**Original Article**

Healthc Inform Res. 2015 October;21(4):271-282.
http://dx.doi.org/10.4258/hir.2015.21.4.271
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

# Service-Oriented Security Framework for Remote Medical Services in the Internet of Things Environment

**Jae Dong Lee, MS, Tae Sik Yoon, MS, Seung Hyun Chung, MD, PhD, Hyo Soung Cha, PhD**
Department of Information Technology Team, National Cancer Center, Goyang, Korea

**Objectives:** Remote medical services have been expanding globally, and this is expansion is steadily increasing. It has had many positive effects, including medical access convenience, timeliness of service, and cost reduction. The speed of research and development in remote medical technology has been gradually accelerating. Therefore, it is expected to expand to enable various high-tech information and communications technology (ICT)-based remote medical services. However, the current state lacks an appropriate security framework that can resolve security issues centered on the Internet of things (IoT) environment that will be utilized significantly in telemedicine. **Methods:** This study developed a medical service-oriented framework for secure remote medical services, possessing flexibility regarding new service and security elements through its service-oriented structure. First, the common architecture of remote medical services is defined. Next medical-oriented security threats and requirements within the IoT environment are identified. Finally, we propose a "service-oriented security framework for remote medical services" based on previous work and requirements for secure remote medical services in the IoT. **Results:** The proposed framework is a secure framework based on service-oriented cases in the medical environment. A comparative analysis focusing on the security elements (confidentiality, integrity, availability, privacy) was conducted, and the analysis results demonstrate the security of the proposed framework for remote medical services with IoT. **Conclusions:** The proposed framework is service-oriented structure. It can support dynamic security elements in accordance with demands related to new remote medical services which will be diversely generated in the IoT environment. We anticipate that it will enable secure services to be provided that can guarantee confidentiality, integrity, and availability for all, including patients, non-patients, and medical staff.

**Keywords:** Telemedicine, Computer Security, Service-Oriented

**Submitted:** August 10, 2015
**Revised:** September 14, 2015
**Accepted:** September 16, 2015

**Corresponding Author**
Hyo Soung Cha, PhD
Information Technology Team, National Cancer Center, 323 Ilsan-ro, Ilsandong-gu, Goyang 10408, Korea. Tel: +82-31-920-1826, Fax: +82-31-920-1929, E-mail: kkido@ncc.re.kr



## I. Introduction

In accordance with the recent increases in human life expectancy and income, the medical·healthcare paradigm is gradually expanding to include post-treatment, prevention, and health management. It has become a serious challenge to meet the rise in expectations regarding medical services, while there is a lack of professionals in the field of welfare among other problems. Narrowly defined, 'remote medical service' means the provision of limited medical services, such as diagnosis and treatment via communication tools as

the medium without direct meeting between patient–doctor or doctor–doctor. However, the range of medical services delivered remotely has steadily expanded, and currently, the concept has expanded to include all types of health management service. Remote medical services can largely be classified into the following three categories: 'telemedicine', which allows for initial diagnosis by the doctor viewing the condition of the patient via a device that supports video imagery; 'remote monitoring', which allows for constant checking of information for an extended period of time and personalized diagnosis for treatment of chronic illness; and lastly, 'remote control' of remote diagnosis·remote treatment, etc., which utilize new information and communications technology [1,2].

Central to acquiring data for medical use is data acquisition and utilization technology in remote medical technologies. Such technology can utilize sensing technology and Internet of things (IoT) technology, which include wearable technology, making more concrete realization possible, and studies in the healthcare field utilizing these applied technologies are actively being conducted nowadays. However, in the IoT environment where a variety of data should be continually transmitted and processed, taking only partial security issues into consideration has led to seemingly small security threats can, in fact, be a threat to human lives. Furthermore, to support remote medical services in the IoT environment, previous studies have attempted to change services in accordance with sub-elements, and there is a constraint in that the entire structure should be restructured when security elements are added or a new service is created. Accordingly, there is a need for a method and structure that can satisfy the security demands of existing remote medical services and can dynamically support security demands regarding newly created services. In short, there is a need for studies regarding a new method and structure for remote medical services in the IoT environment [3,4].

This study aimed to provide flexibility regarding new services and security elements through a service-oriented structure. The proposed framework supports dynamic security elements for each service by including security elements throughout the entire process from the creation to the destruction of data.

## II. Methods

### 1. Common Architecture of Remote Medical Services and IoT

Here, we describe various types of remote medical services and define common elements and structures that serve as a basis for remote medical services in the IoT environment. In addition, the structural and functional limitations of the remote medical environment based on the defined elements are extracted.

First, 'remote treatment' is one type of medical service that is being developed that strives to overcome geographic and time-related obstacles. Remote treatment service was introduced for prisoners of the Full Sutton Prison located in a suburb of the city of York by Airedale NHS Foundation Trust of the United Kingdom in 2006. The kiosk-type unmanned telemedicine system 'HealthSpot Station', which was introduced on Consumer Electronics Show (CES) in 2013, is an installation-type clinic where various types of physical examination in addition to video treatment by a doctor are possible within the designated space. This includes many services, such as WellDoc BlueStar, which is a remote diabetes management mobile software approved by the US Food and Drug Administration, and PhoneDOCTORx, which allows a professional medical team in a remote location to view the abnormal conditions that occur during regular nursing care of a facility resident via video phone to assist in decision-making [5,6].

Next, 'remote monitoring' started with technology introduced in the aerospace program of the former Soviet Union to detected the signals of living organisms for remote communication. This technology also made it possible for NASA to collect biometric data and check predictable physical functions in advance to allow for remote response while astronauts conducted their work. According to the Frost & Sullivan survey, the growth rate of the remote monitoring market has maintained double digits in the past 10 years, and it is currently expected to achieve remarkable advances in the development of wearable devices and data sensing technology centering on IoT. Ultimately, this research will enable medical consumers, such as cancer patients and patients with chronic illnesses, to have their health condition constantly monitored by medical staff and to have a 'designated doctor' who can provide them with medical services regardless of time and place [5,6].

