Edge Computing-Based Medical Information Platform for Automatic Authentication Using Patient Situations

Gyu-Sung Ham[1], Mingoo Kang[2], Suck-Tae Joung[3*] 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: stjoung@wku.ac.kr, scjoo@wku.ac.kr]
[*]Corresponding author: Suck-Tae Joung and Su-Chong Joo

Received December 1, 2022; revised February 2, 2023; accepted March 27, 2023; published April 30, 2023

Abstract

Recently, with the development of IoT, AI, and mobile terminals, medical information platforms are expanding. The medical information platform can determine a patient's emergency situation, and medical staff can easily access patient information through a mobile terminal. However, in the existing platform, emergency situation decision is delayed, and faster and stronger authentication is required in emergency situations. Therefore, we propose an edge computing-based medical information platform for automatic authentication using patient situations. We design an edge computing-based medical information platform architecture capable of rapid transmission of biometric data of IoT and quick emergency situation decision, and implement the platform data flow in emergency situations. Relying on this platform, we propose the automatic authentication using patient situations. The automatic authentication protects patient information through patient-centered authentication by using the patient's situation as an authentication factor, and enables quick authentication by automatically proceeding with mobile terminal authentication after user authentication in emergencies without user intervention. We compared the proposed platform with existing platforms to show that it can make quick and stable emergency decisions. In addition, comparing the automatic authentication with existing authentication showed that it is fast and protects medical information centered on patient situations in emergency situations.

Keywords: Automatic Authentication, Medical Information Platform, Edge Computing, Emergency Situations, Emergency Situation Decisions.

This paper is an extension and enhanced version of the earlier conference papers presented at the KSII 17th Asia Pacific International Conference on Information Science. This paper includes detailed design and data flow charts for each part of this platform, comparison experiments with existing platforms, and experiments on the effectiveness of automatic authentication in emergency situations.

http://doi.org/10.3837/tiis.2023.04.001 **ISSN : 1976-7277**

1. Introduction

A medical information platform is essential for managing and operating medical information in hospitals[1–3]. Medical staff write and manage patient medical information and diagnostic records using electronic medical records (EMR), clinical device information system (CDIS), digital imaging, and communications in medicine (DICOM) within the medical information platform[4]. The medical information platform is expanding with the recent development of the internet of things (IoT), artificial intelligence (AI), and mobile terminals[5–8]. The patient's biometric data can be easily acquired through numerous IoT, and medical device sensors installed in the ward. The data stored in the medical database can be used in various medical fields using machine learning and deep learning models. In addition, the medical information platform can determine the emergency situation of each patient[9–11]. If the patient is in an emergency situation, an emergency message is delivered to the medical staff in charge. The medical staff who have received the emergency message can access patient information after undergoing the authentication required by the medical information platform through the application of the mobile terminal owned by the medical staff.

However, despite the many advantages above, applying IoT, AI, and mobile terminals to medical information platforms faces the following problems. First, due to the physical distance between the IoT and the server of the medical information platform, the transmission delay time of the patient's biometric data occurs[12]. Second, the emergency situation decision time for each patient in the medical information server is unstable. The reason is that a query delay time for searching the patient's emergency condition occurs due to a large number of data stored in the database of the medical information server. In addition, if the medical information server is learning deep learning when processing continuous streaming data coming from the IoT, hardware and network resources are concentrated for learning, so the emergency decision time is delayed due to the resource limitations of a single server[13]. The medical information platform should quickly deliver the patient's emergency situations to the medical staff and provide reliable services. Finally, a fast and enhanced authentication method is required when accessing patient information in emergency situations[14]. Because medical information is sensitive, medical security requirements, including user authentication and mobile terminal authentication, must be met to access patient medical information using a mobile terminal. However, in this case, it is difficult for the medical staff to quickly access patient information through the mobile terminal due to the complicated authentication process[15].

To solve the above problems and to effectively apply the various advantages of IoT, AI, and mobile terminals to the medical information platform, this paper proposes an edge computing-based medical information platform for automatic authentication using patient situations. The main contributions of this study are as follows.

First, we propose an edge computing-based medical information platform capable of fast biometric data transmission of IoT and fast emergency decisions. This platform makes emergency decisions for each patient in the edge computing closer to the IoT data source rather than a medical information server and can reduce biometric data transmission time. In addition, the emergency condition and emergency situation decision AI model are transmitted to edge computing to enable quick emergency situation decisions through localization.

Second, we design and implement data flow to enable stable operation of the platform in case of emergency. AI model learning for emergency decision is performed in the medical information server, and emergency situation decision is separated from the medical information server to be performed in edge computing to prevent overload of the medical information server. In addition, it designs and implements platform procedures in emergency

situations, such as sending emergency messages to medical staff and interlocking with authentication servers for the automatic authentication of medical staff.

Thirdly, relying on the edge computing-based medical information platform, we propose automatic authentication using patient situations. This automatic authentication automatically performs user authentication and mobile terminal authentication for access to medical information only when the patient is in emergency situations. This allows medical staff to authenticate quickly when a patient is in emergency situations.

The remainder of this paper is organized as follows. Section 2 presents an overview of the related works. Section 3 presents the architecture of the edge computing-based medical information platform and the automatic authentication using patient situations. Section 4 shows the data flow of the proposed platform and a detail of implementation. Section 5 presents our experimental results, and finally, Section 6 summarizes the conclusions and future research.

2. Related Works

2.1 Medical Information Platform and Edge Computing

The medical information platform stores medical data in a cloud server and provides services such as analysis, emergency notification, and access to patient information to medical staff. The medical information platform stores medical data in a cloud server and provides services such as analysis, emergency notification, and accessing patient information to medical staff. There are advantages to using a medical information platform: easy access to medical information, cost reduction, productivity and efficiency increase, and scalability according to organizational needs[16-18].

