Hindawi
Security and Communication Networks
Volume 2019, Article ID 8715264, 14 pages
https://doi.org/10.1155/2019/8715264

Research Article

Usability Evaluation Model for Biometric System considering Privacy Concern Based on MCDM Model

Junhyoung Oh,[1] **Ukjin Lee**,[2] **and Kyungho Lee**[1]

[1] *Institute of Cyber Security & Privacy, Korea University, Seoul 02841, Republic of Korea*
[2] *Department of Psychology, Korea University, Seoul 136-713, Republic of Korea*

Correspondence should be addressed to Kyungho Lee; kevinlee@korea.ac.kr

Received 27 December 2018; Accepted 3 March 2019; Published 27 March 2019

Academic Editor: Emanuele Maiorana

Biometric devices play an integral role in consumer's daily life, providing a seamless environment. However, it is essential to measure the usability of biometrics, owing to the elements of biometrics satisfying both usability and security. This study redefines the elements of biometrics pertaining to usability determined in previous studies and adds elements of psychological relevance, such as privacy concerns. To organize the interrelated usability structure systemically, this paper applies the DEcision MAking Trial and Evaluation Laboratory (DEMATEL) to derive the usability structure. Thereupon, the established structure is applied in the clustered weighted Analytical Network Processes (ANP) to generate the proposed usability evaluation model. By these methods, the pertinent relationships between the factors are clarified and the weight of each element is determined. In the empirical study, 106 students measured usability of the fingerprint recognition system, iris recognition system, and facial recognition system employing our usability evaluation model. The results of this model generate the quantitative score of usability for biometric systems and suggest strategies to increase the score. The proposed usability evaluation model can comprehensively assist usability practitioners to evaluate biometric systems.

1. Introduction

Biometric system, an identification system based on people's physiological or behavioural attributes (e.g., iris, fingerprint, voice), has been attracting avid interest due to its accuracy, agility, and ease of use with identification and authentication functions [1]. Biometric devices play a significant role in easing consumer's daily life by providing effective security systems in essentials such as mobile phone, home security, cars, and mobile payment system [2]. Additionally, the use of biometrics is accelerating as the Internet of Things (IoT) becomes pervasive, since IoT devices are better suited for biometric authentication than for passwords, owing to the absence of an input tool.

The trade-off relationship where security improvements result in reduced usability is a shortcoming of the password-based authentication system. Therefore, it has been studied and developed focusing on security rather than usability. However, as biometric systems are enhanced, the requirements of security and usability can both be satisfied, expediting the need to measure usability. In general, the fundamental element in measuring usability of a system is its technical effectiveness or efficiency [3]. Nowadays, biometric authentication systems are highly accurate and easy to use [3], resulting in superior usability in terms of the technical aspects of the system.

Biometric systems are distinct from traditional password-based systems by their use of the user's behavioural and physiological elements as biometric keys [4]. Unlike traditional security systems, which typically have physical keys, users require direct interaction with sensors in the biometric device [4]. A representative example of biometric device is wearable devices in Smart Healthcare. The wearable device attaches to the user's body, thereby measuring and storing information of the user's activity and ultimately providing a customized service to the user. Since such biometric systems interact directly with the user's body, in addition to the usability testing methods of existing equipment they must also be evaluated for ergonomics. That is, biometric systems need to be ergonomically suitable for the user. Therefore, it is necessary to include ergonomics of the biometric systems as an element when developing the usability evaluation model.

Internet of Things (IoT) is the core technology of the hyperconnected society that relies on the Internet network to provide customized services by enabling mutual communication between objects as well as between people and objects. Since the introduction of the concept of Internet of Things by Ashton in 1999, experts have been ardently developing the core technology for application and realization, resulting in its rapid development [5]. Most of the academic researches related to the Internet of Things were predominantly focused on the technical aspects. However, with the popularization of technology, the need to discuss user experiences that focus on user psychology is imperative [6]. Users are required to provide a variety of personal biometric information to use the service. However, individual biometric keys cannot be changed repeatedly. On the other hand, user's biometric data could be easily compromised via their own self-disclosing behaviour (e.g., Selfies uploaded on Facebook disclose their iris information). Hence, biometric systems have a crucial vulnerability with regard to security while having a significant impact on privacy, since biometric information cannot be readily "reset" when compromised by a third party [7]. Not surprisingly, the biometric systems in mobile phones (e.g., iPhone 5s, Galaxy s8) such as fingerprint authentication and iris recognition were tricked by German hackers [8, 9]. Consequently, living in the time heavily embedded with biometric systems, the users face greater security risks than in the days when the traditional authentication methods were used, as determined by previous studies [2, 10, 11]. Therefore, it is necessary to include the psychological aspect of the usability evaluation model of the biometric authentication system.

In earlier studies on usability, the view of usability as a multidimensional structure and the view as a single-dimensional construct coexist in HCI (Human-Computer Interaction) field [10]. However, there have been few attempts to empirically investigate the construct itself or to systematically identify and organize the nature of the interrelations between factors [10, 12]. At the same time, when studying usability as a single dimension, researchers have to address the challenge of handling the usability indicators, both the technical and psychological measures: efficiency, effectiveness versus user satisfaction, in a single dimension [10]. In subsequent studies, a relatively low correlation was found between the technical and psychological components of usability [12, 13], indicating minor interdependencies result in an unreliable usability score [14]. Hence, it is important to divide the two technical and psychological factors into different dimensions to solve the abovementioned problems.

The ultimate evaluation of biometric systems should be user-driven, and the user's perceived usability for biometric devices should be evaluated. ISO/IEC 19795 measured the performance of a biometric system by calculating the Equal Error Rate based on the scenario [15]. However, if usability is primarily evaluated for performance such as error rate or execution time during use of the device, then it is not possible to adequately explain the user's perceived usability of the device. Therefore, we suggest a study of the technical aspects, ergonomic aspects, and psychological aspects to measure the user's perception of the usability of biometrics. The technical aspect consists of the effectiveness and efficiency that have been studied extensively. Ergonomic aspects consider physical and cognitive characteristics such as anthropometry-fit, accessibility, and affordance. Psychological aspect is related to the psychological part of the consumer and is made up of privacy concerns and satisfaction. While each factor for evaluating usability of a biometric system is essential, the existing methodology is inadequate to select a specific evaluation attribute as singularly suited to evaluate a biometric system. Therefore, it is necessary to systematically study the methods of selecting evaluation factors.

The purpose of this paper is to propose a new model for evaluating usability of biometric systems and compare the same with three widely used biometric modalities. To evaluate the various elements of usability systematically, we used the Multiple-Criteria Decision Making (MCDM) model, which is a combination of the DEcision MAking Trial and Evaluation Laboratory (DEMATEL) and the Analytic Network Process (ANP). The DEMATEL method is an effective way to show causality of the various interrelated factors and creates an Impact Relationship Map (IRM). The Analytic Network Process was developed in 1996 and since it analyzes the causality between indicators, it generates superior results from strategic decision making [21]. It is also proficient at deriving relative weights. MCDM model combining DEMATEL and ANP is effective in obtaining interrelation and relative weight of various factors of usability. Hence with this model, relative weights based on correlation can be obtained. We derive the relative weights and combine the scores of those obtained through the empirical study with the SAW (Simple Additive Weighting) method. SAW method is the simplest method available in decision making, where each element is weighted and added. Using these scores, we compare various biometric modalities of the smartphones and illustrate the effectiveness of the developed model.

The rest of this paper is organized in the following order. In Section 2, the concept of usability and description of each subcriterion of this model are introduced. Section 3 describes the computational process. MCDM model using DEMATEL and ANP is described. DEMATEL is utilized to probe interrelations between usability components, and ANP is utilized to derive the relative weight of each. Section 4 details the implementation of the proposed model in an empirical study. The study conducts a questionnaire survey assessing the biometric recognition system of Samsung Galaxy S8, one of the most popular cell phones, to verify the validity of the influence relations. At the end of Section 4, we discuss the results from the study and how to use each subcriterion for evaluation. Section 5 provides the conclusions of the paper.

