sustainability

MDPI

Article

Efficient Mutual Authentication Protocol between Hospital Internet of Things Devices Using Probabilistic Attribute Information

Yoon-Su Jeong [1], Dong-Ryool Kim [2] and Seung-Soo Shin [3,*]

[1] Department of Information and Communication Convergence Engineering, Mokwon University, Daejeon 35349, Korea; bukmunro@mokwon.ac.kr
[2] School of Mechatronics Engineering, Tongmyong University, Busan 48520, Korea; drkim@tu.ac.kr
[3] Department of Information Security, Tongmyong University, Busan 48520, Korea
* Correspondence: shinss@tu.ac.kr

Received: 20 October 2019; Accepted: 12 December 2019; Published: 16 December 2019

check for updates

Abstract: Wearable and portable medical devices are one of the fastest growing sectors in the Internet of Things (IoT) market. However, medical services specialize in the processing of personal health data, which carries issues that are not faced by other industries. In this paper, we propose a multi-dimensional color vector information based IoT device authentication protocol that can provide benefits for medical work, assuming that a hospital has the capability of integrating IoT devices and has access to patient information. The proposed protocol uses multi-dimensional color vectors to help users who use IoT devices to manage their condition in multiple groups, stochastically. In addition, the proposed protocol provides the health and medical service status of users to medical staff in real time using IoT authentication keys generated through the proposed multi-dimensional color vectors. The proposed protocol not only addresses health care problems yet to be tackled in the management of hospital and health services, but also minimizes administrative time and procedures for current medical services. As a result of the performance evaluation, the proposed protocol improved the efficiency of hospital IoT devices by an average of 31.1%, and the time delay for medical services was improved by 19.8%, compared to the existing protocol. By using the proposed protocol and IoT devices, the average overhead of healthcare providers could be reduced by as much as 15.3%.

Keywords: Internet of Things (IoT); healthcare service; big data; probabilistic; authentication protocol

1. Introduction

With the rise of the fourth industrial revolution, Internet of Things (IoT) technology is attracting attention. IoT technology has been used in various fields such as in sensing technology, and the importance of IoT technology will only increase in the future [1–3]. Among the areas where IoT technology is currently being utilized, hospital medical services are trying to provide services that can efficiently manage patient conditions and prevent negative outcomes, based on information collected through IoT devices. However, hospital medical services as they currently operate are inefficient, leading to staff being overworked and poor management of medical information, lowering the quality of medical services.

In addition, in the existing hospital system, management supervision and monitoring procedures for patients are often performed manually by the nursing staff, which causes an efficiency bottleneck [4,5].

Various studies have been carried out to ensure that the connection between IoT devices and medical services have a positive effect on medical service efficiency, and result in cost reductions [6–8]. However, integrating IoT devices into the hospital system causes various security vulnerabilities related to patient privacy issues. In particular, newly developed IoT devices have different security requirements than existing wired and wireless network-based services [9,10]. It is difficult to converge most IoT-based and services, as they are often provided through unique platforms. Because IoT-based platforms and services do not comply with related security standards, it is necessary to develop a common open platform for IoT-based medical services, to solve the problem of the difficulty in connecting services due to the lack of compatibility between medical services.

Phunchongharn et al. studied the interference of E-healthcare applications caused by IoT devices installed in hospitals [6,7]. However, this approach did not address mobile medical services that are not supported when an emergency occurs in areas outside the hospital.

Shen et al. investigated whether data was normal or not, according to the amount of power when wirelessly monitoring a patient condition in the vicinity of a hospital IoT device [8]. However, their approach did not solve the problem of high power being used for RF transmission, which can adversely affect hospital IoT devices.

In this paper, we propose an efficient authentication protocol to provide services to automatically connect hospital IoT devices according to patient illness, in order to improve the convenience of medical services for hospital patients, and to reduce medical staff workloads. The proposed protocol has the characteristics of minimizing the time required for administrating treatment and procedures by automatically communicating measured information (weight, body fat, BMI, heart rate, air pollution, etc.) through devices attached to patients through Wi-Fi or Bluetooth using IoT healthcare platforms (Withings, Fitbit Flex, SAMI, etc.). In addition, information collected through IoT devices can be utilized in initial diagnoses, and medical teams can determine whether or not additional medical services are needed, depending on the condition of the patient. Hospitals often have different medical service systems, so the IoT devices provided by hospitals may also be different. The proposed protocol provides a means for the use of IoT equipment in hospitals with respect to the condition of the patient.

The proposed protocol has four aspects which utilize the authentication key, allowing use of hospital IoT devices for the entire medical service.

First, staff register the basic information of patients in order to receive pre-certification keys to IoT devices, which ensure compatibility with hospital medical services. The medical institution minimizes the time required for administration and procedures by providing information to medical staff on a patient's health status and the status of medical service provisions in real time.

Second, if a patient visits a hospital due to a sudden deterioration in their condition, the hospital will be able to access the information necessary for emergency treatment through medical records stored in the pre-registered IoT device.

Third, in order to shorten the time required for hospital medical staff to assess a patient, it is possible to provide medical services directly to the patient by using disease management information from patient information registered on their condition, and the hospital IoT device usage record.

Fourth, the proposed protocol collects patient information through the hospital IoT device and minimizes the time required for procedures, treatment, and administration of patients with similar conditions.

The proposed protocol can improve hospital services through hospital IoT devices by generating authentication keys with probabilistic vector approximations through the interconnection of IoT devices. In addition, the proposed protocol does not use any additional algorithm like existing authentication methods, instead extracting arbitrary color information used for the authentication key by using the multi-dimensional color vector method in hospital IoT devices. The proposed protocol improves the efficiency of hospital IoT devices by allowing medical staff to accurately understand the health status of patients by integrating the sensor information generated in the hospital IoT device, in real-time.

The composition of this paper is as follows. In Section 2, we discuss hospital IoT device-based medical services and existing research. Section 3 proposes a medical service model using a hospital IoT device. Section 4 evaluates the security of the proposed model and its performance, and compares it with the existing model. Finally, we conclude in Section 5.

2. Preliminaries

2.1. Hospital IoT Device-Based Medical Services

Hospital IoT devices Medical services mean services that combine IoT devices with medical devices to simplify the process of existing medical services and to improve the healthcare of users. In a recent study involving hospital IoT devices, various studies are underway to improve the quality and cost of medical services by linking hospital medical systems with IoT. In particular, there are active attempts to utilize IoT devices to provide the medical cost reductions and service enhancements that are constantly proposed for existing medical services. Hospitals that have recently adopted IoT devices in their medical systems can easily check users' health conditions anytime, anywhere in real-time and are changing so that users can provide medical services immediately in case of sudden emergencies. Beginning several years ago, hospitals and medical device companies have been trying to support patient-centered medical services by combining various platforms and wearable devices related to IoT into hospital medical services [8]. However, in order to integrate IoT devices into hospital medical services, we provide customized medical services that can efficiently manage the user's symptoms (heart disease management, diabetes management, hypertension management, and exercise tracking) using a variety of different types of sensors [11].