As the amount of sensing data increases, medical information platforms using edge computing, a distributed computing technology, are being researched according to the needs of hospitals and researchers. Edge computing is a computing technology built close to data sources, and performs IoT device management, data preprocessing, and monitoring[19]. Subahi et al. [18] summarized the limitations of existing medical information systems and the requirements, strengths, and limitations of cloud and edge-based medical information platforms. Min Chen et al. [13] concentrated edge computing hardware resources on the emergency patient by handover the intelligent devices connected to edge computing to other edge computing when an emergency occurs to the patient. Yan He et al. [12] implemented an EdgeCNN network that can perform electrocardiogram classification in edge computing while reducing communication costs. Rahmani et al. [20] proposed an edge-fog-based gateway structure that can determine emergency situations through various sensors in the IoT environment. Like previous studies, medical information systems combine edge computing with networking, big data processing, and AI to provide various services to medical staff and researchers. In our study, we design an edge computing-based medical information platform that can quickly determine emergency situations, and conduct research combining system authentication.

2.2. System Authentication in Medical Field

System authentication consists of an authentication step to confirm the subject's identity using authentication factors such as ID/password and an authorization step to grant authority to the authenticated subject[21]. In the medical field, system authentication is critical because medical data includes the patient's diagnosis and personal information[22]. Therefore, more

robust authentication is required for medical staff to access patient information. In particular, with the development of mobile terminal technology, medical staff can easily access patient medical information using their mobile terminal, so authentication for mobile terminals must be added at the system level according to medical security requirements[14].

However, as authentication targets and procedures are strengthened, security increases while convenience decreases[15]. Complicated authentication procedures cause an uncomfortable situation for medical staff who need to quickly access patient information through a mobile terminal in emergency situations for emergency treatment. Accordingly, various studies have been conducted on fast and enhanced authentication steps in emergency situations[14,23–25]. However, due to the limitations of rule-based authorization, medical staff can access patient information whenever possible. Therefore, we include the patient's situation as an authentication factor and study the authorization considering the patient's situation.

3. Edge Computing-Based Medical Information Platform Architecture for Automatic Authentication Using Patient Situations

3.1. Edge Computing-Based Medical Information Platform Architecture

In this subsection, we propose the architecture of the edge computing-based medical information platform that can quickly determine a patient's emergency with a short delay time of the sensors for providing automatic authentication using patient situations, as shown in **Fig. 1**. The architecture composes of smart space device part, edge computing part, medical information management part, and mobile terminal part.

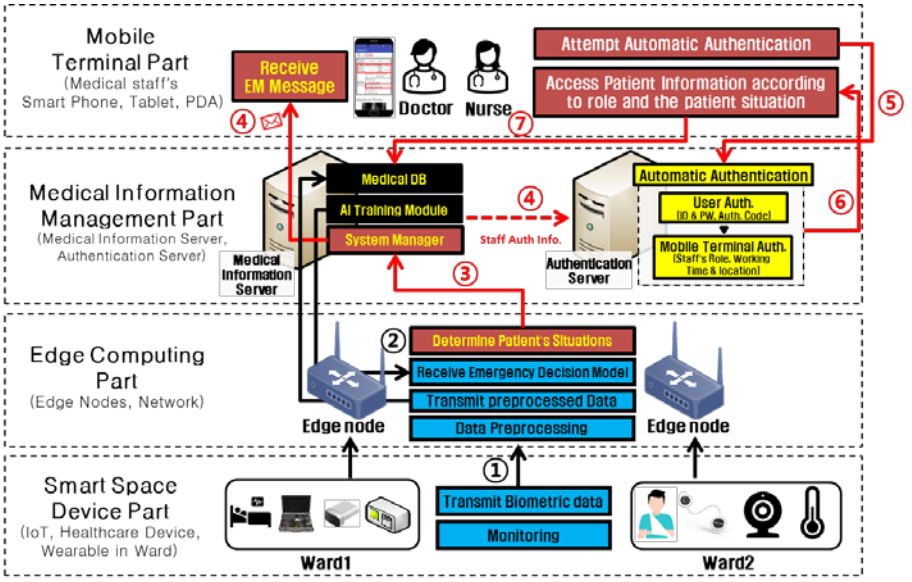

Fig. 1. Edge computing-based medical information platform architecture for automatic authentication using patient situations.

The smart space device part involves a series of IoT, healthcare devices and wearable such as pulse oximeter, electrocardiogram, blood pressure monitor, respirometer and so on. They monitor various physical indicators of the patient and generate biometric data. The biometric data types include SpO2, heart rate, temperature, NIBP, ECG, and more. These devices cannot

effectively process biometric data due to hardware limitations in computing power and storage space[26]. They are responsible for transmitting the generated biometric data to the edge computing part.

The edge computing part performs preprocessing of biometric data before going to the medical information server and determines the patient's situation. Since the edge computing unit is performed close to the data source, biometric data transmission time can be reduced. Furthermore, since many IoT connections are taken from edge computing, the network transmission bandwidth of the medical information server can be saved. Since the sensor data is preprocessed by edge computing before being stored in the medical information server, efficient data storage in the medical information server is also possible. On the other hand, since each patient has a different disease, various heterogeneous sensors are located in each ward. Therefore, the emergency situation decisions performed by edge computing in each ward differ from ward to ward. The medical information server transmits patient-customized emergency conditions and emergency decision models derived through machine learning and deep learning using patient information and data from medical databases to edge computing in each ward and the edge computing perform them.

The medical information management part consists of a medical information server and an authentication server. The medical information server manages the overall hospital using a medical data management system such as EMR and stores massive medical data in the medical database. The stored medical data of the patients are graded according to security sensitivity. One of the medical information server's core functions is centralized machine learning and deep learning model for patient disease prediction, diagnosis, and analysis. In our platform, the medical information server trains various AI models for patient-customized emergency conditions and sends them to edge computing for execution. The authentication server provides authentication and authorization for the medical staff to access patient information using a mobile terminal. The authentication server performs automatic authentication, which is the core of this study, and the details of automatic authentication are in subsection 3.2. The authentication server manages the authentication information of the medical staff according to the patient situation. When the patient situation is an emergency, the medical information server transmits authentication information for the automatic authentication of the medical staff to the authentication server. The authentication server grants graded access rights to medical staff who have completed the automatic authentication according to the patient's situation and the role of the medical staff. Through this, the medical staff can quickly access patient information in emergency situations and access high-level medical information. The authentication server and the automatic authentication allow the medical staff to quickly access patient information in emergency situations and to access high-level medical information.