2. Background and Related Works

2.1. Usability for Biometrics. Usability is the attribute that makes a product easy to understand, easy to learn, easy to use, and attractive to users [22, 23]. The term usability has various definitions, sometimes defined as "how usable is something" [4]. In the HCI field, for a long time, researchers

Table 1: Subcriterion covered in major prior works.

Major Prior works	Effectiveness	Efficiency	Anthropometry-fit	Accessibility	Affordance	Privacy Concern	Satisfaction
ISO 9241-11 [3]	✔	✔					✔
Toledanos et al. [16]	✔	✔					✔
Theofanos et al. [17]	✔	✔					✔
ISO/IEC 25062 [18]	✔	✔					✔
Theofanos et al. [19]	✔	✔		✔	✔		✔
ISO 9241-210 [20]	✔	✔	✔	✔			✔
Kukula et al. [4]	✔	✔	✔	✔			✔

have been investigating which factors increase usability [24]. Since Shackel attempted to define usability systematically [25], many HCI researchers shifted their focus to studying usability factors, such as learnability, ease of use, memorability, efficiency, and user satisfaction. Prior studies considered various factors when evaluating usability. Table 1 shows the factors considered in the main studies among the factors covered in this paper. The International Organization for Standardization classifies usability into three components: effectiveness with regard to suitability for a particular purpose, efficiency, which means the time or process required for the task, and user satisfaction [3]. ISO has primarily defined usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" [3]. Recently, usability has been further defined as "easy and effective to use, and enjoyable from the user's perspective" [26]. Based on its varied definitions, it is evident that usability is not just "look and feel" of biometric systems [10].

One of the main purposes of measuring usability is to provide a method to evaluate the user experience for the interaction designer [26]. While several studies attempted to evaluate the usability of biometric systems, most studies used the concept of usability as defined by ISO 9241-11. According to ISO 9241-11, usability comprises three factors: effectiveness, efficiency, and satisfaction. Theofanos et al. [19] argue that the user is a key component of the biometric system and evaluate usability based on this concept. Lewis et al. [27] proposed the usability evaluation by dividing the components into usable elements and learnable elements. NIST also used the same concept when exploring the usability of biometric systems [17, 28].

Currently, the most important factor in usability evaluation is "performance of function" or "ease of operation". While this is an appropriate usability evaluation when simply evaluating the performance or function of a given product, it is not suitable when evaluating a user's psychological experience with it. For example, following are some standards related to usability evaluation of biometrics. ISO 9241-11 is a basic standard covering general principles and techniques for measuring the usefulness of a product. It defines usability and suggests ways that the product can be specified and evaluated [3]. ISO 9241-210 covers human-centric design for interactive systems while also focusing on the user experience [20]. ISO/IEC 25062 constructs experimental groups and evaluates efficiency, effectiveness, and subjective satisfaction to obtain statistically significant totals. ISO/IEC 25062 features a standardized reporting format for usability. Though this standard is currently used worldwide, it does not address privacy concerns [18].

The Human-Biometric-Sensor Interaction Evaluation Method was proposed to assess usability, ergonomics, and biometric system performance when applied to usability evaluation for biometric systems [4]. However, the HBSI model does not consider the psychological factors. As mentioned, this paper suggests the concept of usability evaluation that considers the technical aspects, ergonomic aspects, and psychological aspects.

Additionally, in the case of biometric systems that incorporate IoT technology, it is difficult to assess the emotional usability just by operating time or error rate, since the quality of the device and service have an impact on the fun, emotion, and experience during use rather than just the performance of the device. Based on recent trends that emphasize user emotional wellness, it is essential to evaluate how users perceive usability of the device by self-reporting methods like surveys.

Currently, most usability evaluations of biometric systems are performed to measure quantitative performance such as time and accuracy. Hence, it is necessary to transform the conventional usability evaluation standard, into a design that emphasizes the real user experience. Details are given in the following subsection.

2.2. Factor Description. We measure the usability of biometrics by evaluating the technical aspects through effectiveness and efficiency, the ergonomic aspects through anthropometry-fit, accessibility, and affordability, and the psychological aspects through handling of privacy concerns and overall satisfaction. A summary of each subcriterion is depicted in Table 2.

2.2.1. Technical Aspects

(i) Effectiveness. It refers to how good a product is at doing what it is supposed to do [26]. According to ISO 9241-11, effectiveness is also defined as "the accuracy and completeness with which users have achieved specified goals". It is measured by how accurately and perfectly the user performs a specific task [29]. Observation of the biometric systems while in use is the method of evaluating effectiveness [19]. Metrics for evaluation of a biometric application may include

Table 2: Explanation of criteria.

Criteria & evaluation criteria	Descriptions
Technical aspect	
T1: Effectiveness	The perceived accuracy and completeness with which users have achieved specified goals
T2: Efficiency	The perceived mental or physical resources expended in relation to the accuracy and completeness with which users achieve goals
Ergonomic aspect	
E1: Anthropometry-fit	The perceived degree of considering inherent characteristics for better fitness between device and targeted users
E2: Accessibility	The perceived attribute which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use
E3: Affordance	The perceived attribute of an object that allows people to know how to use it
Psychological aspect	
P1: privacy concern	The perceived threat of the consequences about problems and how this affects their behaviour
P2: Satisfaction	The perceived degree to which the product meets the users' overall expectations, a subjective response of enjoyment, comfort, or frustration

quality, errors, and accuracy, or self-reporting method via surveys [19, 30–32]. For example, effectiveness of fingerprint recognition can be measured by the effect an angle has on the quality of the captured image, or survey items such as SUS questionnaires [31].

(ii) Efficiency. It refers to the way a product supports users mentally and physically in carrying out their tasks [26]. According to ISO 9241-11, it is defined as "the resources expended in relation to the accuracy and completeness with which users achieve goals". Efficiency is measured by the resources spent for achieving a particular goal [29]. Metrics may include task time or throughput, or self-reporting method [3, 31, 32]. For example, efficiency of fingerprint authentication can be measured by the effect an angle has on the time required to capture fingerprint images, or survey items such as SUS. Efficient systems lead users to perceive them favourably for completing a specific task or procedure to reach a particular goal within an acceptable amount of time, with reasonable effort, cognitive load, and mental resources.

2.2.2. Ergonomic Aspects

(i) Anthropometry-Fit. It refers to the degree to which inherent characteristics are analysed for better fitness between device and targeted users [17, 33]. While these measures are effective in minimizing errors and maximizing quality for the biometric data presented to the system, the physical presentation of that biometric data by the subject to the system involves many anthropometric factors that have been largely ignored [17]. Recently, the study of usability issues when interacting with biometric systems, including ergonomics, is garnering more attention [4].

(ii) Accessibility. It is defined as the degree to which a product or system can be used by people with the widest range of characteristics and capabilities, to achieve a specified goal in a specified context of use [26, 34]. Usability practitioners evaluate accessibility by questioning how the technology might be adapted for the use of people with disabilities [35]. Usability is dependent on the level of accessibility factors, such as culture (e.g., face modality would not be a good choice at places where most of the females use veils for religious convictions) and environment (e.g., iris modality may be more suitable for workers in dark coal mines) [2]. Besides, accessibility impacts the functioning of biometric systems in the following situations: poor vision; mental problems; temporal disability such as sprained ankle or pregnancy [4].

