BMC Medical Informatics and Decision Making

RESEARCH ARTICLE Open Access

Risk management-based security evaluation model for telemedicine systems

Dong-won Kim, Jin-young Choi and Keun-hee Han*

Abstract

Background: Infectious diseases that can cause epidemics, such as COVID-19, SARS-CoV, and MERS-CoV, constitute a major social issue, with healthcare providers fearing secondary, tertiary, and even quaternary infections. To alleviate this problem, telemedicine is increasingly being viewed as an effective means through which patients can be diagnosed and medications prescribed by doctors via untact Thus, concomitant with developments in information and communication technology (ICT), medical institutions have actively analyzed and applied ICT to medical systems to provide optimal medical services. However, with the convergence of these diverse technologies, various risks and security threats have emerged. To protect patients and improve telemedicine quality for patient safety, it is necessary to analyze these risks and security threats comprehensively and institute appropriate countermeasures.

Methods: The security threats likely to be encountered in each of seven telemedicine service areas were analyzed, and related data were collected directly through on-site surveys by a medical institution. Subsequently, an attack tree, the most popular reliability and risk modeling approach for systematically characterizing the potential risks of telemedicine systems, was examined and utilized with the attack occurrence probability and attack success probability as variables to provide a comprehensive risk assessment method.

Results: In this study, the most popular modelling method, an attack tree, was applied to the telemedicine environment, and the security concerns for telemedicine systems were found to be very large. Risk management and evaluation methods suitable for the telemedicine environment were identified, and their benefits and potential limitations were assessed.

Conclusion: This research should be beneficial to security experts who wish to investigate the impacts of cybersecurity threats on remote healthcare and researchers who wish to identify new modeling opportunities to apply security risk modeling techniques.

Keywords: Telemedicine security, Medical information security, Smart medical security, Telecare security

Background

Healthcare is evolving towards preventive medical services for lifelong personal health management [1]. Concomitant with the fusion of healthcare with information and communication technology (ICT), various new services and networked medical devices have been developed. These networked devices provide services such as telemedicine, health information exchange, and precision medicine. As these devices have immediate effects on the lives of patients, security management is critical [2–12]. In particular, data transmission from wired to wireless networks requires specific security guidelines for data processing and management and medical device development [13].

In addition, infectious diseases such as COVID-19 [14, 15], SARS-CoV [16], and MERS-CoV [17] cause major social problems and are known to result in severe

* Correspondence: khhan@formal.korea.ac.kr
Information Security Department, Korea University, Seoul, Republic of Korea

respiratory or gastrointestinal complications when they infect animals or people. Coronavirus (CoV) was previously considered to be a pathogen that causes minor symptoms in the community in the form of endemic infection, but there is a growing need to introduce telemedicine that can be utilized to diagnose and prescribe appropriate medication owing to the growing fear of secondary and tertiary infections [15].

Many recently developed medical devices are upgradable, which further increases the potential security threats that can affect them. For example, the vulnerability of insulin pumps to hacking was reported both in 2010 and 2013 [18]. Additionally, in August 2016, an intensive care unit infusion pump sensor without communication functionality was hacked using a low-cost infrared laser [19].

Telemedicine can be broadly categorized into five types: ① videoconference-based patient consultations using the Picture Archiving Communications System in large hospitals, ② multimedia transmission to provide remote services such as first-aid directions, ③ remote home care, ④ remote training of patients or health professionals, and ⑤ online medical counseling and health information sharing [20].

With recent advances in internet of things technology, connectivity between objects is being driven by the medical/electronic sector [21, 22]. Healthcare services value prevention and management over the treatment of future diseases, which can be extended to diagnosis, surgery, and treatment [23]. The healthcare field is being labeled as the "next big thing," and innovative developments are highly anticipated [24–26]. Implantable medical devices (IMDs), which monitor patient health and heal affected body parts, are vital in healthcare [27]. Examples of IMDs include cardiac pacemakers and defibrillators, which monitor and treat heart conditions; deep brain simulators, which treat epilepsy or Parkinson's disease; drug delivery systems in the form of infusion pumps; and bio-instruments that acquire and process bio-signals [28].

However, IMDs, which are equipped with advanced computing and communications capabilities, also entail security and privacy threats. In some cases, such threats can have fatal consequences. Deliberate attacks can result in death if they cause intentional malfunctions, and intentional attacks can be considerably more difficult to detect than accidental attacks [29]. IMDs also store and transmit highly sensitive medical information that should be protected under the laws of Europe (e.g., Directive 95/46/ECC) and the United States (e.g., CFR 164.312) [30, 31]. Experiments have demonstrated how treatment functions can be disabled or reprogrammed to induce shock conditions in patients through wireless connections, as a part of an attack on an IMD [32–34]. Moreover, the device can be sabotaged by intentionally discharging the battery. In such cases, it is often necessary to replace the IMD through surgery. For cardiac IMDs, the power can be switched off using a magnetic field [35], which led to former U.S. Vice President Dick Cheney disabling the Wi-Fi function of his implantable cardioverter–defibrillator to prevent remote assassination attempts [2].

Security requirements pertaining to the processing and management of large amounts of data transmitted wirelessly are essential, and the importance of cybersecurity in the development of medical devices is growing [3]. Various medical devices that have evolved in recent years have had several functional advances, but the potential security threats have also continued to grow. The possibility of hacking of medical devices has already been reported in several articles [4, 6], and research has demonstrated the possibility of healthcare-related security accidents.

A common paradigm in the performance of cyber risk assessment is to form two adversarial teams consisting of a "red team" whose job is to think like an attacker and a "blue team" that seeks to defend the system by developing countermeasures [36]. In many situations, red team information is applied to model the systems using techniques such as attack trees [10], attack-defense trees [37], event trees [38, 39], Markov models [40], decision diagrams such as binary decision diagrams [41], and fault trees [42, 43].

The "attack tree" process [10] is a systematic method for determining the characteristics of system security based on all attacks to which a system is exposed [6–9]. Identifying all possible defined attacks facilitates analysis of all possible cyberattack access paths and selection of the best-suited countermeasures and their optimal deployment. An attack tree consists of nodes, edges, and connectors, with each node corresponding to an attack step. The root node represents the ultimate goal of the attacker, while the children of a given node represent the subgoals. The edges represent the state change caused by the actions of the attacker. A connector is a gate (either OR (disjunctive) or AND (conjunctive)) for the nodes with two or more children for advancement to reach the attack goal [10].

In this study, the most popular modeling approach, an attack tree, was utilized, with the attack occurrence probability (AOP) and attack success probability (ASP) as variables, to develop a risk assessment method, and the benefits and potential limitations of this method were assessed.

The remainder of this paper is organized as follows. Section II describes the telemedicine system architecture and discusses potential security threats and scenarios that may arise therefrom. Section III outlines the

proposed risk assessment method based on an attack tree with the AOP and ASP as variables. Section IV presents and analyzes the experimental results obtained and discusses the assumptions and limitations of the study. Finally, Section V provides the conclusions and outlines future research directions.

Telemedicine system architecture

A telemedicine system [1] can be divided into two sections according to its components: (1) components accessible to the user (or patient), such as the telemedicine terminal, and (2) components available to the telemedicine service provider only, such as the telemedicine system and medical team. The possible security threat scenarios based on information flow through the various components are summarized below [11, 12] (Fig. 1):

1 Spreading of malicious code in the sensing (measurements) hardware, breaching the security barrier, accessing sensitive patient information, and gaining access to the main server via the sensing device.
2 Information leakage or data forgery in the medical data transmission section.
3 Sensing (measurement) data breach risks due to vulnerabilities in the personal computer (PC), smart device, or gateway used for data transmission by the repository or medical staff.
4 Cyberattack risks due to a vulnerable main server and repository in the provider area.

Telemedicine system threat extraction and identification

To identify the threats suitable for constructing the telemedicine attack tree, we extracted typical and scenario-based security threats in accordance with ISO/IEC 27005 Annex C. Examples of typical threats [19] and healthcare-related security threats were extracted based on ISO/IEC 27799 Annex A [44], and the collected data were reorganized. Finally, to identify the telemedicine system vulnerabilities, we reorganized the extracted threats to make them amenable to the telemedicine environment based on ISO/IEC 27005 [19]. The resulting data were used as the components of the telemedicine attack tree. Based on the system architecture and the identified security threats and vulnerabilities, we pinpointed seven telemedicine security threat areas (Fig. 2).