Finally, Remote 'Diagnosis·Treatment·Control' management are being attempted along with various technological developments. First, da Vinci (Intuitive Surgical Inc., Sunnyvale, CA, USA), which is famous for application in robot-assisted surgical procedures, has proven the effect by attempting an operation from a remote location focusing on many large domestic hospitals. In addition, IBM Watson analyzes big data within 3 seconds, focusing on 600,000 clinical data and 42 medically related DB, in providing a practical advice service to medical staff. Furthermore, Asklepios Hospital, located in Hamburg, Germany, has attempted to utilize augmented reality by overlapping an actual photograph based

 http://dx.doi.org/10.4258/hir.2015.21.4.271

on a pre-operation clinical image of the patient in operation. Various efforts are being made around the world to provide diverse remote medical services, including Changi General Hospital in Singapore, which uses QR codes to manage personalized administration for each patient via robot [5,6].

The technology that serves as the basis for the remote medical services mentioned above is presented in Figure 1. The structure makes data collection from sensors and devices, processing, transmission, execution, analysis, and other actions possible to support remote medical services. For remote medical services in such a structure, change in service is inevitable in accordance with sub-elements, including network technology, protocol, sensor, device, etc. Also, there is a constraint in that the structure should be restructured whenever a new service is created. The same problem occurs when a security service and technology is applied to a remote medical environment.

When the required factors of IoT, human, object, and service are applied to the remote medical environment, 'human' is subdivided into classifications of patient, medical personnel, and non-patient. 'Object' refers to all objects and infrastructure on the internet located around the 'human' element, in other words patients, medical personnel, and non-patients. Lastly, 'service' is media that expresses and supports medical communication between human-object-infrastructure. Accordingly, remote medical services with an IoT architecture can be classified into the following three layers: 1) the perception layer, which receives health signal entries from various sensors; 2) the network layer, which takes on the role of transmitting the health data from the perception layer to the application layer; and 3) the application layer, which provides various services and interfaces via the health data received from the network layer [7-9].

Consequently, the security elements of the remote medical architecture should be included at the initial design level because simple cyber-attacks can be directly connected to threats against patients' lives. A service-oriented architecture is flexible and can support a combination of applications depending on telemedicine environmental changes. Therefore, this study was focused on designing a service-oriented architecture and security for remote medical services.

## 2. Security Threats and Requirements

If remote medical services are carried out in the IoT environment, security vulnerability in the general remote medical setting and security vulnerability in the IoT environment will both be present. Therefore, in this section, the remote medical security threats in the IoT environment that take both conditions into consideration are extracted, and then security demands regarding these threats are described.

### 1) Threat in remote medical services with IoT

We describe the threats that can occur if certain elements are not considered during the provision of remote medical services in the IoT environment. 1) If device authentication is not taken into consideration: in other words, if access to all devices is indiscreetly permitted without certifying the device (or sensor) in the remote medical services in IoT environment, the credibility of the collected medical data cannot be guaranteed. 2) If role and situation-based access control is not taken into consideration: accurate decision and control regarding various conditional device (or sensor) accesses, which can occur during the provision of remote medical services in the IoT environment, will be difficult. 3) If user authentication is not taken into consideration: if authentication regarding patients and medical staff, who are the main agents of telemedicine, is not considered, remote monitoring, and control, are unclear. In such a case, preventing medical

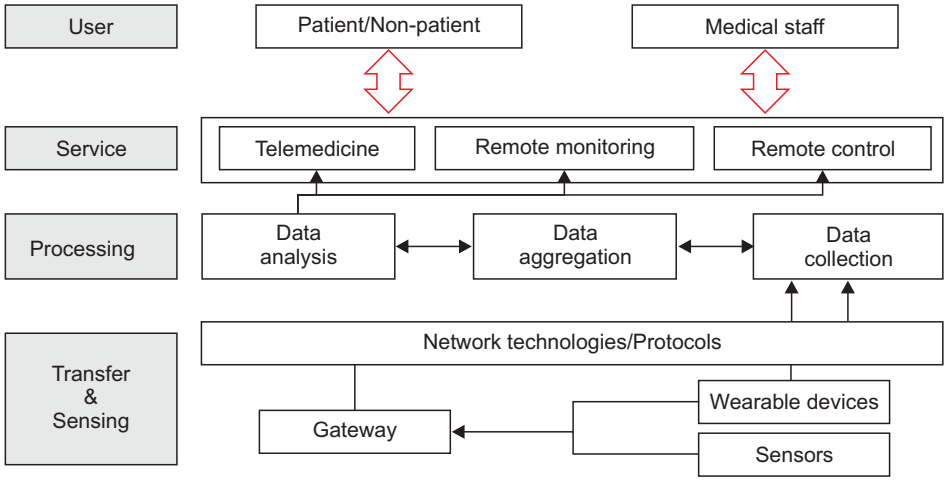


Figure 1. Common architecture of remote medical services.

Table 1. Security threats of Internet of things (IoT) and remote medical services

| Type | IoT | Remote medical servies |
|---|---|---|
| Device | Device masquerade attack | Non-authorized access |
| | No encryption | Modification |
| | Weak password | Copy of medical data |
| | Vulnerability of firmware | Leakage of trans-data |
| | Hardcoded access information | |
| Infrastructure | DDoS/DRDoS | |
| | SSDP reflection attack | |
| | Spoofing | |
| | Eavesdropping | |
| Service | Repudiation of behavior | Masquerade as a medical staff |
| | Invasion of privacy | Repudiation of medical behavior |
| | | Invasion of health records (medical history, disease information) |

practice of unauthorized person, misuse of remote medical services, and accountability of medical practice will be impossible. In addition, security threats that can be caused by IoT, as well as the structure and characteristics of remote medical services also exist, as seen in Table 1 [7-11].

