Security Risk Assessment System Based on the Similarity to Victims

Masahito Kumazaki
Graduate School of Informatics
Kyoto University
Kyoto, Japan
e-mail: kumazaki@inet.\
media.kyoto-u.ac.jp

Hirokazu Hasegawa
Center for Strategic
Cyber Resilience R & D
National Institute of Informatics
Tokyo, Japan
e-mail: hasegawa@nii.ac.jp

Hiroki Takakura
Center for Strategic
Cyber Resilience R & D
National Institute of Informatics
Tokyo, Japan
e-mail: takakura@nii.ac.jp

***Abstract*—In the current situation where the damage caused by targeted attacks is becoming more serious, it is important to minimize their damage through early detection and response. However, there are problems with speed and coverage in the investigation methods based on suspicious IP addresses and Indicators of Compromises(IoC), which are common responses. Therefore, we propose a security risk assessment system based on the similarity to victims. This system uses elements other than IP addresses and IoCs, such as used software and logged-in users, and assesses the possibility of intrusion based on similarity to the victim. In this paper, we show the effectiveness and potential of this system by evaluating it using a prototype.**

Keywords-cyber security, risk assessment, incident response

I. INTRODUCTION

In the current situation where the damage caused by targeted attacks is becoming more serious, it is important to minimize their damage by improving detection and response measures. In particular, many researchers have been discussing various proposals for detection methods aimed at minimizing damage.

In general, responders collect attack traces such as suspicious IP addresses from the victim and devices on the attack route, and also collects Indicator of compromises (IoC) from the provider on the internet. Based on the information collected in these ways, they estimate the scope of the intrusion and the attack technique, and attempts to minimize the damage. However, the following problems exist with this method.

- Coverage of suspicious IP addresses
- Reliability of IoC providers
- Time required for information collection

Therefore, we propose a system for assessing the security risk of neighboring terminals using the similarity to the victim. In this paper, "security risk" refers to the possibility that other terminals will be attacked using the same techniques as the victim. The system uses the user's input to collect information on victim and neighboring terminals from various sources and assess the security risk of neighboring terminals. The system can assess the scope of the intrusion earlier than existing IP address/IoC-based methods, making it possible to minimize the damage. In addition, even in situations where little information is available about an attack, such as a zero-day attack, it is possible to predict the occurrence of damage by using a device with a configuration similar to the device that was first affected.

The outline of this paper is as follows. In Section 2, we introduce related works from the perspectives of security risk assessment and attack detection, and point out the issues that exist in them. Section 3 describes the system we propose, and Section 4 performs a simple evaluation using a prototype. We discuss the improvements to the system in Section 5, and we present our conclusions and future works in Section 6.

II. RELATED WORK

In existing studies on security risk assessment, researchers have assessed risk from a variety of perspectives. The first perspective is risk assessment focusing on important assets within an organization. Kumar et al. proposed a framework called integrated Cybersecurity Risk Management (i-CSRM) that identifies important infrastructures, assesses the risk of vulnerabilities in those infrastructures, and evaluates the safety of current operations[1]. From another perspective, there is also study on risk assessment that focuses on the costs required to implement security measures. Lee proposed a framework that realizes the optimal security improvement procedure by estimating the existing threats and economic losses used these, as well as the necessary costs for countermeasures, based on the situation inside and outside the organization[2]. There are also studies that focus on physical and human factors. Ganin et al. pointed out that existing risk assessment methods based on threats, vulnerabilities and consequences[3][4] do not cover physical or social vulnerabilities, and proposed a framework using multi criteria decision analysis (MCDA) to cover them[5]. There is also study that focuses on the possibility of a intrusion to the terminal, which is the same perspective as ours, such as Sugimoto et al.[6]. They assess the security risk of each device from three points of view: accessibility to the device, the number of routes, and the scope of the intrusion after the attack, in order to determine the priority of dealing with vulnerabilities. These studies function as a pre-emptive measure against attacks, and do not discuss the security risk in response to detection. In terms of post-detection response, it is important to minimize the scope of the intrusion and the damage it causes, so it is necessary to evaluate the risk from the perspective of being able to achieve this and in a short period of time.