Use cases: seven telemedicine security threat areas

- Threat #1: User or patient

Users receiving telemedicine (i.e., patients) are most likely residents or senior citizens who live in remote areas. Most of them have never received cybersecurity training and have little interest in cybersecurity. Therefore, their use of telemedicine terminals easily attracts security threats related to device use errors, weak passwords, device loss, phishing, etc. [28].

- Threat #2: Telemedicine devices

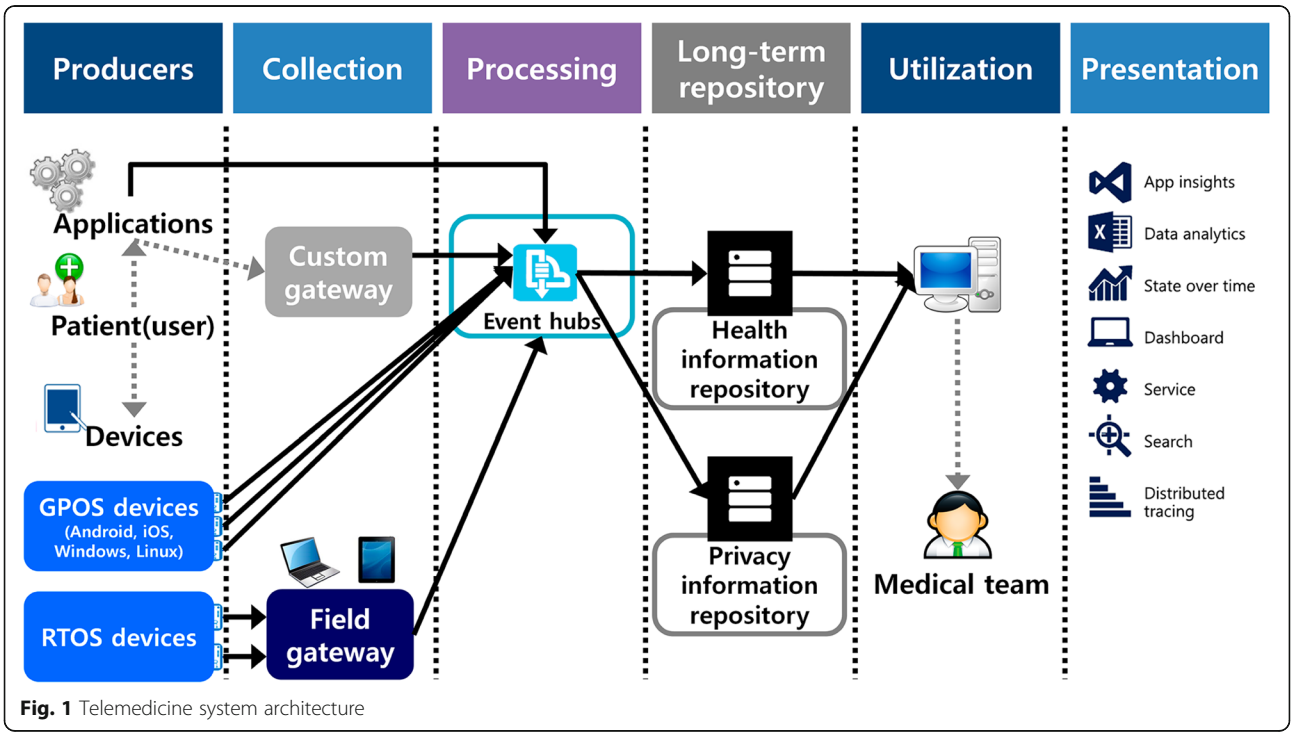

Fig. 1 Telemedicine system architecture

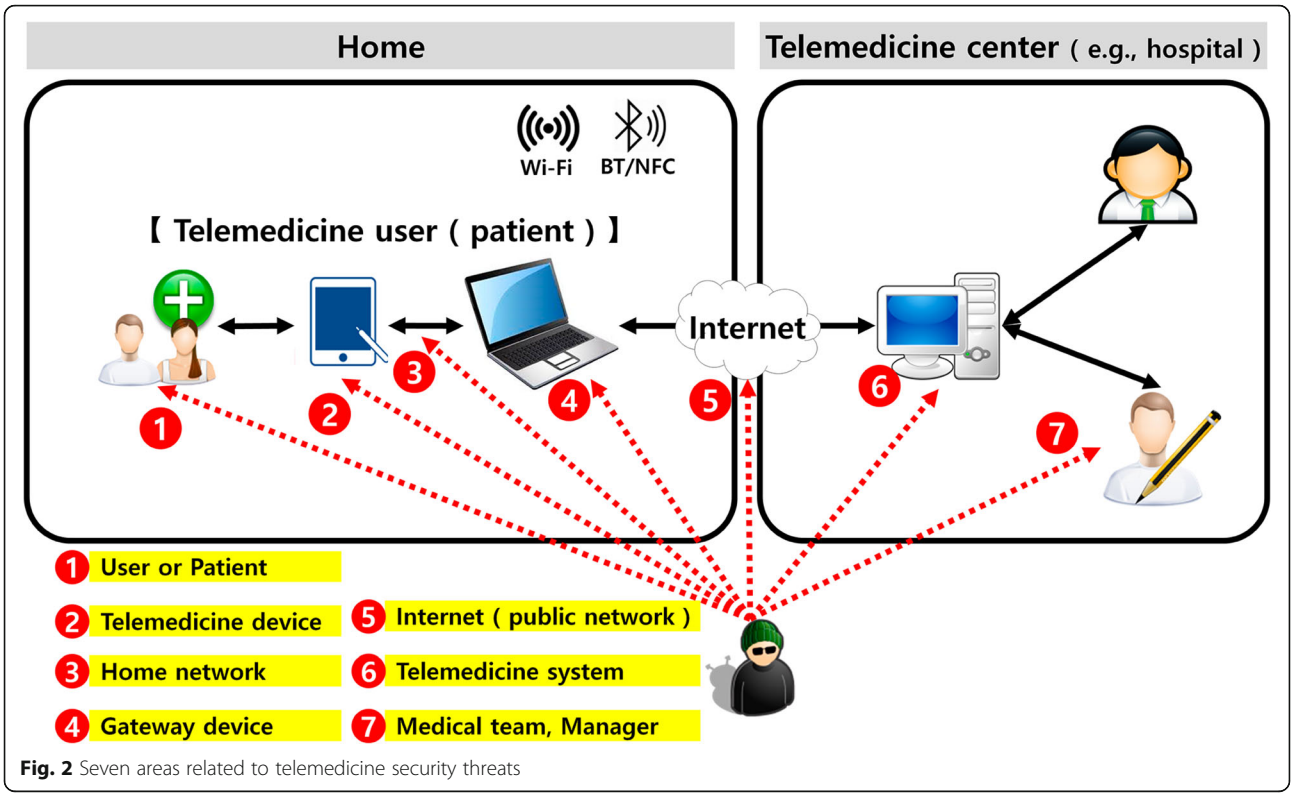

Fig. 2 Seven areas related to telemedicine security threats

A telemedicine terminal is based on either a general-purpose operating system (GPOS) or an embedded-type real-time operating system (RTOS). RTOS-based devices are safe from unauthorized access because they are optimized for specific functions at the design and production stages. Conversely, GPOS-based devices such as smartphones are vulnerable to security threats because they use external apps. The use of telemedicine terminals in such environments makes them vulnerable to security threats owing to the data saving and