Accordingly, we extracted threats from this case and Table 1 to prevent security threats against remote medical services in the IoT environment and to protect the privacy of patients. A method that can overcome the challenges regarding confidentiality, integrity, and availability is needed.

### 2) Requirements for secure remote medical sevices in the IoT

Collection of various types of data from devices (or sensors) should be secure. Also remote medical services should not be modified or wiretapped during transmission. Therefore, the following security requirements should be satisfied for the entire process from acquisition to destruction [10,12,13].

• Confidentiality: Personal health information should not be disclosed to unauthorized access during transmission. Therefore, only authorized devices, networks, and users should be able to use the information after the authentication process between the perception layer, network layer, and application layer. Furthermore, a function that allows confidentiality selection should be provided regarding items related to invasion of privacy in which individual specifics exist.

• Integrity: The data transmitted by the sender and the data received by the receiver should be consistent. Measures including authentication, encryption, security channel, and others are requested for the protection of integrity during data transmission. An integrity protection measure is also necessary to prevent unauthorized data modification regarding previously stored data.

• Availability: Delays, bottlenecks and other problems that degrade availability should not occur in data processing, even when it includes security measures with confidentiality, integrity, authentication, non-repudiation, and so on. In particular, sensitive devices and services that can be directly related to a patient's life, require 2–3 layers of guarantee measure for availability.

• Authentication: Authentication is the process to determine whether or not someone is an actual user, and it is required before data access. In particular, access control of remote medical services considering a variety of factors should meet the demands for mobility and timeliness.

• Non-repudiation: Non-repudiation is required to ensure accountability regarding specific acts. In the remote medical environment specifically, certification of authentication technology based on a public-key is required to secure reliability between medical activities.

• Privacy: Privacy means that personal secrets cannot be disclosed without consent. In remote medical services with IoT, security measures should be provided for handling sensitive information (e.g., name, address, health history, disease information, etc.) related to individuals.

## 3. Architecture

The proposed framework is composed of a total of five layers, including the *Application Service Layer*, *Service Support Layer*, *Network Layer*, *Perception Support Layer*, and *Perception Layer*. Figure 2 shows the structure of the proposed framework.

The *Application Service Layer* offer a convenient user interface to patients, medical staff, and non-patients. It is supplied with data and resources from the *Service Support Layer* based on requests by the service. In each of the service applications, independent service with reinforced security exists.

The *Service Support layer* manages data and resources which serve as the basis for the efficient performance of the *Application Service Layer*. It takes the data transmitted by the *Perception Support Layer* and stores it in an integrated database through the second access controller. The Service Mgr (Service Management), Data Mgr (Data Management), Resource Mgr (Resource Management), and System Clock manage and supply service, data, resource, and time data regarding the application service. The A_En/Decryptor encrypts (or decrypts) the data received from the A_Commu-

 http://dx.doi.org/10.4258/hir.2015.21.4.271

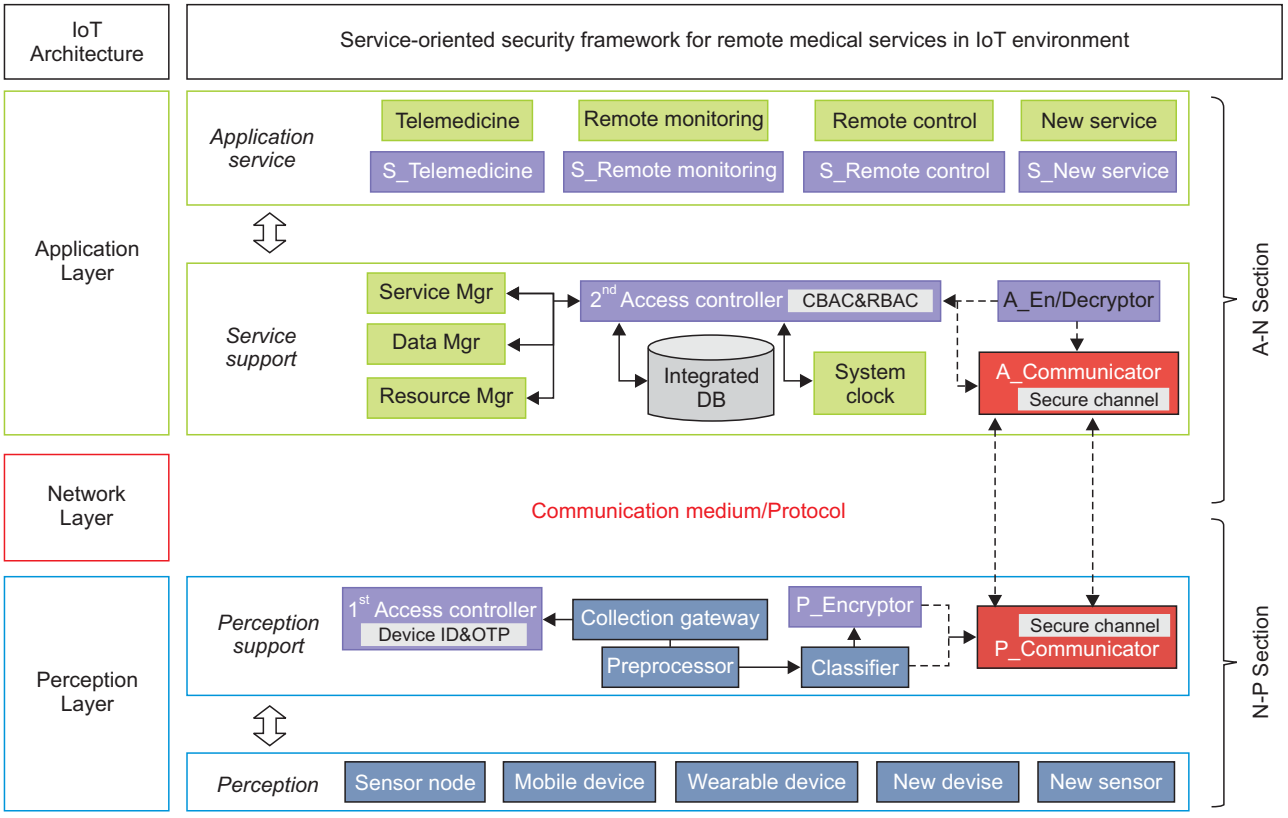


Figure 2. Architecture of proposed framework matching Internet of things (IoT) architecture.

nicator. The A_Communicator receives the data from the P_Communicator, and then the data is forwarded to the second access controller (or A_En/Decryptor).