The mobile terminal part consists of mobile terminals such as smartphones and tablets. When the patient is in emergency situations, the mobile terminal receives an emergency message from the medical information server. The medical staff can access patient information through applications provided by the medical information platform. Due to sensitive medical information, in order to access patient information, the platform must provide systematically enhanced authentication. In our platform, we set different authentication methods and access rights according to the patient situation. If the patient is in a normal situation, only user authentication is required, and only low-level medical information access is allowed. If the patient's situation is emergency situations, the medical staff can perform automatic authentication, which automatically performs mobile terminal authentication without medical intervention after user authentication in emergency situations. After the automatic authentication, medical staff can access high-level medical information that could not be seen

under normal situation.

3.2. Automatic Authentication Using Patient Situations

3.2.1. Motivation

When a patient's emergency situation occurs, the medical staff must quickly access the patient's information for emergency treatment. However, due to the complexity of the existing authentication process and limited regulations for protecting medical information, the existing authentications are inconvenient in emergency situations. In addition, unlike a fixed PC located in a hospital, authentication for mobile terminals with mobility is essential[27]. Existing medical staff-centered authentication in mobile terminals also raises the problem of medical information leakage, as medical staff can easily access patient information whenever and wherever they want[28].

This section introduces automatic authentication using patient situations for fast and enhanced authentication in emergency situations. Our automatic authentication uses the patient situation as an authentication factor, so it is not the existing medical staff-centered authentication, but a patient-centered authentication that has not existed. In addition, automatic authentication is provided instead of complicated authentication procedures to medical staff only in emergency situations of patients so that more robust and faster authentication can be performed. Since our automatic authentication uses the patient context, it is suitable for a medical information platform that can grasp the patient's situation in real-time. This study's scope of research is system authentication, which does not deal with cryptography for physical communication. It aims at efficient and enhanced system authentication in emergency situations.

3.2.2. Procedure for The Automatic Authentication.

In order to access the patient's medical information in emergency situations, the medical staff attempts the automatic authentication to the authentication server using a mobile terminal owned by the medical staff. The automatic authentication consists of user authentication and mobile terminal authentication.

User authentication is performed for the medical staff who are users on the platform. The authentication method of user authentication is ID and Password, and in emergency situations, even the authentication code included in the emergency message is used.

Mobile terminal authentication is to authenticate the mobile terminal of the medical staff. Mobile terminal authentication is to authenticate the mobile terminal of the medical staff. Mobile terminal authentication is automatically performed without user intervention after user authentication in emergency situations. The authentication factors of mobile terminal authentication are the medical staff's role, working hours, and working location. The working location checks whether the mobile terminal is connected to the internal network of the medical information platform and can be confirmed through the service set identifier (SSID).

When automatic authentication is completed, the authentication server grants upper-level access to medical information according to the role of the medical staff and the patient situation. The medical staff who have been granted access to upper-level medical information can check the upper-level medical information of patients that they could not see under normal situation. The bottom of **Fig. 2** shows the automatic authentication procedure.

We graded patients' medical and personal information into three levels according to security sensitivity[29]. We classify access rights as shown in **Table 1** according to the role of the medical staff and the patient situation[18]. If the patient is in an emergency situation, the

doctor receives an emergency message and performs automatic authentication. A certified doctor can access patient information corresponding to levels 1, 2, and 3. When the patient's emergency treatment is finished and the patient's situation is changed from emergency to normal, the access right that the doctor has gained is lost and can no longer access upper-level medical information.

Table 1. Classified access right according to the role of medical staff and the patient situation.

Role	Normal	Pre-Emergency	Emergency
Nurse	Level 1	Level 1, 2 (Level 1)	Level 1, 2
Cooperating doctor	Level 1, 2 (Level 1)	Level 1, 2, 3 (Level 1, 2)	Level 1, 2, 3 (Level 1, 2)
Doctor in charge	Level 1, 2	Leve. 1, 2, 3 (Level 1, 2)	Level 1, 2, 3

4. Data Flow and Implementation of The Proposed Platform

4.1. Platform Scenario

This subsection presents details of the interaction of the parts of the platform. **Fig. 2** shows the flow chart for the whole scenario of our platform. **Table 2** lists the command sets designed for this platform.

Each patient in the smart space device part wears IoT, medical devices, and wearables. The devices transmit the patient's biometric data to edge computing in each ward. After preprocessing the received patient biometric data, edge computing determines the patient's emergency situations through the emergency condition and emergency situation decision model of each patient received from the medical information server.

If the patient is in an emergency situation, edge computing notifies the emergency situation to the medical information server. The medical information server checks the database to identify the patient's medical staff. The medical information server generates an authentication code and transmits the authentication information of the medical staff to the authentication server for automatic authentication. At the same time, an emergency message, including an authentication code, is transmitted to the mobile terminal of the medical staff. Upon receiving the emergency message, the medical staff attempts automatic authentication to access the upper-level medical information of the patient. At this time, the only action that the medical staff does is input the password, and ID, the authentication code, and SSID information are automatically included.

The authentication server performs automatic authentication requested by the medical staff. After authentication, the authentication server grants upper-level medical information access rights to the mobile terminal and the medical staff according to the role of the medical staff and the patient situation. According to their authority, medical staff can access the patient's medical and personal information through the mobile terminal.