(iii) Affordance. It refers to the attribute of an object that allows people to know how to use it [26]. In simpler terms, to afford means "to give a clue" [26]. When the affordances of a physical object are perceptually obvious, it is easy to know how to interact with it [26]. For instance, to scan fingerprints, the shape and configuration of the scanner should convey where the users place their fingers and when the prints have been captured [19]. A fingerprint scanner that requires lengthy instructions has poor affordance [19]. If iris recognition system has poor affordance, it would be difficult and time-consuming for the user to deal with the device [26].

2.2.3. Psychological Aspect

(i) Privacy Concerns. It can be defined as the fear of difficulty and behaviour that changes due to this fear [26]. It is measured by an individual's awareness or perceived seriousness regarding the risks taken by using the biometric systems. It is closely related to the protection motivation theory, which could influence an individual's intention and behaviour [36]. As mentioned earlier, the usage of biometric systems is significantly dependent on user's privacy concerns than on any other security mechanism [2, 10, 11]. Studies on privacy

issues [11, 37] demonstrate that the benefits of biometrics are not always evident to users primarily due to the possibilities of misuse and invasion of privacy is a complicated problem that is not adequately understood [38]. Sometimes users find biometric systems intrusive or personally invasive.

(ii) Satisfaction. According to ISO 9241-11, it is defined as "freedom from discomfort, and positive attitude to the use of the product". It refers to the extent of how people feel about a product and their pleasure and satisfaction while using the product [26]. It includes their overall impression of how good it is to use [26]. Satisfaction is also measured by the extent to which the product meets the users' expectations, a subjective response of comfort or frustration [19, 29]. A user satisfaction questionnaire is primarily used to find out how users actually feel about using the product after interacting with it [26]. For a system to be satisfactory, both the practitioners and the users must be content with the system [39]. This is determined by the willingness of both vendors and users to rely on and reuse the system [39]. It is important to be aware that the satisfaction is notably affected by the vendors' and the users' mood.

3. Computational Process

In the real world, criteria cannot be defined independently. The DEMATEL has been used for decades to measure the relationships between potential elements that make up the criteria, since various factors play a role in evaluating diverse topics in the real world. In recent years, the DEMATEL combined with ANP has been used for the evaluation for MCDM (Multiple-Criteria Decision Making) problems. Zhou et al. [40] used DEMATEL to calculate the influence of relationships and develop a model for assessing the job satisfaction. Jeng et al. [41] applied DEMATEL to examine the behavioural intention of medical professionals to develop a new Clinical Decision Support System. Hsu et al. [42] explored the factors influencing the quality of blog interfaces from the perspective of the followers with DEMATEL. Zoie et al. [43] adopted DEMATEL to analyze the cloud users' requirements.

Using ANP can improve the accuracy of the model where the magnitude of importance is unclear. However, in ANP the importance of each cluster is the same. Therefore, we solve this problem by assigning weights to each cluster using the DEMATEL. The combination of DEMATEL and ANP is classified into four major categories [44].

(i) Network Relationship Map of ANP. As the most similar approach to general ANP, DEMATEL is used to grasp the overall structure, inner dependency, and outer dependency, and the weights are obtained by ANP.

(ii) Inner Dependency in ANP. The inner dependency is determined by using the DEMATEL, and the overall structure is determined based on the DEMATEL or the expert evaluation.

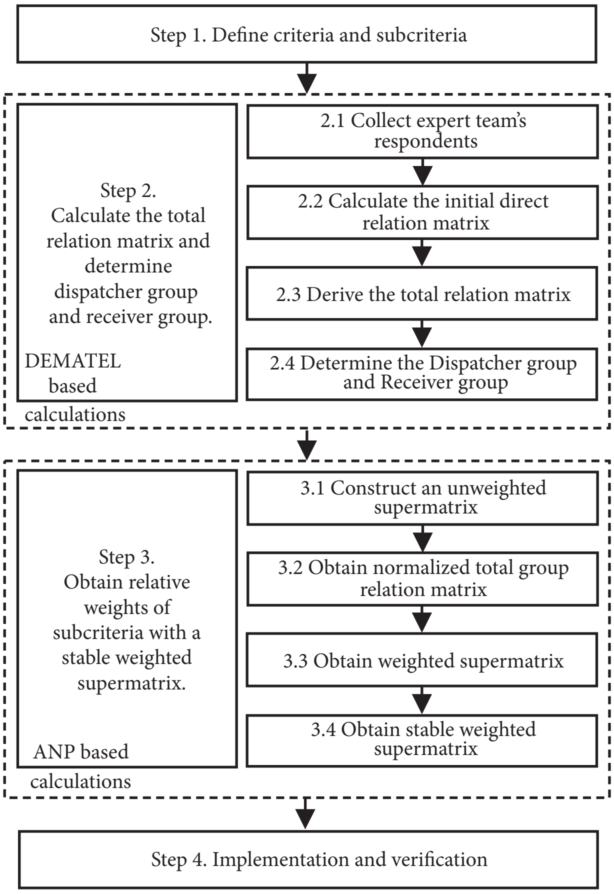


Figure 1: General process of proposed method.

(iii) Cluster-Weighted ANP. We use the DEMATEL to obtain the total structure and weight. Next, inner and outer dependency are obtained using ANP.

(iv) DEMATEL-Based ANP (DANP). This is a combination of various hybrid techniques. The structure, inner dependency, outer dependency, and weight are all obtained using DEMATEL.

In this study, the proposed methodology is based on the Clustered-Weighted ANP, as this method is effective at integrating the effects of unequal cluster weights on the formation of the supermatrix [44]. Of course, DANP is also effective in weighting each cluster. However, DANP is modified to reduce the complexity of the pairwise comparison when there are many criteria. In this study, the number of criteria was not too large. Hence, we selected the Clustered-Weighted ANP and use the traditional pairwise comparison questionnaire for higher accuracy. The overall process is depicted in Figure 1.

3.1. Computational Steps

Step 1. Establish criteria and subcriteria through literature review and expert consultation.

Step 2. Calculate the total relation matrix using the direct relation matrix, and then determine the dispatcher group and the receiver group.

Step 2.1. Collect expert team's respondents. All experts evaluate the degree of influence of subcriterion i on subcriterion j and express it as matrices $E_1, E_2, E_3, \ldots, E_k$, where k stands for the number of experts. In order to compare influences relatively, 0: no influence, 1: low impact, 2: common influence, 3: high influence, 4: very high impact [45], each expert creates a direct relation matrix.

Step 2.2. Calculate the initial direct relation matrix A. Each matrix E is the result of the expert response. Matrix A shows initial effects between each subcriterion. Initial direct relation matrix A is calculated as the average of $E_1, E_2, E_3, \ldots, E_k$ when there are k experts in the team.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \tag{1}$$

$$a_{ij} = \frac{1}{k}\sum_{t=1}^{k} e_{ij}^{t} \tag{2}$$

Step 2.3. Derive the total relation matrix T. The normalized direct relation matrix D is obtained by dividing A by s. Each element of D is between 0 and 1. Total relation matrix T is determined by (5) where I denotes the identity matrix.

$$s = \max\left(\max_{1\le j\le n}\sum_{i=1}^{n} a_{ij}, \max_{1\le i\le n}\sum_{j=1}^{n} a_{ij}\right) \tag{3}$$

$$D = \frac{A}{s} \tag{4}$$

$$T = D + D^2 + \cdots + D^n = D\left(I - D\right)^{-1} \tag{5}$$

Step 2.4. Determine the Dispatcher group and Receiver group. The c vector is calculated by adding all values in the row of total relation matrix T. The r vector is calculated by adding all values in the column of total relation matrix T. If (r_i-c_i) is a positive number, it becomes a Dispatcher group. If (r_i-c_i) is negative, it becomes a Receiver group, and the smaller the value, the greater the degree of influence. (r_i+c_i) represents the degree of relationship with other criteria. The higher the value of (r_i+c_i), the greater the relationship with other criteria.

$$r = \left[r_i\right]_{n\times 1} = \left(\sum_{j=1}^{n} t_{ij}\right)_{n\times 1} \tag{6}$$

$$c = \left[c_j\right]_{1\times n} = \left(\sum_{i=1}^{n} t_{ij}\right)_{1\times n} \tag{7}$$

Step 3. Obtain relative weights of subcriteria with a stable weighted supermatrix.

