Computers, Materials & Continua
DOI:10.32604/cmc.2022.015610
Article

Tech Science Press

Design of an Information Security Service for Medical Artificial Intelligence

Yanghoon Kim[1], Jawon Kim[2] and Hangbae Chang[3,*]

[1]Department of Cyber Drone Bot Military Engineering, Shinhan University, Uijeongbu-si, 11644, Gyeonggi-do, Korea
[2]Department of Security Convergence, Graduate School, Chung-Ang University, Dongjack-gu, 06974, Seoul, Korea
[3]Department of Industrial Security, Chung-Ang University, Dongjak-gu, 06974, Seoul, Korea
[*]Corresponding Author: Hangbae Chang. Email: hbchang@cau.ac.kr
Received: 30 November 2020; Accepted: 23 May 2021

Abstract: The medical convergence industry has gradually adopted ICT devices, which has led to legacy security problems related to ICT devices. However, it has been difficult to solve these problems due to data resource issues. Such problems can cause a lack of reliability in medical artificial intelligence services that utilize medical information. Therefore, to provide reliable services focused on security internalization, it is necessary to establish a medical convergence environment-oriented security management system. This study proposes the use of system identification and countermeasures to secure system reliability when using medical convergence environment information in medical artificial intelligence. We checked the life cycle of medical information and the flow and location of information, analyzed the security threats that may arise during the life cycle, and proposed technical countermeasures to overcome such threats. We verified the proposed countermeasures through a survey of experts. Security requirements were defined based on the information life cycle in the medical convergence environment. We also designed technical countermeasures for use in the security management systems of hospitals of diverse sizes.

Keywords: Medical artificial intelligence; medical information; security; convergence environment

1 Introduction

Nowadays, many industries apply information and communication technologies (ICT). Furthermore, through the fusion of ICT and industry, we have entered the era of the Fourth Industrial Revolution in which all things are connected, enabling us to evolve into a more intelligent society. Radio-frequency identification and ubiquitous sensor network technologies, designed for connection anytime and anywhere, have been made smaller, more active and intelligent by expanding them into the Internet of Things (IoT). The IoT is a system in which automated data can be transmitted without human interference, and which can collect massive amounts of diverse data. Big data collected through the IoT are now being analyzed using advanced technologies such as artificial intelligence (AI).

The medical convergence industry, which is a convergence of the medical industry and ICT, continuously creates and utilizes a huge corpus of information. The industry is now making the transition from a treatment-oriented environment to a prevention-oriented one, and many hospitals, having traditionally conducted all their treatments offline, now receive much patient health information through smart devices. As such, hospitals can establish an ICT convergence environment and plan future decisions through data analysis. New technologies such as IoT, big data, and AI can service valuable new business areas through data acquired from patients and third parties among others.

However, the medical convergence industry is distinct from other industries [1] in that it faces severe medical business-oriented security threats. The medical industry is characterized by specialized devices and environments and is focused on the public good and the provision of medical services. Because of these characteristics, hospitals can experience various security threats in the convergence service environment [2]—for example, CDs containing magnetic resonance imaging (MRI) results can contain malware [3], or patient data can be leaked due to a failure of the authority responsible for managing electronic medical records (EMR). Hospitals, as the key players in the medical convergence industry, are divided into large facilities that employ security experts, and small/medium-sized hospitals that do not employ such experts, a failing which inevitably has an impact on a hospital's system security capabilities.

Given this complex situation, ISO 27799 [4] was proposed as a standard for the construction of security frames for medical institutions. This standard protects personal medical information in healthcare settings and enables the implementation of information security controls. If medical institutions observe this standard, it will benefit the availability, integrity, and confidentiality of their personal medical information. Nevertheless, ISO 27799 cannot be applied at a hospital if it lacks the human resources and money required to implement it. Therefore, the medical convergence industry should have a systematic and business-oriented security framework based on the convergence environment.

To determine a reliable medical AI support framework, this study analyzed the medical information life cycle in order to propose an optimization plan for implementing a systematic security environment. The authors conducted a detailed analysis of the flow of external IoT medical devices as they entered the hospital's medical information to be stored, processed, and utilized. The study also proposes a secure security system encompassing each endpoint of the life cycle, while focusing on the most-utilized technology. Finally, a prototype was developed based on a security system design and feasibility analysis.

2 Related Works

2.1 Characteristics and Status of Medical Convergence Security

The medical convergence industry is a new high-value biomedical service industry created through the convergence of new technologies such as information technology (IT), biotechnology, and nanotechnology [5]. The industry is divided into the silver industry, which is associated with the current phenomenon of the aging society; the lifestyle industry, which is oriented toward diseases associated with modern lifestyles; and an industry focused on technology that aims to advance life expectancy and provide the world's best medical services. The main areas of medical convergence include medical technologies and services used in the process of diagnosis, treatment, and rehabilitation, as well as in disease prevention and health promotion. These can consist of medical devices, medications, and medical organization systems.

In the medical convergence industry, the industrial boundaries and areas are expanding in line with recent changes in the social environment [6]. The medical industry is a public good, and since these services directly deal with human life, their reliability is crucial. With the ongoing changes in society, the economy, and technology, the demand for continuous medical services is increasing due to the introduction of IoT devices and their widespread application to the healthcare industry.

The medical convergence industry is gradually switching from the provision of treatment services to the delivery of healthcare services for patients [7], accompanied by a paradigm shift toward a continuous health management support system based on collected data.

