ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20230328000486
Original scientific paper

Computer Vision-Based Risk Assessment on Heterogeneous Mobile Network Operating Environments

Youngjun KIM, Namkyun BAIK*

Abstract: In order to logically prioritize the urgent risks in the heterogeneous mobile network operating environment, we derive environmental factors that can reflect the characteristics of the heterogeneous network operating environment and present them as an improved security risk assessment formula. The prioritized risks derived through this improved risk assessment formula can visually express the severity of the risk by using computer vision. The purpose of this study was to derive environmental factors that can reflect the security control characteristics of various heterogeneous network operating environments and to apply them to security risk evaluation formulas to prioritize urgent risks and easily identify the degree of security risks. In the existing risk assessment formula, risk is calculated based on three indices: the importance of the asset, the vulnerability score, and the threat score. However, two problems were derived from the existing risk assessment. First, the existing risk assessment formula is insufficient to reflect the controlled environment characteristics of each network because the risk level is calculated based on individual assets. Second, if the same systems with the same purpose (same settings) are operated in different heterogeneous network operating environments, they are counted at the same risk level, and action cannot be prioritized quickly. To solve these problems, we propose an indicator called environmental factor (*E*), which is a combination of three indices. The three indices are "Network Diversity Index (*NDI*), network Zone Separation Index (*ZSI*) and Control Level Index (*CLI*)". *NDI* expressed the diversity of networks numerically. *ZSI* is a numerical expression of the complexity of the network zone. *CLI* is a numerical expression of the degree of network control level. Results of the study showed that the risk assessment formula applying the proposed risk assessment factors can quickly identify urgent risks and act quickly. In heterogeneous mobile network operating environment in which numerous systems are operated, really urgent risks among the risks calculated through the proposed risk assessment will be handled quickly and logically.

Keywords: heterogeneous network; quantitative risk model; risk analysis; risk assessment; risk management

1 INTRODUCTION

The elements of business complexity and uncertainty are escaping from the existing Internet Data Center (IDC) based infrastructure operation environment, and the shift to cloud services with excellent elasticity, flexibility, and efficiency is accelerating [1-4]. The legacy operating environment, which is a contrasting expression to the cloud operating environment, is intended to be defined as an environment (referred to as 'legacy operating environment') in which a network is configured and operated based on the existing IDC, data center, computer room, and server room. The cloud operating environment refers to the operating environment for providing cloud services such as IaaS, PaaS, and SaaS and includes public, private, and hybrid methods [5, 6]. A network operating environment in which the cloud operating environment and the legacy operating environment coexist is defined as a heterogeneous operating environment. The operating environment composed of these various networks is used in the mobile network, and as this also changes rapidly and its complexity increases, the number of intrusion incidents is also increasing rapidly [7]. In such a heterogeneous operating environment, it is important to prevent cyber incidents in advance. It requires a method to identify, analyze, and assess risks in advance to identify risks with high risk (impact), and to act quickly according to priority (importance). Risk assessment, which is one area of risk management, is a high-level concept that includes asset importance assessment, vulnerability assessment, and threat assessment, and methods (equations & formulas) using various assessment factors have been studied [8-15]. In a heterogeneous operating environment where various types of mobile networks coexist, a problem was found in that the logic of risk assessment results was not guaranteed. Two shortcomings were derived from the existing risk assessment. First, the existing risk assessment formula is insufficient to reflect the controlled environment characteristics of each network because the risk level is calculated based on individual assets. Second, if the same systems with the same purpose (same settings) are operated in different heterogeneous network operating environments, they are counted at the same risk level, and action cannot be prioritized quickly. In this study, in a heterogeneous mobile network operating environment where various networks (IDC, Public Cloud, Private Cloud, Hybrid Cloud) coexist, an evaluation factor to reflect the characteristics of an individual network operating environment is derived, and a risk evaluation technique is proposed. The structure of the thesis explains the background, purpose, and scope of this study in I. Introduction. In II. Literature Review, this paper introduces research related to existing risk assessment methods. In III. Research methodology, an improved risk assessment method suitable for the heterogeneous network operating environment is proposed. In IV. Results and discussions, the proposed method verifies the difference from the existing method and presents the results. In V. Conclusion, the key points of this study are summarized and presented as a conclusion.

2 LITERATURE REVIEW

2.1 ISO 31000 and ISO 31010

ISO 31000: Risk Management Guidelines [16] deal with general risk types and management methodologies, not risk types and approaches that are specific to a specific industry (field). The risk management framework and risk management process covered by this standard systematically apply policies, procedures, and practices to risk management activities to be covered by the organization, and guide risk management matters to assess, handle, monitor, review and report risks.

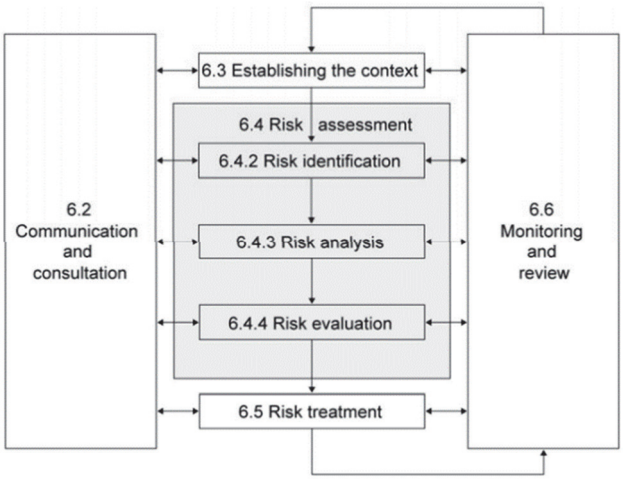

Figure 1 Process for risk management

As shown in Fig. 1, risk assessment consists of risk identification, risk analysis, and risk evaluation. In this paper, the proposal is limited to the risk assessment technique. ISO 31010: Risk Assessment Techniques [17] introduces various techniques applied to risk assessment. The main content consists of uses of risk assessment techniques, implementing, and selecting risk assessment techniques. In particular, Annex B.10.3 introduces the consequence/likelihood matrix, which is a technique of expressing a matrix or a heat map method that is primarily used to record and present the risk assessment process and results. A representation called a probability matrix is a square matrix in which every item is a non-negative real number representing a probability. Risk assessment is basically expressed as Eq. (1) by calculating the impact level of a potential outcome and the likelihood that such a result will occur.

$$R = CL \tag{1}$$

R (Risk), C (Consequence), L (Likelihood).

