Section 3.2. The mobile terminal receives emergency messages, attempts the automatic authentication to the authentication server, and accesses the patient's graded information according to access rights.

3.2 Details of the Automatic Authentication in Our Platform

Fig. 2 shows the automatic authentication procedure in emergency conditions. If the edge node determines the patient's condition as an emergency condition, the edge node notifies the patient's emergency to the medical information server. The medical information server immediately transmits an emergency message, including an authentication code required for user authentication of the automatic authentication. At the same time, the medical server transmits the authentication information of the medical staff in charge to the authentication server. The transmitted authentication information is ID/PWD, the authentication code, role, working time, and working hours of the medical staff.

To access a patient's medical information in emergency conditions, the medical staff attempts the automatic authentication through an application on the mobile terminal owned by the medical staff. The proposed automatic authentication is an authentication system that strengthens the transparency of access and enables rapid authentication of medical staff in emergency conditions of patients[17]. The automatic authentication consists of user authentication and mobile terminal authentication. The user authentication is performed with the ID/PWD of medical staff, and the authentication code is added in case of emergency conditions. After user authentication complication, mobile terminal authentication is

performed automatically without the intervention of medical staff. The medical staff's role, working hours, and working location are used as mobile terminal authentication means. The medical staff who have completed the automatic authentication get higher access rights and can access upper-level medical information of patients. Suppose the patient's condition changes from emergency to normal condition after completing emergency treatment. In that case, the medical staff's access rights obtained in the emergency are lost, and they no longer have access to upper-level patient medical and personal information.

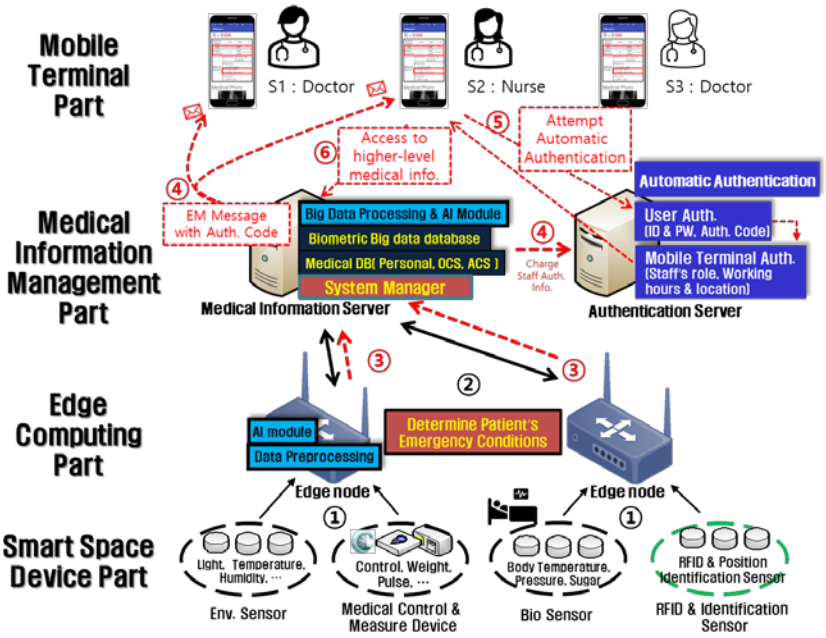

Fig. 1. The structure of the extended automatic authentication-supported medical information platform using bigdata processing, AI mechanism, and edge computing