In the past, treatment-oriented services encompassing a patient's hospital visits, repeated treatments, and renewed prescriptions constituted a hospital's primary services. Today, however, data are collected and utilized through various remote healthcare and medical devices prior to hospital visits. This change in the service minimizes the patient's life risk by generating healthcare data through long-term data archiving and reducing the risk of inappropriate treatments due to a lack of patient health data. In addition, it makes it possible to provide customized medical services to patients by preemptively solving the problem of excessive treatment.

2.2 *The Status of Medical Convergence Services*

A variety of ICT systems are currently being used to process patient-customized medical services [8] in the medical convergence environment.

Data for medical services are collected outside hospitals using personal health devices (PHDs), such as blood pressure monitors, weight scales, and blood glucose meters. This type of use particularly targets places where medical access is difficult, such as remote islands and mountainous areas, as well as patients for whom it is necessary to collect a significant amount of health information over a long period of time [9].

Hospitals that directly collect and utilize data for their medical services are now using health information systems such as EMRs, order communication systems and picture archiving. To secure highly reliable medical services and ensure their quality and appropriateness, the latest medical knowledge and technologies need to be used to the maximum possible extent.

Hospitals can also overcome the limitations of service distance among regions by establishing a telemedicine system between hospitals [10] and between hospitals and patients. This type of practice can help to secure expertise in medical services, provide preventative medical services, and ensure service provision. In recent years, based on the application of mobile devices such as smartphones, a comprehensive medical service system has been secured by establishing both an effective management system and a system capable of measuring a patient's health status after treatment.

2.3 *The Security Risk of Medical Convergence Services*

Medical information refers to integrated personal data such as patient (customer) name, gender, age, photo, and medical payment details. Personal medical information collected through the treatment process is used by several hospital departments. It is also transmitted to pharmaceutical companies, medical device manufacturers, and government agencies for external use. As medical information [11] is personally sensitive information related to one's current health status and treatment process, its exposure could inflict mental, social, and economic damages on an individual. Unfortunately, the security level of hospital data is currently very insufficient.

Furthermore, medical devices used in hospitals are manufactured through a supply chain spanning multiple countries. The devices installed when a hospital first opens are often used for a long time without being replaced. If a given hospital's medical service period is ten years, this means that there are devices that may have been used for ten years. Therefore, a standalone medical device has its own security risk. However, if it is connected to a PC and collects information, the problem of compatibility may arise when installing another software program since the PC is optimized for the connected medical device. In addition, when a hospital's operating system functions in an old legacy format, such as Windows XP, it may encounter other problems such as an inability to operate when it is updating or during the installation of a security solution. In other words, security threats, medical device vulnerabilities, and old operating systems are key problems [12–14].

Many researchers are trying to overcome security threats in the medical convergence environment. Shin et al. [15] investigated the privacy problem with respect to hospital size and proposed countermeasures. Pirbhulal et al. [16] proposed a security framework for wearable healthcare systems, and also studied security countermeasures for the medical convergence environment. However, these studies had a limitation in that they only considered fragmentary security countermeasures. Therefore, this study considers the information life cycle in order to propose security countermeasures.

2.4 The Status of AI in the Medical Convergence Environment

AI technology seeks to realize human perception, reasoning, and learning through computer programs [17]. Generally, AI in a medical convergence environment implements medical diagnosis services based on large amounts of diverse types of medical information. For example, a lung diagnosis AI technology recently developed by the medical startup Lunet [18] is being used to read images of suspected COVID-19 patients. With this technology, patients can be classified more than ten times faster than with normal chest X-ray reading, which is a great help in the initial screening process. These medical AI technologies can also be of great help when the number of patients is rapidly increasing and the medical system's resources are limited.

However, in order to implement such AI technology in the medical convergence environment, an enormous amount of big data must be learned. This requirement causes security problems because such medical information is sensitive. It is difficult to check how data is collected and stored or where it exists on which server. Furthermore, it is hard to know the details of leakage incidents for secondary and tertiary purposes. Security threats such as hacking or leakages of medical information also arise. Therefore, this paper proposes a security countermeasure for medical information to support the use of AI technology.

3 Analysis of Security Risks and Requirements Based on the Information Life Cycle of the Medical Convergence Environment

This study proposes technical security countermeasures to minimize security threats in a medical convergence environment. First, the authors of this study analyzed the characteristics and status of the medical convergence environment on the basis of previous studies; then they checked the status of medical convergence services and analyzed the security risks in those medical convergence services. In addition, the study checked the status of AI technology in the medical convergence environment and the requirements for safe AI technology applications. To propose multidimensional security countermeasures, security risks and security requirements were identified based on the medical information life cycle. Then, security countermeasures based on the life cycle [19] were derived and proposed, and a statistical verification was conducted by hospital size, as shown in Fig. 1.