In Eq. (1), Consequence is the effect on the environment when an event occurs, and Likelihood is the probability that an impact on the environment will occur. The matrix method in Eq. (1) is a method of calculating the risk score and grade by combining the qualitative or semi-quantitative evaluation of the result and the score of the level of 3 of 19 probabilities that a specific result will occur. Various other risk management standards can be found in Risk Management Standards [18].

2.2 Threat Vulnerability and Risk Analysis (TVRA)

TVRA [18, 19] presents a method to analyze the threat of the system and evaluate the risk based on the attack potential and impact level. TVRA's process consists of a total of 10 steps (Step 10), of which Step 4 (Systematic inventory of vulnerabilities) is related to risk assessment. In Step 4, assets are classified into physical, human, and logical lists, and the value of asset impact is calculated. Step 5. (Systematic identification of vulnerabilities) is a step to systematically identify vulnerabilities and consists of security weaknesses, vulnerabilities, attack methods, and threat agent identification. Step 6. (Calculation of the likelihood of the attack and its impact) is a step to quantify the attack potential and its impact and presents a method of mapping the threat level and vulnerability level to identify the attack potential. Step 7. (Establishment of the risk) is the stage of determining the risk, and the results of various attack strengths and impacts are "Asset Impact, Attack Intensity, Resulting Impact, and occurrence". A method for determining the risk value based on these factors is presented.

2.3 Quantitative Cyber Security Scoring System Based on Risk Assessment Model

Cybersecurity evaluation in Quantitative Cyber Security Scoring System based on Risk Assessment model [20] is a method of evaluating the risk level of assets and systems through asset analysis, threat analysis, and vulnerability analysis. This includes the process of identifying the vulnerabilities of each component through asset analysis of the system, determining the possibility of occurrence of threats using vulnerabilities, and determining the degree of impact on the system when a threat occurs. Risk analysis for quantitative evaluation is the process of determining the impact of a threat on a system based on a single threat to an asset and the degree of probability that the threat will succeed. It is expressed by the following Eq. (2).

$$R = TV,\ R = IP \tag{2}$$

R (Risk), T (Threat), V (Vulnerability), I (Impact Factor), P (Probability Factor).

In the risk analysis model of Eq. (2), T (Threat) quantifies the impact of a threat on the system according to its level. V (Vulnerability) can be quantified as a threat's success probability by calculating a vulnerability level according to the nature and number of vulnerabilities. In addition, the risk is calculated through a quantitative risk model through I (Impact Factor) and P (Probability Factor). In other words, the risk to an asset is a function with a threat as a parameter that is derived as a probabilistic expected value by applying the probability to the impact on the asset per threat.

2.4 Quantitative Scoring System on the Importance of Software Vulnerabilities

Quantitative Scoring System on the Importance of Software Vulnerabilities [21] analyzes CVSS (Common Vulnerability Scoring System) [22, 23] and CWSS (Common Weakness Scoring System) [24] and presents an improved vulnerability importance quantitative evaluation system. CVSS is a method of evaluating the severity of software and hardware vulnerabilities with a numerical score, and CWSS is a method of expressing the importance of software vulnerabilities with a numerical score. In composing the evaluation scale, six essential evaluation categories (appearance, system importance, technical impact, attack difficulty, response difficulty, and excavation level) are set and the scale is selected accordingly so that balanced analysis can be achieved, and the importance of security vulnerabilities Scores are presented objectively. Eq. (3) is a method of calculating

such a vulnerability score, an excavation level score, and a response difficulty score.

$$V = \left(IF + (1 - IF)S\right)(RR \times 0.8) + (TD \times 0.2) \times \left((AV + PR + DOI)\left(\frac{POI}{3}\right)\right) \quad (3)$$

Vulnerability Score (*V*), Influence (*I*), Appearance (*A*), Attack Difficulty (*AD*), Infringement Form (*IF*), Seriousness (*S*), Ripple Range (*RR*), Target Distribution (*TD*), Attack Difficulty (*AD*), Approach Vector (*AV*), Permission Request (*PR*), Degree Of Interaction (*DOI*), Possibility Of Infringement (*POI*).

2.5 Risk Rating Process of Cyber Security Threats

In Risk Rating Process of Cyber Security Threats in NPPI&C [25], the risk estimation process for each threat of the nuclear power plant instrumentation and control system is proposed. When calculating the risk, four evaluation items for the likelihood of occurrence of a security threat (*L*) and six evaluation items for the threat zero (*I*) were designed. To enable quantitative evaluation of each item, detailed criteria for each item were defined and a score of 0 to 9 was given. As shown in Eq. (4), the risk calculation formula was designed and a method of evaluating the risk level as high, medium, or low (*H*/*M*/*L*) was suggested using the evaluation results of the probability (*L*) and impact (*I*) of the security threat.

$$\begin{aligned} H &: N_2 \le \left(\sum_{i=1}^{4}\frac{L_i}{4}\right)\left(\sum_{i=1}^{6}\frac{I_i}{6}\right) \\ M &: N_1 \le \left(\sum\nolimits_{i=1}^{4}\frac{L_i}{4}\right)\left(\sum\nolimits_{i=1}^{6}\frac{I_i}{6}\right) \le N_2 \\ L &: \left(\sum_{i=4}^{4}\frac{L_i}{4}\right)\left(\sum_{i=6}^{6}\frac{I_i}{6}\right) \le N_1 \end{aligned} \quad (4)$$

$L_{1\sim4}$: Threat Likelihood Criteria
$I_{1\sim6}$: Threat Impact Criteria

2.6 Risk Scoring System for Software Vulnerability Using Public Vulnerability Information [26]

A risk assessment method is proposed by considering not only the inherent characteristics of the vulnerability but also the weaknesses and attack patterns related to the vulnerability. The evaluation scale is based on CWSS and consists of obtainable privileges that are not covered by CVSS, detectability of attack codes, and the scope of violation of vulnerabilities. Vulnerability Score is shown in Eq. (5) to be calculated by classifying it into Impact Score, Appearance Score, and Level of Difficulty Score.

$$VS = IS + AS + LDS \quad (5)$$

VS (Vulnerability Score), *IS* (Impact Score), *AS* (Appearance Score), *LDS* (Level of Difficulty Score).