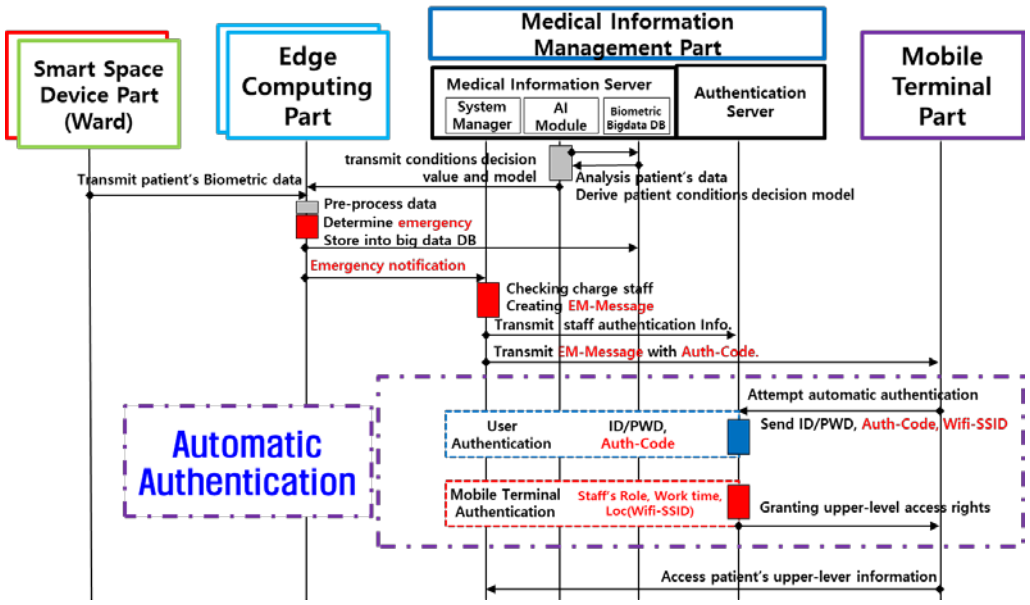

Fig. 2. The automatic authentication procedures using the patients' emergency conditions.

3.3 Categorizing patient's medical and personal information and setting access rights

As shown in **Table 1**, We categorized patients' medical and personal information into three levels. The rule of categorizing patient information was set regarding the sensitivity of medical information[27].

Table 1. An example of graded medical and personal information of patients

	Medical Information	Personal Information
Lv.1	Representative medical image, Medical department, Room-num.	Name, Age, Sex, Weigh Birthdate
Lv.2	Current hospitalization diagnosis record	Guardian's name, Home number, Home Address
Lv.3	Real-time IoT medical data, Additional medical imaging pictures, previous diagnosis	Social security number, phone number Health insurance ID

In addition, we set access rights according to the patient's conditions for the certified medical staff, as shown in **Table 2**. For example, a doctor attempts user authentication to access the patient's information in the patient's normal condition. After the user authentication, the doctor can access only level 1 and 2 medical information and personal information. Conversely, in emergency conditions, the doctor attempts the automatic authentication and can access levels 1,2,3 medical and personal information that could not be seen in the normal condition.

Table 2. An example of access rights by conditions

Role	Normal	Pre-Emergency	Emergency
Nurse	Lv. 1	Lv. 1, 2 (Only Medi Info)	Lv. 1, 2
Cooperating doctor	Lv. 1, 2 (Level 1)	Lv. 1, 2, 3 (Only Medi Info)	Lv. 1, 2, 3 (Level 1, 2)
Doctor in charge	Lv. 1, 2	Lv. 1, 2, 3 (Only Medi Info)	Lv. 1, 2, 3

3.4 Finding Emergency Conditions for The Automatic Authentication

3.4.1 Biometric Data and ECGs Used for Finding Emergency Conditions

In this paper, we used the patient's emergency condition as the authentication means for the automatic authentication. The patient's underlying diseases such as hypertension, diabetes mellitus, and arrhythmias are considered when determining emergency conditions. We used blood pressure and blood sugar data from National Health Insurance Sharing Service(NHISS) to detect hypertension and diabetes mellitus[28] and used MIT-BIH Arrhythmia ECG Databases to detect arrhythmia[29].

The NHISS data is 1 million data, and the data collection period is from 2013 to 2014 and was collected through general health checkups and "life transition health checkups" [28]. This data consists of the patient's biometric attributes: sex, age group(BTH_G), systolic blood

pressure(SBP), diastolic blood pressure(DBP), fasting blood sugar(FBS), body mass index(BMI), and diagnosis(DIS) meaning underlying diseases. The detail of blood pressure and blood sugar data from NHISS is shown in **Table 3**.

Table 3. Detail of blood pressure and blood sugar data from NHISS

Attribute	Description	Code / Value
Sex	Sex	1: Man
		2: Woman
BTH_G	Age Group	1: 20 ~ 24 age
		2 ~ 26: grouped by 2 years
		27: 75+ group
SBP	Systolic Blood Pressure	82-190 (mmHg)
DBP	Diastolic Blood Pressure	50-120(mmHg)
FBS	Fasting Blood Sugar	60-358(mg/dL)
BMI	Body Mass Index	14.8-40.3(kg/m^2)
DIS	Diagnosis	1: Complication(HTN/DM)
		2: Hypertension(HTN)
		3: Diabetes Mellitus(DM)
		4: None

The MIT-BIH Arrhythmia ECG Database is representative data among ECG open sources[29]. This database was selected from approximately 4000 records measured by the Holter method at Beth Israel Hospital Arrhythmia Laboratory from 1975 to 1979. The MIT-BIH Arrhythmia ECG Database of 48 records is selected from the same database, with 23 randomly selected and 25 data for rare but clinically significant phenomena. **Fig. 3**. illustrates an ECG signal and a sample labeled R from the MIT-BIH Arrhythmia ECG Database.