IoT technology is developing so that patients are better connected to doctors through remote monitoring and virtual visits. To simplify the overall process and reduce medical costs by automating patient management workflows, IoT technology being utilized for the health and medical fields in six areas (Public health, Chronic disease management, Smart sleep, Medication Refills, Streamlining Hospital Care, Remote Care, and Monitoring), as shown in Table 1. As shown in Table 1, IoT technologies are lowering the prices of medicines by optimizing their manufacturing processes to reduce errors in inefficient performance. In addition, IoT is increasingly being used in the medical field to maintain quality control and manage sensitive items, even during transport.

Table 1. A Case Study on the Utilization of IoT Technology in the Health and Medical Sector.

Utilization Field	Company	How it is Using IoT
Public Health	NEXLEAF	- Provides a wireless remote temperature monitoring function in the vaccine refrigerators of rural clinics and health facilities. -Public health personnel can better manage disease and lifesaving injections.
	SYSTEMONE	- Sends medical diagnostic data to doctors and other healthcare workers around the world in real-time to help them stay in better shape.
	ACLIMA	- Understanding "City Life and Breathing" Using the Mobile Sensing Platform.
Chronic Disease Management	QUIO	-Uses a cloud platform that wirelessly connects various medical devices related to drugs, activities, and health in patients with chronic diseases.
	PFIZER/IBM	- Strengthens communication between doctors and patients while tracking the effects of Parkinson's drugs and adjusting the required dosage in real-time.
	SPRY HEALTH	- Continuous bio-signal data monitoring and patient health monitoring. -Providing cloud and actionable insights that provide better care.
Smart Sleep	EIGHT	- Analyzes the data collected from the mattress and send the data to the smart phone to determine the ideal sleep temperature.
	BEDDIT	- Keeps track of breathing rate, heart rate, and snoring (which also works on a CPU) and sleep environment. - Improves sleep quality through monitors.
	HAPPIEST BABY	- Daily sleep records, mobile alerts, and various settings that can be adapted to the age and sensitivity of the baby are linked to specific apps.

Table 1. *Cont.*

Utilization Field	Company	How it is Using IoT
Medication Refills	ADHERETECH	- The patient receives a free AdhereTech smart medicine with a special drug used as a common bottle and issues a notification of the missing dose via text or phone. - Provides ease of personalized support for drug refills and health problems.
	AERIS COMMUNICATIONS	- Provides plug-and-play platforms to help medical device manufacturers and service providers communicate with patients and comply with medical advice such as drug dosage and frequency.
	OTSUKA AMERICA PHARMACEUTICAL	- Provide data to family members and friends, as well as your doctor or other medical professionals.
Streamlining Hospital Care	G.E. HEALTHCARE	- Monitors up to 1200 beds, handles 80-bed requests at a time, and tracks other patient requirements, such as nurse proximity.
	PHILIPS E-ALERT	- A sensor is fitted that measures environmental factors for a specific MRI threshold and triggers an alert when it is exceeded.
	STANLEY HEALTHCARE	- RFID facilitates real-time patient positioning, providing a way for suppliers to monitor patients in a more personalized way than required by individuals.
Remote Care and Monitoring	HONEYWELL	- Connecting patients to remote-position healthcare providers receiving biometric data sent through the patient dashboard.
	R-STYLE LAB	- Quickly analyzes health issues, diagnose health conditions, and provide real-time support using sensor readings and other methods.
	ENSA	- Synchronizes health records and biometric sensors to provide users with recommendations for health and supplements.

2.2. *Security Issues with Hospital IoT Devices*

The hospital IoT device is shown in Figure 1, which summarizes the security weaknesses and threats that can occur when sending and receiving a user's medical information to the hospital personnel (doctor, nurse, pharmacist, etc.) when the user receives medical service [12].

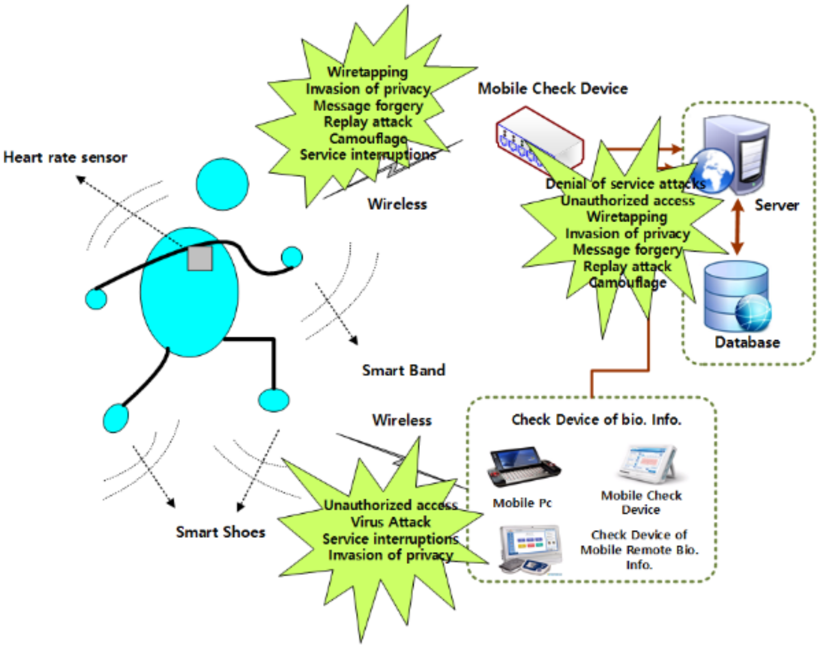

Figure 1. Security Threats of a u-Healthcare Environment.

The security vulnerabilities that can occur in the hospital environment when using hospital IoT devices as shown in Figure 1 include a type of medical information eavesdropping/forgery attack, a type of DoS attack that attacks the server supporting the service, the types of illegal access attacks possible through the wired and wireless infrastructure, Virus/worm hacking attack types, off-line crime prevention system breakdowns, artificial device paralysis, jamming, fire, or other malicious acts.

Recently, security studies on hospital IoT devices have studied the use of concealed devices or sound signals to protect users' privacy or to use additional external devices such as access tokens or communication lovers. In addition, access control studies have been carried out using access and no alarms, as well as research on the rejection of long-range wireless interactions with implanted devices without proximity verification [13].

3. Related Works

Recently, hospitals have been applying hospital IoT devices to user medical service businesses to improve the quality of users' medical service. Research on hospital IoT devices applied to hospital medical systems has been steadily increasing in recent years [14,15]. Khattak et al. model proposed a model that can generate a federated ID that can be safely managed by the management system so that the information collected through the sensor inserted in the user body cannot be misused by an adversary [16]. However, this model has a problem in that a reliable relationship between the client and the identifier provider must be established based on the security model. Gao et al. model uses a dynamic trust policy language to dynamically establish a trust policy between the medical staff and the user in order to dynamically represent the federated identity in the hospital system [17].

Zhou et al.'s technique can generate the mandate itself to use the signature key of the user receiving the medical service [18].

Mambo et al. proposed a technique based on the discrete algebra problem to generate proxy signatures [19]. However, this technique has a disadvantage in that a double signature algorithm must be used to perform a surrogate signature, and a condition meaning that stable forgery cannot be stably satisfied.