Step 3.1. Construct an unweighted supermatrix. All experts evaluate the degree of importance of the subcriterion i on the subcriterion j. The unweighted supermatrix is calculated as the average value of each expert's evaluation.

$$W = \begin{pmatrix} W_{11} & W_{12} & \cdots & W_{1n} \\ W_{21} & W_{22} & \cdots & W_{2n} \\ \vdots & \vdots & & \vdots \\ W_{n1} & W_{n2} & \cdots & W_{nn} \end{pmatrix} \tag{8}$$

Step 3.2. Obtain normalized total group relation matrix T_{gs}. Total group relation matrix T_g represents the extent to which each criterion affects all the others. So, it is the mean value of the sum of the influence of the subcriteria in the total relation matrix T. Normalized total group relation matrix T_{gs} is obtained by normalizing T_g.

$$T_g = \begin{pmatrix} t_g^{11} & t_g^{12} & \cdots & t_g^{1m} \\ t_g^{21} & t_g^{22} & \cdots & t_g^{2m} \\ \vdots & \vdots & \ddots & \vdots \\ t_g^{m1} & t_g^{m2} & \cdots & t_g^{mm} \end{pmatrix} \tag{9}$$

$$t_g^{ij} = \frac{\sum_{i\in m_i, j\in m_j} t_{ij}}{N_i \times N_j} \tag{10}$$

$$d_i = \sum_{j=1}^{m} t_g^{ij} \tag{11}$$

$$T_{gs} = \begin{pmatrix} \frac{t_g^{11}}{d_1} & \frac{t_g^{12}}{d_1} & \cdots & \frac{t_g^{1m}}{d_1} \\ \frac{t_g^{21}}{d_2} & \frac{t_g^{22}}{d_2} & \cdots & \frac{t_g^{2m}}{d_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{t_g^{m1}}{d_m} & \frac{t_g^{m2}}{d_m} & \cdots & \frac{t_g^{mm}}{d_m} \end{pmatrix} \tag{12}$$

Step 3.3. Obtain weighted supermatrix W_w. Total group influence matrix T is obtained by reconstructing T_{gs}. Multiply each element of T_s and unweighted supermatrix W to obtain weighted supermatrix W_w.

$$T_s = \begin{pmatrix} t_{gs}^{11} & t_{gs}^{11} & \cdots & t_{gs}^{12} & t_{gs}^{12} & \cdots & t_{gs}^{1m} & t_{gs}^{1m} \\ t_{gs}^{11} & t_{gs}^{11} & \cdots & t_{gs}^{12} & t_{gs}^{12} & \cdots & t_{gs}^{2m} & t_{gs}^{2m} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ t_{gs}^{m1} & t_{gs}^{m1} & \cdots & t_{gs}^{m2} & t_{gs}^{m2} & \cdots & t_{gs}^{mm} & t_{gs}^{mm} \\ t_{gs}^{m1} & t_{gs}^{m1} & \cdots & t_{gs}^{m2} & t_{gs}^{m2} & \cdots & t_{gs}^{mm} & t_{gs}^{mm} \end{pmatrix}_{n\times n} \tag{13}$$

$$W_w = \begin{pmatrix} W_{11} \times t_s^{11} & W_{12} \times t_s^{21} & \cdots & W_{1n} \times t_s^{n1} \\ W_{21} \times t_s^{12} & W_{22} \times t_s^{22} & \cdots & W_{2n} \times t_s^{n2} \\ \vdots & \vdots & & \vdots \\ W_{n1} \times t_s^{1n} & W_{n2} \times t_s^{2n} & \cdots & W_{nn} \times t_s^{nn} \end{pmatrix} \quad (14)$$

Step 3.4. Obtain stable weighted supermatrix W_s. It is calculated by converging the weighted supermatrix W_w by infinite power.

$$W_s = \lim_{k \longrightarrow \infty} {W_w}^k \quad (15)$$

4. Implementation of This Model

In this section, an empirical study is illustrated to implement the model. Network relationship map is derived from the survey of an expert team. Relative weight of each subcriterion is determined by using the network relationship map. Total usability is scored by the relative weights and a survey of the participants.

4.1. Data Collection. First, we have gathered an expert team of three professors and two practitioners, with more than 15 years of experience. Their major fields are biometric system development, usability evaluation, etc., and are suitable for this research. Each expert answered a questionnaire using a pair comparison. Details on data collection by the expert team are provided in Appendix A. With these answers, the influence relation of each subcriterion is obtained by the DEMATEL. And the relative weight of each subcriterion is derived using the ANP method.

Then, we recruited 106 participants in Seoul, South Korea (57.7% women, M age = 23.62, SD = 2.48). Participants ranged in age from 19 to 48. Participants signed up through the university website. In this study, all participants were provided with sufficient explanation about the research and agreed to contribute to the study. The study was to evaluate the usability of three biometric authentication systems installed in the mobile phone. These biometric authentication systems consist of fingerprint recognition system, iris recognition system, and facial recognition system. The expert team selected Samsung Galaxy S8, which is one of the most popular phones, to minimize the perceptible differences between the daily biometric use and the experimental biometric use in terms of technical, ergonomic, and psychological aspects. Meanwhile, this study anonymized Samsung Galaxy 8 as "Mobile phone A" in order to control the influence of personal preference on specific products or brand.

Before starting the session, participants were asked to fully understand usability subcriteria. We gave the participants a detailed description of each subcriterion. After a brief conversation, they confirmed that they understood the subcriteria and in case of need additional clarification was provided. Participants were also given questionnaires related to this experiment. Appendix B shows a questionnaire on the fingerprint recognition system. When the session started, the participants registered the fingerprint of right hand on the mobile phone. We then let the participant perform the unlock two times using the fingerprint. Thereafter, the fingerprint of the left hand was processed in the same manner. Thus, two fingerprints were registered and four unlocks were performed. Upon completion of the activity, they were asked to rate each element of the mobile phone fingerprint recognition system and briefly state the reason for the rating. After that, we conducted experiments on participants' iris recognition in the same way. They also performed one iris enrollment and two unlocks for both the right and left iris, respectively. In the case of face recognition, since there is no distinction between left and right, the participant registered the face twice in total and unlocked four times. Participants rated both iris recognition and face recognition immediately after each experiment. The score is rated by the following standards.

(i) Effectiveness (1 = very low effectiveness, 5 = very high effectiveness)

(ii) Efficiency (1 = very low efficiency, 5 = very high efficiency)

(iii) Anthropometry-fit (1 = very low anthropometry-fit, 5 = very high anthropometry-fit)

(iv) Accessibility (1 = very low accessibility, 5 = very high accessibility)

(v) Affordance (1 = very low affordance, 5 = very high affordance)

(vi) Privacy concern (1 = very high privacy concern, 5 = very low privacy concern)

(vii) Satisfaction (1 = very low satisfaction, 5 = very high satisfaction)

This investigation took 30-50 minutes per person. The inconsistency rate of this questionnaire is 4.5%, under 5%. It means no additional questionnaire is required. The credibility is 97.1%, which is meaningful. This experiment to verify the performance of each biometric system was made with reference to ISO/IEC 19795 [15].

Table 3: Initial direct relation matrix A.