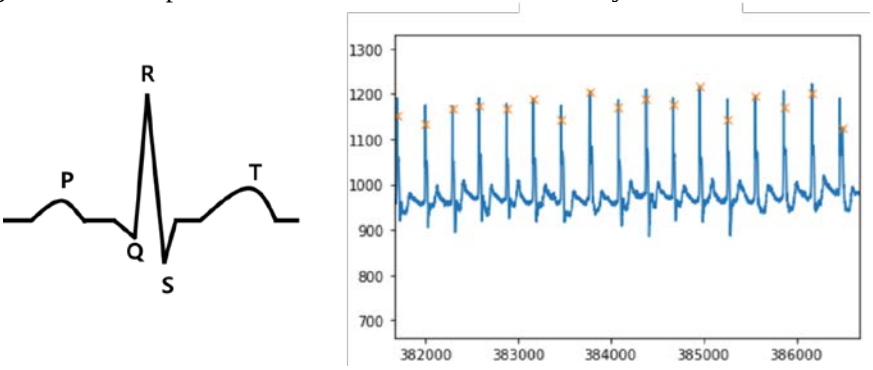

Fig. 3. Illustration of ECG signal and a sample labeled R from the MIT-BIH database.

3.4.2. Applying Big data Processing and AI Mechanism

To detect hypertension(HTN), diabetes mellitus(DM), and complications(HTN/DM) of a patient's underlying diseases when determining the patient's emergency conditions, we use the NHISS data and SVM of the machine learning mechanism. The SVM is used in classification or regression analysis and has excellent performance, especially in

classification[25]. Input data $x = (x_1, x_2, \ldots, x_n)$ of SVM are sex, BTH_G, SBP, DBP, FBS, BMI, and output data y is DIS. Duplication of the NHISS data was removed, the input data were normalized, and the sex attribute was processed by One-Hot Encoding. We split the training data and test data in a ratio of 7:3. We used ThunderSVM in the Python library because of the fast-learning time of the big data. The training time took 2 minutes, and the accuracy is 99.5% for training data and 74.1% for test data. The HTN and DM can be detected through NHISS data and SVM, and it is used as context information for the automatic authentication.

The MIT-BIH data is used to detect arrhythmias via 1-D CNN of deep learning models. The 1-D CNN architecture is shown in **Fig. 4**. This model classifies ECG heartbeat into five categories according to Association for the Advancement of Medical Instrumentation(AAMI) standards: Normal Beat, Supraventricular Ectopic Beat(SVEB), Ventricular Ectopic Beat(VEB), Fusion Beat, and Unknown Beat[30].

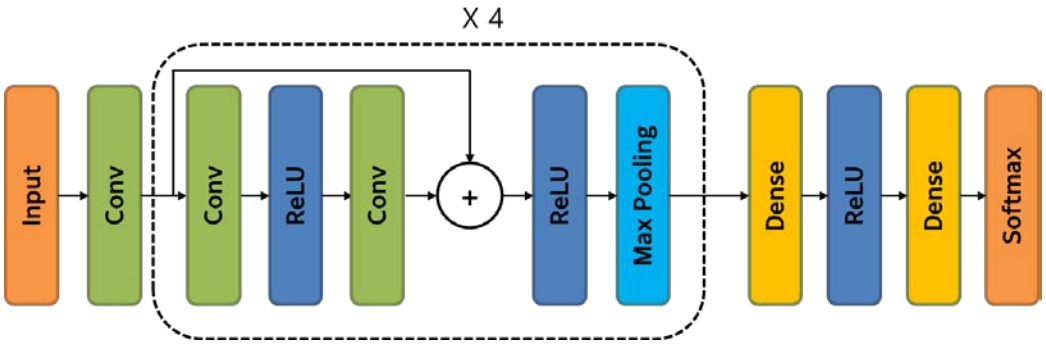

Fig. 4. The architecture of the 1-D CNN model.

ECG input data were normalized and segmented based on the R wave. The length of segmented data was fixed through zero padding. This architecture extract features through 4 blocks composed of 2 convolutional kernels with ReLU and max pooling. The feature is fed to a sequential Dense Fully Connected Layer, and the result is input into SoftMax to classify the five types of arrhythmias. The average model accuracy was 93.2% at 100 epochs and five iterations. This model has 94% accuracy for Normal Beat, 93% for SVEB, 95% for VEB, 88% for Fusion Beat, and 96% for Unknown Beat, as shown in **Fig. 5**. We can detect a patient's arrhythmia through the 1-D CNN, and we use it to find a patient's emergency conditions.