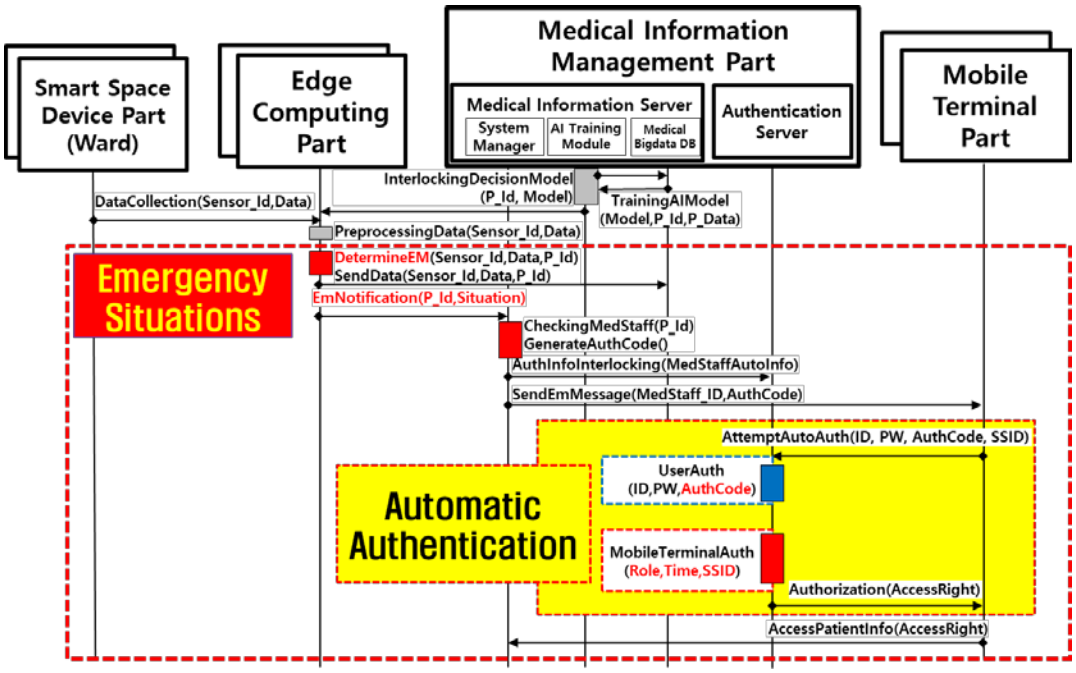

Fig. 2. The flow chart for the whole scenario of our platform.

Table 2. Overview of the critical command set.

Command	Functionality	Part
DetermineEM (Sensor_Id,Data,P_Id)	Determine a patient situation using the emergency condition and decision models received from the medical information server	Edge Computing
EmNotification (P_Id,Situation)	Notify the patient's emergency situation to the medical information server	
InterlockingDecisionModel (P_Id,Model)	Interlocking emergency condition and decision model for patient-customized situation decision	Edge Computing, Medical Information Server
TrainingAIModel (Model,P_Id,P_data)	Analysis patient’s data and derive emergency conditions and decision model using machine and deep learning	Medical Information Server
CheckingMedStaff(P_Id)	Check the patient's medical staff's information	
GenerateAuthCode()	Generate authentication code required for mobile terminal authentication	
SendEmMessage (MedStaff_ID,AuthCode)	An emergency message including an authentication code is transmitted to the mobile terminal of the medical staff. Notify patient's emergency	
InterlockingAuthInfo (MedStaffAutoInfo)	Interlocking the authentication information of the medical staff in charge for automatic authentication	Medical Information Server, Authentication Server
UserAuth (ID,PW,AuthCode)	Authenticate for user using ID, PW, and AuthCode	Authentication Server
MobileTerminalAuth (Role,Time,SSID)	Authenticate for mobile terminal using Role, Time, and SSID	
Authorization (AccessRight)	Grant access rights according to the patient situation and the role of the medical staff	
ReceiveEmMessage (AuthCode)	Receive emergency message with authentication code	Mobile Terminal
AttemptAutoAuth (ID, PW, AuthCode, SSID)	Medical staff try automatic authentication using mobile terminal applications to access upper-level medical information	
AccessPatientInfo (AccessRight)	Access to upper-level medical information of patients with granted access rights	

4.2. Patient-Customized Emergency Situation Decisions and Interactive Process of Edge Computing and Medical Information Server

The medical information server uses medical database data to provide patient-customized emergency conditions and AI models into edge computing, and the edge computing determines the patient's emergency situation. **Table 3** lists the patient emergency condition reference[30]. We divide the patient situation into three levels, i.e., normal, pre-emergency, and emergency. The adopted indexes of real-time biometric data include SpO2, heart rate, respiration rate, temperature, and systolic blood pressure. The adopted indexes of emergency situation decision model include hypertension, diabetes, complications, and arrhythmias. The real-time biometric data indicates the patient's biological status. When checking a patient's emergency situation, the patient's situation is determined according to the numerical value of each biometric data, so AI technology is not required. For example, if a patient's temperature is over 40℃, it's clear that the patient is in an emergency situation. However, detecting underlying disease and arrhythmia is difficult using one biometric data type. Therefore, we used machine learning and deep learning algorithm to detect the patient's underlying disease and arrhythmia with one or more biometric data.

Table 3. Patient emergency conditions and decision model reference.

Type	Data / AI model		Patient Situation		
			Normal	Pre-Emergency	Emergency
Emergency Condition Using 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
Emergency Situation Decision Model Using Machine and Deep Learning	Detecting Underlying Diseases Model	Systolic Blood Pressure, (mmHg) / Decision Tree	-	Hypertension	Complications
		Fast Blood Sugar (mg/DL) / Decision Tree	-	Diabetes	Complications
	Arrhythmia Detect Model	ECG / 1-D CNN		-	Arrhythmia Detection

The detecting underlying disease models are developed using Decision Tree with blood pressure and blood sugar data from the National Health Insurance Sharing Service(NHISS)[37]. The NHISS data has 1 million data and includes systolic blood pressure(SBP), diastolic blood pressure(DBP), fasting blood sugar(FBS), patient information(sex, age, BMI), and diagnosis information(DIS). The diagnosis information

includes normal, diabetes, hypertension, and complications. We trained various machine learning models using NHISS data. The trained models were Naive Bayes, K-nearest Neighbor, Decision Tree, and SVM. As a result of the training, the learning time of the Decision Tree was 0.85926 seconds, and the validation accuracy of the Decision Tree was 76.476%, showing the best performance among the trained models. Therefore, we used Decision Tree to determine the patient's underlying disease.