Other related study of proposed is attack detection. Since the proposed system is used repeatedly from the initial stage of attack response, it is assumed that there will be a conflict with the timing of use with existing attack detection technology. Some of these studies includes improving detection accuracy using intrusion detection systems (IDS)[7][8] and security

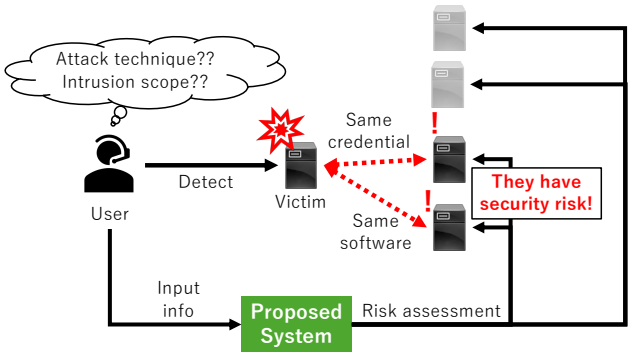

Figure 1. Proposed system's concept

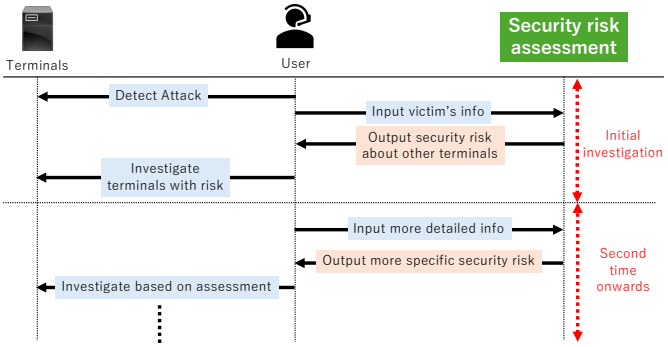

Figure 2. Proposed system's usage flow

information and event management (SIEM)[9][10]. Studies using these systems may show effectiveness in detection, but this does not necessarily mean they are effective in response. Mohsenabad et al. showed that it is possible to improve the detection accuracy of IDS by selecting feature values used in machine learning based on various algorithms[7]. However, the detection results of IDS at this time are limited to information such as victim and attack techniques, so additional investigation is required to learn the details of the attack. In such cases, users can learn about the security risks of the neighboring terminals by entering the IDS's result into the proposed system, and they can narrow down the scope of their investigation based on this information. In this way, we consider that our system does not conflict with these attack detection technologies, but rather coexists with them.

III. Proposed System

A. Outline

We propose a risk assessment system for neighboring terminals based on the similarity of victims. The Figure 1 shows the concept of proposed system. We assume that users of this system are people who are familiar with networks and security, such as those who respond to security incidents. If the user detects an attack, they will want to know the details of the attack and the scope of the intrusion, but this takes time and effort. In such cases, the user inputs the victim's information into the proposed system, and the system assesses the security risk of the neighboring terminals based on similarities to the victim (e.g. same users, same software, etc.). In this way, the system supports the user's response by narrowing down the scope of the investigation and providing information about vulnerabilities that may exist in the terminals.

The Figure 2 shows system usage. This system is designed to support users in their repeated use of the system from the initial stage of an investigation. In the initial investigation, it supports narrowing down the terminals that have security risk and used attack techniques, based on the limited information. In the second time onwards, the users can input more detailed info, so the system also outputs more accurate information on the scope of intrusion, attack techniques and vulnerability information to them.

B. Assumption

The proposed system collects various information about the terminal in order to evaluate similarity. So we assume that devices providing services such as asset management, firewalls, and file servers exist with in the range accessible from this system.