2.7 Security Risk assessment management

In Security Risk Assessment and Management [27], the risk equation is defined as the following Eq. (6).

$$R = P_A\left(1 - P_E\right)C \quad (6)$$

R (Risk associated with adversary attack), P_A (likelihood of attack), P_E (Probability that the security system is effective against the attack), $(1 - P_E)$ = system ineffectiveness, *C* (Consequence of the loss from the attack).

2.8 Vulnerability analysis evaluation model

The risk scenario in the vulnerability analysis and evaluation model [28] is to determine the correlation between an asset (*A*) vulnerability (*V*) threat (*T*) counter measures. The risk calculation is a method of mapping the importance, threat, and vulnerability of the asset and writing the risk of the asset as a matrix of risk estimation criteria as follows (Tab. 1).

Table 1 Matrix-based risk calculation criteria table

T		*L*				*M*				*H*				*V*			
V		*L*	*M*	*H*	*V*	*L*	*M*	*H*	*V*	*L*	*M*	*H*	*V*	*L*	*M*	*H*	*V*
A	*L*	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7
	M	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
	H	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9
	V	4	5	6	7	5	6	7	8	6	7	8	9	7	8	9	10

In the risk assessment, the CIA assessment method (confidentiality, integrity, availability) is used for the asset, and the value of the asset is also calculated as the degree of influence of the main function of the asset. Vulnerability is a potential weakness of all assets and refers to "weakness in the organization, procedure, personnel, management, HW, SW, physical arrangement or information management". Vulnerability levels are calculated as very vulnerable (*V*), relatively vulnerable (*H*), moderate (*M*), and hardly vulnerable (*L*). A threat is evaluated as the importance of a threat by considering both the impact of the threat and the threat occurrence cycle. (Tab. 2) is a risk assessment matrix indicating the degree of such a threat.

Table 2 Threat assessment metrics

TI	*L*				*M*				*H*				*V*			
CO	*L*	*M*	*H*	*V*	*L*	*M*	*H*	*V*	*L*	*M*	*H*	*V*	*L*	*M*	*H*	*V*
TL	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
TR	1	2	2	3	2	2	3	3	2	3	3	4	3	3	4	4

Threat Impact (*TI*), Cycle of Occurrence (*CO*), Threat Level (*TL*), Threat Rating (*TR*).

2.9 Guides to Information Security Management System Risk Management

Guide to Information Security Management System Risk Management [29] consists of the risk analysis methodology and risk management plan. In the risk analysis methodology, the degree of risk is evaluated based on asset value evaluation, threat and occurrence evaluation, vulnerability evaluation, and existing security measures evaluation. In addition, the risk analysis methodology presents and explains four approaches: the baseline approach, the informal approach, the detailed risk analysis, and the complex approach. In risk assessment, there are a quantitative method and a qualitative method. In a quantitative way, the value of an asset is assessed as a monetary value, threats as annual occurrences, and vulnerabilities as a percentage (%). The expected loss that

the threat (T) to the asset (A) can cause per year is expressed by Eq. (7) as follows.

$$AL(A, T) = VA(\$) \times ANOT \times AVT(\%) \tag{7}$$

Annual Loss (AL), Value of Asset (VA), Annual Number of Occurrences of threat T ($ANOT$), A's Vulnerability to T (AVT).
In the qualitative method, the assets, threats, and vulnerabilities are expressed in stages (level 3 or 5). It is a method of calculating the risk value by multiplying or adding the values of assets (A), threats (T), and vulnerabilities (V), and this is expressed in (Tab. 3).

Table 3 Step 3 Qualitative risk assessment metrics

R	T	1			2			3		
	V	1	2	3	1	2	3	1	2	3
A	1	3	4	5	4	5	6	5	6	7
	2	4	5	6	5	6	7	6	7	8
	3	5	6	7	6	7	8	7	8	9

2.10 The Security Risk Assessment Methodology

The risk assessment method mentioned in The Security Risk Assessment Methodology [30] is a method of calculating the risk for each asset by synthesizing the results of threat assessment, vulnerability assessment, and impact assessment [31]. Threat (T) determines the probability that a threat will occur, vulnerability (V) evaluates vulnerability to threat (T), and impact (I) identifies and evaluates the degree of impact when a threat occurs and is the same as Eq. (8).

$$R = T \times V \times I \tag{8}$$

The index range and rating of the risk derived according to Eq. (8) is composed of five sections as shown in (Tab. 4). As can be seen from the various risk assessment cases discussed above, necessary evaluation factors are derived in consideration of various environments and characteristics, and the evaluation method is optimized by applying them.

Table 4 Step 3 risk range and rating

Criteria	T	V	I	Risk	
				Range	Rating
Very High	5	5	5	91 ~ 125	5
High	4	4	4	45 ~ 90	4
Medium	3	3	3	16 ~ 44	3
Low	2	2	2	3 ~ 15	2
Very Low	1	1	1	1 ~ 2	1

3 RESEARCH METHODOLOGY

In general, risk assessment in the same network operating environment such as a legacy operating environment was sufficient to determine the level of risk with only three indices (importance of assets, threat level, and vulnerability level). However, in a heterogeneous operating environment that combines various cloud environments as well as IDC, these three indices alone are insufficient to reflect the characteristics of various network operating environments. In other words, the characteristics of various networks to be considered in risk assessment are not reflected in the existing risk assessment factors. The following are the things to consider: First, in an operating environment where heterogeneous networks coexist, the characteristics of the operating environment must be reflected. Second, the network areas should be separated according to the purpose and importance of use in the network. Third, the network access control policy should be applied. Some environmental factors are not reflected in the risk assessment. By adding environmental factors to the existing risk assessment factors (asset, threat, and vulnerability grade), the main characteristics to be considered in various heterogeneous operating environments are reflected in the risk assessment. Through the proposed environmental factor (E), it is expected that the risk assessment method in a heterogeneous operating environment will yield more objective and logical results.