Lu et al. has proposed a technique based on the difficulty of the Rabin-based and factorial decomposition problems in order to use surrogate signatures [20]. However, this technique has a problem because the signer must confirm the validity of the signature when sending the proxy to the proxy signer.

4. A Medical Service Model Using Hospital IoT Devices

In recent years, as the 4th industrial revolution has proceeded, interest in IoT has increased, and the hospital medical environment has provided various methods to maximize the convenience of medical service to users, but the complaints of medical service users who visit hospitals still has not decreased [21–24]. This section proposes an efficient authentication protocol for hospitals IoT devices to improve the medical environment of medical staff performing many medical tasks while shortening the time of medical service for users visiting the hospital. The proposed protocol aims to shorten the user's medical service time and minimize the workload of medical staff.

4.1. Overview

Recently, hospitals have begun to apply IoT devices to hospital medical services to minimize the difficulties of user management supervision and reduction of medical expenses [25]. In particular, the IoT devices used in hospitals are used for measuring and diagnosing the health values of users by using cameras, microphones, accelerometers, gyro sensors, and the like. In addition, IoT devices operating in hospitals can measure biometrics such as user's calorie consumption, sleep pattern, activity, and a number of steps, as well as real-time clinical medical data such as oxygen saturation, blood pressure, blood glucose, body temperature, and the electrocardiogram You can check. However, even if the hospital IoT device performs many functions, the user's health conditions still cannot be continuously checked [26].

In the proposed protocol, when the user visits a hospital, the purpose is to minimize the waiting time of the medical service provided by the user by allocating the hospital IoT device suitable for the user's medical service. Another goal of the research is to improve the quality of medical services for users by minimizing the burden of the medical staff providing medical services. In the proposed protocol, in order to provide the optimal hospital IoT device according to the medical service, the user must generate an authentication key for synchronizing the user and the hospital IoT. In the proposed protocol, instead of the encryption research method used in the existing research, a group of hospital IoT devices corresponding to the scope of the user's medical service is grouped to generate an authentication key for processing the authentication service. At this time, the proposed protocol randomly extracts the color information used in the color model according to the number of hospital IoT devices in order to improve the authentication processing speed. The extracted arbitrary information is vectorized to obtain key information necessary for user authentication as a sum of orthogonal vectors.

In order to use the hospital IoT device, the user's personal information is delivered to the medical staff in real-time by using the IoT device (e.g., bracelet, heart rate sensor, smart band, smart shoe service, etc.). This paper shows the healthcare service structure of the proposed protocol that can minimize the shortening and administrative processing. As shown in Figure 2, in order to provide delay-free medical service to the user, the proposed protocol should be largely divided into the IoT device part and the server part. In the IoT device part, the sensor detects the user information and confirms the user information. In the server part, the hospital IoT devices are allocated to the users through the sensed user information and the hospital IoT devices to manage the resources efficiently.

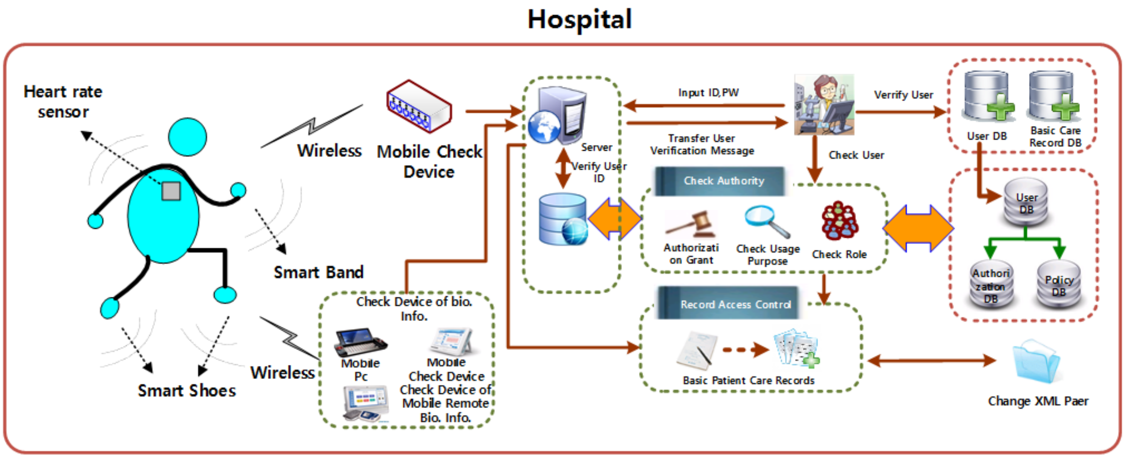

Figure 2. Overall Process of The Proposed Scheme.

4.2. Notations

The Notations used in this paper are shown in Table 2.

Table 2. Notations.

Notation	Description
ID_i	User identification information
x_n	Multidimensional color vector information
g	Keys used to authenticate hospital IoT devices
e	Errors
c_i	a constant
p_n	Attribute information for hospital IoT devices
w_{ij}	Correlation information between Hospital IoT device attribute information
R	User-generated random number
SK_i	Shared key
h()	Hash function
$\|\|$	XOR(exclusive or) operation

4.3. Hospital IoT Key Generation Process Using Probabilistic Vector Approximation

In order to improve the safety of the hospital IoT device used for patient care, this section outlines a process of generating a key with a stochastic vector approximation to the hospital IoT device, so that the key assigned to the hospital IoT device improves the management of the hospital IoT device.

We proposed a protocol that generates a cartesian vector space so that the n multidimensional color vector information $x_1, x_2, \cdots, x_n$ generated by the server are orthogonal to each other for hospital IoT device authentication. In Figure 3, the n vector information located in the Cartesian vector space uses arbitrary color information extracted based on probability. The key for the unique hospital IoT device first selects two of the three orthogonal vectors and obtains the vector g as shown in Equation (1)

$$\mathrm{g} \cong c_1x_1 + c_2x_2 \tag{1}$$

where the vector g means a primary information value for generating a key used for authenticating the hospital IoT device. The constants c_1 and c_2 are the only constant values used to obtain the vector g.