	T1	T2	E1	E2	E3	P1	P2
T1	0	2.8	3.6	3.0	2.0	2.4	3.2
T2	3.0	0	3.4	2.6	2.4	1.6	3.2
E1	2.8	2.4	0	2.8	1.6	2.0	2.4
E2	2.2	2.0	2.8	0	3.0	1.6	2.8
E3	1.6	2.2	2.0	3.0	0	2.8	1.8
P1	1.8	1.8	2.2	1.8	2.6	0	2.6
P2	3.2	3.2	2.8	2.8	2.0	2.6	0

4.2. Measuring Relationships with DEMATEL. Initial direct relation matrix A is calculated by (1)-(2) based on the written questionnaire and is shown in Table 3. Table 4 shows the total relation matrix, which is calculated by (3)-(5) and the total influences matrix T_G can be obtained by considering the effects of all sides. Table 5 is obtained by (6)-(7) which identifies and separates the influencing and receiving elements.

Table 4: Total relation matrix T.

	T1	T2	E1	E2	E3	P1	P2
T1	1.042	1.164	1.345	1.269	1.065	1.046	1.275
T2	1.155	0.987	1.295	1.213	1.047	0.978	1.235
E1	1.024	0.990	0.992	1.090	0.902	0.887	1.071
E2	1.009	0.986	1.145	0.965	0.977	0.884	1.099
E3	0.913	0.926	1.034	1.041	0.769	0.878	0.985
P1	0.898	0.886	1.014	0.960	0.875	0.716	0.992
P2	1.182	1.163	1.290	1.239	1.049	1.038	1.098

Table 5: The sum of influences given and received on subcriteria.

	r_i	c_i	r_i+c_i	r_i-c_i
Effectiveness	7.224	8.205	15.429	-0.981
Efficiency	7.103	7.911	15.013	-0.808
Anthropometry-fit	8.115	6.955	15.07	1.159
Accessibility	7.776	7.065	14.841	0.711
Affordance	6.684	6.547	13.231	0.137
Privacy concern	6.427	6.341	12.768	0.085
Satisfaction	7.755	8.059	15.814	-0.304

Table 6: Unweighted supermatrix W.

	T1	T2	E1	E2	E3	P1	P2
T1	0.417	0.524	0.467	0.524	0.533	0.583	0.583
T2	0.583	0.476	0.533	0.476	0.467	0.417	0.417
E1	0.552	0.400	0.370	0.370	0.381	0.272	0.370
E2	0.206	0.285	0.370	0.370	0.381	0.272	0.370
E3	0.242	0.314	0.259	0.259	0.238	0.455	0.259
P1	0.500	0.500	0.688	0.688	0.385	0.626	0.688
P2	0.500	0.500	0.313	0.313	0.615	0.374	0.313

Table 7: Total group relation matrix T_g.

Criteria	Technical	Ergonomic	Psychological
Technical	1.087	1.198	1.280
Ergonomics	1.039	1.066	1.147
Psychological	1.002	1.028	1.048

The network relationship map is depicted in Tables 3 and 5. It shows the effect of the subcriterion on each other. We assume that the average value of the elements in Table 3 is set to the threshold value. Figure 2 illustrates the effect of the subcriteria that exceed the threshold on each other.

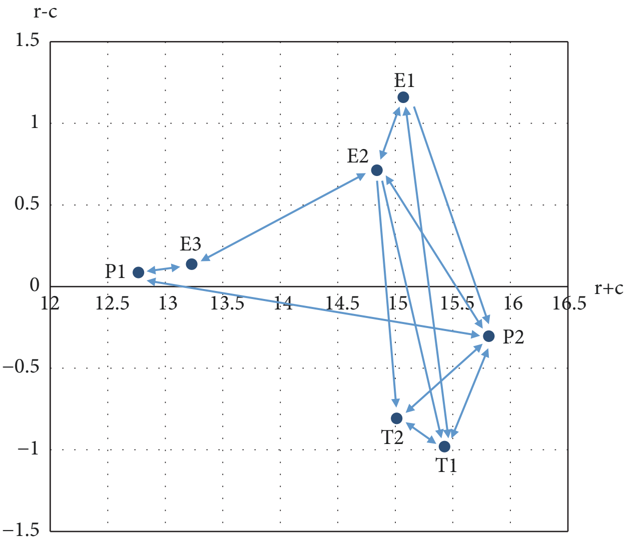


Figure 2: Network relationship map.

Table 8: Normalized total group relation matrix T_{GS}.

	T1	T2	E1	E2	E3	P1	P2
T1	0.305	0.305	0.320	0.320	0.320	0.326	0.326
T2	0.305	0.305	0.320	0.320	0.320	0.326	0.326
E1	0.336	0.336	0.328	0.328	0.328	0.334	0.334
E2	0.336	0.336	0.328	0.328	0.328	0.334	0.334
E3	0.336	0.336	0.328	0.328	0.328	0.334	0.334
P1	0.359	0.359	0.353	0.353	0.353	0.340	0.340
P2	0.359	0.359	0.353	0.353	0.353	0.340	0.340

Table 9: Weighted supermatrix W_w.

	T1	T2	E1	E2	E3	P1	P2
T1	0.127	0.16	0.149	0.167	0.170	0.190	0.190
T2	0.178	0.145	0.170	0.152	0.149	0.136	0.136
E1	0.185	0.134	0.121	0.121	0.125	0.091	0.124
E2	0.069	0.096	0.121	0.121	0.125	0.091	0.124
E3	0.081	0.106	0.085	0.085	0.078	0.152	0.087
P1	0.180	0.180	0.242	0.242	0.136	0.213	0.234
P2	0.180	0.180	0.110	0.110	0.217	0.127	0.106

Table 10: Stable weighted supermatrix W_w.

	T1	T2	E1	E2	E3	P1	P2
T1	0.165	0.165	0.165	0.165	0.165	0.165	0.165
T2	0.152	0.152	0.152	0.152	0.152	0.152	0.152
E1	0.128	0.128	0.128	0.128	0.128	0.128	0.128
E2	0.103	0.103	0.103	0.103	0.103	0.103	0.103
E3	0.101	0.101	0.101	0.101	0.101	0.101	0.101
P1	0.205	0.205	0.205	0.205	0.205	0.205	0.205
P2	0.146	0.146	0.146	0.146	0.146	0.146	0.146

4.3. Weighting Each Criterion with ANP. Unweighted supermatrix is determined by the expert team and it is shown in Table 6, which is obtained by (8). Table 7 is obtained by the mean score of the subcriteria belonging to each criterion from Table 4 and shows the effect of each criterion. Table 8 shows the normalized effect of each criterion and is obtained by (9)-(12). Table 9 shows the initial signs of each subcriterion and is used to calculate the stable weighted supermatrix. It is obtained by (13)-(14). Table 10 is stable weighted supermatrix, obtained by (15). The relative weight of the subcriteria is determined through the stable weighted supermatrix. Table 10

Table 11: Weights of criteria and total usability of biometric systems.

	Weighting by ANP		Usability evaluation by SAW		
	Local weight	Global weights	Fingerprint recognition system	Iris recognition system	Face recognition system
Effectiveness	0.165	0.159	3.566	3.066	3.245
Efficiency	0.152		3.962	2.321	2.557
Anthropometry-fit	0.128	0.111	3.019	3.151	3.019
Accessibility	0.103		2.302	2.566	2.349
Affordance	0.101		2.358	2.623	2.698
Privacy concern	0.205	0.176	2.122	2.368	1.830
Satisfaction	0.146		2.679	2.425	2.594
Total score	-	-	*2.879*	*2.631*	*2.579*

Example for SAW (Simple Additive Weighting):
Calculating the total usability score of fingerprint recognition system:
$0.165*3.566+0.152*3.962+0.128*3.019+0.103*2.302+0.101*2.358+0.205*2.122+0.146*2.679=2.879$

summarizes the results of the stable weighted supermatrix, showing the relative weight and ranking of each subcriterion. The relative weight of the subcriterion and the responses of the participants are combined through the SAW method to calculate the usability score for each biometric system.