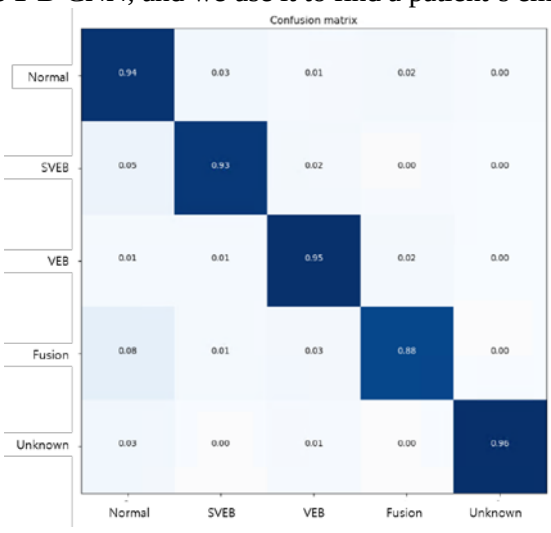

Fig. 5. Accuracy confusion metrics of the 1-D CNN model.

Table 4 shows the patient's emergency conditions decision model for detecting the patient's underlying disease using SVM and 1-D CNN and the patient's emergency conditions decision values for patient information and real-time data[31]. The medical information server transmits the patient-customized emergency conditions decision value and model based on the patient's record to the edge node. The edge node determines the patient's condition using this value and model.

Table 4. Patient's emergency conditions decision value and model

Type	Data	Normal	Pre-Emergency	Emergency
Real-Time Biometric Data	SpO2 (%)	≥95	≥90	≥85
	Heart Rate (/min)	60 - 90	91 - 119	120 - 130
	Respiration Rate (/min)	12 - 20	9 - 11, 21 - 24	≤ 8, ≥ 25
	Temperature (℃)	36.1 - 38.0	35.1 - 36.0 38.1 - 39.0	≤ 35.0, ≥ 39.1
Detecting Underlying Diseases Model	SBP / SVM (mmHg)	-	HTN	Complications (HTN/DM)
	FBS / SVM (mg/DL)	-	DM	Complications (HTN/DM)
	ECG / 1-D CNN	-	-	Arrhythmia Detection

4. Implementation of the Extended Medical Information Platform

3.1 Implementation of the Components of the Proposed Platform

To implement the smart space device part, as shown in **Fig. 6**, we used a Bio-Medical System Development Kit(BMS-AE-DK)[32] that can measure ECG, NIBP, Respiration, SpO2, and Impedance, and an S-Patch that is wearable ECG single-lead Holter monitoring sensor[33]. These sensors transmit biometric data to connected edge nodes.

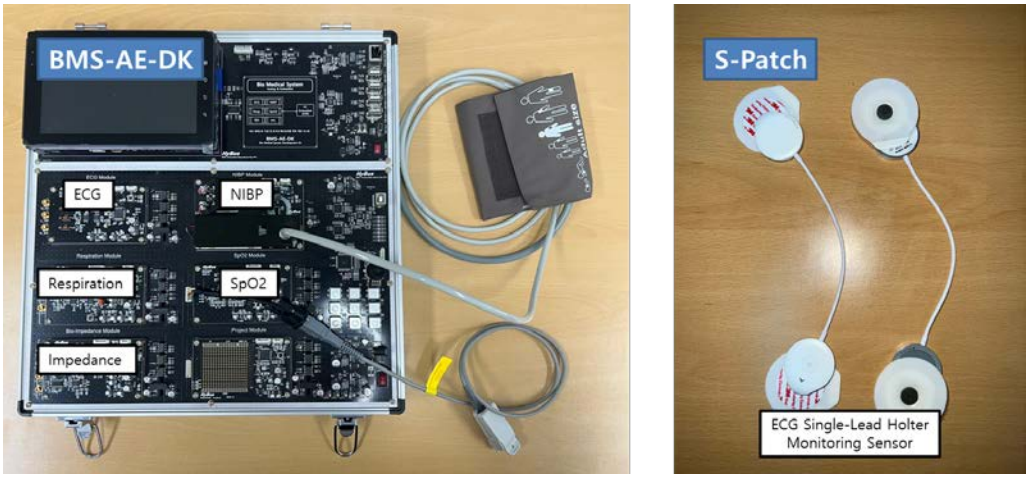

Fig. 6. BMS-AE-DK biometric sensor and S-Patch ECG sensors in smart space device part

The edge computing part was implemented using four Raspberry Pi 4 8 GB units, and the medical information server and authentication server were implemented using desktop Ubuntu OS. Also, we implement a web server using Apache2, PHP, and MySQL on the edge computing, the medical information server, and the authentication server. The mobile terminal part was implemented using Android Studio. Each component communicates through the HTTP JSON standard.