In addition, this system is designed to be used in an attack response. Of course, it is best to be aware of the security risk of all terminals in advance. However, given the large number of terminals and the easy introduction of terminals such as mobile devices, this is unrealistic. Therefore, this system is designed to be used in an attack response and to be useful for investigating terminals and vulnerabilities that have not been identified at that time.

In this proposal, the user can specify the range of assessments by defining a neighboring terminal as a terminal with a number of network hops from the victim that is less than or equal to a threshold. If the user use the system for a specific segment (e.g. server segment), they can set the threshold to 1. If the user expect an intrusion into another segment, they can adjust the threshold accordingly, and apply the system to any range them want.

When the user confirms a security incident, the system assesses the security risk of neighboring terminals through user input. The system focuses on the following attack stages and outputs the attack techniques and vulnerability risks associated with them.

- External intrusion that has occurred
- Lateral movement from the victim

However, as this paper is initial prposal, we will only discuss external intrusion. Therefore, this paper does not discuss lateral movement such as intrusion into other services from the victim.

C. System Architecture

The risk assessment system consists of four modules as shown in Figure 3. It performs input and output with users in the dialogue module, and the other modules collect information and assesses security risks in response to the input in the dialogue module.

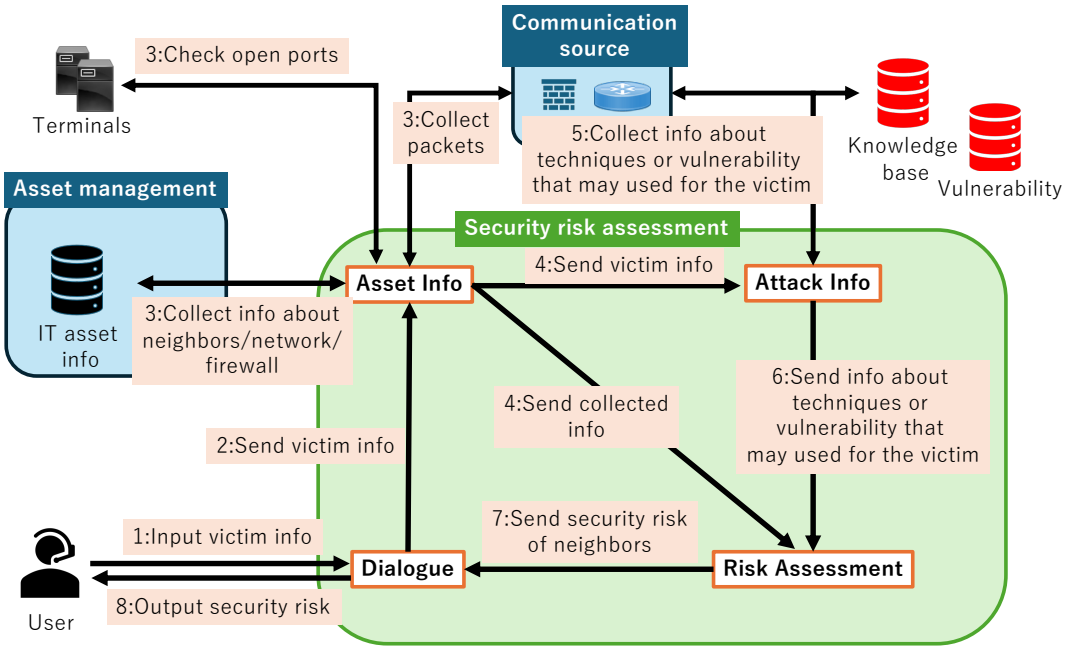

Figure 3. Proposed system's architecture

TABLE I. INPUT BY USER

Contents		Required or Optional
Threshold for neighbors		Required
Occurrence time		Optional
Victim info	IP address	Required
	Role	Optional
	Admin account	Optional
Attacked software/hardware		Optional
Used technique/vulnerability		Optional

1) Dialogue Module: The Dialogue Module receives input about the victim information from users and outputs the results of the assessment of security risks to users. Table I shows the victim information that the user enters. With regard to the input, the threshold for neighbors and the victim IP address are required, and the rest are optional. If a user inputs optional information such as attacked software or used techniques, the module attaches a "Used" tag. Regarding the "Used" tag, the Asset/Attack Info Module collects information only for the software/techniques with that tag.