The *Network Layer* functions as a transmission medium and protocol. It handles direct and indirect data communication between the *Service Support Layer* and *Perception Support Layer*.

The *Perception Support Layer* collects the data received from the *Perception Layer* and controls bad data and unauthorized access. After that, it performs pretreatment to ensure that the data collected from different types of devices and sensors can be used appropriately. The P_Encryptor encrypts the data received from the Classifier, and the P_Communicator sends the data that was received from the P_Encryptor and Classifier.

The *Perception Layer* is the domain in which the device (or sensor) that creates data exists. Various types of data created in this layer are transmitted to the *Perception Support Layer*.

In the next section, we focus on the perception side layer and application side layers, which are the core territories of remote medical services with IoT, in adding each network elements to propose framework, which will be separated into two sections, namely, the A-N section and N-P section, in the explanation. The N-P section refers to the *Perception Support Layer*, *Perception Layer*, and *Network Layer*, while the A-N section refers to the *Application Service Layer*, *Service Support Layer*, and *Network Layer*.

### 1) A-N section

The A-N section of the proposed framework includes parts that perform important functions, including management of the *Application Service Layer* and supplying data and resource, and thorough access control should be conducted regarding this. Access control is handled by the contextual-based access control (CBAC) technique, which is based on time and spatial data and takes timely and migratory characteristics of the subject of control into consideration, as well as role-based access control (RBAC), which allows flexible control in accordance with a complex environment and group. Next, we explain the access control process utilizing CBAC and RBAC. The terms and constraints used in CBAC are presented in Table 2.

- Authentication by CBAC: Uses CBAC, which is a technique that controls access through contextual information. It verifies whether the confirmed timely-spatial information and system standard time value are within the permitted range (MIN: minimum value, MAX: maximum value). If the result is true, access validity is decided after verification that the scanned access location is within the permitted location

**Table 2. Definitions and constraints of CRBAC in second access controller for services**

Definitions
- User: Written as U, and refers to subject of authority identification that verifies time, location, role.
  U={u1,u2……u N}
- Role: Written as R, and refers to the range of resource that can be utilized by a specific group.
  R={r1,r2……r N}
- Location: One of the conditions that compose authority, and refers to authorized location. The L value is composed of value (x) that signifies the abscissa and value (y) that signifies the ordinate
  $L \subseteq X \times Y$
  L={l1,l2……l N}
  location=(x,y)
  X={x1,x2……x N}
  Y={y1,y2……y N}
- System Time: Written as T, and refers to time value of the system. It is one of the conditions composing authority. T value that refers to allowed time is composed of start value (ST) and end value (ET).
  T={t1, t2……tn}
  t=(ST, ET)
  ST,ET=(year, month, day, hour, minute, second)
- Permission: Written as P, and refers to the range reached by user. It is composed of time value (T) and location (L).
  P={p1,p2……p N}
  p=(T,L)

Constraints
- User–Role: $UR \subseteq U \times R$
  UR=(ur1, ur2……ur N)
  ur=(u, r)
- Role–Permission: $RP \subseteq R \times P$
  RP=(rp1, rp2……rp N)
  rp=(r, p)
- User-Role-Permission: UR → RP

**Table 3. Logic of first authentication by CBAC**

```
IF ((Permitted ST ≤ Current Time) AND (Permitted ET ≥ Current Time)) then
        R1 = TRUE
        IF (Permitted L(MIN) ≤ Scanned L) AND (Permitted L(MAX) ≥ Scanned  L)) then
                R2 = TRUE
                IF (R1 AND R2) then
                        Valid access
                Else
                        Access denied (to service)
            Else
                Access denied (to service)
        Else
                Access denied (to service)
```

range. The first authentication process is shown in Table 3.

• Authentication by RBAC: In this stage, RBAC is used, which controls access via role information. Limited to access with first round of authentication complete, the access profile of the service access attempter and previously registered access profile stored into DB, are checked for consistency. If the result is true, the role is verified to check whether the requested role is an authorized role in deciding the second round of authentication. The second authentication process is shown in Table 4.

### 2) N-P section

The N-P section is the part that handles device and sensor access as well as preprocessing, classification, and processing

 http://dx.doi.org/10.4258/hir.2015.21.4.271

of the data received from it, and security measures during data processing should be available. Device ID and OTP are used for device authentication. Security during data processing uses data authentication, encryption, and security channel of reliable device. Next, we explain device authentication and data security processing.

• Authentication of device: Valid devices are identified by comparing the initially verified device ID and device ID with authorized access. In the case of a valid device, the device ID and the current time from the device (sensor) and collection gateway are put through exclusive-OR. Then, based on the created value, each of the created OTP values is compared in completion of the final first authentication. The device authentication process is shown in Table 5.

In the proposed framework, for secure and prompt processing of various types of health data obtained from sensors and devices, the data is processed separately in classification stages, including preprocessing in a secure mode that processes it into an appropriate form for processing and an actual processing stage. Figure 3 illustrates that process and shows details regarding each stage.

• Preprocessing: This stage divides the data into efficient data processing units and removes mixed in data that exceeds the range or is not permitted, prior to processing. In this stage, security mode application usage can be selected, on user designated hardware ID.