3.1 Factors to be Considered in a Heterogeneous Operating Environment

The cloud operating environment different from the existing legacy operating environment (IDC, server room, & computer room) is built in various ways (Public, Private, & Hybrid) and is provided as various types of services (IaaS, PaaS, SaaS, & FaaS). Among cloud operating environments, the private cloud is built by combining resources provided from physical hardware into a shared pool using virtualization technology, and is mainly located within the user's firewall. However, the public cloud operating environment is located outside the user's firewall as it is configured through numerous public cloud service providers (AWS, Azure, GCP, IBM, Alibaba Cloud, NCP, &KT) around the world. Hybrid Cloud refers to an operating environment in which two or more heterogeneous cloud methods are combined. Multi-Cloud refers to an environment composed of two or more public (or private) clouds provided by two or more cloud vendors. The cloud operation and management environment are very diverse for each service provider, and the level of risk also varies depending on the user's configuration and management competency (level). In various cloud environments with various complexity of these various categories, objective and logical risk assessment cannot be performed only with risk assessment factors (asset importance, vulnerability grade, & threat level) considered in the existing legacy IT operating environment. For example, there are web servers (Web server A1 in Server Room, Web Server A2 in IDC, Web Server A3 in the cloud) operated in different network operating environments as in Fig. 2. When performing risk assessment on these web servers, the same risk level is calculated for the same vulnerable item (Z item).

$$R = A + V + T \text{ or } R = A \times V \times T \tag{9}$$

R (Risk Rating), A (Asset Rating), V (Vulnerability Rating), T (Threat Rating).

As can be seen from the result (Tab. 5) derived from Eq. (9), WEB Servers A1, A2, and A3 for the same purpose have the same risk for the same vulnerability item. In other words, if the scores of the three indices (A, V, T) applied to the risk assessment are the same, the risk result will be the same. First, since the importance of an asset is calculated according to the purpose of use of the system, the

corresponding systems are calculated with the same asset importance if the purpose is the same. Second, the same vulnerability items of the same type of system are calculated as the same vulnerability level. Third, the threat level is mainly calculated through the probability and impact level, and since it is also mapped (related) with the vulnerability item and calculated as the probability of occurrence and the impact level at the time of occurrence, it is also calculated at the same level. Therefore, when evaluating only these three indices (*A*, *V*, *T*), systems with the same purpose operating in different heterogeneous network operating environments have the same level of risk, so risk factors or control levels faced by each network cannot be reflected in detail. There is a problem. That is, the existing method is insufficient to reflect the environmental factors to be considered in various ways.

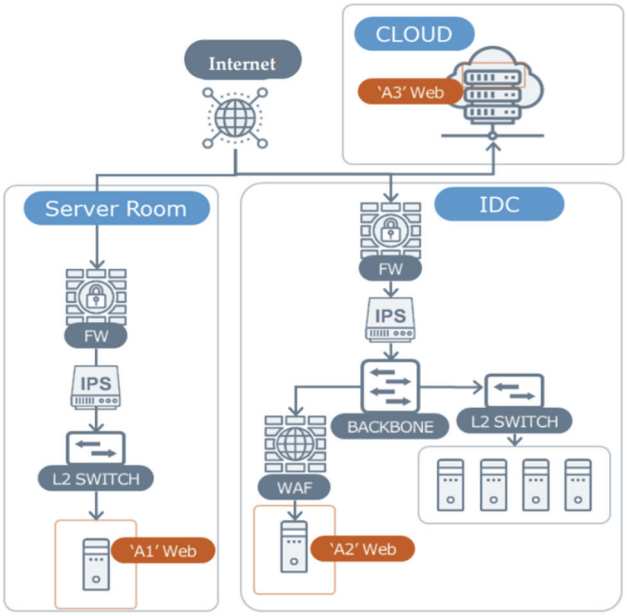

Figure 2 Web server operating on a heterogeneous operating environment

Table 5 Risk rating

Name	Location	*A*	*V*	*T*	*R*
A1	Server Room	3	2	2	7
A2	IDC	3	2	2	7
A3	Cloud	3	2	2	7

3.2 Risk Assessment Method in the Heterogeneous Operating Environment

In a heterogeneous network operating environment where legacy and cloud operating environments coexist, the utility and effectiveness of risk assessment can be increased by applying network diversity, complexity, and controllability. In other words, as key factors to be considered in risk assessment in a heterogeneous network operating environment, "network diversity, network complexity (zone separation), and network control level" are derived and applied as factors. First, the index expressing network diversity is an index expressing the complexity of the network operating environment when heterogeneous operating environments coexist after classifying the network operating environment. We would like to present the "Network Diversity index (*NDI*)" as shown in Tab. 6.Tab. 6. In the *NDI* index, a single network operating environment has an *NDI* index of 0. The multiple network operating environment corresponding to the *NDI* of 0.5 consists of two or more types of the same type of network. This does not apply to cases based on different types (heterogeneous) networks. In the case of a heterogeneous network operating environment, the *NDI* becomes 1. In other words, when an IDC-based network environment and a cloud-based network operation environment are operated simultaneously, the *NDI* corresponds to 1 as a heterogeneous network operation environment.

Table 6 Network diversity index (*NDI*)

Division	Heterogeneous	Multiple	Singular
Criteria	Heterogeneous Network	Multiple Network	Singular Network
NDI	1	0.5	0

Second, the network zone separation index (*ZSI*) is an adequacy evaluation index for network zone separation. Zone separation of the network is a method of applying access control to a group of systems grouped according to purpose or importance, rather than applying access control to each system. It is a necessary method to effectively and efficiently manage access control of numerous systems. It is a method in which the network is operated separately according to internal/external importance, and the separation grade is expressed as an index. For example, a Zone that requires Internet (external) access (usually called DMZ), an internal Zone (Server Zone) that does not require direct access to the Internet, and a Zone that stores only important (confidential) data even in the internal zone (Data) The network is divided into Server Zone or DB Zone. Therefore, according to the purpose and importance of the system, the grade was calculated according to whether the zone was separated so that only the restricted system and users could access it from the inside/outside access zone. This was expressed as the network zoning index *ZSI* (Tab. 7).