The module sends these information to the Asset Info module.

2) Asset Info Module: The Asset Info module collects asset information with in an organization. The Figure 4 shows functions and flow of operation. The module works in the following way.

- Receive the victim's information from the victim
- Collect information about the victim and network around it from the asset management system
- Based on the information about the network around the victim, determines which devices are neighboring devices
- Collect following information

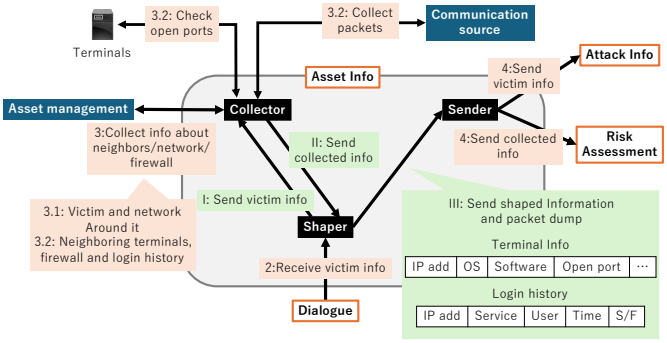

Figure 4. Functions and operation flow of Asset Info module

  - From asset management system: Neighboring terminals, firewall rule and login history of each service
  - From Terminals: Open ports
  - From communication source: Mirroring packets
- Send shaped information to each module

3) Attack Info Module: The Attack Info module collects information about the techniques and vulnerabilities that could be used for the victim. The module receives information about the victim from the Asset Info module. This information includes the victim's operating system and software, service login history on the victim, etc.. Based on the information, the module collects the security holes that exist in the victim by the following ways.

- Based on the open ports, services and login history, the module collects the related attack techniques from vulnerability

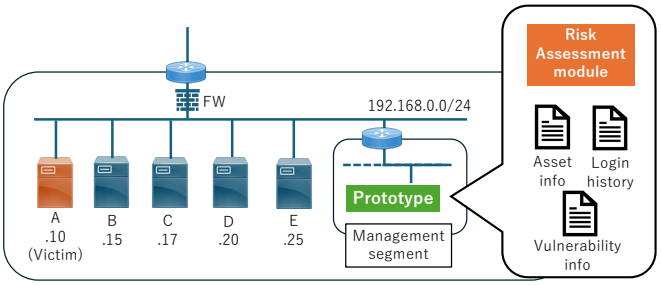

Figure 5. Assumed network in evaluation

knowledge base such as MITRE ATT&CK[1]

- Based on the OS and software, the module collects vulnerabilities from vulnerability databases such as the National Vulnerability Database (NVD)[2]

The module shapes the collected information in a form that includes IDs and their requirements, and sends it to Risk Assessment module. As we pointed out in Section 1, there is very little publicly available information on zero-day attacks, so information based on the NVD is not mandatory.

4) Risk Assessment Module: This module assesses the security risk of neighboring terminals based on the information received from each module. The information sent from Asset Info module contains data about neighboring terminals and victims, and the information sent from Attack Info module contains information about each attack that could occur on the victim. The module assesses the risk of each attack for each neighboring terminal. If the user enters the attack technique or vulnerability used in the Dialogue module, the module also assesses its risk.

In this paper, security risks are classified into three levels: *high*, *medium*, and *low*. For each technique or vulnerability, the module assesses the security risk for each terminal as follows.