3.2 The Proposed Platform's Implementation Procedures and its results

Fig. 7 shows an implementation of patient information input, determining patient's emergency, and procedures in emergency conditions. The medical staff registers the patient's information, which is sex, age, underlying diseases, FBS, SBP, etc. The medical information server's big data processing module and AI module derive the patient-customized conditions decision value and model based on the patient information and transmit it to the edge node connected to the patient. If the edge node determines the emergency conditions of the patient, the edge node notifies emergency conditions to the medical information server. The system manager of the medical information server checks the patient ID and the medical staff information in charge. Then the system manager generates an authentication code required for user authentication of the automatic authentication in case of emergency conditions. The system manager transmits the authentication information of the medical staff in charge with the authentication code to the authentication server to prepare for the automatic authentication. The transmitted information is the ID, PWD, the authentication code, role, working hours, and working location(Wi-Fi SSID) of the medical staff. At the same time, the system manager transmits an emergency message with the authentication code to the mobile terminals of the medical staff in charge through Google Firebase Cloud Messaging Service. With this, the medical staff in charge can attempt automatic authentication in the patient's emergency conditions and can quickly access the patient's upper-level information via the automatic authentication.

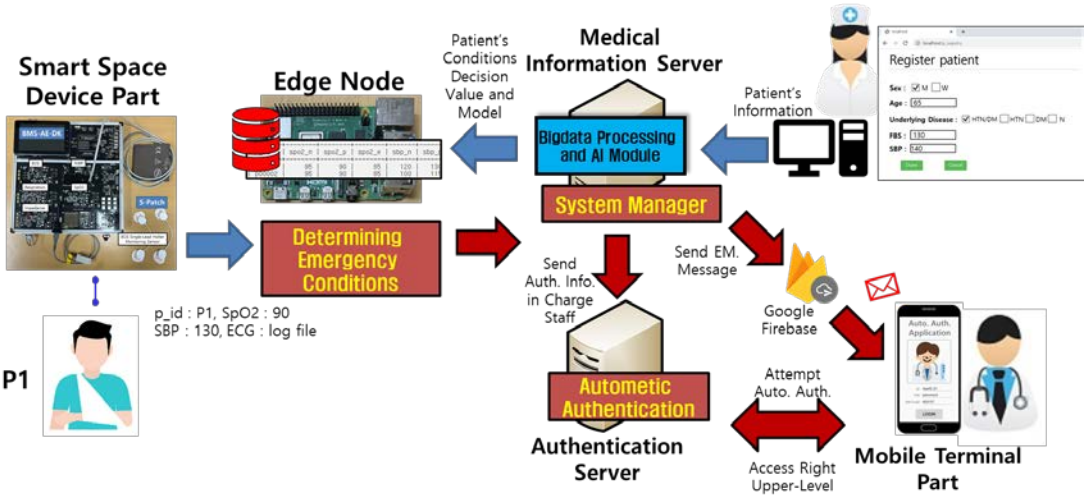

Fig. 7. Entering patient information, determining the patient's emergency condition, and procedures in emergency conditions.

When the medical staff receives the emergency message alarm, the authentication code box is automatically filled. The medical staff input PWD and attempted the automatic authentication, and the mobile terminal transmitted ID, PWD, the authentication code, and a

connected Wi-Fi SSID. The authentication server performs the automatic authentication. After the automatic authentication is completed, the authentication server grants higher access rights to the medical staff and the mobile terminal according to the role of the medical staff and the patient's condition, as shown in **Table 2**.

Fig. 8. Accessing to graded medical information of patients in each normal and emergency condition through a mobile terminal

The medical staff can access upper-level medical and personal information that could not be seen under normal condition, as shown in **Fig. 8**. When the patient's treatment is completed, the upper-level access rights are lost, and the medical staff no longer has access to the upper-level information.

5. Comparison

Some existing authentication studies in medical information services and platforms were investigated to structurally compare the automatic authentication-supported medical information platform. The comparison items are as follows: authentication subject, authentication target, authentication means, media for information access, authorization, and visualization of medical information, as shown in **Table 5**.

The investigated authentication studies only authenticate the target user. However, the proposed platform authenticates not only the users but also the mobile terminals. The proposed platform satisfies the medical information authentication model that requires two-step authentication of users and mobile terminals.

In the authorization stage, most studies have adopted the rule-based method. The authorization of the rule-based method is a method of granting authorization according to the role in the domain of the authentication target. In other words, authorization varies according to the roles within the medical information platform, such as doctors, nurses, patients, and system administrators. The proposed platform grants authority to consider the rule-based method and the patient's conditions as context information. Through this, context information can be used as an authentication means, and patient condition-oriented medical information access is possible.