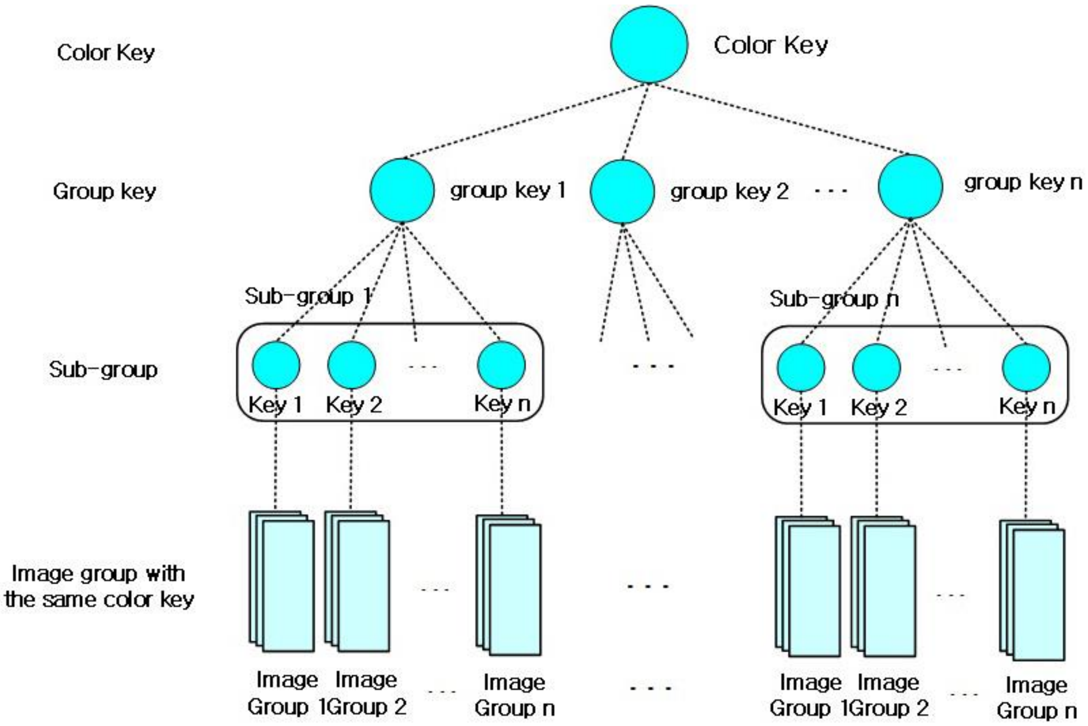

Figure 3. Scalable Color Image Structure of the Proposed Scheme.

In the proposed protocol, error e is extracted to approximate the vector g in order to improve the reliability of the key of the hospital IoT device. The error e used in the proposed protocol is performed as in Equation (2), and minimizes the error e for approximating the vector g

$$\mathrm{e} = \ (c_1x_1 \ + c_2x_2) \tag{2}$$

where error e means the vertical value of the plane connecting x_1 and x_2, while c_1x_1 and c_2x_2 means the values at which the error e reaches its minimum when calculating the vector g in the plane connecting x_1 and x_2.

In order to generate the key of the hospital IoT device, the proposed protocol generates the n-dimensional color vector information $x_1, x_2, \cdots, x_n$, which is generated by the server as Equation (1) to (2). At this time, the image group with the same color key groups as the n-dimensional color vector information $x_1, x_2, \cdots, x_n$ is generated by the server in a probabilistic manner.

In the proposed protocol, the optimal approximation for the vector g is obtained as Equation (3) so that the n-dimensional color vector information $x_1, x_2, \cdots, x_n$ are orthogonal to each other.

$$\mathrm{g} \cong c_1 x_1 + c_2 x_2 \ + c_n x_n \tag{3}$$

In this case, the constants $c_1, c_2, \cdots, c_n$ are obtained using the Equation (4) so that the vector g is no longer an approximation but is an identity equation.

$$c_i = \frac{\langle g,\ x_i \rangle}{\langle x_i,\ x_i \rangle} = \frac{1}{\|x\|^2} < \mathrm{g},\ x_i > \quad \mathrm{i} =\ 1,\ 2,\ 3, \ldots, \mathrm{n} \tag{4}$$

The key of the hospital IoT equipment used in the proposed protocol should be the same condition as the Equation (5) in order to obtain the vector g in which all the color information vectors $\{x_1\}$ are mutually orthogonal.

$$\langle x_m,\ x_n \rangle = \begin{cases} 0 & m \neq n \\ |m|^2 & m = n \end{cases} \tag{5}$$

4.4. Hospital IoT Device Authentication Process

In this section, we show the process of authenticating the hospital IoT device using the vector g generated by using the color information.

4.4.1. Hospital IoT Device Attribute

In order to authenticate the hospital IoT device, the proposed protocol first assigns attribute information as shown in Table 3 according to the IoT device information used in the hospital.

Table 3. IoT Device Information.

IoT Device ID	**IoT Detail Information**			**Timestamp**	**Property**
	IoT Serial Number	**IoT Location**	**Date of IoT Manufacture**		
Hos_0001&Rev_00	12341234	37;30;24.7/126;53;22.1	M20190101	2019-05-25 10:44:20	A1
Hos_0002&Rev_01	12345678	27;50;22.7/124;50;21.1	M20190102	2019-06-25 10:44:20	A2

The hospital server is represented by a correlation matrix such that a set of attribute values w_{ij} can be hierarchically distributed in an n-bit format such as Equation (6) so that attributes can be assigned to a hospital IoT device used in a hospital. At this time, it is assumed that the number of attributes of the hospital IoT device is n.

$$p_n = \begin{cases} 0 & w_{12} & \cdots & w_{1n} \\ w_{21} & 0 & \cdots & w_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n1} & w_{n2} & \cdots & 0 \end{cases} \tag{6}$$

where w_{ij} denotes correlation information between the hospital IoT device attribute information.

If the attribute p_n is 0 in Equation (6), then the correlation between the attribute information w_{ij} becomes a meaningless result.

4.4.2. Hospital IoT Device Authentication

Hospital IoT device authentication uses the server-generated color vector key g. The color vector key g synchronizes the user and the hospital IoT device when a user visiting the hospital applies for the medical service so that the user can easily use the hospital medical service.

When the user and the hospital IoT device are synchronized, the authentication process is performed so that a third party cannot see the information of the hospital IoT device unless they are an administrator. In particular, the color vector key g used in the authentication process is used to perform mutual authentication between the hospital IoT device and the user, together with information obtained by dividing the random number R generated by the user into arbitrary sizes. This process does not require additional cryptographic calculations for hospital IoT devices and users, which results in low computational costs. The hospital IoT device authentication process consists of eight steps.

Step 1: The server asks the user for pre-registered information to verify the identity of the visiting user. When the requested information is verified, the server automatically generates an arbitrary random number using the user information as shown in Equation (7), confirms the hospital IoT devices which will be used for provide medical services for the user, and calculates a random number based on the number of hospital IoT devices divided into an arbitrary size.

$$\mathrm{R} = \sum_{i=1}^{n}\left(\prod_{j=1}^{i} R_j\right) \tag{7}$$

Step 2: The server combines the random number R_i randomly divided by the number of hospital IoT devices with the color vector key g(g $\oplus R_i$) to generate and transmit the shared key SK_i to the user. The shared key SK_i is used to perform mutual authentication between the hospital IoT device and the user, together with the user identifier ID_i, which can confirm the identity of the user.

Step 3: The server encrypts the random number R_i and the user identifier ID_i, as the equation (8) using the shared key SK_i. Then, the server XOR(exclusive or)s the random number R generated by the user with the shared key SK_i and assigns it to the hash function, and sends Equation (10) to the user through the challenge together with Equation (8)

$$E_{SK_i}(\mathrm{R},\ ID_i) \tag{8}$$

$$h_R(R_i \parallel SK_i) \tag{9}$$

$$\mathrm{Transfer}E_{SK_i}\big(\mathrm{R},\ ID_i\,),\ h_R(R_i \,\big\|\, SK_i) \tag{10}$$

Step 4: The user extracts the hash value (= $h_R(R_i \parallel SK_i)$) using random number R, which is randomly generated by the user, and obtains the shared key SK_i. This process can prevent unauthorized spoofing attacks by intercepting user information by accessing hospital IoT devices. The user concatenates the hash value received from the server with the user identifier ID_i to obtain a random number R_i to be used by the hospital IoT device. The user attempts to synchronize with the hospital IoT device supporting the hospital medical service using the random number R_i, and if the communication connection state of the current session normally appears, then the current session information SI_i is transmitted to the other information (random number R_i and the identifier ID_i), which is encrypted with the shared key SK_i and transmitted to the server.

$$\mathrm{Transfer}\ E_{SK_i}(SI_i,\ R_i,\ ID_i) \tag{11}$$

Step 5: The server decrypts it with the shared key SK_i to extract the session information SI_i received from the user. The random number R_i and the user identification ID_i of the decrypted information are used to verify whether the user is a normal user.