Table 7 Zone Separation Index (*ZSI*)

Division	Absent	Insufficient	Suitable
Criteria	Zone not separated	Some separation (Outside/Inside Zone)	Complete Separation (Outside/Inside/ Secret Zone)
ZSI	1	0.5	0

In Tab. 7, if the network zone is not separated, the *ZSI* index becomes '1'. If only the outer and inner zones are partially separated, the *ZSI* index becomes '0.5'. (ex. External Zone & Server zone), In case of separation into server zone and data zone (ex. External Zone, Server zone & Data zone) If zone separation is properly separated, the *ZSI* index becomes '0 '. Third, the control level index (*CLI*) is an index that expresses the appropriateness of the inter-network blocking policy (Rules) divided into zones in terms of the control policy (Rule) management level. In other words, it is an index of whether the control is effectively applied through control equipment such as firewalls. In the Control Level Index (*CLI*), the level of access control (Rules) and the level of control management (Rule management) between separate zones, such as the control level between external and internal zones and the control level between internal zones, was expressed as an index. The index is calculated according to the following criteria.

Table 8 Control level index (*CLI*)

Division	Absent	Insufficient	Suitable
Criteria	No Control	Some Control	Full Control
CLI	1	0.5	0

In Tab. 8, it is classified as "Absent, Insufficient, Suitable" according to the judgment criteria. In the absence of access control such as a firewall, the *CLI* index becomes 1. If some control is performed through various access control systems (firewall, server access control, DB access control, & network access control.), the *CLI* index becomes 0.5. When an appropriate policy is applied and operated through the control equipment, the *CLI* index becomes '0'. The environmental factor (*E*) is proposed by combining these three indices. The environmental factor (*E*) is calculated as in Eq. (10) through the Network Diversity Index (*NDI*), the Zone Separation Index (*ZSI*), and the Control Level Index (*CLI*).

$$E = NDI\left(\frac{(ZSI + CLI)}{2}\right) \tag{10}$$

In the newly established Eq. (10), the level of risk reflecting the security characteristics of individual networks in a heterogeneous network environment can be calculated as shown in Tab. 9 by adding the environmental grade (*E*) index. Also, in an environment other than a heterogeneous network, it can be applied as in Eq. (11) with the *NDI* index removed.

Table 9 Environmental factors (E) Status Table

E		*NDI*								
		0			0.5			1		
		ZSI								
		0	0.5	1	0	0.5	1	0	0.5	1
CLI	0	0	0	0	0	0.125	0.25	0	0.25	0.5
	0.5	0	0	0	0.125	0.25	0.375	0.25	0.5	0.75
	1	0	0	0	0.25	0.375	0.5	0.5	0.75	1

$$E = \frac{ZSI + CLI}{2} \tag{11}$$

Eq. (12) is a risk assessment formula that considers the environmental factor (*E*) presented in this paper, and becomes a risk assessment formula that reflects the environmental characteristics of only various networks.

$$R = (T + V + A) + E$$
$$R = (T + V + A) + \left(NDI\left(\frac{(ZSI + CLI)}{2}\right)\right) \tag{12}$$

In Eq. (12), the environmental factor (*E*) calculated from "Network Diversity Index (*NDI*), network Zone. Separation Index (*ZSI*) and Control Level Index (*CLI*)" was added. The main characteristics of the network operating environment that were not previously considered in risk assessment were reflected in the risk assessment. These three indices have a great influence on risk assessment. However, the actual risk assessment failed to reflect this objectively and logically. Therefore, it is suggested as a way to further improve the logic and objectivity of the risk assessment result by applying the environmental factor (*E*).

4 RESULTS AND DISCUSSIONS

4.1 Comparison of Risk Assessment Methods

Existing risk assessments analyze the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat [30, 31]. The existing risk assessment formula introduced in previous studies is Eq. (13), and the risk assessment formula proposed in this paper is Eq. (14) and Eq. (15).

$$R = (T + V + A) \tag{13}$$

$$R = (T + V + A) + E \tag{14}$$

$$E = NDI\left(\frac{(ZSI + CLI)}{2}\right) \tag{15}$$

Tab. 10 shows the risk calculated through the conventional evaluation formula (Eq. (13)) in a table. In Tab. 10, the range of risk (*R*) calculated through the existing risk assessment Eq. (13) has a total of 7 values (3 - 9).

Table 10 The range of risk calculated through Eq. (13)

Risk1		*T*								
		1			2			3		
		V								
		1	2	3	1	2	3	1	2	3
A	1	3	4	5	4	5	6	5	6	7
	2	4	5	6	5	6	7	6	7	8
	3	5	6	7	6	7	8	7	8	9

The range of the risk (*R*) calculated through the newly proposed risk assessment Eq. (14) can be seen in Tab. 11 "*E* (environmental factor)" has been added, and the range of the result value is (3 ~ 10), which is an increase of "1" compared to the previous one. However, the details of the actual risk value have been expanded from the existing 7 values to 43 values. The range of these values can logically and objectively calculate risk according to *NDI*, *ZSI*, and *CLI*. As shown in Tab. 11, the risk (*R*) is defined as a value between 3 and 10.

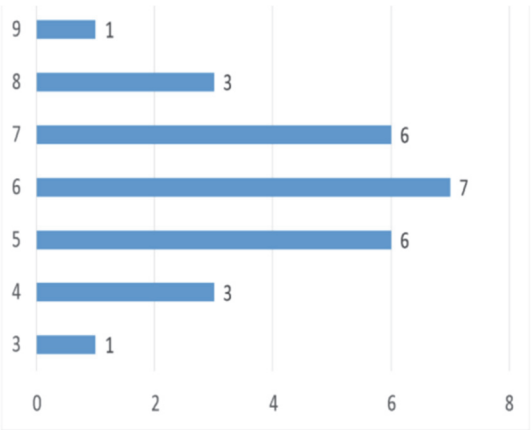

Figure 3 Risk distribution status through Eq. (13)

Fig. 3 is a graph expressing the risk in Tab. 10 as the number of times counted for each risk. That is, the *Y* axis represents the risk ($R = 3 \sim 9$) result value, and the *X* axis represents the number of times the risk (*R*) result value was counted as a graph. It is a method of expressing the distribution of the derived risk in a graph. Fig. 4 is a graph expressing the number of times the risk was counted by each risk level (43) in the Tab. 11. The *Y* axis represents the risk (*R*) result value, and the *X* axis represents the number of times the risk (*R*) result value was counted. This is a method of expressing the distribution of the derived risk (189 including duplicates) in a graph. The part that can be confirmed through this distribution graph is that the existing risk calculates the risk from 7 (3 to 9) values, but in the newly proposed method, detailed risk values are calculated from 43 (3 to 10) values. This risk level provides a level of risk that reflects the characteristics of *NDI*, *ZSI*, and *CLI* for the network operating environment. Therefore, the risk is calculated by minimizing the subjective opinion and human error that lacks consistency. Therefore, it is logically possible to identify the priority and urgency of the derived risk.