There was no mention in most studies of the visualization of the medical information stage. Ren X Zhai et al. [38] applied a watermark to the screen shown in the mobile terminal application and de-identified the medical information. The proposed platform graded the

medical information and personal information, as shown in **Table 1** and **Table 2**, and displayed the patient's information according to the patient's condition and the role of medical staff in the mobile terminal, as shown in **Fig. 8**. For example, if the patient is in a normal condition, the medical staff can access only lower-level information such as name, age, and simple diagnosis records. However, suppose the patient is in an emergency condition. In that case, the medical staff can access higher-level information such as all diagnosis records, medical records, and insurance status. The proposed platform visualizes graded medical information according to the patient's condition to prevent medical information from being leaked in the patient's normal condition.

Table 5. Structural comparison of authentication studies

	Auth. Subject	**Auth. Target / Auth. Means**	**Media for Info. Access**	**Authorization**	**Visualization of Medical Info.**
[34]	Patient	**User**: Username, Password, Bio-Info.	Mobile, Web	Only Personal Info.	-
[35]	Medical Staff	**User**: ID, Password, Digital-Sign, Working Time	Web	Role Based Authorization Group	-
[36]	Patient / Medical Staff	**User**: ID, Password, Face Identity	Web	Only Personal Info. / Authorization Group	-
[37]	Medical Staff	**User**: FIDO (Fingerprint)	Mobile	No mentioned	-
[38]	Medical Staff	**User**: Password, SMS	Mobile	Role Based Authorization Group	Watermark, De-identification
The Proposed Platform	Medical Staff	**User**: ID, Password, Auth. Code **Mobile Terminal**: Working Time, Working Location	Mobile	Role Based Authorization Group & Patient's Condition	De-identification, Grading Medical Information

6. Conclusion

In this paper, we studied on finding emergency conditions for the automatic authentication using big data processing and AI mechanism on the extended medical information platform with the added edge computing system. The SVM and 1-D CNN of AI mechanisms were used to find emergency conditions based on the patient's underlying disease and use it as context information for the automatic authentication. By adding edge computing system to the medical information platform, it was possible to quickly determine the patient's emergency conditions at the edge node instead of the medical information server. If the edge node determines the patient's emergency conditions, it sends the medical information server an emergency message as soon as it transmits the emergency message to the patient's medical staff in charge. At the same time, the medical information server transmits the authentication information of the medical staff in charge to the authentication server. This allows the medical staff to attempt the automatic authentication to the authentication server in case of an emergency of the patient. The medical staff performs the automatic authentication using a mobile terminal to access the upper-level information of the patient in emergency conditions. After the automatic authentication is completed, the medical staff can access the patient's upper-medical information that was not seen in the normal condition.

This paper's contributions are as follows: we found emergency conditions of patients considering patients' underlying diseases from ECG and biometric big data, and the emergency conditions are used in the automatic authentication in our platforms. In addition, we proposed the automatic authentication-supported medical information platform with an expanded structure by adding the edge computing system. The proposed platform can help medical fields that want to apply patient condition-centered authentication, big data processing, AI mechanisms, and edge computing system.

For future research and direction, our proposed platform will evaluate for platform's executability. By applying the proposed platform to a medical field using ECG data, we will study data preprocessing and AI techniques suitable for field data for patient arrhythmia detection. In addition, by applying the proposed platform to the medical field, we will evaluate the performance and executability of the platform's components.

Acknowledgement

This research was supported by Wonkwang University in 2021. We thank Wellysis Co. that providing the S-Patch Cardio of a wearable electrocardiogram device and for their helpful comments.

References

[1] X. Liu, Y. Zhu, Y. Ge, D. Wu and B. Zou, "A Secure Medical Information Management System for Wireless Body Area Networks," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 1, pp. 221-237, Jan. 2016. Article (CrossRef Link)

[2] P. Pace, G. Aloi, R. Gravina, G. Caliciuri, G. Fortino and A. Liotta, "An Edge-Based Architecture to Support Efficient Applications for Healthcare Industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 481-489, Jan. 2019. Article (CrossRef Link)

[3] Darshan K R and Anandakumar K R, "A comprehensive review on usage of Internet of Things (IoT) in healthcare system," in *Proc. of 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, pp. 132-136, 2015. Article (CrossRef Link)

[4] Min Chen, Wei Li, Yixue Hao, Yongfeng Qian and Iztok Humar, "Edge cognitive computing based smart healthcare system," *Future Generation Computer Systems*, vol. 86, pp. 403-411, Sep. 2018. Article (CrossRef Link)

[5] M. A. Rahman, M. S. Hossain, N. A. Alrajeh and N. Guizani, "B5G and Explainable Deep Learning Assisted Healthcare Vertical at the Edge: COVID-I9 Perspective," *IEEE Network*, vol. 34, no. 4, pp. 98-105, Jul. 2020. Article (CrossRef Link)