Step 6: The server uses the shared key MSK shared between the server and the IoT device to resynchronize with the hospital IoT device if the user's information is matched. Then, the server obtains the user identifier ID_i, the random number R_i and color vector key g. Otherwise, the user and the hospital IoT device detect that the deactivation has occurred, and retransmit $h_R(R_i \| SK_i)$ with the synchronization request message to the user.

Step 7: The server accesses the database, searches the user's information, and compares the user with the user ID_i. The server compares the random number R_i received from the user. If the matching user information is delivered from the server, the random number R_i of the user and the current session information SI_i are updated. Otherwise, the communication is terminated.

Step 8: After the user confirmation, the server gives the attribute p_n to the hospital IoT device according to the medical service applied by the user, and transmits a confirmation message to the hospital IoT device so that the user does not have trouble receiving the medical service.

4.4.3. Control Access to User Medical Records

In order to access IoT devices installed in hospitals, authentication keys that are created for mutual connection between IoT devices are needed. At this point, the authentication key performs the same approach as Figure 4 to extract any color information used for the authentication key. Unlike previous authentication techniques, access control of medical service records stored in hospital IoT devices can be integrated and managed for hospital IoT devices without using additional cryptographic algorithms. In this case, the server restricts attempts by third parties to access medical service records using the attribute value p_n given to hospital IoT devices and authority level information based on the status of hospital officials (doctors, nurses, etc.) to prevent attempts by third parties to illegally access users' medical service records stored on hospital IoT devices.

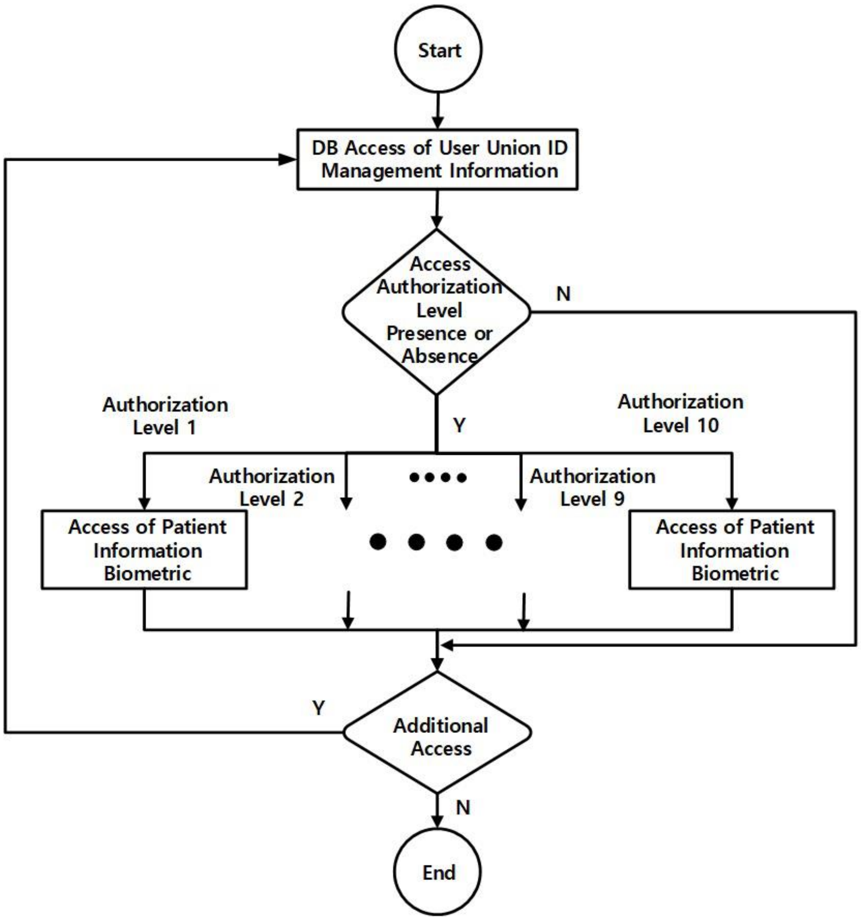
Start
DB Access of User Union ID Management Information
Access Authorization Level Presence or Absence
N
Y
Authorization Level 1
Authorization Level 2
Authorization Level 9
Authorization Level 10
Access of Patient Information Biometric
Access of Patient Information Biometric
Y
Additional Access
N
End

Figure 4. Access Control Processes of Patient records.

Hospital officials are granted authority levels by the server, but the level of authority of the hospital staff can vary depending on the work environment of each area operated by the hospital, so hospital officials with lower levels of authority cannot access basic care of the users who receive medical services.

If the patient's biometric information is available in a hospital or has information about a specific illness with a high level of access, then the hospital official will ask the other hospital to share the user's information. At this time, the use of the assigned user identifier ID_i is prevented from illegally abusing the authority of the user or the hospital personnel. In addition, according to the proposed protocol, the hospital personnel can access the patient 's medical records using the separation of duties and minimum privileges according to the security grade policy set by the hospital, thereby preventing leakage of the patient's personal information and loss of medical information.

5. Evaluation

The proposed protocol was divided into security evaluation and performance evaluation. Security evaluation was performed focusing on internal attacks and external attacks. In the performance evaluation, the efficiency of the hospital IoT device, the delay time of the medical service, and the overhead of the medical staff providing the medical service were evaluated.

5.1. Security Evaluation

The proposed protocol uses the color vector information g and the shared key SK_i to update the user's information even if the user's information is captured by the attacker using the user identifier ID_i and the hash function h(). Therefore, even if the communication between the user and the hospital IoT device, the hospital IoT device, and the server is intercepted, the safety of the information is guaranteed. Also, since the proposed protocol uses a different random number R_i for each hospital IoT device, the third party does not recognize the user's privacy information even if the user copies the information.

In the proposed protocol, the random number R generated by the user is used to extract the hash value (= h_R(R||SK_i)) and then obtains the shared key SK_i. The third-party cannot generate the shared key SK_i because it does not know the color vector key g even if it tries to obtain the shared key SK_i, so it is safe from a third party's spoofing attack. In addition, in the proposed protocol, even if h_R(R||SK_i) is used in other hospitals after assuming that the attacker is a legitimate user, the proposed protocol can prevent attacks by using random number R of different hospital IoT devices as h_R(R||SK_i) to prevent attacks.

In the proposed protocol, we extract the hash value (= h_R(R||SK_i)) using the random number R randomly generated by the user who wants to receive the medical service for each hospital and obtain the shared key SK_i. The personal medical information of the user is not exposed by the person. The server automatically counts the temporary security identifier SID whenever someone accesses the user's information to prevent unauthorized use of the user's information and stores it in the hospital database to update the information.