• Classification: Security mode application usage is determined regarding data that has had unnecessary raw data and error values removed and separated into efficient processing units. The units are distributed into secure mode and normal mode with applied security processing in accordance with the mode value for each hardware ID defined in preprocessing.

• Processing: If general data without security application is processed, it is classified into normal mode, which applies the general processing method, and secure mode, which se-

**Table 4. Logic of second authentication by RBAC**

```
IF (Stored Connection profile = Detected Connection profile) then
        R3 = TRUE
        IF (Permitted R = Requested R) then
                R4 = TRUE
                IF (R3 AND R4) then
                        2nd Authentication
                Else
                        Access denied (to service)
        Else
                Access denied (to service)
Else
        Access denied (to service)
```

**Table 5. Logic of device authentication**

```
        IF (Permitted Device ID = Detected Device ID) then
                R5 = GenerateOTP.value (Device' ID XOR Current time)          // in device (or sensor)
                R6 = GenerateOTP.value (Permitted Device ID XOR Current time)  // in collection gateway
                        IF (R5 = R6) then
                                1st Authentication
                        Else
                                Access denied (to service)
                Else
                        Access denied (to service)
```

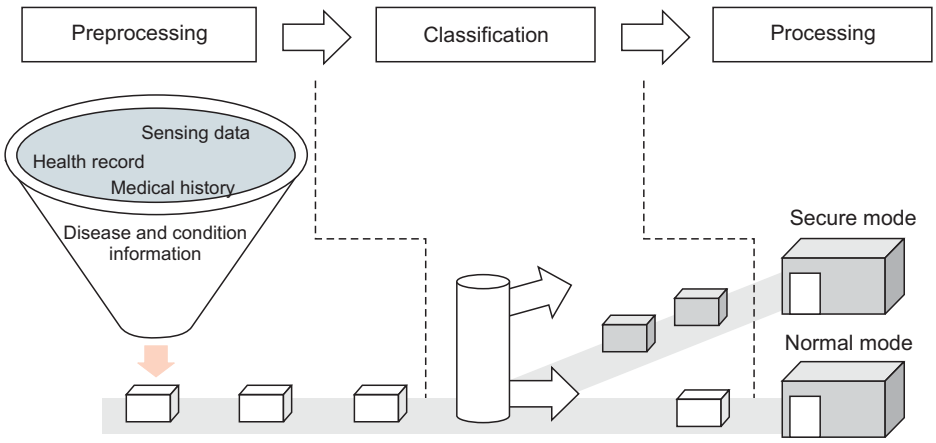


**Figure 3. Data flow overview of *Perception Support Layer* for each stage.**

lectively applies security measures, including authentication, encryption, security channel, etc., in situations requiring security.

Next, we describe how the data classified into secure mode for the purposes of secure processing of data are processed. Table 6 shows an example that defines whether or not the security elements are applied to Authentication, Secure Channel, Data Encryption regarding received data from applicable devices and sensors after the security mode has been determined for each device and sensor.

As shown in Figure 4, secure mode applies the security element in accordance with security level (1–3). First, the required item authentication is applied. Then, data encryption/decryption and secure channel are selectively applied, following the user definition. The applied method uses each hardware ID and application mode, encryption and security channel application execution of hardware ID and secure mode table as reference in processing.

• Authentication (essential): Authentication, which is the process of verifying the validity of a user, blocks unauthorized access regarding important data or personal data that should kept confidential through authentication of data classified as secure mode.

• Data Encryption/Decryption (optional): By encrypting the data with a mathematically verified symmetric key encryption and algorithm, it prevents plaintext exposure of transmitted sensitive data. If the encrypted data was modulated during transmission, data integrity can also be verified because decoding is not possible.

• Secure Channel (optional): During network transmission between two points, an asymmetric key encryption algorithm and electronic signature should be used to prevent exposure of transmission status and transmission data by composing a security channel (virtual network) during the connection of a separate sender and receiver in cases of data requiring stronger security.

Table 6. Cases of secure mode in perception support layer for applying security

| Hardware ID | Mode | Authentication | Secure channel | Data encryption |
|---|---|---|---|---|
| #00000101 | Secure | TRUE | TRUE | FALSE |
| #00000202 | Normal | - | - | - |
| #00000303 | Secure | TRUE | FALSE | TRUE |
| #00000404 | Normal | - | - | - |
| #00000505 | Secure | TRUE | FALSE | FALSE |

## 4. Service Scenario

Here, we present a medical service scenario in which a secure remote medical service is provided in the IoT environment with proposed framework application. Table 7 defines the medical service-oriented terms and Figure 5 displays a diagram based on the proposed framework. Whether security technology is applied to each of stages ①–⑥ is explained in relation to the process.

① Transfer of perception data: verify through DA between device (or sensor)-device (or sensor), device (or sensor)-collection gateway, and transmit data securely through SC, DED during data transmission.

② The collected data transferring and preprocessing from device (or sensor): After completing DA on the collection gateway, CBAC and RBAC should be applied to transmit the collected data. If additional security is required, DED and SC should be used because they make it possible to provide strong security service.

③,④ Transferred data update and access to electronic medical records: The UA used when accessing the electronic medical records of the medical staff and others, including DED, SC, CBAC, and RBAC are shown in ①.

⑤,⑥ Providing the services to users: DA is used when device and sensor transmit data from the user (non-patient, patient). On the other hand, when the user wishes to access a service, the UA is used. The application of CBAC and RBAC is required during data transmission between user-service; SC and DED are selectively provided for stronger security.

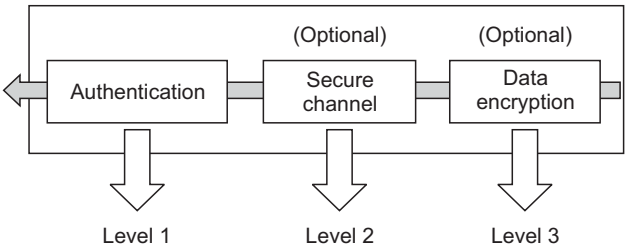


Figure 4. Selectable function for security levels.