4.4. Follow-Up Interviews. Through follow-up interviews, various opinions about each subcriterion were derived.

For effectiveness, the size of the fingerprint scanner and the accuracy when trying to authenticate in various directions was mentioned. For efficiency, the focus was the time taken to recognize and unlock, when the fingerprint sensor was pressed and face or iris is captured by the camera sensor. While fingerprints can be captured quickly with the finger, in the case of the iris recognition system or the facial recognition system, additional time is needed as the camera needs to be adjusted. Among them, the iris recognition system is cumbersome to match the eyes.

For anthropometry-fit, most comments were related to fingerprint and camera sensors. It is important for the finger, eyes, and face to point to the sensor when holding the cell phone naturally. For accessibility, there were many opinions that it would be difficult for elderly people to use easily. The fingerprint registration process was not plain and the message was not clearly visible. However, the facial recognition system has relatively higher accessibility because everyone has a face. For affordance, most of the respondents mentioned that the fingerprint recognition system did not contain any features or components related to behavioural induction. While iris recognition system and facial recognition system induce the behaviour, it feels compulsive since the user cannot use the system unless certain behaviours are displayed.

For privacy concern, there are significant consequences in cases where biometric information has been compromised. When using the body to authenticate the risk was higher, body-based information could not be easily changed when the information was compromised. People also expressed concerns about special situations, such as when someone is forced to use their finger or face while sleeping. Some participants voluntarily erased their biometric information after the experiment. For satisfaction, most of the opinions were related to convenience, and opinions on the other six subcriteria sparse.

4.5. Discussions. In this section, we analyze the weights of each criterion in Table 11, and the usability scores of the biometric systems in Table 11 using the network relationship map of Figure 2. Since the importance of each subcriterion is different, we derive the weights systematically using DEMATEL and ANP. As shown in Figure 3, privacy concern (0.205) is the most important subcriterion when measuring the usability of biometric systems. Usability practitioners should endeavour to lower the privacy concerns to improve the usability of the biometric system. In general, to reduce privacy concerns, it is important to increase the security of the system and raise awareness of the same in users. As technology advances, the system's minimum security will be guaranteed, which entails improved user awareness. However, if users remain uninformed, it can exacerbate the user's privacy concerns as they consider their own personal privacy needs [46]. Therefore, it is essential that the usability practitioners endeavour to educate the users of the enhanced security features. Additionally, privacy concern is followed by effectiveness (0.165), efficiency (0.152), and satisfaction (0.146). This result shows that the traditional method of measuring the usability of biometric systems such as ISO 9241 is powerful. Ergonomic factors tend to be relatively less important. However, as shown in the network relationship map, effectiveness and efficiency are affected by anthropometry-fit and accessibility. Therefore, it is important for the usability practitioner to consider all the interrelationships between the factors in order to increase the usability of the biometric system.

As shown in Figure 4, total usability score is the highest for fingerprint recognition system (2.879), while iris recognition system score is 2.631 and facial recognition system score is 2.579. Since the maximum score is 5, the score of fingerprint recognition system is 57.58 out of 100.

The score of the fingerprint recognition system is 9.4% higher than that of the iris recognition system and 11.6% higher than that of the facial recognition system. This is owing to effectiveness and efficacy scores of the fingerprint

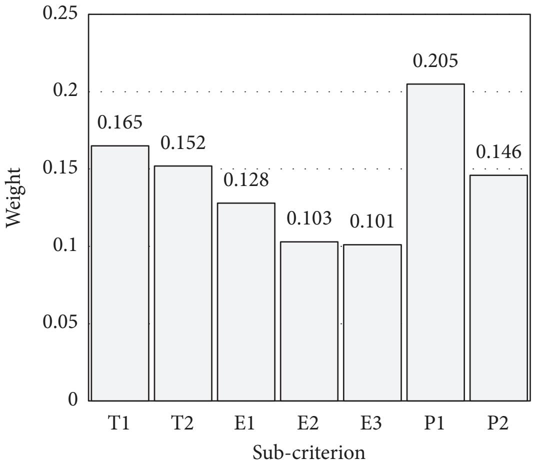


Figure 3: Weights of each subcriterion.

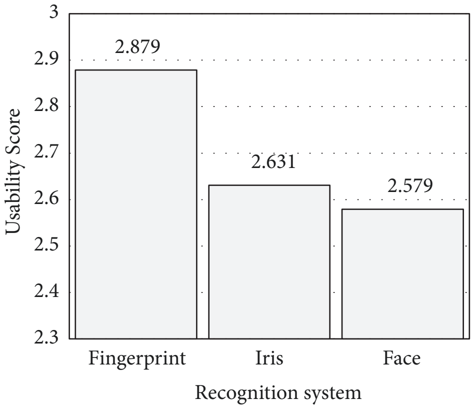


Figure 4: Usability score of each recognition system.

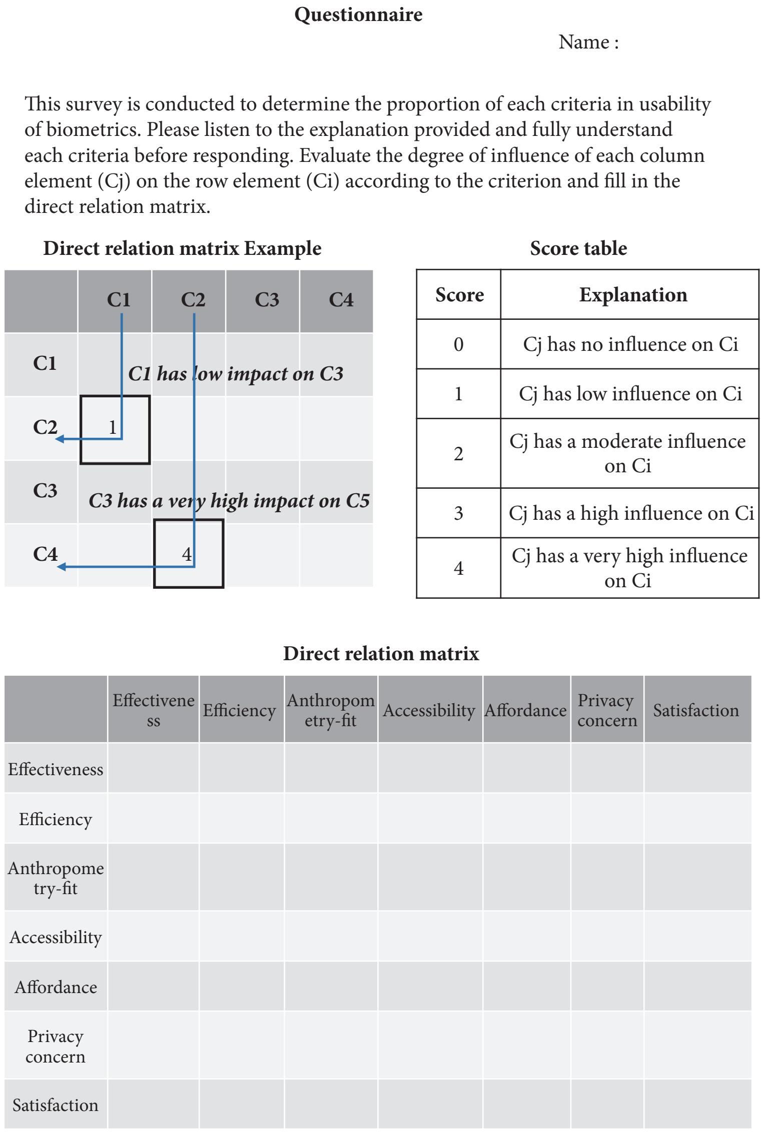
recognition system being significantly higher than those of the iris recognition system and the facial recognition system. Furthermore, the weights of effectiveness and efficiency also impact the score. It can be concluded from the scores that since users are familiar with the use of fingerprint recognition system, they perceive it to be easier to user. Therefore, the variation of total usability scores will narrow as time goes by.