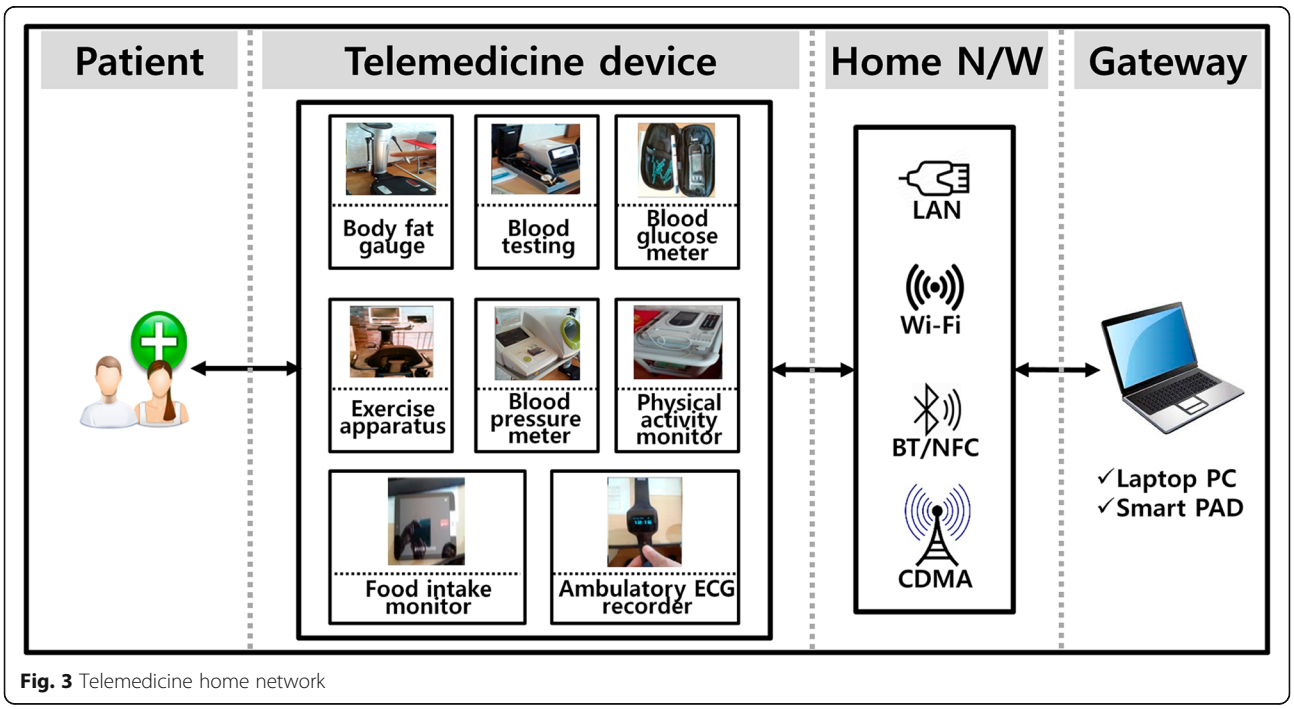

Fig. 3 Telemedicine home network

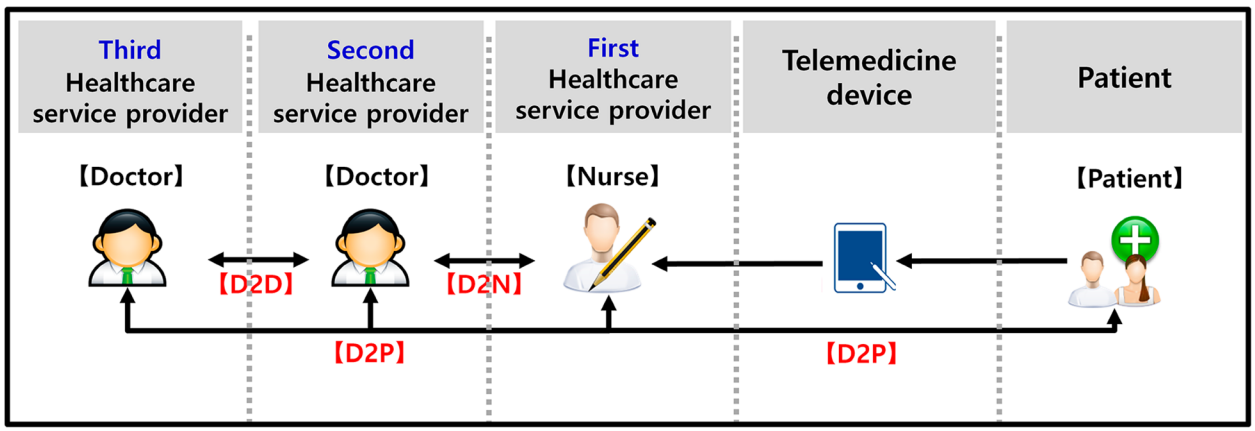

Fig. 4 Telemedicine service provider

sharing functionalities of these devices and the risk of device loss/theft, app vulnerabilities, and plaintext transmission [28, 30, 45–47].

- Threat #3: Home network

Information transmission between the telemedicine terminal in the private space of the patient (home or office) and the telemedicine system occurs primarily via a wireless network. As illustrated in Fig. 3, the types of networks used in home environments include LAN (local area network), Wi-Fi, Bluetooth, NFC (near field communication), and third and fourth generation/long-term evolution networks. While some embedded-type devices need to be connected to LANs, GPOS-based smart devices can communicate with telemedicine systems via multiple paths. In such environments, home-network-based telemedicine service systems are exposed to security threats associated with end-to-end plaintext transmission and man-in-the-middle (MITM) attacks (Fig. 3) [28, 48].

- Threat #4: Gateway devices

A gateway plays an intermediary role between the patient and telemedicine system, exposing the system to security threats associated with rogue gateways as well as the loss/theft of the gateways and MITM attacks [28, 49].

- Threat #5: Internet (public network)

Communication between the patient and telemedicine system occurs via a public network (the Internet). As private, medical, and health information along with prescriptions are transmitted via the publicly accessible Internet, it is important to establish end-to-end security guidelines. In addition, encrypted data transmission is essential. In this environment, the telemedicine system is vulnerable to security threats associated with sniffing, forgery/alteration, and privilege escalations [28].

- Threat #6: Telemedicine system

The telemedicine system is situated at the location of the telemedicine service provider. It consists of a PC and the software necessary for remote consultations, and its users are the medical staff, nursing personnel, and system administrators (security officer and other support staff). This system is very important because it handles all of the data of the patients receiving the telemedicine services. Moreover, if the telemedicine system is