Table 11 Risk status calculated through Eq. (14)

R	*T*	1								
	V	1			2			3		
	A	1	2	3	1	2	3	1	2	3
E	0	3	4	5	4	5	6	5	6	7
	0.125	3.125	4.125	5.125	4.125	5.125	6.125	5.125	6.125	7.125
	0.25	3.25	4.25	5.25	4.25	5.25	6.25	5.25	6.25	7.25
	0.375	3.375	4.375	5.375	4.375	5.375	6.375	5.375	6.375	7.375
	0.5	3.5	4.5	5.5	4.5	5.5	6.5	5.5	6.5	7.5
	0.75	3.75	4.75	5.75	4.75	5.75	6.75	5.75	6.75	7.75
	1	4	5	6	5	6	7	6	7	8
R	*T*	2								
	V	1			2			3		
	A	1	2	3	1	2	3	1	2	3
E	0	4	5	6	5	6	7	6	7	8
	0.125	4.125	5.125	6.125	5.125	6.125	7.125	6.125	7.125	8.125
	0.25	4.25	5.25	6.25	5.25	6.25	7.25	6.25	7.25	8.25
	0.375	4.375	5.375	6.375	5.375	6.375	7.375	6.375	7.375	8.375
	0.5	4.5	5.5	6.5	5.5	6.5	7.5	6.5	7.5	8.5
	0.75	4.75	5.75	6.75	5.75	6.75	7.75	6.75	7.75	8.75
	1	5	6	7	6	7	8	7	8	9
R	*T*	3								
	V	1			2			3		
	A	1	2	3	1	2	3	1	2	3
E	0	5	6	7	6	7	8	7	8	9
	0.125	5.125	6.125	7.125	6.125	7.125	8.125	7.125	8.125	9.125
	0.25	5.25	6.25	7.25	6.25	7.25	8.25	7.25	8.25	9.25
	0.375	5.375	6.375	7.375	6.375	7.375	8.375	7.375	8.375	9.375
	0.5	5.5	6.5	7.5	6.5	7.5	8.5	7.5	8.5	9.5
	0.75	5.75	6.75	7.75	6.75	7.75	8.75	7.75	8.75	9.75
	1	6	7	8	7	8	9	8	9	10

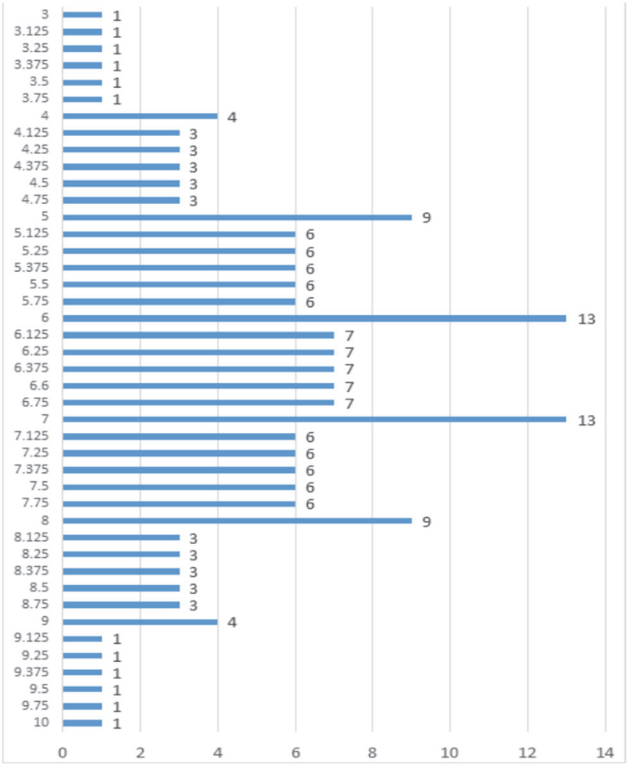

Figure 4 Risk distribution status through Eq. (14)

4.2 Comparison of Risk Assessment Results

In risk assessment, various factors that impair subjective views and consistency should be suppressed, and the results of risk assessment should be compared and verified in a more logical and objective way. Therefore, we want to verify it through the following test case (Test-C). In Test-C, heterogeneous networks exist, and the networks are A-Network configured in Server Room, B-Network configured in IDC, and C-Network configured in Public Cloud. Systems for the same purpose are operating in the networks.

Table 12 Test-C results through Eq. (13)

Division		*T*	*V*	*A*	*R*	*Priority*
A	Web	3	2	2	7	7
	DBMS	3	3	3	9	1
	Network	2	2	1	5	10
	Security	2	3	3	8	4
B	Web	3	2	2	7	7
	DBMS	3	3	3	9	1
	Network	2	2	1	5	10
	Security	2	3	3	8	4
C	Web	3	2	2	7	7
	DBMS	3	3	3	9	1
	Network	2	2	1	5	10
	Security	2	3	3	8	4

Through Eq. (10), the evaluation results as shown in Tab. 12 can be derived. That is, systems with the same purpose located in heterogeneous networks have the same risk. Since there are numerous equal degrees of risk, many of the same imminent risks cannot be identified more readily.

However, Tab. 13 is the result of applying Eq. (15) including environmental factors. Therefore, even for systems with the same purpose operating on different networks, the risk is calculated differently depending on the environmental factors that reflect the characteristics of individual networks. Tab. 14 expresses the general range of the distribution values of the environmental factors (E) for which the *NDI*, *ZSI*, and *CLI* factors were calculated.