Table 7. Definition of terminology for service scenario

| |
|---|
| User authentication : UA |
| Device (sensor) authentication : DA |
| Secure channel : SC |
| Data en/decryption : DED |
| Contextual-based access control : CBAC |
| Role-based access control : RBAC |
| Secured status : 🔓 |


http://dx.doi.org/10.4258/hir.2015.21.4.271

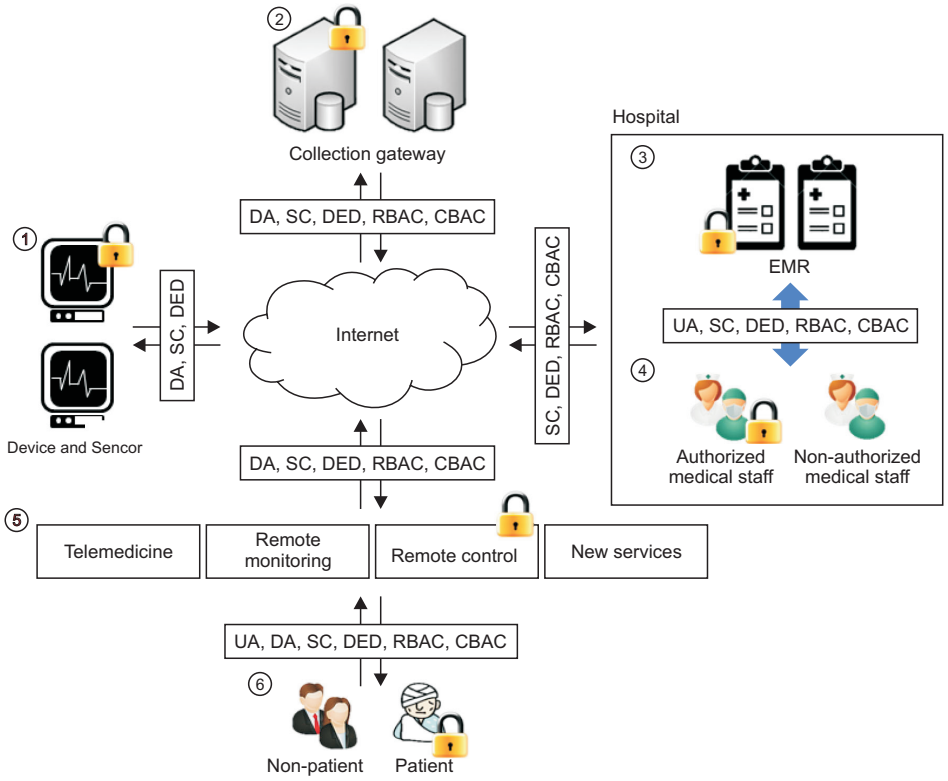


Figure 5. Service scenario for the applied framework. UA: user authentication, DA: device (sensor) authentication, SC: secure channel, DED: data en/decryption, CBAC: contextual-based access control, RBAC: role-based access control.

Table 8. Comparison of confidentiality

| Type | Li et al. [15] | Moosavi et al. [17] | Zaidan et al. [14] | Savola et al. [16] | Proposed framework |
|---|---|---|---|---|---|
| Confidentiality | +++ | +++ | +++ | ++ | +++ |
| Integrity | +++ | ++ | +++ | + | +++ |
| Availability | ++ | +++ | + | ++ | +++ |
| Privacy | ++ | + | ++ | + | ++ |

+++: strong, ++: medium, +: weak.

## III. Result

### 1. Analysis

Excluding survey-type theses from the previous research considered, four studies that took confidentiality, integrity, availability, and privacy into consideration were used in conducting a comparative analysis against the proposed framework. The comparative analysis of the proposed framework was conducted with the security element as the standard, which was the selection standard of the previous research and previous studies. The security comparison results are shown in Table 8.

• Confidentiality: The proposed framework provides confidentiality via device- and user-based authentication and status- and role-based access control and security channel, encryption, etc., for the purpose of confidentiality between device (or sensor), device (or sensor)-collection gateway, service and user. Zaidan et al. [14] mentioned the network structure and secure transmission regarding health information exchange via verified encryption and hash algorithm. Li et al. [15] mainly focused on secure patient-oriented personal health record access and efficient key management. Savola et al. [16] suggested maintaining confidentiality via an adaptive management model and focused on the role of security metrics. Moosavi et al. [17] tested authentication and authorization in the IoT healthcare environment through a certificate-based DTLS handshake protocol-based structure and proposed a technology for IP confidentiality in the IoT environment.

• Integrity: If an integrity verification measure is not available during data transmission and reception, there is a concern about too much data modulation; this is particularly important in the case of medical data. Accordingly, to guarantee integrity, it should be possible to check for data modulation in each section. In the proposed structure, the integrity of transmitted and received data in each section is guaranteed through the first and second authentication. Also data integrity can be maintained by the cryptographic algorithm. Zaidan et al. [14] proposed an encryption and hash algorithm for network-focused health information exchange; verification is not performed in each section. In addition, as

there is no mention of non-repudiation, it is difficult to ensure accountability regarding medical care. Li et al. [15] attempted to prevent access to unauthorized self-health information and to ensure accountability regarding data access. In Savola et al. [16], role metrics on access control exists; however, there is no specific mention about that method of access control. Moosavi et al. [17] consider the only integrity of data in transmit-receive section.

• Availability: The framework proposed in this paper makes it possible to selectively apply encryption and a security channel that excludes authentication in each section, in providing confidentiality and integrity; thus, flexibly securing availability is possible. The framework proposed by Zaidan et al. [14] was designed only taking confidentiality and integrity into consideration. The method proposed by Li et al. [15] raises a concern because it can decrease availability in an environment where large amounts of data are obtained from various types of devices and sensors. Savola et al. [16] proposed availability metrics that include various elements, such as QoS, resilience, scalability, etc., but there is no specific mention about details. The structure proposed by Moosavi et al. [17] is structurally dispersed in key management and is comparatively more secure than the state of the art centralized delegation-based structure; therefore, it is more secure from availability attack.