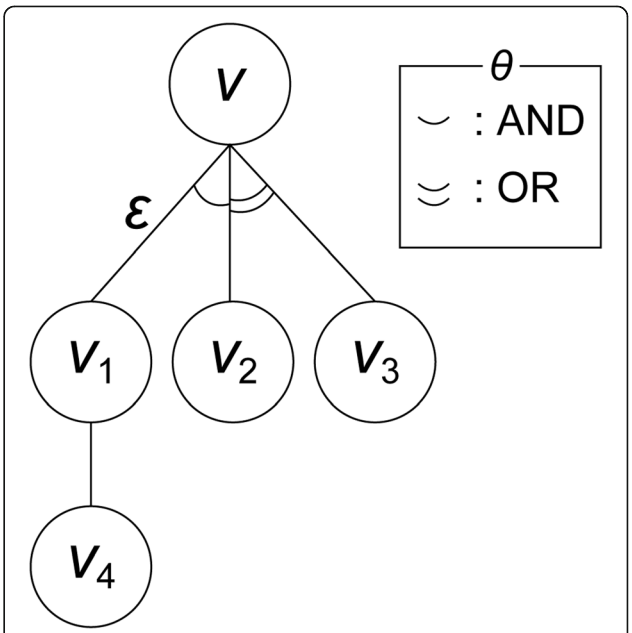

Fig. 5 Attack tree

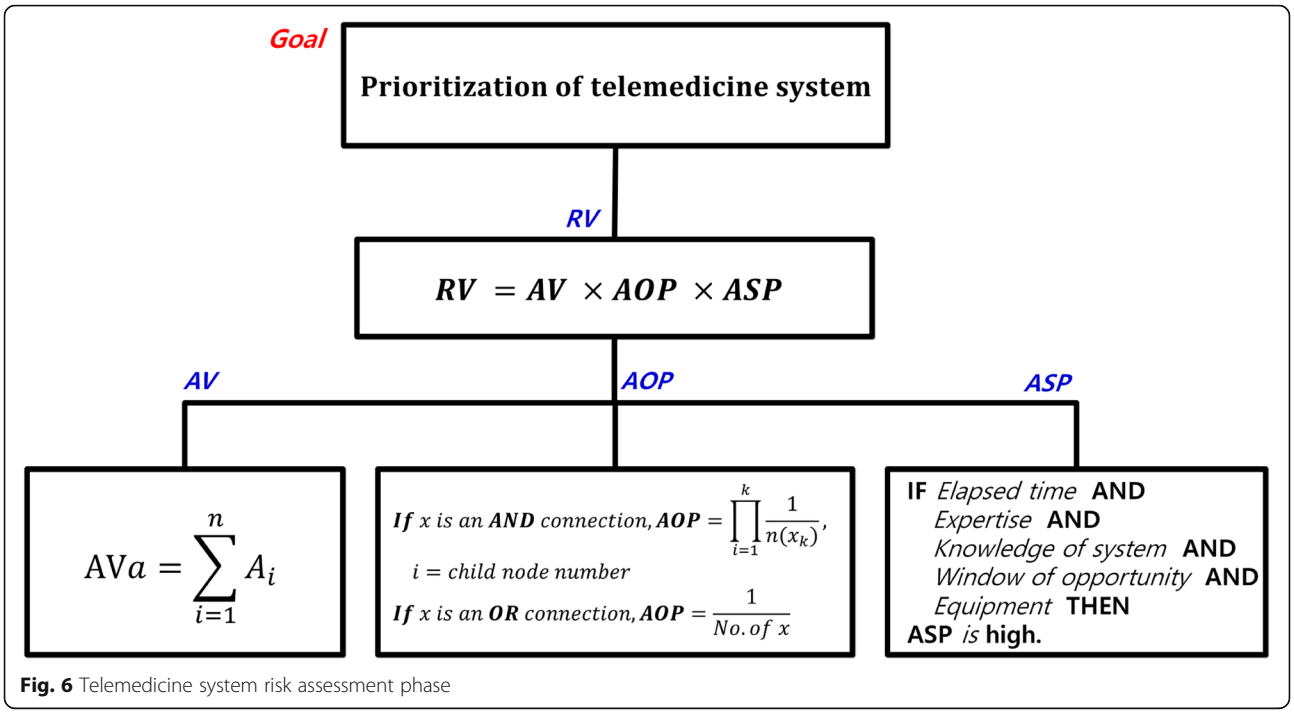

Fig. 6 Telemedicine system risk assessment phase

connected to the relevant agencies via the government network hub, stringent security guidelines are necessary to prevent infiltration of the government system. In special cases, telemedicine systems are also used for wireless communication between the exercise equipment used by patients and computers used for remote consultation in telemedicine clinics. In such environments, telemedicine systems can attract security threats associated with MITM attacks, malicious code, telemedicine app forgery/alteration, and illegal network access via physical security checks circumvention [28].

- Threat #7: Telemedicine service provider

Telemedicine systems primarily involve doctor-to-doctor (D2D) and doctor-to-patient (D2P) interactions. D2D telemedicine is characterized by the sharing and monitoring of health and medical information and requires higher-level cybersecurity because it involves remote consultation, including the writing of prescriptions. Figure 4 shows a block diagram of D2D and D2P interactions. In this environment, the telemedicine system can attract security threats associated with MITM attacks, malicious code, telemedicine app forgery/alteration, and illegal access of Korea-Net by circumventing the physical security checks present [28]. It can also be vulnerable to security threats associated with device use errors, prescription alterations, leakage of important data, and wiretapping (see Fig. 4).

The security threats likely to be encountered in each of the seven telemedicine service areas above were used as the basic data to calculate the AOP from the attack tree, which was constructed as described in Section III.

Methods

Overview

The first step in telemedicine risk assessment is to identify the assets involved and calculate their values. The attack tree is used to estimate all security threats likely faced by each asset, as identified in each of the seven telemedicine security threats areas. As illustrated in Fig. 5, the AOP is calculated using the OR and AND connectors, which are the gates for each node representing attack advancement towards the goal (see Fig. 5).

The main advantage of an attack tree is that it allows defenders to identify potential attacks and appropriate countermeasures. Furthermore, attack trees are originally "self-documented" to facilitate interpretation. The downsides of this approach are that it is difficult to enumerate all of the actions of the attackers and that the expressive power to model attacks that involve simultaneous actions is lacking. In this study, risk assessment methods including ASP and AOP variables were investigated to address these shortcomings [37] and allow more

Table 1 Asset value evaluation criteria [19, 44, 49–52]

Division	Low	Moderate	High
Confidentiality	1	2	3
Integrity	1	2	3
Availability	1	2	3
Asset contribution	1	2	3

Table 2 Categorization of asset values [19, 44, 49–52]

Security objective	Potential impact	Description
Confidentiality	High	Should be available internally to authorized persons only; unauthorized exposure can result in harm to individual privacy and/or fatal damage to telemedicine system
	Moderate	Can be disclosed internally but in case of external exposure may cause significant problems with respect to individual privacy and/or telemedicine system
	Low	If exposed to external persons, will have negligible effect on individual privacy and telemedicine system
Integrity	High	Accidental or intentional changes may result in extreme harm to individual privacy or telemedicine system
	Moderate	Accidental or intentional changes may cause significant damage to individual privacy or telemedicine system
	Low	Accidental or intentional changes will have negligible effect on individual privacy or telemedicine system
Availability	High	Service interruption may cause fatal damage to operation of telemedicine system
	Moderate	Service interruption may result in significant damage to telemedicine system
	Low	Service interruption will cause negligible damage to telemedicine system
Asset Contribution	High	Asset is essential to telemedicine system services
	Moderate	Asset is partially necessary for telemedicine system services
	Low	Asset plays a supporting role in telemedicine system services

accurate identification of attack methods involving attacker behavior.

In principle, the ASP of a potential attack increases in direct proportion to the motivation of the attacker and in inverse proportion to the effort required for mounting the attack. In this study, the asset value, AOP, and ASP were used as the parameters to assess the security risks associated with telemedicine.

Figure 6 presents an example of how risk assessment is conducted. The risk assessment procedure can be summarized as follows.

(1) Evaluate the AV of the telemedicine system (see Tables 1, 2, and 3).
(2) Estimate the AOPs of internal and external attacks on the telemedicine system (see Table 4).
(3) Estimate the internal and external ASPs of the telemedicine system (see Tables 5, 6, and 7).

Table 3 Definitions of grades for information classification [19, 44, 49–52]

Importance grade	Total score	Description
1	4–5	May cause damage to assets but has almost no influence on telemedicine system
2	6–7	If asset is damaged, has little effect on related domain or system
3	8–9	Asset damage results in significant loss to telemedicine business
4	10–11	Asset damage leads to very significant loss to telemedicine business
5	12	Asset damage leads to very high loss to telemedicine business, which may stop functioning

(4) Select a priority target for security application of the telemedicine system (see Tables 8 and 9).

The procedure enables the actual telemedicine system to identify both hardened targets and targets that require security.

Asset value

The U.S. National Institute of Standards and Technology (NIST) developed a risk management framework (RMF) to protect computer networks from cyberattacks [53]. The NIST-RMF guidelines categorize risk management activities into the following six security lifecycle steps: (1) categorize, (2) select (based on factors such as minimum security requirements and cost analysis), (3) implement (tailor to the given security environment), (4) assess (determine whether the operation is as intended), (5) authorize (determine whether the risk is acceptable), and (6) monitor (detect changes or signs of attack). Federal Information Processing Standards Publication 199 (FIPS PUB 199) defines the categorization criteria for information and information system security (based on the potential impact of the system) to provide a common framework for taxonomy. It sets three security objectives (confidentiality, integrity, and availability) and defines the levels of the potential effects of security

Table 4 AOP evaluation criteria [51, 52]

Division	Low	Moderate	High
	1	2	3
AOP	1–50%	51–80%	81–100%

Table 5 Ratings for various aspects of attack potential [51, 52]

Factor	Level	Value
Elapsed time	≤1 day	0
	≤1 week	1
	≤1 month	4
	≤3 months	10
	≤6 months	17
	> 6 months	19
	not practical	∞
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge of system	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Window of opportunity	Unnecessary/unlimited	0
	Easy	1
	Moderate	4
	Difficult	10
	None	∞
Equipment	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

breaches on individuals and organizations as low, moderate, and high [54].