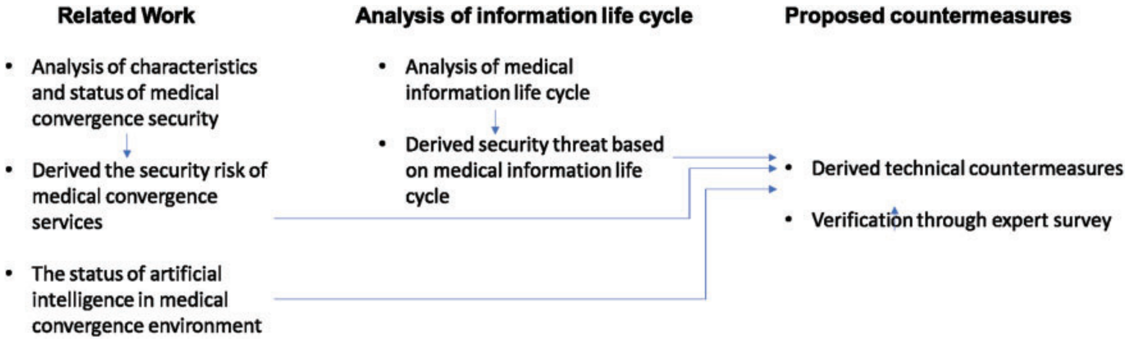
Related Work
Analysis of characteristics and status of medical convergence security
Derived the security risk of medical convergence services
The status of artificial intelligence in medical convergence environment
Analysis of information life cycle
Analysis of medical information life cycle
Derived security threat based on medical information life cycle
Proposed countermeasures
Derived technical countermeasures
Verification through expert survey

Figure 1: Medical information life cycle process

3.1 *Analysis of Security Risks based on the Medical Information Life Cycle*

The term "information life cycle" refers to a series of processes ranging from the creation to the destruction of various types of information. This study defines the information life cycle as a personal information life cycle. The information life cycle is composed of a series of cycles and consists of stages of creation/collection, storage/processing, provision/utilization, and destruction/disposal. Fig. 2 shows the medical data life cycle process, while Tab. 1 defines each step in the information life cycle.

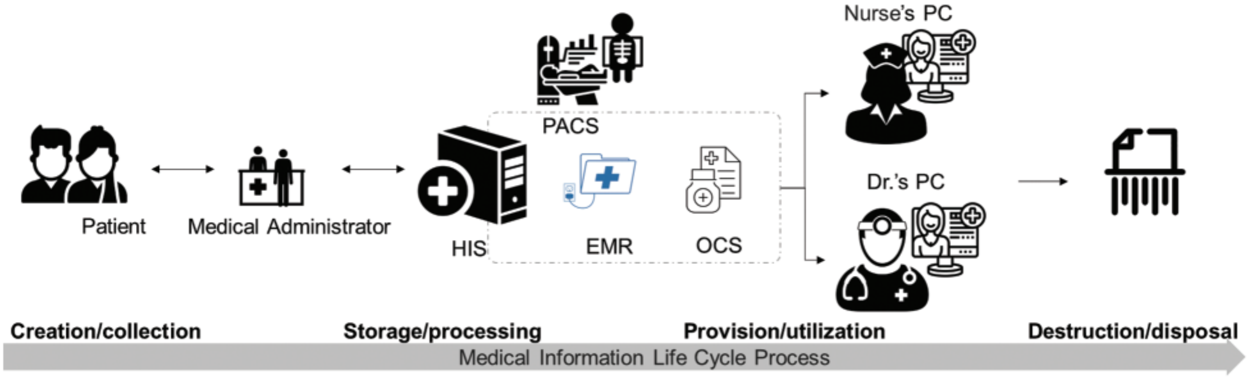

Figure 2: Medical information life cycle process

Table 1: Steps in the information life cycle and their meaning

(Personal) information life cycle step	Meaning
Creation/collection	This step involves the provision of general and sensitive information, such as unique information held by the information subject and newly created information for utilization in the provision of various services.
Storage/processing	This step involves the storing and processing of information collected from multiple data subjects for information provision services.
Provision/utilization	This step involves the sharing of information between internal departments and between agencies for agency-related work and the provision of services, such as medical collaboration and insurance.
Destruction/disposal	This step involves the destruction/disposal of personal information either upon the legitimate request of an information subject, or when there is no longer any need for the information concerned.

In the medical convergence industry, various security risks may arise from the standpoint of the medical information life cycle, including medical information integrity problems due to the malfunction of medical devices, the misuse of patient personal information, cyber-attacks on medical devices from outside, and leakages of medical information by internal employees. Moreover, vulnerabilities may appear when sharing medical information because hospital collection methods vary and because there are external distribution channels for medical information. There may also be legalities that run counter to the safe processing of medical information. Also, medical information can be used for diverse purposes such as tracking major disease trends, analyzing the prescription drug market, checking medical locations, and develpoing insurance products based on secondary information processing. Thus, the social costs occasioned by infringements of medical information are very high compared to other industries. Security threats and vulnerabilities are analyzed based on cases according to the life cycle of medical information used by medical institutions, as presented in Tab. 2.

Table 2: Analysis of security requirements in the medical convergence environment

Medical information life cycle	Cases of security threats and vulnerabilities
Creation/collection	—From the viewpoint of information managers, intentional omission of patients'consent to the provision and use of their medical information. —From the viewpoint of information managers, the use of the patient/customer's collected personal information for other purposes. —From the viewpoint of the online provision of patient (customer) information, external attacks can be launched against the home page. —From the viewpoint of the online provision of patient (customer) information, personal information leakages could occur.
Storage/processing	—Omission of encryption of sensitive information. —Omission of log records of users who access the database (random deletion).

(Continued)

Table 2: Continued

Medical information life cycle	Cases of security threats and vulnerabilities
Provision/utilization	—Granting of excessive access rights to medical information to employees/departments. —Arbitrary access to sensitive patient (customer) personal information by the internal staff (doctors, nurses, administrative staff, etc.) regardless of their position or department. —Information may be leaked by external staff (authorized third parties) who are responsible for the maintenance of medical information system (home page, etc.) or the storage of patient (personal) information. —When transmitting medical information to external related organizations (external provision), security weaknesses include forgery and alteration of the information itself. —Medical information is illegally provided to external organizations or individuals outside the scope of medical information protection.
Destruction/disposal	—After use by the medical institution (hospital) that collects it and the external institution that receives it, the medical information is stored even though it must be destroyed. —Provision of medical information for destruction by other external organizations or individuals.