In the proposed protocol, the server requests information registered in advance by the user to confirm the identity of the user visiting the hospital. After the verification of the requested information is completed, the server automatically generates an arbitrary random number using the user information, we check the hospital IoT device to receive medical service and divide the random number into arbitrary size according to the number of hospital IoT devices, so that information exposure is prevented. In addition, since the random number is applied to the hash function using a random number generator for each session that establishes synchronization between the IoT device and the user, the third party cannot predict what value will be outputted, and it is practically impossible to trace the hospital IoT device or the user.

5.2. Performance Evaluation

For the performance evaluation of the proposed protocol, the experimental environment as shown in Table 4 was set and performance evaluation was performed using the Opnet simulator. The data used for the proposed protocol were tested using the same Intel Galileo board used in references [27,28] to increase objectivity for performance evaluations. The reason why Intel's Kalilio board of Figure 5 was used in the proposed protocol was that it was designed for Intel Quark SoC X1000, chip compact core products, and low power consumption. In addition, the Kalireo board has the ability to run a Linux kernel, and the onboard Ethernet port provides a network. The underside of the calico board offers a mini PCI and is designed to add Wi-Fi connections using an Express slot card for Intel wireless networks.

Table 4. Parameter Setup.

Parameter	Setting
Number of Medical IoT Devices	nmiotd = {1, 2, 5, 10}
Number of User	nu = {10, 25, 50, 100, 250}
Number of Property adopted to IoT device	np = {1, 2, 3, 4, 5}
Threshold	th = {1, 3, 5}
Authentication info. generation interval	0.01 ms
Compressed data size (Bytes) through number of IoT devices	Nn = {20, 30, 50, 60, 80}
Average Compress time (ms)	30
Average Decompression time (ms)	20

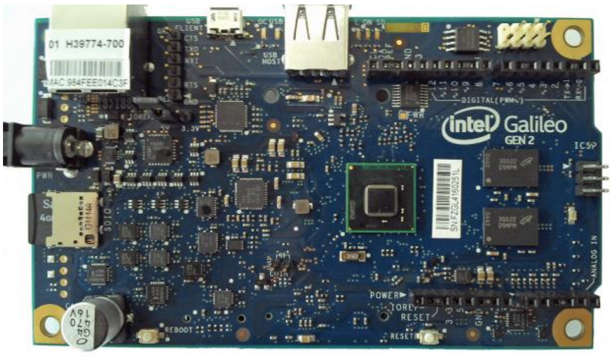

Figure 5. Intel Galileo board used for simulation.

5.2.1. Efficiency for Hospital IoT Devices

Figure 6 compares the effectiveness of a hospital IoT device installed in a hospital with the existing hospital system that does not use the hospital IoT device when applied to the user's medical service. As a result of the experiment shown in Figure 6, the efficiency of the proposed protocol is improved by 31.1% for the hospital IoT device compared to the protocol used by the existing hospital system. This result shows that the proposed protocol performs the iterative process needed to generate the key for providing the medical service to the user so that the n multidimensional color vector information $x_1, x_2, \cdots, x_n$ generated by the hospital server are orthogonal to each other. At this time, in the proposed protocol, the image groups with the same color key are stochastically grouped. In addition, the proposed protocol does not perform the additional task conducted by the medical staff because it sends the user's medical service result through the color vector information from the optimal state to the medical staff in real-time. Through this process, the efficiency of the proposed protocol increases as the number of hospital IoT devices increases. However, even though the existing protocol increases the number of medical staff performing the role of hospital IoT device, the work process is inefficient and work efficiency is not proportionally increased.

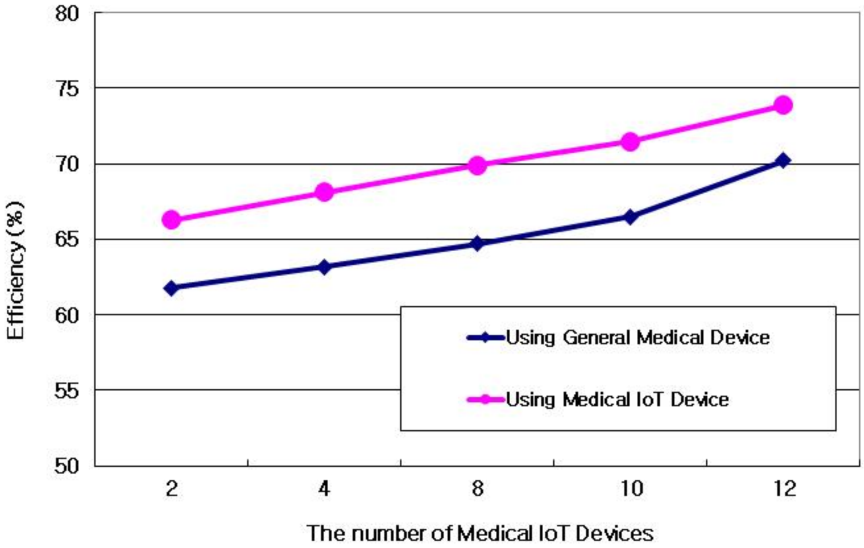

Figure 6. Trace and Monitoring Efficiency of the Patients and Staff.

5.2.2. Delay Time of Medical Service

Figure 7 assesses the delays in the work of medical staff who use hospital-installed IoT devices for health care work. As a result of the experiment shown in Figure 7, the delay time of the medical service of the proposed protocol is improved by an average of 19.8% over the existing protocol. This result is the result of the hospital IoT device diagnosing the user's disease and automatically storing the diagnosis result in the server so that the medical staff could complete the analysis of the user's disease state in advance before consulting with the user. As shown in Figure 6, the proposed protocol has a lower delay time as the disease diagnosis sensor increases in the hospital IoT device. However, since the existing protocol does not integrate the diagnosis process of the medical service, the delay time increases as the operation time increases.

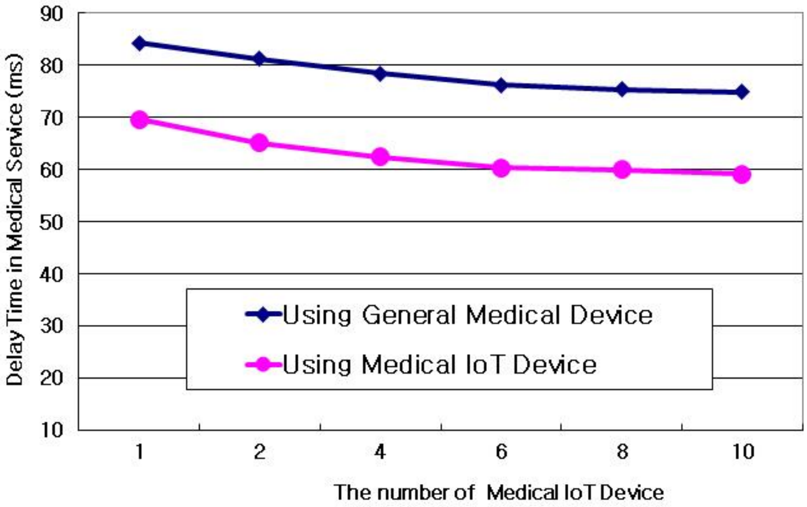

Figure 7. Efficiency between IoT Devices and the Medical Sensor.