When categorizing threats, the total asset value for each asset to be protected is calculated as follows:

$$\mathrm{AV}a(asset\ value) = \sum_{i=1}^{n} A_i\ , \tag{1}$$

where AV_a is the sum of the asset values (3–12) of asset a, calculated as the sum of the areas associated with the asset values (1–3: contributions of confidentiality, integrity, and availability). Table 1 lists the criteria for asset value evaluation. The asset values of each of the four evaluated items (security objectives) are rated on a three-point scale. The total asset value score is calculated by adding all of the individual scores, and the asset value grade is determined based on the calculated result.

Table 6 ASP ratings [51, 52]

Values	Attack potential required to identify and exploit attack scenario	ASP
0–9	Basic	5
10–13	Enhanced-basic	4
14–19	Moderate	3
20–24	High	2
≥25	Beyond high	1

The asset value is assessed in terms of each of the four security objectives (confidentiality, integrity, availability, and asset contribution) at three levels corresponding to the potential effects of each security objective, as described in Table 2, and varies between 3 and 12. By substituting the calculated value into Eq. (1), the asset-value-dependent importance grade, which ranges from 1 to 5, can be obtained.

Table 3 presents the definitions of each of the importance grades categorized above. The evaluated asset values are analyzed using mutatis mutandis, ISO/IEC 27005 [19], and ISO 31000 RM [50] and examined using mutatis mutandis, the risk assessment method based on confidentiality, integrity, and availability, as per NIST 800–37 RMF, FIPS PUB 199, and failure mode, effects, and criticality analysis [55].

AOP

The AOP is defined as the ratio of the number of attack events of all of the children to the number of attack nodes linked to the parent node in order to achieve the attack goal of the parent node. It is calculated as follows [53]. Let the child node ("X") be a leaf node; then, AOP = 1 (see Eqs. (2) and (3)).

$$If\ x\ is\ an\ AND\ connection, AOP = \prod_{i=1}^{k} \frac{1}{n(x_k)}, i = child\ node\ number \tag{2}$$

$$If\ x\ is\ an\ OR\ connection,\ \ AOP = \frac{1}{No.of\ x} \tag{3}$$

However, such an attack tree scenario has two major limitations. First, no weight is assigned to the nodes, even though every node has a different risk level and its potential threat can result in different degrees of damage. Second, in lieu of comparison of the node occurrence probabilities, only the probability for achieving the upper node goal is indicated without considering the node occurrence frequency and risk level of each node, making it difficult to quantify the security threat vulnerabilities of telemedicine devices. The AOP is calculated by designing an attack tree for each security threat scenario according to the seven telemedicine security threats areas, as illustrated in Fig. 7.

The AOP for the example in Fig. 7 can be calculated as follows. Because v_8 or v_9 can be selected to move to v_4, v_2 has an AOP of 1/2. Further, as one of the methods represented by v_4, v_5, v_6, and v_7 must be selected to achieve v_4, its AOP is 1/4. Because the single node v_3 is selected to achieve v_1, its AOP is 1. Consequently, if the

Table 7 Examples of ASP estimates [51, 52]

Attack	Elapsed time	Expertise	Knowledge of system	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Leakage of patient information from telemedicine device	0	6	7	4	4	21	High
Forgery via wiretapping and spoofing	0	3	0	4	4	11	Moderate
MITM attacks using rogue AP	0	6	3	10	4	23	High
Health information sniffing	0	0	0	4	4	8	Basic

attack target is the user, the AOP for patient information leakage is calculated to be 6.25%, as follows:

$$AOP = \frac{1}{2} \times \frac{1}{4} \times \frac{1}{2} = \frac{1}{16} \times 100. \quad (4)$$

Following attack tree construction for each of the seven telemedicine security threat areas, the AOP of each attack tree is calculated, and a score assigned to each area accordingly. An AOP assessment grade is allocated to each area based on a three-point scale, as per the AOP value calculated by Eq. (4) and in keeping with the evaluation criteria (Table 4).

Asp

The ASP, defined in ISO/IEC 15408 [51] and ISO/IEC 18045 [52], is assessed based on the following factors [52]:

- Time taken by an attacker to identify a vulnerability, develop an attack method, and mount the attack
- Specialist expertise required
- Knowledge of the system under investigation
- Window of opportunity to access the attack target
- IT hardware/software or other equipment required to identify and exploit a vulnerability

These factors affecting the ASP are not independent, but rather are interchangeable from various angles. For example, the expertise and equipment needed can be replaced by the elapsed time (see Table 5).

The ASP is calculated by applying the factor value (Table 5) as per the attack scenario for the seven telemedicine security threat areas. Subsequently, a rating is assigned based on the attack potential value (see Table 6), and categorization is performed based on the attack potential level (see Table 7). To calculate the ASP of each security threat, the categorized ASP levels are mapped onto the leaf nodes of the attack tree. For example, each leaf node in Fig. 7 is mapped at the ASP level assigned to it according to the ASP estimates (see Table 7).

Table 8 RV ratings [51, 52]

Values	Grade
1–12	Low
13–32	Normal
≥33	High

Risk

The telemedicine risk value (RV) is the product of the AV, AOP, and ASP:

$$RV = \mathrm{AV} \times \mathrm{AOP} \times \mathrm{ASP} \quad (5)$$

The calculated RVs are assessed at three levels: low, normal, and high (see Table 8).

When interpreting the risk assessment results, the higher the AV, AOP, and ASP, the higher the RV (see Fig. 8).

Results

The telemedicine risk analysis results represent the security threat risk levels and can be interpreted in terms of the relative effect of a given attack. It is necessary to establish the appropriate security guidelines based on the AV of each threat while considering its AOP and ASP (see Table 9).

In this study, the most popular modelling method, an attack tree, was applied to the telemedicine environment, and the security concerns for telemedicine systems were found to be very large. Risk management and evaluation methods suitable for the telemedicine environment were identified, and their benefits and potential limitations were assessed.

Discussion

In this study, data were collected via on-site verification and security vulnerability analysis (intrusion testing, threat modeling) of the telemedicine system shown in Table 7, and models were analyzed based on assumptions. Table 1 lists the three-point classification approach employed based on the RMF [19, 44, 49–52]; in addition, the importance of the telemedicine system can be evaluated by referring to Tables 2 and 3. The proposed model uses attack tree modeling to evaluate the ASP and AOP to estimate the total risks of remote healthcare systems, accounting for security threats. This report provides a method of evaluating cybersecurity risks in remote medical systems, an area of technological

Table 9 Examples of telemedicine risk assessment estimates

Asset		AV	Concern	AOP	ASP	RV	
Telemedicine device	RTOS/ GPOS/ gateway	5	Patient information leakage	1	2	10	L
		5	Weak password set	2	5	50	H
		5	Critical information transmitted owing to device operation errors	3	4	60	H
		5	Loss due to improper management of telemedicine device	2	5	50	H
		5	Access to internal system used by unapproved device	1	1	5	L
		5	Information leakage by device because of malware infection	1	1	5	L
		5	Saving important information in device	2	4	40	H
		5	Leakage of significant information from lost/stolen device	2	4	40	H
		5	Access to internal system and disclosure of important information owing to application vulnerabilities of device	2	4	40	H
		5	Device ↔ plaintext transmission between internal system	3	5	75	H
		5	Device ↔ plaintext transmission between telemedicine system	3	5	75	H
		5	Device ↔ MITM attacks between telemedicine system	3	1	15	M
		5	Gateway ↔ plaintext transmission between internal system	3	3	27	M
		5	Information leakage because of malware infection (vaccine or latest patch)	1	2	10	L
		5	Significant information disclosure by gateway hacking	2	1	10	L
		5	MITM attacks using rogue gateway	2	1	10	L
		5	Significant information leakage from lost/stolen gateway device	2	3	30	M
PC	PC	4	Forgery via wiretapping and spoofing	3	5	60	H
		4	Unauthorized access via MITM attacks	2	3	24	M
		4	Gateway ↔ plaintext transmission between telemedicine system	3	5	60	H
		4	MITM attacks using rogue AP	2	1	8	L
		4	Information leakage because of malware infection (vaccine or latest patch)	1	2	8	L
		4	Significant information disclosure owing to gateway hacking	1	1	4	L
		4	Internal access to national communication networks by bypassing physical security controls	1	1	4	L
		4	Internal access to national communication networks by exploiting wireless network vulnerability	1	1	4	L
		4	Leaving working seat for a long period after logging in	2	5	40	H
		4	Nonrepudiation failure by not saving accessed records	1	5	20	M
		4	Accident due to telemedicine system operation errors	1	5	20	M
S/W	Telemedicine software	4	Access to internal system and important information disclosure by exploiting vulnerabilities of application used for telemedicine treatment	1	1	4	L
		4	Access to internal system via update files for application used for telemedicine treatment	1	1	4	L
	Data transmission software	3	Access to internal system and important information disclosure by exploiting vulnerability of application used for data transmission	1	1	3	L
	Patient medical information software	3	Access to internal system via update files for software	2	1	6	L
	Monitoring software	2	Access to internal system via update files for software	2	1	4	L
	ECG software	5	Access to internal system via update files for telemedicine system	2	1	10	L
Information	Personal information	4	Sniffing	3	3	36	H
	Health information	4	Health information sniffing	3	3	36	H
	Medical information	5	Sending invalid prescriptions by changing medical information during telemedicine treatment	1	1	5	L
		5	Misuse of medical information by analyzing network packets during telemedicine treatment	2	1	10	L