3.2 Derivation of Security Requirements Based on the Medical Information Life Cycle

The main security threats and weaknesses based on the medical information life cycle of medical institutions are as follows. Physical security requirements are excluded from the scope of this study due to the fact that the physical security system is designed to process printed hard copy information. The physical system considerations mainly concern locking devices, CCTV, and access control devices. Legal security requirements are excluded from this study because the system differs markedly in different regions and countries.

Table 3: Security requirements for the medical information life cycle

Classification	Content
Requirements for management	—There is a need for a security management system that is designed for immediate use and which is oriented toward security organization, security education, and security countermeasures. —There is a need for a security management system specifically designed for the medical life cycle.
Requirements for technology	—There is a need for integrity in a hospital information system that deals with medical information. —There is a need for access control and user identification at the contact point that provides medical information. —There is a need for responsible traceability of information throughout the entire life cycle of medical information.

4 Medical Information Security System Design for Reliable AI Support

4.1 Medical Information Life Cycle Based on Security Technology Derivation

An analysis specific to the medical industry, the convergence of security vulnerabilities, and medical industry security requirements necessitates the design of an information life cycle that reflects the business interests of the medical industry. Tab. 3 shows the core flow and transfer points of information requiring a life cycle-based security system.

To design the medical information security system, the stages and contents of the life cycle stated within brackets, which are mainly used to locate information movements, were analyzed Tab. 4.

Table 4: Designing the security requirements for the medical information life cycle and storage

Location	Life cycle	Information flow location	Security requirements (function)
External hospital (personal)	Creating/Collecting	① PHD IoT	User Identification Security Protocol
	Creating/collecting	② Mobile GW Security GW	Security GW
Network [Security Protocol]			
Internal hospital	Saving/Processing	③ Healthcare Data Server	Information Encryption Malicious Code Prevention/Treatment
	(Creating/collecting) (Saving/processing) Offering/utilizing (Destruction/disposal)	④ HIS (OCS, EMR)	Information Encryption Malicious Code Prevention/Treatment Access Control User Identification Right of Authority SDocument security
	Creating/collecting	⑤ PACS	Malicious Code Prevention/treatment User Identification Anonymous/non-identification
	Saving/Processing (Offering/utilizing)	⑥ Main Server	Information Encryption Malicious Code Prevention/Treatment Access Control User Identification Right of Authority
	Offering/utilizing	⑦ Patients	Anonymous Non-identification

(Continued)

Table 4: Continued

Location	Life cycle	Information flow location	Security requirements (function)
Network [Security Protocol]			
External hospital	Offering/utilizing (Destruction/disposal)	⑧ Pharmacy (Pharmaceutical company) OCS	Information Encryption
	Offering/utilizing	⑨ Patients	Non-identification
	Offering/utilizing (Destruction/Disposal)	⑩ Other Hospitals	Information Encryption
	Offering/utilizing (Destruction/Disposal)	⑪ External Agency	Information Encryption

① PHD IoT

The PHD connected to the IoT is a small, low-cost device that measures blood pressure, blood sugar, heart rate, and sleep. The PHD measures an individual's health condition and remotely sends the collected information to a designated hospital via an outside gateway. This can involve direct transmission from inside the hospital by using designated equipment to access the data stored and processed in personal health records. PHDs should be able to identify users in order to send some information from outside gateways or from designated hospitals. The International Standard for ISO/IEEE 11073 is a PHD communication protocol; it covers the exchange of PHD information, medical information, and IoT device information.

PHD communication often uses Bluetooth due to its advantages of low cost and usability. The protocol presented in the standards does not need to apply related security content to transfer personal health/medical data. The standard defines a total dependence on the security of the transport layer. This means the security level depends on the transport layer; it has the disadvantage of retaining vulnerability if the transport layer is vulnerable. Therefore, IEEE 11073 has security on the presented protocol and integrity, and the confidentiality of personal physical and health information should be secure in transport layer protocols such as Bluetooth.

② (Mobile) Gateway (GW)

The PHD needs a gateway that plays an interim role in collecting and delivering medical information such as healthcare data. The IoT can use such gateways as a router or a separate server, but it mainly uses mobile gateways, which often involve smartphones. Multi-species, large-quantity, and multi-person convergence healthcare data produced by an IoT PHD are collected. The gateway is also a reliable intermediary system that transmits data to hospitals, thus allowing a large amount of data to be collected. Lastly, it must defend itself from external cyber-attacks and establish an environment that can prevent forgery.

Because the information transfer location used in ③ to ⑥ is an internal hospital system, the location includes access control and authority management functions based on user authentication and medical personnel classification. In the case of an introduced 'Timeworn' system, if the purchase and connection of new equipment or the existing system cannot be upgraded, it is necessary to have a function that can prevent malicious codes from entering the system. For example, it may be that the operating system is Windows XP optimized with PACS. In this case, a corresponding window should be established in order to enable the use of an appropriate method of defense against malicious codes on the fetch program and to rectify the situation.

③ Healthcare Data Server

A hospital's healthcare data servers collect, store, and process data from external mobile gateways or from patients who have visited the hospital in person. In some hospitals, they are utilized through a server linked with the hospital's information system. To secure the healthcare data servers, an encryption function is required for databases and data collections.