[6] G.-S. Ham and S.-C. Joo, "Development of Authentication Service Model Based Context-Awareness for Accessing Patient's Medical Information," *Journal of Internet Computing and Services*, vol. 22, no. 1, pp. 99–107, Feb. 2021. Article (CrossRef Link)

[7] J.-Y. Hong and H.-H. Kim, "A Study on Awareness Levels of Personal Information Protection in Health Care Workers," *Journal of the Korea Entertainment Industry Association*, vol. 13, no. 8, pp. 647–659, Dec. 2019. Article (CrossRef Link)

[8] J. Kim and K. Chung, "Prediction Model of User Physical Activity using Data Characteristics-based Long Short-term Memory Recurrent Neural Networks," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 4, pp. 2060-2077, Apr. 2019. Article (CrossRef Link)

[9] J. Y. Cho, D. Ko and B. G. Lee, "Strategic Approach to Privacy Calculus of Wearable Device User Regarding Information Disclosure and Continuance Intention," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 7, pp. 3356-3374, Jul. 2018. Article (CrossRef Link)

[10] Park M, Oh H, Lee K, “Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Conditional Awareness Perspective,” *Sensors*, vol. 19, no. 9, May. 2019. Article (CrossRef Link)
[11] IBM, “Cost of a Data Breach Report 2021,” 2021. [Online]. Available: https://www.ibm.com/security/data-breach
[12] D. Eom, H. Lee, and H. Zoo, “Medical Information Privacy Concerns in the Use of the EHR System: A Grounded Theory Approach,” *Journal of Digital Convergence*, vol. 16, no. 1, pp. 217–229, Jan. 2018. Article (CrossRef Link)
[13] El-hajj, Mohammed, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni, “A Survey of Internet of Things (IoT)- Authentication Schemes,” *Sensors*, vol. 19, no. 5, p. 1141, 2019. Article (CrossRef Link)
[14] Yi Yu, Jingsha He, Nafei Zhu, Fangbo Cai, Muhammad Salman Pathan, “A new method for identity authentication using mobile terminals,” *Procedia Computer Science*, vol. 131, pp. 771-778, 2018. Article (CrossRef Link).
[15] Jayabalan, Manoj, and Thomas O’Daniel, "A study on authentication factors in electronic health records," *Journal of Applied Technology and Innovation*, vol. 3, no. 1, pp. 7-14, 2019.
[16] Su-Chong Joo, “Automatic Authentication Method based on Dynamic Context for Transparent Access for Medical Information,” South Korea Patent 10-2026018, Sep. 2019.
[17] Ahmed Ismail, Samir Abdlerazek and I. M. El-henawy, “Big Data Analytics in Heart Diseases Prediction,” *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 11, pp. 1970-1980, Jun. 2020. Article (CrossRef Link)
[18] Singh, S.P., Nayyar, A., Kumar, R. et al. “Fog computing: from architecture to edge computing and big data processing,” *J Supercomput*, vol. 75, pp. 2070–2105, Apr. 2019. Article (CrossRef Link)
[19] Nishita Mehta, Anil Pandit, “Concurrence of big data analytics and healthcare: A systematic review,” *International Journal of Medical Informatics*, vol. 114, pp. 57-65, Jun. 2018. Article (CrossRef Link).
[20] Lorkowski J., Grzegorowska O., Pokorski M., “Artificial Intelligence in the Healthcare System: An Overview,” in *Best Practice in Health Care, Pokorski M. eds.*, vol. 1335, Ed. Poland, Springer, 2021, pp. 1-10
[21] Lee, C. H., & Yoon, H. J., “Medical big data: promise and challenges,” *Kidney research and clinical practice*, vol. 36, no. 1, pp. 3–11. Mar. 2017. Article (CrossRef Link)
[22] Edward Min, “The Application of Deep Convolutional Networks for the Classification of ECG Signal,” GitHub, 2019. [Online]. Available: https://github.com/eddymina/ECG_Classification_Pytorch
[23] F. J. P. Montalbo, "A Computer-Aided Diagnosis of Brain Tumors Using a Fine-Tuned YOLO-based Model with Transfer Learning," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 12, pp. 4816-4834, Dec. 2020. Article (CrossRef Link).
[24] Harimoorthy, K., Thangavelu, M., “Multi-disease prediction model using improved SVM-radial bias technique in healthcare monitoring system,” *J Ambient Intell Human Comput*, vol. 12, pp. 3715–3723, 2021. Article (CrossRef Link)
[25] Kai Hwang, Min Chen, *Big-data analytics for cloud, IoT and cognitive computing*, Hoboken, New Jersey: Wiley, Apr. 2018.
[26] A. Rasheed, P. H. J. Chong, I. W. Ho, X. J. Li and W. Liu, "An Overview of Mobile Edge Computing: Architecture, Technology and Direction," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 10, pp. 4849-4864, Oct. 2019. Article (CrossRef Link)
[27] Milne, G.R., Pettinico, G., Hajjat, F.M. and Markos, E., “Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing,” *J Consum Aff*, vol. 51, no. 1, pp. 133-161. 2017. Article (CrossRef Link)
[28] “Blood Pressure and Blood Sugar Data,” National Health Insurance Sharing Service(NHISS) Korea. [Online]. Available: https://nhiss.nhis.or.kr/bd/ab/bdabf003cv.do
[29] Moody GB, Mark RG, “The impact of the MIT-BIH Arrhythmia Database,” *IEEE Eng in Med and Biol*, vol. 20, no. 3, pp. 45-50, Jun. 2001. Article (CrossRef Link)