Table 9 Examples of telemedicine risk assessment estimates *(Continued)*

Asset	AV	Concern	AOP	ASP	RV	
	5	Accidents caused by telemedicine system operation errors	2	5	50	H
	5	Forgery via network eavesdropping and spoofing during patient information exchange	2	3	30	H

convergence for recently illuminated untact (i.e., non-face-to-face) [56] medical services.

The limits of the proposed model are that the technical environment of the hospital should be considered when applying the model to the telemedicine system and the participation of telemedicine professionals is necessary. Another limitation is that biomedical engineers may not always be able to accept the outcome of security threat prioritization, and the weight of each criterion and/or the severity of the assigned security grade may have to be reassessed and reassigned. The analysis of security threats in a telemedicine environment requires the participation of information security experts with medical expertise and the cooperation of medical professionals. Such analyses can be performed using methods such as those employed to intelligently analyze forecasting data mining techniques. Intelligent analysis of prediction data mining techniques is widely used to support optimization of future decision-making in various fields, including healthcare and medical diagnoses. The methods used include Chi-squared Automatic Interaction Detection (CHAID), Exchange Chi-squared Automatic Interaction Detection (ECHAID), Random Forest Regression and Classification (RFRC), Multivariate Adaptive Regression Splines (MARS), and Boosted Tree Classifiers and Regression (BTCR) [57–64].

Nevertheless, this research will contribute significantly to the literature by facilitating the assessment and prioritization of cybersecurity risk factors lacking prior research in the telemedicine sector.

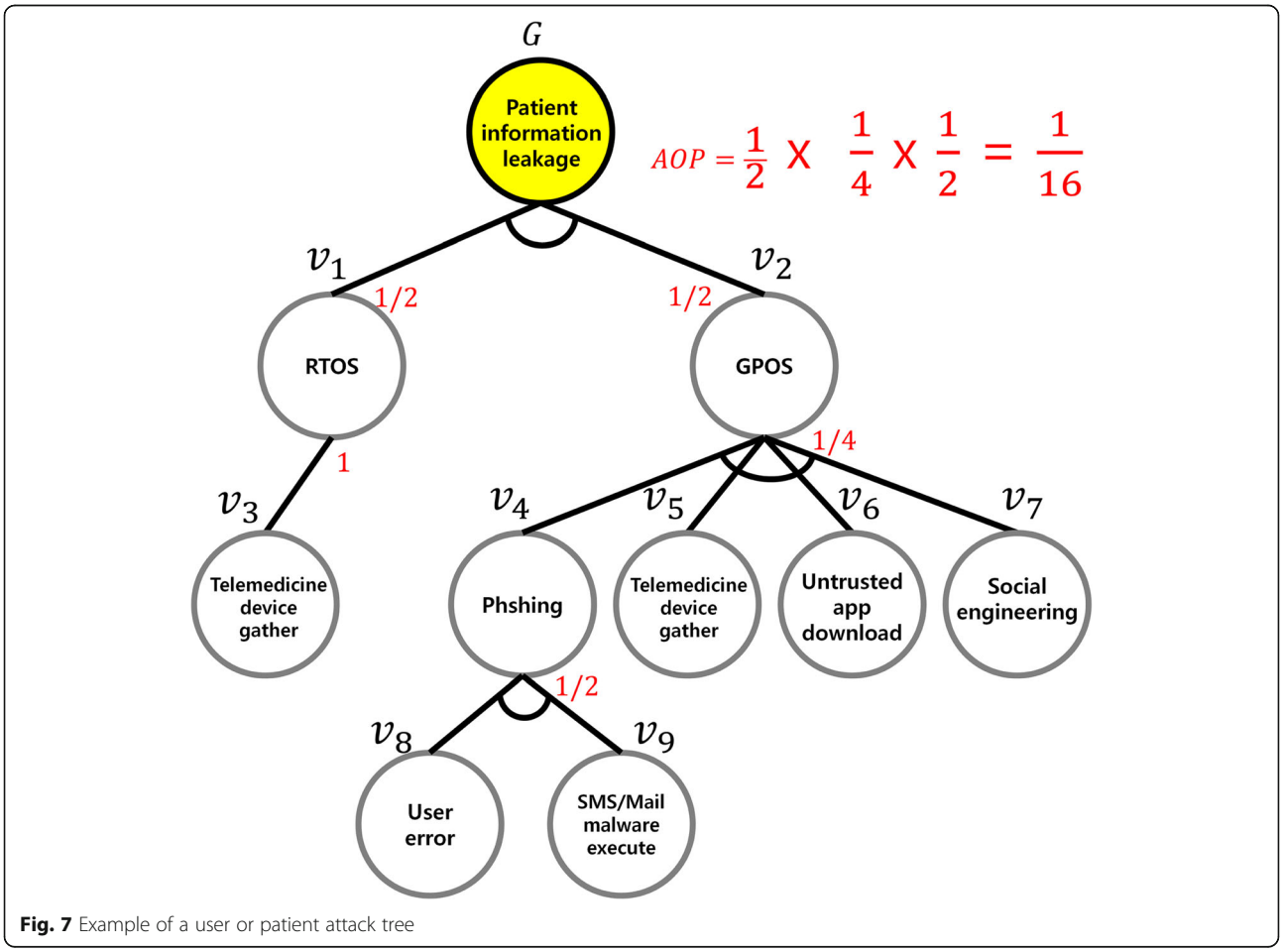

Fig. 7 Example of a user or patient attack tree

RV = AV × AOP × ASP						
AV	AOP	ASP				
		Beyond high	High	Moderate	Enhanced -basic	Basic
Grade 5	Low	5	10	15	20	25
	Moderate	10	20	30	40	50
	High	15	30	45	60	75
Grade 4	Low	4	8	12	16	20
	Moderate	8	16	24	32	40
	High	12	24	36	48	60
Grade 3	Low	3	6	9	12	15
	Moderate	6	12	18	24	30
	High	9	18	27	36	45
Grade 2	Low	2	4	6	8	10
	Moderate	4	8	12	16	20
	High	6	12	18	24	30
Grade 1	Low	1	2	3	4	5
	Moderate	2	4	6	8	10
	High	3	6	9	12	15

Fig. 8 Examples of RV estimates

In addition, at a time when the need for noncontact medical care is growing due to concerns about infectious diseases such as CoV, countermeasures against new security threats resulting from the convergence of ICT with the medical sector, such as through telemedicine and precision medicine, are essential.

Conclusions

The range of cybersecurity problems associated with telemedicine services necessitates the implementation of security guidelines for the maintenance and management of appropriate security measures that address the security threats posed to each of the seven areas of telemedicine services identified in this paper. The results of the security threat assessment and analysis performed in this study should serve as the basis for establishing efficient security guidelines in telemedicine environments. In the current healthcare service environment, wherein telemedicine services are provided by outsourced ICT personnel without medical security backgrounds, telemedicine is highly prone to cyberattacks.