The arrhythmia detection model used MIT-BIH ECG data[38] and the 1-Dimension Convolution Neural Network(1-D CNN) Deep learning algorithm. The MIT-BIH arrhythmia ECG data is one of the most famous arrhythmias ECG open-source data. This model was designed to classify five arrhythmia categories according to the AAMI standard [39]. As a result of testing the trained arrhythmia detection model, the average F1 score was 98% for the five arrhythmia categories. This model is a reliable level for arrhythmia detection on ECG data. If there is an AI algorithm with better performance in determining emergency situations, it can be replaced on the proposed platform.

The medical information server creates a patient's emergency condition and decision model with machine learning and deep learning from the patient's biometric data and medical information. The medical information server transmits the result to the edge computing installed in the patient's ward. This enables faster decision-making by transmitting and localizing conditions and models on the edge computing rather than the medical information servers.

4.3.Implementation of Patient Information Access According to Access Right

The implementation details are as follows. For the implementation of the Smart Space Device Department, we used the Bio-Medical System Development Kit (BMS) that can measure ECG, NIBP, Respiration, and SpO2[31] and used the wearable device S-Patch, which can measure ECG[32]. We implemented the edge computing part with Raspberry Pi 4 8GB, which is the most widely used instrument for implementing edge computing. The medical information management part was implemented with desktop ubuntu, and the mobile terminal part was implemented with Android Studio.

Fig. 3 shows the implementation details of checking emergency message confirmation, attempting automatic authentication, and accessing patient information in the medical staff's mobile terminal. **Fig. 4** shows that certified medical staff have access to medical information according to the patient's situation and the role of the medical staff.

For example, a doctor accesses level 2 medical information after user authentication in a patient's normal situation. If the patient is emergency situations, the doctor attempts the automatic authentication and can access level 3 medical information. It allows access to sensitive information such as detailed medical records, medical images, social security numbers, phone numbers, guardians, and insurance status that could not be seen under normal situation. If the patient's situation changes from emergency situation to normal situation after emergency measures, the upper medical level is released, and the patient's sensitive medical and personal information can no longer be accessed. Through the automatic authentication using the patient situation, the platform can protect medical information centered on the patient situation rather than the medical staff situation, and quick authentication is possible in emergency situations.

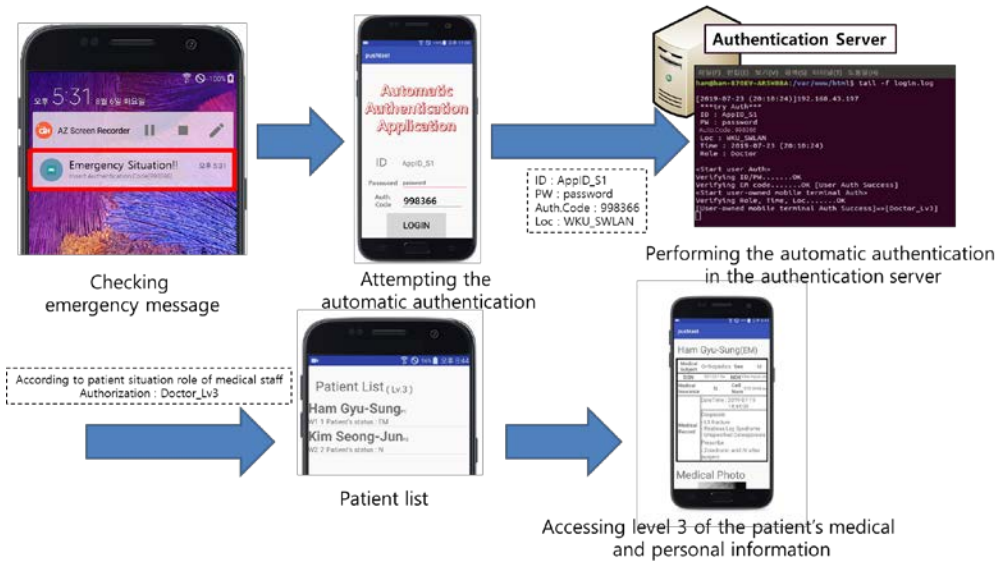

Fig. 3. The implementation details of checking emergency message confirmation, attempting automatic authentication, and accessing patient information in the medical staff's mobile terminal.

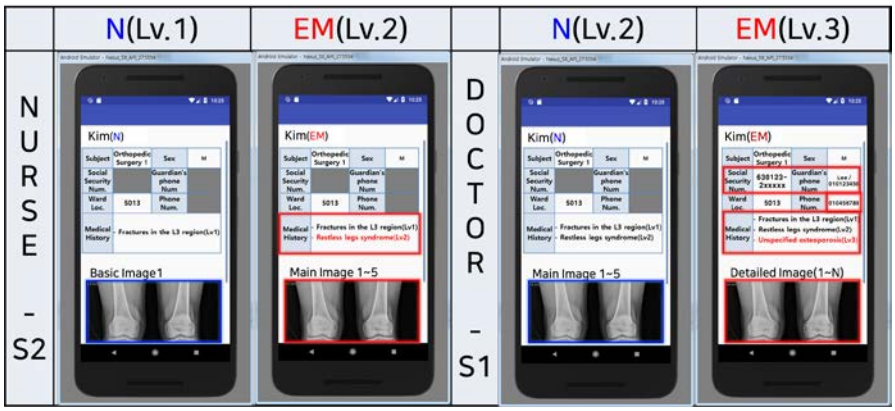

Fig. 4. Accessing medical information according to the patient's situation and the role of the medical staff.

5. Executability Evaluation

5.1. Comparison of Two Different Platform

In this section, we evaluate the executability and performance of the edge computing-based medical information platform for automatic authentication. Emergency decision time and transmission delay are evaluated by comparing the proposed platform with existing platforms, and structural network properties in emergency situations are compared.

First, we experiment to compare the transmission delay of the two platforms. Transmission delay is an important indicator used to evaluate platform performance. We implemented a test bed, as shown in **Fig. 5**, and as a measurement item for transmission delay, biometric data transmission time from the sensor part t1, and execution time of emergency situation decision t2. **Table 4** shows the average of the times measured ten times in the test bed environment.