[30] AAMI, “Testing and reporting performance results of cardiac rhythm and ST segment measurement algorithms,” ANSIAAMI EC38, Tech. Rep., 1998. Article (CrossRef Link)
[31] Habib, Carol, et al., "Health risk assessment and decision-making for patient monitoring and decision-support using wireless body sensor networks," *Information fusion*, vol. 47, pp. 10-22, May. 2019. Article (CrossRef Link)
[32] Hybus, [Online]. Available: http://hybus.net/ko/sub/product/view.asp?p_idx=68&s_cate=1217
[33] Wellysis, [Online]. Available: https://www.wellysis.com/
[34] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," *IEEE Access*, vol. 8, pp. 52018-52027, 2020. Article (CrossRef Link)
[35] Kim Jeom Goo, “Implementation of Role-based Multi-authentication System for Secure Smart Home,” *the journal of Korean institute of next generation computing*, vol. 17, no. 4, pp. 59-68, 2021. Article (CrossRef Link)
[36] S.-C. Bae, Y.-S. Lee, and S.-W. Choi, “Vision-based Authentication and Registration of Facial Identity in Hospital Information System,” *Journal of the Korea Society of Computer and Information*, vol. 24, no. 12, pp. 59–65, 2019. Article (CrossRef Link)
[37] Y. Kim and Y. J. Choi, “Design and Implement of Authentication System for Secure User Management for Secure on Medical ICT Convergence Environment,” *Journal of Information and Security*, vol. 19, no. 3, pp. 29–36, 2019. Article (CrossRef Link)
[38] Ren, X., Zhai, Y., Song, X., Wang, Z., Dou, D., & Li, Y., “The application of mobile telehealth system to facilitate patient information presentation and case discussion,” *Telemedicine and e-Health*, vol. 26, no. 6, pp. 725-733, 2020. Article (CrossRef Link)

Gyu-Sung Ham received a B.S. degree in Computer Engineering from Wonkwang University in 2018. He received an M.S. degree in Computer Engineering from Wonkwang University in 2020. Currently, he is in Ph.D. candidate in the Dept. of Computer Engineering from Wonkwang University. His main research interests include Distributed Systems, Authentication Systems, Healthcare Services, Medical Bigdata, and AI.

MinGoo Kang has been a professor in the Dept. of IT Transmedia Contents at Hanshin University, South Korea, since 2000. He has received his B.S., M.S., and Ph.D. degrees from Yonsei University, Seoul, Korea, all in Electronic Engineering in 1986, 1989, and 1994, respectively. He was a research engineer at Samsung Electronics from 1985 to 1997. His research interests include Wireless Communication Algorithms, Smart Mobile IoT, and Blockchain Security.

Su-Chong Joo received a B.S. degree in Dept. of Computer Engineering from Wonkwang University in 1986. He received an M. S. and Ph. D. degrees from the Dept. of Computer Science and Engineering from Chung-Ang University in 1988 and 1992, respectively, in South Korea. He is currently a professor in the Dept. of Computer · Software Engineering at Wonkwang University. From Jul. 1993 to Aug. 1994, he was a Post-Doctoral Fellow at Dept. of Electrical and Computer Engineering in University of Massachusetts at Amherst. Also, from Dec. 2002 to Jan. 2005 and from Jul. 2009 to Jul. 2010, he was a visiting professor at Dept. of Electrical Engineering and Computer Science in University of California at Irvine. He served as the Dean of Wonkwang University College of Engineering from 2015 to 2017. He is a member of KISS, IASTED, IEEE and IEEE computer society. His main research interests include Distributed Middleware Computing, Multimedia Database Systems, and Ubiquitous Computing(u_Home and Healthcare Services).