• Privacy: The proposed framework decreases the exposure of sensitive information compared to other studies by applying a security channel and encryption during the transmission of sensitive information between network sections. Also, privacy is made more secure by only allowing personnel with authorized roles to access data within the permitted time regarding specific medical staff and by applying UA, CBAC, RBAC during EMR access by the medical staff. The frameworks proposed by Moosavi et al. [17] and Zaidan et al. [14] do not mention any technology to provide privacy. The method suggested by Li et al. [15] allows flexible handling of personal health record access policy. Savola et al. [16] discussed privacy protection through privacy metrics, but they did not suggest a specific method.

## IV. Discussion

### 1. Previous Research

Utilizing the databases of PubMed, Springer, IEEE, ScienceDirect, BMC thesis, 'remote medical' and 'IoT' were searched under the AND condition, and 'telehealth', 'mobile health', 'telemedicine' were each searched under a combination of OR condition. The search range was 2011 to 2015. As a result, approximately 1,200 papers were searched, and among these, a total of 30 were extracted based on a standard of abstract containing security elements. As with the security threats classified in Table 1, the searched papers were classified into device (or sensor), infrastructure, and service for discussion of the previous research in each category.

• Device (included sensor): Doukas et al. [10] described digital certificates and PKI data encryption based on a gateway for aggregation of health sensor data and to resolve security problems. Hsu and Pan [11] proposed agent-based telemedicine based on a P2P networking architecture. Camara et al. [13] explained the main security goals for the next generation of implantable medical devices and analyzed the most relevant protection mechanisms. Simplicio et al. [18] presented a lightweight framework for security. It focuses on protection of shared data's collection and lost/stolen device's data.

• Infrastructure: Saleem et al. [19] propose a framework for security based on IEEE 802.15.4. Also, in [12], the security vulnerabilities and major attacks in the context of wireless body area network (WBAN) were identified. Zhang and Zhang [20] introduced a secure and flexible platform based on IoT and cloud computing that uses short-distant ambient communication protocols for medical purposes. Shini et al. [21] described data storage and sharing through cloud computing. Their study highlights the different types of security problems that affect cloud users. Chen et al. [22] proposed an enhanced authentication scheme that overcomes the weaknesses inherent in Khan et al.'s scheme, and they demonstrated that their scheme is more secure and robust for use in a telecare medical information system. Al Ameen et al. [12] described security and privacy issues in WBAN, and they proposed measures for healthcare application in WBAN. Li et al. [15] focused on a multiple data owner scenario and divided the users in the PHR system into multiple security domains. Doing this greatly reduces the key management complexity for owners and users. Jiang et al. [23] proposed a secure and efficient authentication scheme with user privacy preservation which is practical for a telecare medical information system. Das and Goswami [24] proposed a robust remote user authentication scheme for connected health care that preserves uniqueness and anonymity. Kim and Lee [25] proposed cryptanalysis that discourages any use of the two schemes under investigation in practice, and they revealed some subtleties and challenges in designing this type of scheme. Das and Goswami [26] proposed a novel and secure biometric-based remote user authentication scheme to withstand the security flaw found in Awasthi-Srivastava scheme and enhanced the features required for an idle user authentication scheme. The architecture proposed by Moosavi et al.

 http://dx.doi.org/10.4258/hir.2015.21.4.271

[17] is more secure than a state-of-the-art centralized delegation-based architecture because it uses a more secure key management scheme between sensor nodes and the smart gateway. Zaidan et al. [26] proposed their secure framework for health information transmission within a central cloud-based model.

• Service for remote medical: Savola et al. [16] proposed adaptive security management mechanism based on security metrics. And they described protection methods of confidentiality, integrity, availability in eHealth IoT application. Shin [27] introduced a framework for secure remote health-monitoring systems using a realistic risk model for sensor-data quality. Abie and Balasingham [29] described a risk-based adaptive security framework for IoTs in eHealth that estimates and predicts risk damages and future benefits using game theory and context-awareness techniques. The framework proposed by Al-Haj and Amer [29] is implemented on a block-level of the partitioned-image for integrity, thus enabling the localized detection of tampered regions.

In Table 9, the searched papers were first classified into device, infrastructure, and service. Then, they were sorted according to how they include the main security elements, such as confidentiality, integrity, availability, and privacy in understanding the characteristics and tendency of previous researches related to remote medical security.

In the infrastructure field, it is evident that many studies took various security elements into consideration. However, it is evident that there has been less research in this area than in the device and service fields. Accordingly, there is a need to reflect various security elements in all domains of service, infrastructure, and device.

Table 9. Classification of previous researches

| Type | Contents |
|---|---|
| Device | [C,I] : Doukas et al. [10] |
| | [C,I,A] : Hsu and Pan [11], Simplicio et al. [18] |
| | [C,I,A,P] : Camara et al. [13] |
| Infrastructure | [C,I]: Chen et al. [22], Kim and Lee [25], Das and Goswami [26] |
| | [C,I,A]: Saleem et al. [19], Zhang and Zhang [20], Shini et al. [21], Moosavi et al. [17] |
| | [C,I,P]: Jiang et al. [23] |
| | [C,I,A,P]: Al Ameen et al. [12], Li et al. [15], Zaidan et al. [14] |
| Service | [C,I]: Shin [27], Abie and Balasingham [28] |
| | [C,A]: Al-Haj and Amer [29] |
| | [C,I,A,P]: Savola et al. [16] |

[C]: confidentiality, [I]: integrity, [A]: availability, [P]: privacy.