The privacy concern score of the facial recognition system is significantly lower than that of fingerprint recognition system and iris recognition system. The interviews with the participants reveal that the increased privacy concerns stem from sharing of photos. When people use fingerprint or iris for authentication, their belief is that since it is their body, they are the only ones to use them. Although face is part of their body, they think that it is distributed indiscriminately on the Internet in the form of photographs, and people often do not perceive the photographs as personally sensitive information. In fact, in ISO/IEC 30107 [47], research on sensor attacks related to fingerprint recognition and face recognition has been actively conducted. There is a result that the face recognition system is vulnerable to spoofing attack [48]. In addition, the iris recognition system and the facial recognition system are similar in overall score but score differently on privacy concerns. In view of the relative weight of the privacy concerns, it was not reversible with a small difference in scores of other subcriteria.

The MCDM model combining DEMATEL and ANP method can be evaluated quantitatively considering each factor of usability and it is significant to be able to derive various interpretations. In particular, we have confirmed that the privacy concerns, which were not addressed in previous studies, are a key factor in this model.

5. Conclusions

The importance of usability measurement is reinforced as biometric systems become more prevalent in everyday life. However, previous studies did not evaluate the various factors influencing the usability of biometric systems. In addition, the existing evaluation models were not developed in a systematic way. This paper introduces the novel concept of usability that takes privacy concerns into consideration. Relative weights are determined for various factors and



Questionnaire

Name :

This survey is conducted to determine the proportion of each criteria in usability of biometrics. Please listen to the explanation provided and fully understand each criteria before responding. Evaluate the degree of influence of each column element (Cj) on the row element (Ci) according to the criterion and fill in the direct relation matrix.

Direct relation matrix Example

	C1	C2	C3	C4
C1				
C2	1			
C3				
C4		4		

C1 has low impact on C3

C3 has a very high impact on C5

Score table

Score	Explanation
0	Cj has no influence on Ci
1	Cj has low influence on Ci
2	Cj has a moderate influence on Ci
3	Cj has a high influence on Ci
4	Cj has a very high influence on Ci

Direct relation matrix

	Effectiveness	Efficiency	Anthropometry-fit	Accessibility	Affordance	Privacy concern	Satisfaction
Effectiveness							
Efficiency							
Anthropometry-fit							
Accessibility							
Affordance							
Privacy concern							
Satisfaction							

Figure 5

usability of three biometric authentication systems is scored utilizing an empirical study.

The research was conducted in two sessions. First, based on the evaluation of the expert team, we derive the influence of relations and relative weights between the subcriteria of usability. Next, based on the evaluation of 106 participants, usability scores of fingerprint recognition system, iris recognition system, and facial recognition system are derived. The fingerprint recognition system has the highest score. However, several strategies are discussed for effective use of the proposed model for other biometric systems.

The proposed usability evaluation model in this study can be universally applicable. In particular, when dealing with privacy concerns, a factor that has not been considered in earlier studies and has the highest relative weight. While this study is notable for the proposed model, which has been demonstrated to be effective, the inclusion and the lack of validation of ergonomic and psychological elements in usability make the model vulnerable. Therefore, further verification of the model to validate the other elements can be done as future work.

Appendix

A. Questionnaire for Expert Team

See Figure 5.

B. Questionnaire for Participants

See Figure 6.

Data Availability

There is no need for data availability because it has only the result of the survey.

Questionnaire

Name :

Thank you very much for participating in this study.

The purpose of this study is to examine your thoughts. There is no answer to every question, please answer candidly with your usual thinking. We promise that your personal information will be thoroughly protected and used only for statistical purposes with respect to your response.

Thank you again for participating in the study.
Contact: Oh Junhyoung (E-mail: ohjun02@korea.ac.kr)

1. Fingerprint recognition system

You will register the fingerprint of right hand on the mobile phone. Then perform the unlock two times using the fingerprint. Thereafter, perform the fingerprint of the left hand in the same way. And then, you should answer to rate each element. Each element is rated from 1 to 5 and is distributed from very low to very high. And state why you rate the score for each element.

	1(Very low)	2(Low)	3(So so)	4(High)	5(Very high)
- Effectiveness	○	○	○	○	○

Why?

	1(Very low)	2(Low)	3(So so)	4(High)	5(Very high)
- Efficiency	○	○	○	○	○

Why?

	1(Very low)	2(Low)	3(So so)	4(High)	5(Very high)
- Anthropometry-fit	○	○	○	○	○

Why?

	1(Very low)	2(Low)	3(So so)	4(High)	5(Very high)
- Accessibility	○	○	○	○	○

Why?

	1(Very low)	2(Low)	3(So so)	4(High)	5(Very high)
- Affordance	○	○	○	○	○

Why?

	1(Very dangerous)	2(Dangerous)	3(So so)	4(Safe)	5(Very safe)
- Privacy concern	○	○	○	○	○

Why?

	1(Very low)	2(Low)	3(So so)	4(High)	5(Very high)
- Satisfaction	○	○	○	○	○

Why?

Elements	Explanation
Effectiveness	The perceived accuracy and completeness with which users have achieved specified goals
Efficiency	The perceived mental or physical resources expended in relation to the accuracy and completeness with which users achieve goals
Anthropometry-fit	The perceived attribute which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use
Accessibility	The perceived attribute which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use
Affordance	The perceived attribute of an object that allows people to know how to use it
privacy concern	The perceived threat of the consequences about problems and how this affects their behaviour
Satisfaction	The perceived degree to which the product meets the users' overall expectations-a subjective response of enjoyment, comfort, or frustration

Figure 6

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Junhyoung Oh and Ukjin Lee contributed equally to this work.

Acknowledgments

This research was supported by the MSIT (Ministry of Science, ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2015-0-00403) supervised by the IITP (Institute for Information and communications Technology Promotion).

References

[1] L. Coventry, A. De Angeli, and G. Johnson, “Usability and biometric verification at the ATM interface,” in *Proceedings of the SIGCHI conference on Human factors in computing systems*, vol. 5, pp. 153–160, ACM, Paris, France, April 2003.

[2] Z. Akhtar, A. Hadid, M. Nixon, M. Tistarelli, J.-L. Dugelay, and S. Marcel, “Biometrics: In Search of Identity and Security (Q & A),” *IEEE MultiMedia*, 2017.

[3] “ISO 9241-11. Ergonomic requirements for office work with visual display terminals (VDTs),” 45: 9, The international organization for standardization, 1998.

[4] E. P. Kukula, M. J. Sutton, and S. J. Elliott, “The human-biometric-sensor interaction evaluation method: biometric performance and usability measurements,” *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 784–791, 2010.

[5] L. Gao and X. Bai, “A unified perspective on the factors influencing consumer acceptance of internet of things technology,” *Asia Pacific Journal of Marketing and Logistics*, vol. 26, no. 2, pp. 211–231, 2014.

[6] A. M. AL-Momani, M. A. Mahmoud, and M. Sharifuddin, “Modeling the adoption of internet of things services: a conceptual framework,” *International Journal of Applied Research*, vol. 2.5, pp. 361–367, 2016.

[7] Irish Council for Bioethics, “Biometrics: Enhancing Security or Invading Privacy?” 2009.

[8] C. Arthur, “iPhone 5S fingerprint sensor hacked by germany’s chaos computer club,” *The Guardian*, 2013, https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked.

[9] A. Hern, “Samsung galaxy S8 iris scanner fooled by german hackers,” *Theguardian*, 2017, https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security.

[10] N. Tractinsky, “The usability construct: a dead end?” *Human–Computer Interaction*, pp. 1–47, 2017.

[11] A. S. Patrick, “Usability and acceptability of biometric security systems,” *Financial Cryptography*, 2004.