There is a huge risk that life could be affected if a cyberattack modifies information that is normally prescribed for telemedicine services. Thus, telemedicine is a very important system that must be considered for safety as well as security. By presenting a systematic approach for security threat identification and vulnerability diagnosis, this study will further telemedicine usage while ensuring its safe and smooth operation.

In a follow-up study, the AOP values estimated in this study will be verified through mockup tests performed in real-life settings, and a process or security verification algorithm will be developed to counter the security threats faced based on prioritization of the security requirements determined from the risk assessment performed. Additionally, the concept of "precision medicine" has led to a personally customized medical era and the application of optimized diagnosis and treatment based on personal health information such as genetics and lifestyle information. Further research will be required to address the ever-increasing number of cybersecurity threats in the medical paradigm as ICT and medical technologies evolve.

This paper provides a method of attack tree modeling and analysis for cyber risk management. The basic elements of this modeling approach were reviewed, and the limitations of the approach were discussed. In future research, additional cyber risk modeling paradigms will be investigated, such as binary decision-making diagrams and Markov models, to identify the limitations of their representativeness and their abilities to quantify and mitigate risks. In addition, research on ways to identify

and mitigate new security threats to telemedicine will be needed, as the need for untact (i.e., non-face-to-face) [56] medical services increase due to issues related to infectious diseases such as CoV. Theoretical generalizations for these mathematical modeling techniques will then be developed to overcome these limitations.

Abbreviations

ICT: Information and communication technology; PACS: Picture Archiving Communications System; IMD: Implantable medical device; PC: Personal computer; RTOS: Real-time operating system; GPOS: General-purpose operating system; MITM: Man-in-the-middle; D2D: Doctor-to-doctor; D2P: Doctor-to-patient; ASP: Attack success probability; NIST: National Institute of Standards and Technology; RMF: Risk management framework; FIPS PUB 199: Federal Information Processing Standards Publication 199; AOP: Attack occurrence probability; RV: Risk value

Acknowledgements

This research was supported by a grant for the Korea Health Technology R&D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea (grant number: HI19C0811).

Authors' contributions

All authors contributed to the study conception and design. Material preparation, data collection, and analysis were performed by K. D.W., C. J.H., and H. K.H. The first draft of the manuscript was written by and all authors commented on subsequent revisions. All authors read and approved the final manuscript.

Funding

This research was supported by a grant for the Korea Health Technology R&D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea (grant number: HI19C0811).

Availability of data and materials

All data generated or analyzed during this study are included in this published article.

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no conflicts of interest.

Received: 13 February 2020 Accepted: 3 June 2020
Published online: 10 June 2020

References

1. Shaikh A, Memon M, Memon N, Misbahuddin M. The role of service oriented architecture in telemedicine healthcare system. In: International Conference on Complex, Intelligent and Software Intensive Systems. Fukuoka; 2009. p. 208–14. https://doi.org/10.1109/cisis.2009.181.
2. Naked security by SOPHOS. Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking. Available from: https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/. Accessed 5 Jan 2020.
3. Food and Drug Administration. Postmarket management of cybersecurity in medical devices. Silver Spring: Food and Drug Administration; 2016.
4. Paul N, Kohno T, Klonoff DC. A review of the security of insulin pump infusion systems. J Diabetes Sci Technol. 2011;5:1557–62. https://doi.org/10.1177/193229681100500632.
5. Ray I, Poolsapassit N. Using attack trees to identify malicious attacks from authorized insiders. In: di Vimercati SC, Syverson P, Gollmann D, editors. Computer security – ESORICS 2005. ESORICS 2005. Lecture notes in computer science, vol. 3679. Berlin: Springer; 2005. p. 231–46. https://doi.org/10.1007/11555827_14.
6. Abdo H, Kaouk M, Flaus JM, Masse F. A safety/security risk analysis approach of industrial control systems: a cyber bowtie–combining new version of attack tree with bowtie analysis. Comput Secur. 2018;72:175–95. https://doi.org/10.1016/j.cose.2017.09.004.
7. Maciel R, Araujo J, Melo C, Dantas J, Maciel P. Impact assessment of multi-threats in computer systems using attack tree modeling. In: 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Miyazaki; 2018. p. 2448–53. https://doi.org/10.1109/smc.2018.00420.
8. Myagmar S, Lee AJ, Yurcik W. Threat modeling as a basis for security requirements. Symp Requir Eng Inf Secur. 2005;1:1–8.
9. Ten CW, Manimaran G, Liu CC. Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Trans Syst Man Cybern Syst Hum. 2010;40:853–65. https://doi.org/10.1109/tsmca.2010.2048028.
10. Schneier B. Attack trees. Dr Dobbs J. 1999;24:21–9. https://doi.org/10.1002/9781119183631.ch21.
11. Maji A, Mukhoty A, Majumdar A, Mukhopadhyay J, Sural S, Paul S, et al. Security analysis and implementation of web-based telemedicine services with a four-tier architecture. In: Proceedings of the Second International Conference on Pervasive Computing Technologies for Healthcare. Tampere; 2008. p. 46–54. https://doi.org/10.4108/icst.pervasivehealth2008.2518.
12. She H, Lu Z, Jantsch A, Zheng LR, Zhou D. A network-based system architecture for remote medical applications. Asia-Pac Adv Netw. 2007;1:27–31.
13. Park CY. Trend of u-healthcare standardization technology. Electron Telecommun Trends. 2012;25:48–59. https://doi.org/10.22648/ETRI.2010.J.250406.
14. Wu Z, McGoogan JM. Characteristics of and important lessons from the coronavirus disease 2019 (COVID-19) outbreak in China: summary of a report of 72 314 cases from the Chinese Center for Disease Control and Prevention. JAMA. 2020;323:1239–42. https://doi.org/10.1001/jama.2020.2648.
15. Hollander JE, Carr BG. Virtually perfect? Telemedicine for Covid-19. N Engl J Med. 2020. https://doi.org/10.1056/NEJMp2003539.
16. World Health Organization. Cumulative Number of Reported Probable Cases of Severe Acute Respiratory Syndrome (SARS). 2003. https://www.who.int/csr/sars/country/2003_05_20/en/. Accessed 5 Jan 2020.
17. Groot RJ, Baker SC, Baric RS. Middle East respiratory syndrome coronavirus (MERS-CoV): announcement of the coronavirus study group. J Virol. 2013;87:7790–2. https://doi.org/10.1128/JVI.01244-13.
18. Oh AS. A study on home healthcare convergence for IEEE 11073 standard. J Korea Inst Inf Commun Eng. 2015;19:422–7. https://doi.org/10.6109/jkiice.2015.19.2.422.
19. International Organization for Standardization. Information security risk management. (second edition). ISO/IEC 27005:2011; 2011. https://doi.org/10.3403/30125022u.
20. Zetter K. Hospital networks are leaking data, leaving critical devices vulnerable. 2014. Available from: https://www.wired.com/2014/06/hospital-networks-leaking-data/. Accessed 4 Jan 2020.
21. Kim TY, Youm S, Jung JJ, Kim EJ. Multi-hop WBAN construction for healthcare IoT systems. In: 2015 International Conference on Platform Technology and Service. Jeju; 2015. p. 27–8. https://doi.org/10.1109/platcon.2015.20.
22. Jeong YS. An efficient IoT healthcare service management model of location tracking sensor. J Digit Converg. 2016;14:261–7. https://doi.org/10.14400/jdc.2016.14.3.261.
23. Zhang B, Wang XW, Huang M. A data replica placement scheme for cloud storage under healthcare IoT environment. In: 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). Xiamen; 2014. p. 542–7. https://doi.org/10.1109/fskd.2014.6980892.
24. Wehde M. Healthcare 4.0. IEEE Eng Manag Rev. 2019;47:24–8. https://doi.org/10.1109/EMR.2019.2930702.
25. Mohamed N, Al-Jaroodi J. The impact of Industry 4.0 on healthcare system engineering. In: Proceedings of the 2019 IEEE Int Syst Conf; 2019. p. 1–7. https://doi.org/10.1109/SYSCON.2019.8836715.
26. Alloghani M, Al-Jumeily D, Hussain A, Aljaaf AJ, Mustafina J, Petrov E. Healthcare services innovations based on the state of the art technology trend Industry 4.0. In: 2018 11th Int Conf developments in n eSystems engineering (DeSE), vol. 2018. Cambridge. p. 64–70. https://doi.org/10.1109/DeSE.2018.00016.