5.2.3. The Overhead of the Medical Staff Providing Medical Services

Figure 8 compares the work overhead of health care providers working in hospitals. As shown in Figure 8, the proposed protocol automatically collects and analyzes the patient's disease status through the hospital IoT device rather than the existing protocol, so that the overhead of the medical staff is 15.3% lower because it is delivered to the medical staff accurately. This result is a result of the fact that the work of the additional medical staff is not increased because the state of the network is adjusted to the best condition according to the multi-dimensional color vector information value given to the hospital IoT device. In addition, the result is that the medical staff automatically processes the post-medical service contents, even if the medical staff does not proceed to the additional medical service through the color vector information given to the hospital IoT device.

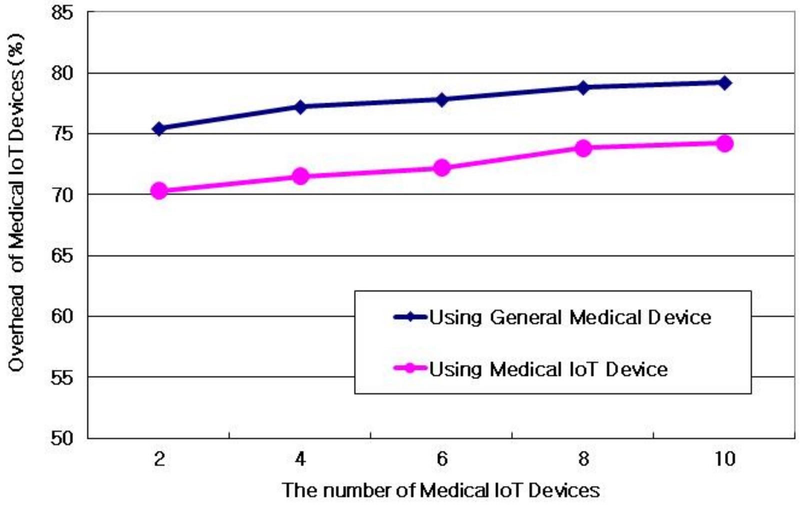

Figure 8. Overhead of IoT devices.

5.2.4. Patient Wait Time for Medical Service

Figure 9 shows the patient's waiting time needed to receive medical services depending on the number of users using the IoT equipment. The data from patients who use IoT equipment will be collected in advance through IoT gateway equipment from the medical department. On average, patients who used IoT equipment waited for five to seven minutes to receive medical services, which was less than the waiting time for other patients. These results are the result of patients receiving medical services by attaching IoT equipment and transferring patient care information to the medical staff at each medical department in real-time. In addition, IoT equipment checks basic patient information and disease information when a patient tries to access the medical department and processes computer tasks that should be handled by the medical department in advance. In addition to patient care and analysis, the clinical workforce has also reduced patient latency.

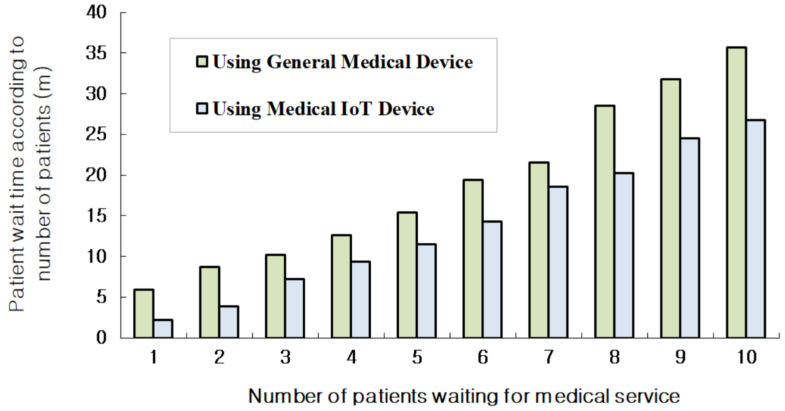

Figure 9. The number of patients waiting for medical service.

5.2.5. Reliability between Medical Staff and Patients

Figure 10 shows the level of trust between medical staff and patients regarding medical services that use IoT equipment. The level of trust between medical staff and patients was 17.1% higher on average in cases when patients used and attached IoT equipment. These results are due to the fact that a medical team can provide medical services for the psychological stability of patients as well as disease treatment, as well as providing a patient with disease information and management methods. In addition, these results came from an improved understanding of the results measured in IoT equipment, as a medical team can accurately convey the meaning of the figures shown through IoT equipment as well as management measures.

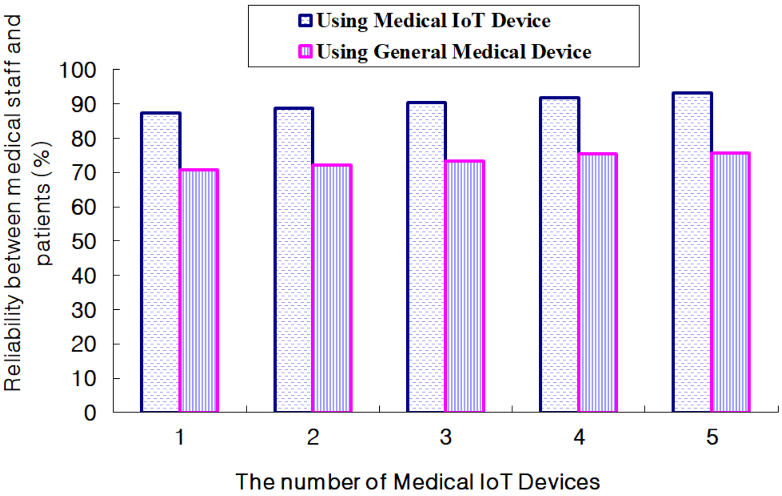

Figure 10. Reliability between Medical Staff and Patients.

6. Conclusions

As diets are becoming westernized worldwide, diseases that have not appeared in the past are now beginning to do so in various countries. To improve the quality of medical services, hospitals are providing medical services to users by introducing hospital IoT devices that incorporate IoT technology into medical devices. In this paper, we proposed an efficient authentication protocol based on multi-dimensional color vector information that can improve efficiency, the quality of medical services, and the work of the medical staff by introducing hospital IoT devices into the hospital system. The proposed protocol required the generation of authentication keys using multi-dimensional color vectors on IoT devices to provide medical services for users visiting hospitals. The proposed protocol provides four distinct services that are different from existing medical services. First, the intercompatibility of IoT devices for medical services in hospitals is supported through the authentication key of hospital IoT devices. Second, real-time information such as users' health status and the status of medical service delivery can be identified. Third, the proposed protocol used color vector values to improve the time and quality of users' medical services. Fourth, the medical team minimized the time and procedures needed for medical services and administrative processing by using hospital IoT devices. As a result of the performance evaluation, the proposed protocol improved the efficiency of the hospital IoT device by an average of 31.1% over the existing protocol. The delay time of the medical service was improved by 19.8% compared to the existing protocol. The average overhead of healthcare providers was also 15.3% lower. Based on the results of this study, future research will apply additional protocols to various hospitals to further study relevant problems and complications.