Table 13 Test-C Results through Eq. (10)

Division		*NDI*	JSI	*CLI*	*E*
A	Web	1	0.5	0.5	0.5
	DBMS	1	0.5	0.5	0.5
	Network	1	0.5	0.5	0.5
	Security	1	0.5	0.5	0.5
B	Web	1	1	0.5	0.75
	DBMS	1	1	0.5	0.75
	Network	1	1	0.5	0.75
	Security	1	1	0.5	0.75
C	Web	1	1	1	1
	DBMS	1	1	1	1
	Network	1	1	1	1
	Security	1	1	1	1

Table 14 Scope of environmental factor (*E*) evaluation

E	*NDI*	0			0.5			1		
	ZSI	0	0.5	1	0	0.5	1	0	0.5	1
CLI	0	0	0	0	0	0.125	0.25	0	0.25	0.5
	0.5	0	0	0	0.125	0.25	0.375	0.25	0.5	0.75
	1	0	0	0	0.25	0.375	0.5	0.5	0.75	1

Tab. 15 shows the calculation results for the new risk assessment including the environmental factor (*E*) in Test-C. The number of systems used in Tab. 12 and Tab. 15 is 12. However, in the field where numerous systems are operated in an actual company, if numerous systems existing between different heterogeneous networks exist at the same risk level, there are problems that cannot take immediate action on an urgent risk target. This is because it is not easy to classify the risks.

Table 15 Test-C results through Eq. (14)

Division		*T*	*V*	*A*	*E*	*R*	*Priority*
A	Web	3	2	2	0.5	7.5	9
	DBMS	3	3	3	0.5	9.5	3
	Network	2	2	1	0.5	5.5	12
	Security	2	3	3	0.5	8.5	6
B	Web	3	2	2	0.75	7.75	8
	DBMS	3	3	3	0.75	9.75	2
	Network	2	2	1	0.75	5.75	11
	Security	2	3	3	0.75	8.75	5
C	Web	3	2	2	1	8	7
	DBMS	3	3	3	1	10	1
	Network	2	2	1	1	6	10
	Security	2	3	3	1	9	4

By applying the environmental factor (*E*) on the network presented in this paper to risk assessment, human error and subjective opinion intervention can be minimized, and more objective and logical risk assessment can be performed. In addition, it provides the advantage of being able to effectively and efficiently respond to risks by identifying high-risk risks at an early stage. In Tab. 16, the risk (*R*) and priority (Priority) of 12 systems existing on the network (*A*, *B*, *C*) are indicated.

Table 16 Test-C Comparison of risk assessment results (Eq. (13) vs. Eq. (14))

Division		Eq. (10)		Eq. (11)	
		R	*Priority*	*R*	*Priority*
A	Web	7	7	7.5	9
	DBMS	9	1	9.5	3
	Network	5	10	5.5	12
	Security	8	4	8.5	6
B	Web	7	7	7.75	8
	DBMS	9	1	9.75	2
	Network	5	10	5.75	11
	Security	8	4	8.75	5
C	Web	7	7	8	7
	DBMS	9	1	10	1
	Network	5	10	6	10
	Security	8	4	9	4

In addition, the results derived from Tab. 17 were compared with the level of risk (*R*), the number of systems with the corresponding level of risk (*Quantity*), and the priority (*Priority*). Through Tab. 16 and Tab. 17, the risk level and priority can be compared intuitively. The risk level of the existing systems of different heterogeneous networks is expressed as a more objective and logical result in the Eq. (11) result. Therefore, it is possible to take measures with high urgency first through these results. In other words, it is possible to establish a more optimal risk action plan than the existing measures by using the resources (manpower, budget, technology, & time) of the company.

Table 17 Test-C Risk distribution and priorities (Eq. (13) vs. Eq. (14))

Eq. (10)			Eq. (11)		
R	*Quantity*	*Priority*	*R*	*Quantity*	*Priority*
5	3	10	5	-	
			5.5	1	12
			5.75	1	11
6	-		6	1	10
			6.5	-	
			6.75	-	
7	3	7	7	-	
			7.5	1	9
			7.75	1	8
8	3	4	8	1	7
			8.5	1	6
			8.75	1	5
9	3	1	9	1	4
			9.5	1	3
			9.75	1	2
			10	1	1

5 CONCLUSION

Currently, it is an era in which legacy operating environments (IDC, DC, Computer rooms, & Server rooms) and operating environments using various cloud services coexist. The heterogeneous network operating environment is rapidly increasing. However, the factors for evaluating the risk that exists in a heterogeneous network are the same. In other words, the risk assessment method is used through "Vulnerability score, Asset importance and Threat factors (VAT) ". However, there is a problem in that the risk assessment results for systems with the same purpose existing on a heterogeneous network are calculated the same every time when risk assessment is performed using only the relevant factors (VAT). In addition, when prioritizing risks to effectively deal with

numerous risks, numerous systems with the same priority exist. Three shortcomings were drawn from the existing risk assessment. First, the existing risk assessment formula is insufficient to reflect the characteristics of the controlled environment of each network because it calculates the risk level centered on each individual asset. Second, if the same system with the same purpose is located in a heterogeneous network, the same risk is calculated without considering factors other than VAT. Third, it is difficult to quickly and logically identify really urgent risks among risks calculated through risk assessment in a heterogeneous operating environment where numerous systems are operated. In this proposed method, various factors were reviewed to solve these problems, and an index called environmental factor (*E*), which combines three indices, was discovered. The three indices are "Network Diversity Index (*NDI*), network Zone Separation Index (*ZSI*) and Control Level Index (*CLI*)". *NDI* expressed the network diversity as a simple index. *ZSI* express the network complexity as a simple index. *CLI* expressed the network controllability as a simple index. Environmental factors (*E*) are calculated through "*NDI*, *ZSI* and *CLI*" and can be applied to the existing risk assessment. The benefit of using the environmental factor (*E*) index is that it allows for a more objective risk assessment that takes into account numerous environmental factors such as the network's operational environment. Even when the same system for the same purpose is located in heterogeneous networks, the optimized risk level reflecting the characteristics of each individual network is calculated. Lastly, in an environment in which numerous systems are operated, it is possible to quickly take action against risks by referring to priorities. The risk assessment method including the environmental factor (*E*) proposed in this paper reflects the various environmental characteristics of the network, which were insufficient in the existing risk assessment. It provides more objective and logical risk assessment results in a heterogeneous network environment. Through this, it is a logical method that has the advantage of being able to check the results of risk assessment that practitioners can logically and quickly judge, and to quickly and effectively deal with risks with high urgency. In this study, there is a limitation that is not based on lots of data collected in real heterogeneous mobile networks. This study intends to continue research from two perspectives in the future. First, it is necessary to conduct a comparative study on lots of results obtained through the existing risk assessment method and the proposed risk assessment method in the existing heterogeneous mobile network environment. Second, factors not considered in environmental factors (*E*) are reviewed by analyzing various results of applying the proposed risk assessment in a real heterogeneous mobile network environment.