④ HIS (OCS, EMR)

An order communication system comprising electronic medical records and other elements is a core system that processes and utilizes healthcare and medical information. In addition to basic security functions, a document security function is needed for information processing and storage.

⑤ PACS

A picture archiving and communications system obtains and stores image information through an imaging diagnostic device in a digital state. It executes the functions necessary to transmit and retrieve readings and medical records together. A system in which multiple components are combined and operated is used after linking medical equipment (CR, DR, reading monitors, etc.), IT equipment (servers, storage, PCs, monitors, networks, etc.) and applications based on a PACS-only software. If the PACS is an older medical video storage transmission system, a defense against malicious codes suitable for the operating system and the PACS should be implemented. If systems in which personal healthcare and medical information are combined into file format data for the reading of images and video information, information about individuals needs to be processed using anonymous and unidentifiable functions.

⑥ Main Server

The database encryption function is essential because the main server is connected to the hospital information system that stores all the information.

⑦ Patients

Patients wait in open spaces where various activities are actively carried out, such as registration for blood collection and examinations such as ultrasound, CT, and MRI. When patients visit a hospital for the first time, they need to fill out various documents before their examination. Therefore, it is necessary to provide anonymous or non-identifying information for personal designation so that personal information cannot be specified during this data collection process.

The eight items specified under Tab. 4's "Information Flow Location" constitute the process of delivering healthcare. As for medical information sent to outside sources upon completion of a patient's treatment, basic information encryption functions and anonymous/non-identification functions are also required.

4.2 Security Frame Design According to the Life Cycle of Medical Information

Healthcare data are collected from patients and stored in a dedicated healthcare data server inside the hospital, and are then processed and used within the hospital information system. The integrated data eventually flow out of the hospital again, where they are used (and finally destroyed) by pharmaceutical companies, disease management government agencies, and pharmacies. Throughout the entire process, individual healthcare data are steadily reused between the individual patient who creates and the medical staff. Such data can support medical AI, and will be discarded upon becoming unusable. The stored data can also be discarded at the patient's request, but arbitrary discards are excluded from this process.

The security framework is designed based on the medical information life cycle shown in Fig. 3. The security method is structured and designed according to the information movement locations described in Section 4.1. The security framework identifies most people involved in hospitals that use big healthcare data, and can be constructed if the human and physical resources are sufficient. In other words, its design is centered on a large hospital.

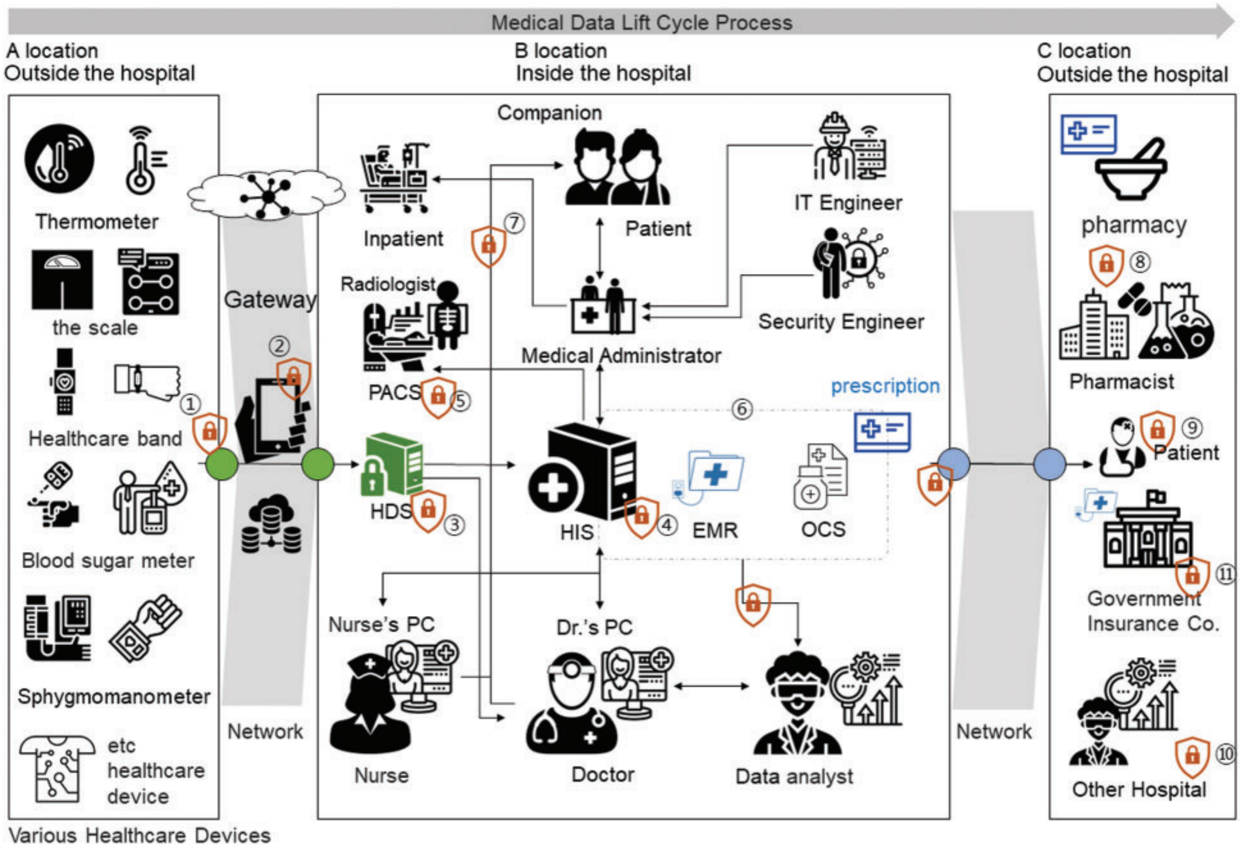

Figure 3: Security frame design according to the medical information life cycle for reliable medical AI support (large hospital)