[12] E. Frøkjær, M. Hertzum, and K. Hornbæk, “Measuring usability: are effectiveness, efficiency, and satisfaction really correlated?” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2000*, pp. 345–352, ACM, The Hague, Netherlands, April 2000.

[13] K. Hornbæk and E. L.-C. Law, “Meta-analysis of correlations among usability measures,” in *Proceedings of the 25th SIGCHI Conference on Human Factors in Computing Systems 2007*, pp. 617–626, ACM, San Jose, CA, USA, May 2007.

[14] J. R. Edwards, “The fallacy of formative measurement,” *Organizational Research Methods*, vol. 14, no. 2, pp. 370–388, 2011.

[15] ISO/IEC 19795-6. Biometric performance testing and reporting, The international organization for standardization, 2012.

[16] D. T. Toledano, R. Fernández Pozo, Á. Hernández Trapote, and L. Hernández Gómez, “Usability evaluation of multi-modal biometric verification systems,” *Interacting with Computers*, vol. 18, no. 5, pp. 1101–1122, 2006.

[17] M. F. Theofanos, S. Orandi, R. J. Micheals, B. Stanton, and N. F. Zhang, *National Institute of Standards and Technology*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2006.

[18] ISO/IEC 25062: Software Engineering - Software product Quality Requirements and Evaluation (SQuaRE)-Common Industry Format (CIF) for Usability Test Reports, 2006.

[19] M. F. Theofanos, R. J. Micheals, and B. C. Stanton, “Biometrics systems include users,” *IEEE Systems Journal*, vol. 3, no. 4, pp. 461–468, 2009.

[20] DIS, “ISO. 9241-210: 2010. ergonomics of human system interaction-part 210: human-centred design for interactive systems” (Chinese), International Standardization Organization (ISO), Switzerland, 2009.

[21] T. L. Saaty, *The Analytic network process : decision making with dependence and feedback*, Rws Publications, Pittsburg, Calif, USA, 1996.

[22] M. Carroll. J, “Human computer interaction-brief intro,” in *Encyclopedia of Human-Computer Interaction*, 2nd edition, 2013.

[23] N. Bevan, “International standards for HCI and usability,” *International Journal of Human-Computer Studies*, vol. 55, no. 4, pp. 533–552, 2001.

[24] Y. Lee and K. A. Kozar, “Understanding of website usability: specifying and measuring constructs and their relationships,” *Decision Support Systems*, vol. 52, no. 2, pp. 450–463, 2012.

[25] B. Shackel, “Ergonomics in design for usability, in people and computer: designing for usability,” in *Proceedings of the 2nd Conference Human-Computer Interaction Specialist Group British computer Society*, M. D. Harrison and A. F. Monk, Eds., Cambridge University press, Cambridge, UK, 1986.

[26] J. Preece, Y. Rogers, and H. Sharp, *Interaction Design: Beyond Human Computer Interaction*, Wiley, New York, NY, USA, 2002.

[27] J. R. Lewis and J. Sauro, “The factor structure of the system usability scale,” in *Proceedings of the International conference on human centered design*, pp. 94–103, Springer, Berlin, Germany, 2009.

[28] M. F. Theofanos, B. Stanton, C. Sheppard, and R. Micheals, “Usability Testing of Face Image Capture for US Ports of Entry,” in *Proceedings of the 2nd International Conference on Biometrics: Theory, Applications and Systems*, pp. 1–6, IEEE, Arlington, VA, USA, September 2008.

[29] T. Jokela, N. Iivari, J. Matero, and M. Karukka, “The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11,” in *Proceedings of the Latin American Conference on Human-Computer Interaction*, pp. 53–60, ACM, Rio de Janeiro, Brazil, August 2003.

[30] S. Hamilton and N. L. Chervany, “Evaluating information system effectiveness - part I: comparing evaluation approaches,” *MIS Quarterly: Management Information Systems*, vol. 5, no. 3, pp. 55–69, 1981.

[31] A. Bangor, P. T. Kortum, and J. T. Miller, “The system usability scale (SUS): an empirical evaluation,” *International Journal of Human-Computer Interaction*, vol. 24, no. 6, pp. 574–594, 2008.

[32] J. Nielsen, *Usability Engineering*, Elsevier, Amsterdam, Netherlands, 1994.

[33] M. Theofanos, R. Micheals, J. Scholtz, E. Morse, and P. May, “Does habituation affect fingerprint quality?” in *Proceedings of the Conference on Human Factors in Computing Systems, CHI EA 2006*, pp. 1427–1432, ACM, Québec, Canada, April 2006.

[34] ISO/IEC/IEEE 24765:2010 Systems and software engineering—Vocabulary.

[35] B. Stanton, M. Theofanos, and C. Sheppard, *A Study of Users with Visual Disabilities and a Fingerprint Process*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2008.

[36] T. Hughes-Roberts, "Reminding users of their privacy at the point of interaction: the effect of privacy salience on disclosure behaviour," in *Human Aspects of Information Security, Privacy, and Trust*, vol. 9190 of *Lecture Notes in Computer Science*, pp. 347–356, Springer International Publishing, Cham, Switzerland, 2015.

[37] M. A. Sasse, "Usability and trust in information systems," *Cyber Trust and Crime Prevention*, pp. 319–348, 2005.

[38] T. Mansfield and M. Rejman-greene, "Feasibility study on the use of biometrics in an entitlement scheme," Report UKPS, DVLA and the Home Office, IMSC/H07/D2, 2003.

[39] Y. M. Hausawi and W. H. Allen, "Usable-Security Evaluation," in *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*, vol. 9190 of *Lecture Notes in Computer Science*, pp. 335–346, Springer International Publishing, Los Angeles, CA, USA, 2015.

[40] J. Zhou, Q. Wang, S. Tsai, Y. Xue, and W. Dong, "How to evaluate the job satisfaction of development personnel," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–8, 2016.

[41] D. J.-F. Jeng and G.-H. Tzeng, "Social influence on the use of clinical decision support systems: revisiting the unified theory of acceptance and use of technology by the fuzzy DEMATEL technique," *Computers & Industrial Engineering*, vol. 62, no. 3, pp. 819–828, 2012.

[42] C.-C. Hsu and Y.-S. Lee, "Exploring the critical factors influencing the quality of blog interfaces using the decision-making trial and evaluation laboratory (DEMATEL) method," *Behaviour & Information Technology*, vol. 33, no. 2, pp. 183–193, 2014.

[43] R. C. Zoie, B. Alexandru, R. Delia Mihaela, and D. Mihail, "A decision making framework for weighting and ranking criteria for cloud provider selection," in *Proceedings of the 20th International Conference on System Theory, Control and Computing, ICSTCC 2016*, pp. 590–595, IEEE, Sinaia, Romania, October 2016.

[44] A. Baykaso, "An analysis of DEMATEL approaches for criteria interaction handling within ANP," *Expert Systems with Applications*, vol. 46, pp. 346–366, 2016.

[45] G. Büyüközkan and D. Öztürkcan, "An integrated analytic approach for Six Sigma project selection," *Expert Systems with Applications*, vol. 37, no. 8, pp. 5835–5847, 2010.

[46] T. Hughes-Roberts, "Reminding Users of their Privacy at the Point of Interaction: The Effect of Privacy Salience on Disclosure Behaviour," in *the Proceedings of the 3rd International Conference on Human Aspects of Information Security, Privacy, and Trust*, vol. 9190, pp. 347–356, Springer-Verlag New York, Inc., Los Angeles, CA, USA, 2015.

[47] ISO/IEC 30107-3. Biometric presentation attack detection, The international organization for standardization, 2017.

[48] S. Kumar, S. Singh, and J. Kumar, "A comparative study on face spoofing attacks," in *Proceedings of the 2017 IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, pp. 1104–1108, IEEE, Greater Noida, India, May 2017.