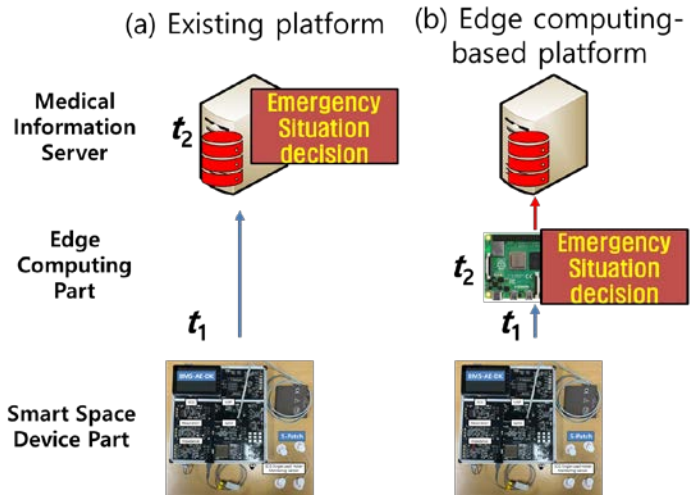

Fig. 5. Test bed for comparison of transmission delay of two platforms. (a) Existing medical information platform without edge computing; (b) Edge computing-based medical information platform.

t_1 on the proposed platform was 1.104*ms* faster than the existing platform. The reason is that the physical communication time can be reduced because edge computing is performed close to the smart space device part. In t_2, the edge computing-based medical information platform was 1.922*ms* faster. The reason is that the number of queries for patient emergency situations performed by edge computing is less than the medical information server in the existing platform. Since edge computing only stores the patient's emergency conditions and AI model requested by the medical information server, it has less information than the medical information server of the existing platform, has all the patient's information, and can reduce query time. This enables localization on edge computing-based platforms, enabling quick emergency situation decisions. The overall transmission delay was reduced by 3.5028*ms* for the edge computing-based medical information platform compared to the existing platform.

Table 4. Measurement results in the testbed environment.

Time	(a) Existing platform	(b) Edge-based platform
t_1	1.580*ms*	1.104*ms*
t_2	6.160*ms*	4.2372*ms*
$t_1 + t_2$	7.7400*ms*	5.3412*ms*

Second, a system-wide comparison for determining emergency situations between the existing platform and the edge computing-based platform is summarized in **Table 5**. The above experiment confirmed that transmission delay for determining emergency situations of the edge computing-based platform, which can process data close to the data source and reduce the number of queries through localization, was lower than the existing platform. Unlike servers in the existing platform where all patient data is exposed to the external network, in the edge computing-based platform, only numerical values and AI models are transmitted to edge computing, and edge computing and sensors are located on the internal network. As a result, edge computing-based platforms are more secure regarding privacy when determining emergency situations. The edge computing-based platform preprocesses the biometric data coming into the distributed edge computing and determines an emergency in each edge

computing. Through this, the edge computing-based platform satisfies high availability and prevents overload. However, in the existing platform, all functions are performed by a single server, so high availability is not satisfied, and overload is likely to occur.

Table 5. The system-wide comparison for determining emergency situations between two platforms.

Attribute	Existing platform	Edge-based platform
Transmission delay	High	Low
Privacy	Insecure	More secure
Scalability	High cost	Low cost
Overload	High availability dissatisfied, Overload occurrence	High availability satisfied, Prevent overload

5.2. The Automatic Authentication Evaluation

Existing authentication uses only user authentication, but with the development of mobile terminals, medical security requires authentication for mobile terminals. Accordingly, in the existing platform, user authentication and mobile terminal authentication must be performed respectively according to the requirements. However, existing authentication studies do not satisfy mobile terminal authentication[33–35]. Our automatic authentication proceeds with mobile terminal authentication after user authentication under emergency situations without user intervention. In addition, existing authentication grants role-based authority[22,36], but this is a medical staff-centered authentication and does not utilize the platform's ability to determine the patient's situation in real-time. Our automatic authentication is suitable for the platform environment where patient situations can be determined in real-time, and patient information is protected through user-centered authentication using patient situations as an authentication factor.

To compare the existing two authentications (user authentication, mobile terminal authentication) and automatic authentication, we compare the authentication request time from the mobile terminal to the authentication server in our platform environment. The total time T for an authentication request mainly consists of four parts: The authentication attempt time from an authentication subject to the authentication server is T_{attempt}, the authentication factor verification time in the authentication server is T_{verify}, the time for authorizing the subject is $T_{\text{authorize}}$, and the return time for authentication request to the subject is T_{return}. Therefore, the authentication request time $T_{\mathbf{subject}}$ can be described as:

$$T_{\mathbf{subject}} = T_{\text{attempt}} + T_{\text{verify}} + T_{\text{authorize}} + T_{\text{return}} \tag{1}$$

According to medical security requirements, the existing authentication time $T_{\mathbf{existing}}$ can be described as the sum of user authentication $T_{\mathbf{user}}$ and mobile terminal authentication $T_{\mathbf{mobile}}$ as follows:

$$T_{\mathbf{existing}} = T_{\mathbf{user}} + T_{\mathbf{mobile}} \tag{2}$$

According to equation (1), (2) can be rewritten as:

$$T_{\mathbf{existing}} = 2 \times (T_{\text{attempt}} + T_{\text{return}}) + T_{\text{verify\_}\mathbf{user}} + T_{\text{verify\_}\mathbf{mobile}} + T_{\text{authoize}} \tag{3}$$

In the existing authentication, since each user authentication and mobile terminal authentication is performed, an attempt time and a return time are additionally generated. When both authentications are completed, authority is granted at once.

On the other hand, our automatic authentication request time $T_{\mathbf{autoauth}}$ is a process that simultaneously handles user authentication and mobile terminal authentication under emergency situations, so it can be described as follows:

$$T_{\mathbf{autoauth}} = T_{\text{attempt}} + T_{\text{verify\_}\mathbf{user}} + T_{\text{verify\_}\mathbf{mobile}} + T_{\text{authorize}} + T_{\text{return}} \quad (4)$$

Compared to (3), the T_{attempt} and T_{return} values are removed, enabling automatic authentication faster than existing authentication in emergency situations.