Hospitals vary in size by region and country, and their financial circumstances also differ. In general, the security frameworks of small and medium-sized hospitals are integrated and operated on a smaller scale. Thus, analyses of small and medium-sized hospitals based on field surveys and expert interviews have confirmed the following differences. First, external healthcare big data collectors cannot handle every type of IoT PHD data. In addition, IT engineers and security engineers are not directly hired, and many hospitals do not have any PACS equipment. Furthermore, cases have been reported in which nurses directly handle the information system without the involvement of any hospital administrative personnel. The internal system is an integrated server system in which the EMR and OCS operate together. Considering these points, it is necessary to establish the appropriate level of security framework by adjusting for cost and workforce limitations, rather than instituting all security technologies for small and medium-sized hospital security frames, as shown in Fig. 4.

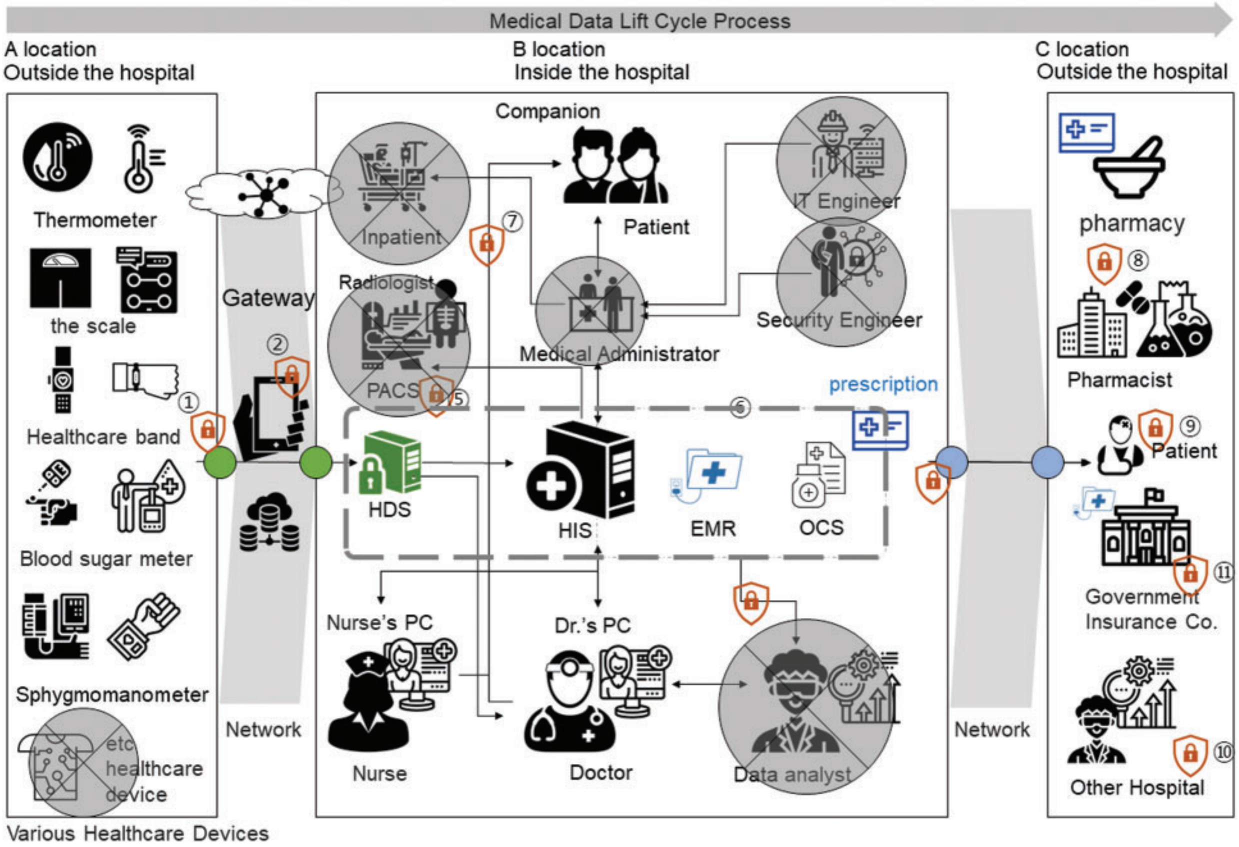

Figure 4: Security frame design according to the medical information life cycle for reliable medical AI support (small and medium-size hospitals)

4.3 Security Frame-Based Prototype Development and Adequacy Verification

A questionnaire survey was conducted to examine the acceptability of the technical limitations and the differences between small/medium-sized hospitals and large hospitals. From March–June 2019, 132 experts, including medical personnel, IT engineers, security engineers, and consultants, were surveyed on the applicability of the security technologies designed in ① to ⑪ based on urgency and justification. A 5-point Likert scale was used to assess the responses to the survey See Tab. 5.