## 2. Conclusions

As the demands and expectations regarding medical services are increasing, various new medical services are being introduced. In particular, there is much interest regarding possible medical activities via remote medical services from long distance, and this is being combined with the new concept of the IoT. However, security element support has remained weak, with security being impossible in some cases or only partial security elements being provided regarding the modification of existing services and the creation of new service. Accordingly, remote medical security in the IoT environment requires a new structure and method to prevent various threats directly connected to the safety of patients' lives.

This paper proposed a service-oriented security framework for remote medical services in the IoT environment. The proposed framework is a service-oriented structure that can support dynamic security elements in accordance with demands regarding various types of new remote medical services that will be created in the IoT environment, which will soon be realized. It enables the provision of secure services that guarantee confidentiality, integrity, and availability for all, including patients, non-patients, and medical staff. Security elements are realized via role- and situation-based access control, user access control, data encryption, and the provision of a security channel.

In future studies, we will conduct an in-depth study regarding techniques that can satisfy demands in accordance with key generation and management. In addition, we plan to enhance the efficiency and availability of the authentication method in the IoT remote medical environment.

# Conflict of Interest

No potential conflict of interest relevant to this article was reported.

# References

1. Liang X, Li X, Barua M, Chen L, Lu R, Shen X, et al. Enable pervasive healthcare through continuous remote health monitoring. IEEE Wirel Commun 2012;19(6):10-8.
2. Li KF. Smart home technology for telemedicine and emergency management. J Ambient Intell Humaniz Comput 2013;4(5):535-46.
3. Xu B, Xu L, Cai H, Xie C, Hu J, Bu F. Ubiquitous data

accessing method in IoT-based information system for emergency medical services. IEEE Trans Industr Inform 2014;10(2):1578-86.
4. Chiuchisan I, Costin HN, Geman O. Adopting the internet of things technologies in health care systems. Proceedings of 2014 International Conference and Exposition on Electrical and Power Engineering (EPE); 2014 Oct 16-18; Iasi, Romania. p. 532-5.
5. Wootton R. Twenty years of telemedicine in chronic disease management: an evidence synthesis. J Telemed Telecare 2012;18(4):211-20.
6. Ryu S. Telemedicine: opportunities and developments in member states: report on the Second Global Survey on eHealth 2009. Healthc Inform Res 2012;18(2):153-5.
7. Nguyen KT, Laurent M, Oualha N. Survey on secure communication protocols for the Internet of Things. Ad Hoc Netw 2015;32:17-31.
8. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. Comput Netw 2015;76:146-64.
9. Vucinic M, Tourancheau B, Rousseau F, Duda A, Damon L, Guizzetti R. OSCAR: object security architecture for the Internet of Things. Ad Hoc Netw 2014;32:3-16.
10. Doukas C, Maglogiannis I, Koufi V, Malamateniou F, Vassilacopoulos G. Enabling data protection through PKI encryption in IoT m-Health devices. Proceedings of 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE); 2012 Nov 11-13; Larbaca, Cyprus. p. 25-9.
11. Hsu WS, Pan JI. Secure mobile agent for telemedicine based on P2P networks. J Med Syst 2013;37(3):9947.
12. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 2012;36(1):93-101.
13. Camara C, Peris-Lopez P, Tapiador JE. Security and privacy issues in implantable medical devices: a comprehensive survey. J Biomed Inform 2015;55:272-89.
14. Zaidan BB, Haiqi A, Zaidan AA, Abdulnabi M, Kiah ML, Muzamel H. A security framework for nationwide health information exchange based on telehealth strategy. J Med Syst 2015;39(5):1-19.
15. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans Parallel Distrib Syst 2013;24(1):131-43.
16. Savola RM, Abie H, Sihvonen M. Towards metrics-driven adaptive security management in e-health IoT applications. Proceedings of the 7th International Conference on Body Area Networks; 2012 Sep 24-26; Oslo, Norway. p. 276-81.
17. Moosavi SR, Gia TN, Rahmani AM, Nigussie E, Virtanen S, Isoaho J, et al. SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Comput Sci 2015;52:452-459.
18. Simplicio MA Jr, Iwaya LH, Barros BM, Carvalho TC, Naslund M. SecourHealth: a delay-tolerant security framework for mobile health data collection. IEEE J Biomed Health Inform 2015;19(2):761-72.
19. Saleem S, Ullah S, Kwak KS. A study of IEEE 802.15.4 security framework for wireless body area networks. Sensors (Basel) 2011;11(2):1383-95.
20. Zhang XM, Zhang N. An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine. Proceedings of 2011 International Conference on Computer and Management (CAMAN); 2011 May 19-21; Wuhan, China. p. 1-4.
21. Shini SG, Thomas T, Chithraranjan K. Cloud based medical image exchange-security challenges. Procedia Eng 2012;38:3454-61.
22. Chen HM, Lo JW, Yeh CK. An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems. J Med Syst 2012;36(6):3907-15.
23. Jiang Q, Ma J, Ma Z, Li G. A privacy enhanced authentication scheme for telecare medical information systems. J Med Syst 2013;37(1):1-8.
24. Das AK, Goswami A. A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. J Med Syst 2013;37(3):1-16.
25. Kim KW, Lee JD. On the security of two remote user authentication schemes for telecare medical information systems. J Med Syst 2014;38(5):1-11.
26. Das AK, Goswami A. An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. J Med Syst 2014;38(6):1-19.
27. Shin M. Secure remote health monitoring with unreliable mobile devices. J Biomed Biotechnol 2012;2012:546021.
28. Abie H, Balasingham I. Risk-based adaptive security for smart IoT in eHealth. Proceedings of the 7th International Conference on Body Area Networks; 2012 Sep 24-26; Oslo, Norway. p. 269-75.
29. Al-Haj A, Amer A. Secured telemedicine using region-based watermarking with tamper localization. J Digit Imaging 2014;27(6):737-50.

 http://dx.doi.org/10.4258/hir.2015.21.4.271