$T_{\mathbf{existing}}$ and $T_{\mathbf{autoauth}}$ were measured ten times in our platform environment. Each average was measured at 3.486109*ms* for $T_{\mathbf{existing}}$ and 2.41189*ms* for $T_{\mathbf{autoauth}}$, so the automatic authentication is 1.074219*ms* faster than the existing authentication. In conclusion, our automatic authentication can provide fast and enhanced authentication to medical staff in emergency situations. Furthermore, it enables patient-centered authentication and authorization by granting authorized medical staff considering the patient's situation rather than rule-based authorization.

6. Conclusions

In this paper, we proposed the edge computing-based medical information platform for automatic authentication using patient situations. We designed the architecture and data flow of the edge computing and medical information server so that the patient's emergency situations can be determined in the edge computing, not the medical information server. By arranging edge computing close to the smart space device parts, it was possible to reduce the biometric data transmission time. In each edge computing located in the ward, the emergency situation decision time can be reduced compared to the existing medical information server through localization using only the emergency condition and decision model of each patient. In addition, the proposed platform is more effective in privacy protection, scalability, and overload protection for emergency situations decisions.

In the proposed platform, we proposed the automatic authentication using patient situations. Our automatic authentication enables quick authentication for medical staff by proceeding with mobile terminal authentication after user authentication in emergency situations without user intervention. This automatic authentication grants authorized medical staff access rights considering the patient's situations. Through this, it is possible to protect patient information by enabling authorization based on patient situations rather than authorization based on the medical staff.

As for future research, we will study how to link edge computing and mobile terminals to notify emergency situations to medical staff quickly. The delay in notifying the medical information server of an emergency from edge computing is added, thereby increasing the time for medical staff to receive an emergency message. In order to solve this problem, we will research fast emergency notifications for mobile terminals connected to the internal network of the medical information platform. In addition, we plan to develop an emergency decision model that can cover a wide range of medical fields using cardiac fibrillation data and various medical data.

Acknowledgement

This research was supported by Wonkwang University in 2021.

References

[1] A. K. Gupta, K. S. Mann, "Sharing of Medical Information on Cloud Platform-A Review," *IOSRJCE*, vol. 16, pp. 08–11, Apr. 2014. Article (CrossRef Link)

[2] A. Rashed, A. Ibrahim, A. Adel, B. Mourad, A. Hatem, M. Magdy, N. Elgaml, A. Khattab, "Integrated IoT Medical Platform for Remote Healthcare and Assisted Living," in *Proc. of the 2017 Japan-Africa Conference on Electronics, Communications and Computers (JAC-ECC)*, pp. 160–163, Feb. 2017. Article (CrossRef Link)

[3] T. Ali, J. Hussain, M. B. Amin, M. Hussain, U. Akhtar, W. A. Khan, S. Lee, B. H. Kang, M. Hussain, M. Afzal, et al., "The Intelligent Medical Platform: A Novel Dialogue-Based Platform for Health-Care Services," *Computer*, Vol. 53, pp. 35–45, Feb. 2020. Article (CrossRef Link)

[4] F. Yang, X. Chen, X. Lin, X. Chen, W. Wang, B. Liu, Y. Li, H. Pu, L. Zhang, D. Huang, et al., "Automated Analysis of Doppler Echocardiographic Videos as a Screening Tool for Valvular Heart Diseases," *JACC: Cardiovascular Imaging*, Vol. 15, pp. 551–563, 2022. Article (CrossRef Link)

[5] L. Liu, J. Xu, Y. Huan, Z. Zou, S.-C. Yeh, L.-R. Zheng, "A Smart Dental Health-IoT Platform Based on Intelligent Hardware, Deep Learning, and Mobile Terminal," *IEEE Journal of Biomedical and Health Informatics*, Vol. 24, pp. 898–906, Jun. 2020. Article (CrossRef Link)

[6] Z. Lu, P. Qian, D. Bi, Z. Ye, X. He, Y. Zhao, L. Su, S. Li, Z. Zhu, "Application of AI and IoT in Clinical Medicine: Summary and Challenges," *CURR MED SCI*, Vol. 41, pp. 1134–1150, 2021. Article (CrossRef Link)

[7] P. Malik, M. Pathania, V. K. Rathaur, "Overview of Artificial Intelligence in Medicine," *Journal of family medicine and primary care*, Vol. 8, pp. 2328-2331, 2019. Article (CrossRef Link)

[8] H. Bolhasani, M. Mohseni, A. M. Rahmani, "Deep Learning Applications for IoT in Health Care: A Systematic Review," *Informatics in Medicine Unlocked*, Vol. 23, No. 100550, 2021. Article (CrossRef Link)

[9] M. Fernandes, S. M. Vieira, F. Leite, C. Palos, S. Finkelstein, J. M. Sousa, "Clinical Decision Support Systems for Triage in the Emergency Department Using Intelligent Systems: A Review," *Artificial Intelligence in Medicine*, Vol. 102, No. 101762, Jan. 2020. Article (CrossRef Link)

[10] S. K. Lakshmanaprabu, S. N. Mohanty, S. Krishnamoorthy, J. Uthayakumar, K. Shankar, "Online Clinical Decision Support System Using Optimal Deep Neural Networks," *Applied Soft Computing*, Vol. 81, No. 105487, Aug. 2019. Article (CrossRef Link)

[11] K. A. Fahmy, A. Yahya, M. Zorkany, "A Decision Support Healthcare System Based on IoT and Neural Network Technique," *Journal of Engineering, Design and Technology*, Vol. 20, pp. 727–748, 2022. Article (CrossRef Link)

[12] Y. He, B. Fu, J. Yu, R. Li, R. Jiang, "*Efficient Learning of Healthcare Data from IoT Devices by Edge Convolution Neural Networks*," *Applied Sciences*, Vol. 10, No. 8934. Dec. 2020. Article (CrossRef Link)

[13] M. Chen, W. Li, Y. Hao, Y. Qian, I. Humar, "Edge Cognitive Computing Based Smart Healthcare System," *Future Generation Computer Systems*, Vol. 86, pp. 403–411. Sep. 2018. Article (CrossRef Link)