Table 5: Acceptability of medical information security technology by hospital size

Main security technology	Acceptability	
	Small and medium-sized hospitals	Large hospitals
PHD security solution	3.53	4.92
Medical information security gateway	3.23	4.88
PHD authentication technology	3.15	4.65
HIS (Hospital information system) Authentication technology	4.66	4.82
Access control and authority management	4.52	4.73
Medical environment preventative technology	4.23	4.58
Medical information anonymous and non-identification	3.81	4.81
Average	3.87	4.77

A "PHD Security Solution" provides data encryption for personal healthcare devices and uses a security protocol when transmitting data. A "Medical Information Security Gateway" safely stores the healthcare and medical information received from the PHD and transmits it to the hospital's server. The "PHD Authentication Technology" is a public key-based authentication technology that can identify individual users of individual devices. The "Medical Information System Certification Technology" checks medical personnel (doctors, nurses, administrators, etc.) to identify the medical information systems used in hospitals. "Access Control and Authority Management" is a function that distributes and manages the authority to use medical information to users who are authenticated in the medical information system. The "Medical Environment Disinfecting Technology" designates and protects a specific process so that it is not exposed to cyber-attacks from malicious codes. The "Medical Information Anonymization and De-Identification Technology" uses internal medical information to support AI and prevent leakages of the information of specific individuals.

Most of the technologies presented were found to be appropriate for use in large hospitals. However, the PHD Security Solution for collecting external healthcare data, the medical information security gateway, the PHD authentication technology, and the anonymization and de-identification technology designed to assist external collection and utilization were found to be inappropriate for use in small and medium-sized hospitals. Hence, the deployment of security systems differs between large hospitals and small and medium-sized hospitals.

Finally, the following prototype was developed and analyzed based on the proposed security technology to determine its acceptability as a medical information security system supported with reliable medical AI support. In addition, the following solutions were developed: ① PHD security solution; ② security gateway; ③–⑥ authentication, access control, authority management, disinfecting solution; and ⑦–⑪ anonymization and de-identification solutions (Fig. 3). According to the results of this study's questionnaire, the average level of acceptance of the prototype was 4.59, while the perception of effectiveness was 4.80, as shown in Tab. 6 and Fig. 5.

Table 6: Acceptability and effectiveness of medical information security technology by hospital size

Main security technology	Acceptability		Effectiveness	
	Small and medium-sized hospitals	Large hospitals	Small and medium-sized hospitals	Large hospitals
PHD security solution	–	4.90	–	4.95
Medical information security gateway	–	4.91	–	4.93
PHD authentication technology	–	4.75	–	4.83
HIS (hospital information system) Authentication technology	4.84	4.76	4.81	4.86
Access control and authority management	4.61	4.87	4.71	4.88
Medical environment preventative technology	4.33	4.60	4.13	4.59
Medical information anonymous and non-identification	–	4.85	–	4.88
Average	4.59	4.80	4.55	4.85

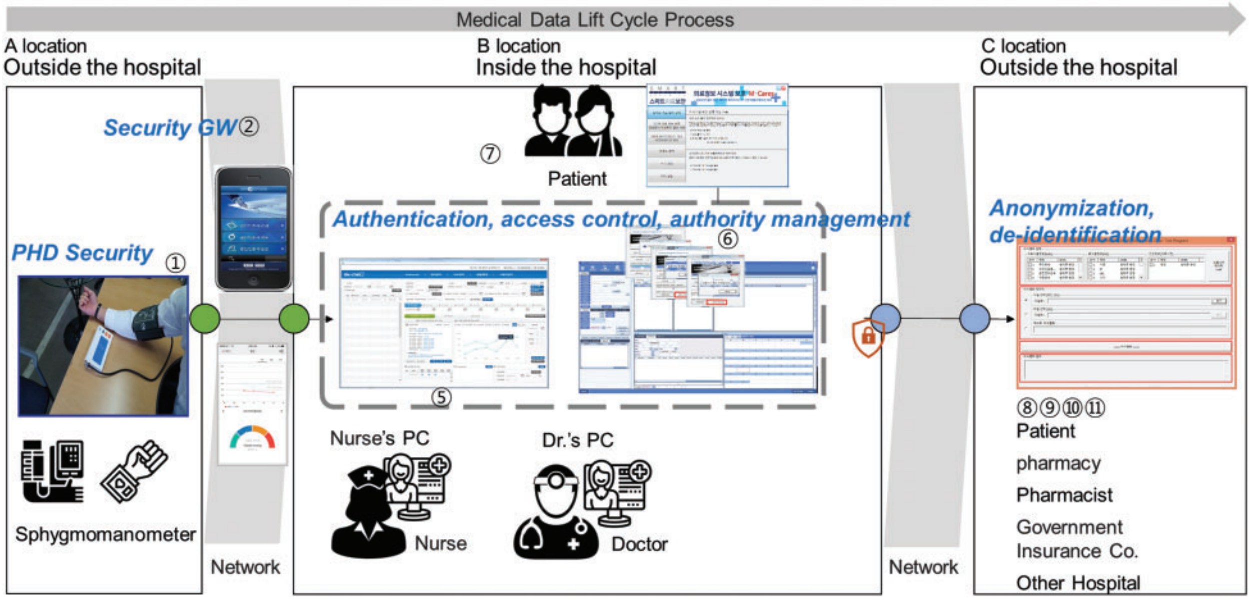

Figure 5: Prototype of a medical information security service with reliable medical AI support

5 Conclusions

The leading technologies of the Fourth Industrial Revolution, such as the IoT, cloud, big data, and mobile phones, are permeating diverse industries and creating new business avenues. In particular, the IoT, which can collect big data linked to AI, provides new and innovative services in various ways. Notably, the paradigm of the medical convergence industry is changing from a treatment-oriented one to a prevention-oriented one. The most striking characteristics of this change are the collection, storage, processing, and analysis of healthcare data using the IoT. This study derived security guidelines that can be applied to analyze information movement locations based on the medical information life cycle, and also designed a framework tailored to hospital size and tested its feasibility with a prototype.