27. Hansen JA, Hansen NM. A taxonomy of vulnerabilities in implantable medical devices. In: Proceedings of the second annual workshop on security and privacy in medical and home-care systems. Chicago: ACM; 2010. p. 13–20. https://doi.org/10.1145/1866914.1866917.
28. Camara C, Peris-Lopez P, Tapiador JE. Security and privacy issues in implantable medical devices: a comprehensive survey. J Biomed Inf. 2015; 55:272–89. https://doi.org/10.1016/j.jbi.2015.04.007.
29. US Food and Drug Administration. Medical device safety. 2017. https://www.fda.gov/medical-devices/medical-device-safety. Accessed 3 Oct 2019.
30. HIPPA. Security standards: Technical safeguards, vol. 2; 2007. p. 1–17.
31. Shivshankar S, Summerhayes K. The challenges of conducting medical device studies. Boston: Institute of Clinical Research; 2007. ISBN-10: 0954934555.
32. Fu K. Inside risks: reducing risks of implantable medical devices. Commun ACM. 2009;52:25–7. https://doi.org/10.1145/1516046.1516055.
33. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, et al. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In: Proceedings of the 29th Annual IEEE Symposium on Security and Privacy. Oakland; 2008. p. 129–42. https://doi.org/10.1109/sp.2008.31.
34. Li C, Raghunathan A, Jha NK. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: 13th IEEE International Conference on e-Health Networking Applications and Services. Columbia; 2011. p. 150–6. https://doi.org/10.1109/health.2011.6026732.
35. Medtronic. Implantable pacemaker and defibrillator information. 2015. https://medlineplus.gov/pacemakersandimplantabledefibrillators.html Accessed 12 Dec 2019.
36. Nagaraju V, Fiondella L, Wandji T. A survey of fault and attack tree modeling and analysis for cyber risk management. In: 2017 IEEE International Symposium on Technologies for Homeland Security (HST). Waltham; 2017. p. 1–6. https://doi.org/10.1109/ths.2017.7943455.
37. Ekstedt M, Sommestad T. Enterprise architecture models for cyber security analysis, Power Systems Conference and Exposition. In, Seattle; 2009. p. 1–6. https://doi.org/10.1109/psce.2009.4840267.
38. Kravitz H, Driessen G, Gomberg R, Korach A. Accidental falls from elevated surfaces in infants from birth to one year of age. Pediatrics. 1969;44(5):869–76.
39. Roth M, Liggesmeyer P. Modeling and analysis of safety-critical cyber physical systems using state/event fault trees. Toulouse: International Conference on Computer Safety, Reliability and Security; 2013.
40. Bernstein S. Sur l'extension du théoréme limite du calcul des probabilités aux sommes de quantités dépendantes [On the extension of the limit theorem of calculating probabilities to sums of dependent quantities]. Math Ann. 1927;97:1–59. https://doi.org/10.1007/BF01447859.
41. Lee C. Representation of switching circuits by binary-decision programs. Bell Syst Tech J. 1959;38:985–99. https://doi.org/10.1002/j.1538-7305.1959.tb01585.x.
42. Watson H. Bell telephone laboratories launch control safety study. In: bell telephone laboratories. Nature: Murray Hill; 1961. https://doi.org/10.1038/183220d0.
43. Vesely W, Goldberg F, Roberts N, Haasl D. Fault Tree Handbook. Washington: Systems and Reliability Research, Office of Nuclear Regulatory Research; 1981.
44. International Organization for Standardization. Health informatics - Information security management in health using ISO/IEC 27002. ISO/DIS 27799:2014(E); 2015. https://doi.org/10.3403/30304351.
45. Arney D, Venkatasubramanian KK, Sokolsky O, Lee I. Biomedical devices and systems security. In: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. Boston; 2011. p. 2376–9. https://doi.org/10.1109/IEMBS.2011.6090663.
46. Industry Canada. Medical devices operating in the 401–406 MHz frequency band. 2010. http://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/rss243.pdf/$FILE/rss243.pdf Accessed 23 Nov 2019.
47. Denning T, Borning A, Friedman B, Gill BT, Kohno T, Maisel WH. Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Atlanta; 2010. p. 917–26. https://doi.org/10.1145/1753326.1753462.
48. Bao SD, Poon CCY, Yuan-Ting Z, Shen LF. Using the timing information of heartbeats as an entity identifier to secure body sensor network. IEEE Trans Inf Technol Biomed. 2008;12:772–9. https://doi.org/10.1109/titb.2008.926434.
49. Partala J, Keräneny N, Särestöniemi M, Hämäläinen M, Iinatti J, Jämsä T, Reponen J, Seppänen T. Security threats against the transmission chain of a medical health monitoring system. In: IEEE 15th International Conference on e-Health Networking, Applications and Services. Lisbon; 2013. p. 243–8. https://doi.org/10.1109/healthcom.2013.6720675.
50. International Organization for Standardization. Risk management. ISO 31000: 2018; 2018. https://doi.org/10.3403/30246105u.
51. International Organization for Standardization. Information technology – Security techniques – Evaluation criteria for IT security Part 1: Introduction and general model. ISO/IEC 15408–1:2009; 2009. https://doi.org/10.3403/bsisoiec15408.
52. International Organization for Standardization. Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045. ISO/IEC 18045; 2015. https://doi.org/10.3403/30325408.
53. Joint Task Force Transformation Initiative. Guide for applying the risk management framework to federal information systems: A security life cycle approach. NIST SP800–37 Rev. 1; 2010. https://doi.org/10.6028/nist.sp.800-37r1.
54. Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J, Gulick J. Guide for mapping types of information and information systems to security categories. NIST SP800–64 Rev. 4; 2008.
55. FMECA. Failure mode, effects and criticality analysis. FMECA MIL-P-1629; 2007. https://doi.org/10.1002/9781118312575.ch12.
56. Lee SM, Lee D. "Untact": a new customer service strategy in the digital age. Serv Bus. 2020;14:1–22. https://doi.org/10.1007/s11628-019-00408-2.
57. Al-Janabi S, Alkaim AF. A nifty collaborative analysis to predicting a novel tool (DRFLLS) for missing values estimation. Soft Comput. 2020;24:555–69. https://doi.org/10.1007/s00500-019-03972-x.
58. Al-Janabi S, Mahdi M. Evaluation prediction techniques to achievement an optimal biomedical analysis. Int J Grid Utility Comput. 2019;10:512–27. https://doi.org/10.1504/IJGUC.2019.102021.
59. Al-Janabi S, Mohammad M, Al-Sultan A. A new method for prediction of air pollution based on intelligent computation. Soft Comput. 2019. https://doi.org/10.1007/s00500-019-04495-1.
60. Patel A, Al-Janabi S, AlShourbaji I, Pedersen J. A novel methodology towards a trusted environment in mashup web applications. Comput Secur. 2014;49: 107–22. https://doi.org/10.1016/j.cose.2014.10.009.
61. Al-Janabi S, AlShourbaji I. A study of cyber security awareness in educational environment in the Middle East. J Inf Knowl Manag. 2016;15:1650007. https://doi.org/10.1142/S0219649216500076.
62. Al-Janabi S, Rawat S, Patel A, AlShourbaji I. Design and evaluation of a hybrid system for detection and prediction of faults in electrical transformers. Int J Electr Power Energy Syst. 2015;67. https://doi.org/10.1016/j.ijepes.2014.12.005.
63. Kalajdzic K, Al-Janabi S, Patel A. Rapid lossless compression of short text messages. Comput Standards Interfaces. 2014. https://doi.org/10.1016/j.csi.2014.05.005.
64. Mahdi M, Al-Janabi S. A novel software to improve healthcare base on predictive analytics and mobile services for cloud data centers. In: International conference on big data and networks technologies. Cham: Springer; 2019. p. 320–39. https://doi.org/10.1007/978-3-030-23672-4_23.

Publisher's Note