Author Contributions: All authors have read and agree to the published version of the manuscript. Conceptualization, Y.-S.J. and S.-S.S.; methodology, Y.-S.J.; software, Y.-S.J.; validation, Y.-S.J., D.-R.K. and S.-S.S.; formal analysis, Y.-S.J.; investigation, D.-R.K.; resources, Y.-S.J.; data curation, S.-S.S.; writing—original draft preparation, Y.-S.J.; writing—review and editing, S.-S.S.; visualization, Y.-S.J.; supervision, D.-R.K.; project administration, S.-S.S.; funding acquisition, S.-S.S.

Funding: This research received no external funding

Acknowledgments: This work was supported by the BB21+ Project in 2019.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Weber, R.H. Internet of Things: New Security and Privacy Challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
2. Choi, S.C.; Ryu, M.W.; Jin, M.; Kim, J.H. Internet of Things platform and service trends. *Inf. Commun. Mag.* **2014**, *31*, 20–27.
3. Haller, S.; Karnouskos, S.; Schroth, C. The Internet of Things in an Enterprise Context. *FIS 2008* **2009**, *5468*, 14–28.
4. Raza, S.; Shafagh, H.; Hewage, K.; Hummen, R.; Voigt, T. Lithe: Lightweight Internet of Things platform and service Trends. *IEEE Sens. J.* **2013**, *13*, 3711–3720. [CrossRef]
5. Jeong, Y.S.; Lee, S.H. U-Healthcare User/'s Privacy Protection Protocol with Implantable Medical Device of State Information. *J. Korea Inf. Commun. Soc.* **2012**, *37*, 297–306.
6. Phunchongharn, P.; Nivato, D.; Hossain, E.; Camorlinga, S. An EMI-Aware Prioritized Wireless Access Scheme for e-Health Application in Hospital Environments. *IEEE Trans. Inf. Technol. Biomed.* **2009**, *14*, 1247–1258. [CrossRef]
7. Phunchongharn, P.; Hossaidsn, E.; Camorlinga, S. Electromagnetic Interference-Aware Transmission Scheduling and Power Control for Dynamic Wireless Access in Hospital Environments. *IEEE Trans. Inf. Technol. Biomed.* **2011**, *15*, 890–899. [CrossRef]
8. Shen, Q.; Liang, X.; Shen, X.; Lin, X.; Luo, H.Y. Exploiting Geo-Distributed Clouds for a E-health Monitoring System with Minimum Service Delay and Privacy Preservation. *IEEE J. Biomed. Health Inform.* **2004**, *18*, 430–439. [CrossRef]
9. Reijula, J.; Reijula, E.; Reijula, K. Healthcare management challenges in two university hospitals. *Int. J. Healthc. Technol. Manag.* **2016**, *15*, 308–325. [CrossRef]
10. Koumanditis, K.; Hussain, T. Personal healthcare records research: Past, present and new dimensions. *Int. J. Healthc. Technol. Manag.* **2018**, *17*, 1–28. [CrossRef]
11. Shnayder, V.; Chen, B.; Lorincz, K.; Jones, T.R.F.F. Sensor networks for medical care. In Proceedings of the 3rd International Conference on EMBEDDED Networked Sensor Systems, San Diego, CA, USA, 2–4 November 2005; p. 314.
12. Jeong, Y.S.; Lee, S.H.; Shin, S.S. Access Control Protocol Based on Privacy Property of Patient in m-Healthcare Emergency. *Wirel. Pers. Commun.* **2014**, *79*, 2565–2578. [CrossRef]
13. Jeong, Y.S.; Shin, S.S.; Han, K.H. High-dimensionality priority selection scheme of bioinformatics information using Bernoulli distribution. *Clust. Comput.* **2017**, *20*, 539–546. [CrossRef]
14. Cheng, C.H.; Chen, C.H.; Chen, Y.S.; Guo, H.L.; Lin, C.K. Exploring Taiwanese's smartphone user intention: An integrated model of technology acceptance model and information system successful model. *Int. J. Soc. Humanist. Comput.* **2019**, *3*, 97–107. [CrossRef]
15. Xu, Z. The analytics and applications on supporting big data framework in wireless surveillance networks. *Int. J. Soc. Humanist. Comput.* **2017**, *2*, 141–149. [CrossRef]
16. Khattak, Z.A.; Sulaiman, S.; Manan, J.A. A study on threat model for federated identities in federated identity management system. *2010 Int. Symp. Inf. Technol.* **2010**, *2*, 618–623.
17. Gao, H.; Yan, J.; Mu, Y. Dynamic Trust Model for Federated Identity Management. In Proceedings of the 2010 4th International Conference on Network and System Security (NSS), Melbourne, VIC, Australia, 1–3 September 2010; pp. 55–61.
18. Zhou, Y.; Cao, Z.; Lu, R. Provably secure proxy-protected signature schemes based on factoring. *Appl. Math. Comput.* **2005**, *164*, 83–98. [CrossRef]
19. Mambo, M.; Usuda, K.; Okamoto, E. Proxy signatures for delegating signing operation. In Proceedings of the Third ACM Conf. on Computer and Communications Security, New Delhi, India, 14–15 March 1996; pp. 48–57.
20. Lu, R.; Cao, Z. Designated verifier proxy signature scheme with message recovery. *Appl. Math. Comput.* **2005**, *169*, 1237–1246. [CrossRef]

21. Zaharia, M.; Chowdhury, M.; Das, T.; Dave, A.; Ma, J.; McCauley, M.; Franklin, M.J. Resilient Distributed Datasets: A Fault-Tolerant Abstraction for In-Memory Cluster Computing. In Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation, San Jose, CA, USA, 25–27 April 2012; p. 2.
22. Andrade, G.; Ramos, G.; Madira, D.; Sachetto, R.; Ferreira, R.; Rocha, L. G-dbscan: A gpu accelerated algorithm for density based clustering. *J. Procedia Comput. Sci.* **2013**, *18*, 369–378. [CrossRef]
23. Zaharia, M.; Karau, H.; Konwinski, A.; Wendell, P. *Learning Spark: Lightning—Fast Big Data Analysis*; O'Reilly Media, Inc.: India, 2013.
24. Cui, X.; Zhu, P.; Yang, X.; Li, K.; Ji, C. Optimized big data K-means clustering using MapReduce. *J. Supercomput.* **2014**, *70*, 1249–1259. [CrossRef]
25. Jeong, Y.S. Tracking Analysis of User Privacy Damage using Smartphone. *J. Converg. Soc. SMB* **2014**, *4*, 13–18.
26. Jeong, Y.S. Design of Security Model for Service of Company Information. *J. Converg. Soc. SMB* **2012**, *2*, 43–49.
27. Ranmon, M.C. *Intel Galileo and Intel Galileo Gen 2*; Springer: Berkeley, CA, USA, 2014.
28. Azariadi, D.; Tsoutsouras, V.; Xydis, S.; Soudris, D. ECG Signal Analysis and Arrhythmia Detection on IoT wearable medical devices. In Proceedings of the 2016 5th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, Greece, 12–14 May 2016; pp. 1–4.