This study makes the following contributions to the body of literature:

1) An analysis of security threats and weaknesses can raise awareness of the importance of security among hospital stakeholders.

2) Security management system requirements are presented based on medical information and the information life cycle.

3) Depending on its size, a hospital can conduct research emphasizing diverse competencies and plan the establishment of a security system.

4) The results of this study, including the acceptability of the proposed security technology, could encourage the use of medical AI support using reliable medical information.

In the future, the authors of this paper intend to conduct research on a model design method with security in order to create a new business concept based on medical data.

Funding Statement: This paper was supported by a Korea Institute for the Advancement of Technology (KIAT) grant funded by the Korean government (MOTIE, No. P0008703) and by a National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT, No. 2018R1C1B5046760).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Kim and H. Chang, “Healthcare security task and future environment,” *OSIA Standards & Technology Review*, vol. 31, no. 2, pp. 4–9, 2018.

[2] H. Chang, “Seoul, Korea: Security NEWS,” Customized Medical Security for Small and Medium Sized Healthcare Institutions, 2018. [Online]. Available: https://www.boannews.com/media/view.asp?idx= 72308 &page= 1&kind= 2.

[3] B. Oh, “Seoul, Korea: Security NEWS,” Malware on the MRI CD Received from the Hospital?, 2012. [Online]. Available: https://www.boannews.com/media/view.asp?idx= 29827&page= 1&kind= 3.

[4] ISO, *ISO 27799: 2016. Health Informatics—Information Security Management in Health Using ISO/IEC 27002*. Geneva, Switzerland: ISO, 2016. [Online]. Available: https://www.iso.org/standard/62777.html.

[5] M. Lee, “Strategies for promoting the medical device industry in Korea: An analytical hierarchy process analysis,” *International Journal of Environmental Research and Public Health*, vol. 15, no. 12, pp. 2659–2672, 2018.

[6] A. H. Sodhro, S. Pirbhulal and A. K. Sangaiah, “Convergence of IoT and product lifecycle management in medical health care,” *Future Generation Computer Systems*, vol. 86, no. 19, pp. 380–391, 2018.

[7] Ġ. P. Eracan, H. K. D. Yildiz and S. Semgzoglu, “Evaluation of next generation healthcare services: Wearable technology products,” in *Proc. Int. Conf. on Humanities, Social Sciences & Interdisciplinary Studies*, Lisbon, Portugal, pp. 14–18, 2019.

[8] P. Ramayya, A. Ramayya, D. Burton, A. M. Pinder and S. Mateti, “Patent Application No. 16/151,802,” 2019.

[9] M. J. Bietz, C. S. Bloss, S. Calvert, J. G. Godino, J. Gregory *et al.,* “Opportunities and challenges in the use of personal health data for health research,” *Journal of the American Medical Informatics Association*, vol. 23, no. e1, pp. e42–e48, 2016.

[10] Y. Zhai, J. Gao, B. Chen, J. Shi, L. Wang *et al.,* “Design and application of a telemedicine system jointly driven by videoconferencing and data exchange: Practical experience from Henan province,” *China Telemedicine and e-Health*, vol. 26, no. 1, pp. 87–98, 2020.

[11] S. Qiu, G. Xu, H. Ahmad and L. Wang, “A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems,” *IEEE Access*, vol. 6, pp. 7452–7463, 2017.

[12] T. Mahler, Y. Elovici and Y. Shahar, “A new methodology for information security risk assessment for medical devices and its evaluation,” 2020. Preprint at https://arxiv.org/pdf/2002.06938.pdf.

[13] I. Stine, M. Rice, S. Dunlap and J. Pecarina, “A cyber risk scoring system for medical devices,” *International Journal of Critical Infrastructure Protection*, vol. 19, pp. 32–46, 2017.

[14] J. Sametinger, J. Rozenblit, R. Lysecky and P. Ott, “Security challenges for medical devices,” *Communications of the ACM*, vol. 58, no. 4, pp. 74–82, 2015.

[15] M. Shin, C. Lee and S. Cho, “A Study on the improvement of personal information protection in small and medium-sized medical institutions,” *Journal of Convergence Security*, vol. 19, no. 4, pp. 123–132, 2019.

[16] S. Pirbhulal, O. Samuel, W. Wu, A. Sangaiah and G. Li, “A joint resource-aware and medical data security framework for wearable healthcare systems,” *Future Generation Computer Systems*, vol. 95, no. 2, pp. 382–391, 2019.

[17] A. Holzinger, C. Biemann, C. Pattichis and D. Kell, “What do we need to build explainable AI systems for the medical domain?,” 2017. Preprint at https://arxiv.org/abs/1712.09923.

[18] M. Salim, E. Wåhlin, K. Dembrower, E. Azavedo, T. Foukakis *et al.,* “External evaluation of 3 commercial artificial intelligence algorithms for independent assessment of screening mammograms,” *JAMA Oncology*, vol. 6, no. 10, pp. 1581–1588, 2020.

[19] G. Shah, K. Voruganti, P. Shivam and M. Alvarez, *Ace: Classification for Information Lifecycle Management*. San Jose, CA, USA: IBM Research Division Almaden Research Center, 2006. [Online]. Available: https://www.cs.yale.edu/homes/shah/pubs/IBM-RJ10372.pdf.