Acknowledgements

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ICAN (ICT Challenge and Advanced Network of HRD) program (IITP-2024-2020-0-01825) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

6 REFERENCES

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2009). Above the clouds: A Berkeley view of cloud computing.

[2] Salameh, A., Zarina, M., & Wan, S. (2019). Impact Aspects of IT Flexibility Specific to Cloud Computing Adoption on IT Effectiveness. *Journal of Theoretical and Applied Information Technology*, *97*(3).

[3] Lim, H. C., Babu, S., Chase, J. S., & Parekh, S. S. (2009). Automated control in cloud computing: Challenges and opportunities. *ACDC '09: Proceedings of the 1st Workshop on Automated Control for Datacenters and Clouds, Barcelona, Spain*. 13-18. https://doi.org/10.1145/1555271.1555275

[4] Sandipan B. (2016). A Study on Selection of Data Center Locations. *International Journal of Innovative Research in Computer and Communication Engineering*, *4*(8).

[5] Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management*, *30*(2), 109. Retrieved from ABI/INFORM Global. https://doi.org/10.1016/j.ijinfomgt.2009.09.004

[6] Accenture and WSP Environment & Energy (2010). Cloud computing and Sustainability: The Environmental Benefits of Moving to the Cloud. Technical Report, Nov.

[7] Mostofa, A., Kendall, E., Rahul, G., Md Minhaz, C., & Nafiz, R. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning-A Review. *Journal of Cybersecurity and Privacy*, *2*, 527-555. https://doi.org/10.3390/jcp2030027

[8] Federal Emergency Management Agency (FEMA) (2005). *FEMA 452, Risk Assessment, A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings*.

[9] NIST (2012). *Information Security-Guide for conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, 4-36.

[10] ISO/IEC 27005 (2018). *Information technology Security techniques - Information security risk management*. Third edition, 8-15.

[11] Kang, D., Lee, J., Lee, Y., Lee, I., & Kim, H. (2013). Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power Industry, *Journal of The Korea Institute of Information Security and Cryptology*, *23*(3), 445-457. https://doi.org/10.13089/JKIISC.2013.23.3.445

[12] Gary, S., Alice, G., & Alexis, F. (2002). Risk Management Guide for Information Technology Systems-Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, *800-30*, 8-26.

[13] Alberts, C., Behrens, S., Pethia, R., & Wilson, W. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVESM) Framework, Version 1 (CMU/SEI-99-TR-017, ADA367718)*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

[14] Alberts, C. & Dorofee, A. (2001). *OCTAVE Criteria, Version 2.0 (CMU/SEI-01-TR-020, ADA396654)*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

[15] Richard, A., James, F., Lisa, R., & William, R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

[16] ISO/IEC 31000 (2018). Risk Management Guidelines.

[17] ISO/IEC 31010 (2019). Risk assessment techniques.

[18] Ensia (2022). Risk Management Standards.

[19] ETSI (2017). CYBER; Methods and protocols Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA), ETSITS 102 165-1 v5.2.3.

[20] Kim, I. & Park, N. (2019). Quantitative Cyber Security Scoring System, Based on Risk Assessment Model. *Journal*

of The Korea Institute of Information Security and Cryptology, *29*, 1179-1189.
[21] Ahn, J., Chang, B. M., & Lee, E. Y. (2015). Quantitative Scoring System on the Importance of Software Vulnerabilities. *Journal of The Korea Institute of Information Security and Cryptology*, *25*, 921-932. https://doi.org/10.13089/JKIISC.2015.25.4.921
[22] FIRST (2019). Common Vulnerability Scoring System (CVSS), v.3.1.
[23] NIST (2022). Measuring the Common Vulnerability Scoring System Base Score Equation. https://doi.org/10.6028/NIST.IR.8409.ipd
[24] MITRE (2014). Common Weakness Scoring System (CWSS), v1.0.1.
[25] Lee, W., Chung, M., Min, B. G., & Seo, J. (2015). Risk Rating Process of Cyber Security Threats in NPPI&C. *Journal of The Korea Institute of Information Security and Cryptology*, *25*, 639-648. https://doi.org/10.13089/JKIISC.2015.25.3.639
[26] Kim, S. K., Oh, S., Kang, H., Kim, J., & Kim, H. K. (2018). Risk Scoring System for software vulnerability Using Public Vulnerability Information. *Journal of The Korea Institute of Information Security and Cryptology*, *28*, 1449-1461.
[27] Betty, E., Biringer, R., Matalucci, V., & Sharon, L. O. (2007). Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures, ch 1.2, 6-7.
[28] KISA (2002), Vulnerability analysis evaluation model.
[29] ISACA (2004). Guide to Information Security Management System Risk Management, ISACA Korea Chapter.
[30] Chunlin, L., Chong-Kuan, T., & Yea-Saen, F.. (2012). The Security Risk Assessment Methodology. *International Symposium on Safety Science and Engineering in China (ISSSE-2012)*, 600-609. https://doi.org/10.1016/j.proeng.2012.08.106
[31] Federal Emergency Management Agency (FEMA) (2003). FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, Dec. 2003.

Contact information:

Youngjun KIM
Busan University of Foreign Studies,
46234 65, Geumsaem-ro 485-gil, Geumjeong-gu, Busan, Republic of Korea
E-mail: 20229804@bufs.ac.kr, yjkim412@gmail.com

Namkyun BAIK
(Corresponding author)
Duksung Women's University,
01369 Samyang-ro, Dobong-gu, Seoul, Republic of Korea
E-mail: namkyun@duksung.ac.kr, researchnamkyunbaik@gmail.com