[14] C. Wang, W. Zheng, S. Ji, Q. Liu, A. Wang, "Identity-Based Fast Authentication Scheme for Smart Mobile Devices in Body Area Networks," *Wireless Communications and Mobile Computing*, Vol. 2018, pp. 1-7. Aug. 2018. Article (CrossRef Link)

[15] A. J. Oluwafemi, J. H. Feng, "Usability and Security: A Case Study of Emergency Communication System Authentication," in *Proc. of the International Conference on Human-Computer Interaction*, Springer, pp. 205–210, 2019. Article (CrossRef Link)

[16] G. S. Ham, M. Kang, S. C. Joo, "Executability Evaluation of Automatic Authentication Supported Medical Information Platform Applying Edge Computing, Big Data Processing, and AI Model," in *Proc. of APIC-IST 2022*, pp. 198–200, 2022.
[17] G.S. Ham, M. Kang, S.C. Joo, "A Study on Finding Emergency Conditions for Automatic Authentication Applying Big Data Processing and AI Mechanism on Medical Information Platform," *KSII Transactions on Internet & Information Systems*, Vol. 16, No. 8, pp. 2772-2786, Aug. 2022. Article (CrossRef Link)
[18] A. F. Subahi, "Edge-Based IoT Medical Record System: Requirements, Recommendations and Conceptual Design," *IEEE Access*, Vol. 7, pp. 94150–94159, Jul. 2019. Article (CrossRef Link)
[19] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, D. S. Nikolopoulos, "Challenges and Opportunities in Edge Computing," in *Proc. of the 2016 IEEE International Conference on Smart Cloud (SmartCloud)*, IEEE, pp. 20–26, Dec. 2016. Article (CrossRef Link)
[20] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, P. Liljeberg, "Exploiting Smart E-Health Gateways at the Edge of Healthcare Internet-of-Things: A Fog Computing Approach," *Future Generation Computer Systems*, Vol. 78, pp. 641–658, 2018. Article (CrossRef Link)
[21] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, S. Samad, "Authentication Systems: A Literature Review and Classification," *Telematics and Informatics*, Vol. 35, pp. 1491–1511, Aug. 2018. Article (CrossRef Link)
[22] Y. Kim, Y. J. Choi, "Design and Implement of Authentication System for Secure User Management for Secure on Medical ICT Convergence Environment," *Convergence Security Journal*, Vol. 19, No. 29–36, Sep. 2019. Article (CrossRef Link)
[23] X. Hei, X. Du, "Biometric-Based Two-Level Secure Access Control for Implantable Medical Devices during Emergencies," in *Proc. of the 2011 Proceedings IEEE INFOCOM*, IEEE, Shanghai, pp. 346–350, Apr. 2011. Article (CrossRef Link)
[24] C. L. Hsu, T. V. Le, M. C. Hsieh, K.Y. Tsai, C. F. Lu, T. W. Lin, "Three-Factor UCSSO Scheme with Fast Authentication and Privacy Protection for Telecare Medicine Information Systems," *IEEE Access*, Vol. 8, pp. 196553–196566, Oct. 2020. Article (CrossRef Link)
[25] B. D. Deebak, F. H. Memon, S. A. Khowaja, K. Dev, W. Wang, N.M.F. Qureshi, "In the Digital Age of 5G Networks: Seamless Privacy-Preserving Authentication for Cognitive-Inspired Internet of Medical Things," *IEEE Trans. Ind. Inf.*, Vol. 18, pp. 8916–8923, May. 2022. Article (CrossRef Link)
[26] N. D. Lane, S. Bhattacharya, P. Georgiev, C. Forlivesi, and F. Kawsar, "An Early Resource Characterization of Deep Learning on Wearables Smartphones and Internet-of-Things Devices," in *Proc. of the 2015 International Workshop on Internet of Things towards Applications*, *Association for Computing Machinery*, pp. 7–12, Nov. 2015. Article (CrossRef Link)
[27] R. Mayrhofer, S. Sigg, "Adversary Models for Mobile Device Authentication," *ACM Comput. Surv.*, Vol. 54, No. 9, pp. 1-35, 2021, Article no. 198. Article (CrossRef Link)
[28] Cost of a Data Breach 2022. [Online]. Available: https://www.ibm.com/reports/data-breach
[29] G. R. Milne, G. Pettinico, F. M. Hajjat, E. Markos, "Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing," *Journal of Consumer Affairs*, Vol. 51, pp. 133–161, 2017. Article (CrossRef Link)
[30] C. Habib, A. Makhoul, R. Darazi, R. Couturier, "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)
[31] HyBus. [Online]. Available: http://hybus.net/ko/sub/product/view.asp?p_idx=68&s_cate=1217
[32] Wellysis. [Online]. Available: https://www.wellysis.com/
[33] M. A. Khan, M. T. Quasim, N. S. Alghamdi, 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, Mar. 2020. Article (CrossRef Link)
[34] Jeom Goo Kim, "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, Aug. 2021. Article (CrossRef Link)

[35] S. C. Bae, Y. S. Lee, 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. Dec. 2019. Article (CrossRef Link)
[36] X. Ren, Y. Zhai, X. Song, Z. Wang, D. Dou, Y. Li, "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, Jun. 2020. Article (CrossRef Link)
[37] "Blood Pressure and Blood Sugar Data," National Health Insurance Sharing Service(NHISS) Korea. [Online]. Available: https://nhiss.nhis.or.kr/bd/ab/bdabf003cv.do
[38] 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)
[39] AAMI, "Testing and reporting performance results of cardiac rhythm and ST segment measurement algorithms," ANSIAAMI EC38, Tech. Rep., 1998. 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 College of AI · Software 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.

Suck-Tae Joung received the a B.S. degree in Dept. of Computer Science from Chonnam National University in 1989. He received an M.S. and Ph.D. degrees in Dept. of Computer Engineering from Tsukuba University, in 1996 and 2000, respectively, in Japan. He is currently a professor in the Dept. of Computer·Software Engineering at Wonkwang University. His research interests include Visual System, Facial Animation, and Healthcare Services.

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 an Emeritus professor in the Dept. of Computer · Software Engineering at Wonkwang University from March 1, 2023. 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).