- The terminal satisfies the requirements for the method or vulnerability: *high*
- There are similarities with the victim in multiple contexts (e.g. software used, login history, etc.): *medium*
- Otherwise: *low*.

Finally, the module sends the results of the assessments to the Dialogue Module.

IV. Evalution

In order to evaluate the proposed system, we implemented and tested a prototype of the Risk Assessment module. Since Asset Info and Attack Info modules have not been implemented yet, their outputs were prepared in advance and provided as inputs for the Risk Assessment module.

A. Evaluation Method

The figure 5 shows the assumed network in the evaluation. There were 5 terminals in the assumed network. Terminal A was the first victim, and Terminals B, C, D, and E were on the same network segment, i.e., a hop count of 0.

[1]https://attack.mitre.org/
[2]https://nvd.nist.gov/

TABLE II. Asset Info in evaluation

Terminal	IP address	OS	Software	Open ports
A	192.168.0.10	Windows	WordPress, 5.8	22,80
			OpenSSH, 9.7	
B	192.168.0.15	Windows	WordPress, 6.0	22,80
			OpenSSH, 9.9	
C	192.168.0.17	Windows	WordPress, 5.9	80
D	192.168.0.20	Windows	OpenSSH, 9.7	22
E	192.168.0.25	Windows		22,80

TABLE III. Login history (Only terminals A and B)

Terminal	Service	User	Time	S/F
192.168.0.10	OpenSSH	Alice	2025/2/3 10:23:51	S
		Hack	2025/2/4 00:31:20	F
		Hack	2025/2/4 00:31:21	F
		Hack	2025/2/4 00:31:21	F
	WordPress	Alice	2025/2/4 10:25:14	S
		Bob	2025/2/4 13:08:05	S
192.168.0.15	OpenSSH	Bob	2025/2/3 13:41:35	S
		Black	2025/2/4 01:20:54	F
		Black	2025/2/4 01:20:54	F
		Black	2025/2/4 01:20:55	F
	WordPress	Bob	2025/2/4 13:08:05	S

The prototype of Risk Assessment module was on the terminal in the management segment. As we explained, the information sent from the Asset Info and Attack Info modules is prepared as JSON files in advance. These json files also existed on the terminal in the management segment. The Asset Info file contained information about A, B, C, D, and E, the Login History file contained login histories for the services provided on each terminal, and the Vulnerability Info file contained information about the vulnerabilities that may exist on A. The contents of each file are shown in Tables II, III and IV respectively. Based on the input from these files, the prototype performed a risk assessment using the method shown in Section III-C4, and output the result as a json file.

B. Evaluation Result and Findings

The output result is shown in Figure 6 and Table V. Regarding the vulnerability CVE-2024-6387, the prototype of Risk Assessment module is thought to assess the risk of each terminal for the following reasons.

- B: This terminal used the same software as A and the login history was similar, so the risk was *medium*.
- C: This terminal didn't use the OpenSSH that was a requirement, so the risk was *low*.
- D: This terminal satisfied requirements (used the OpenSSH and this version was less than 9.8), so the risk was *high*.
- E: It was not known what software was used on this terminal. However, from the information about open ports and softwares of A, B and D, the prototype estimated that E

TABLE IV. Attack Info in evaluation

ID	Requirement	
CVE-2024-6387	Software: OpenSSH	Version: <9.8
CVE-2022-21661	Software: WordPress	Version: <5.8.3

TABLE V. SECURITY RISK ASSESSMENT RESULTS AND REASON ASSUMPTIONS

Vulnerability	CVE-2024-6387			
Terminal	B	C	D	E
Risk	*medium*	*low*	*high*	*high*
Reason	Similarity in software and login status	No similarity	Satisfy requirement	Satisfy requirement (possibly)
Vulnerability	CVE-2022-21661			
Terminal	B	C	D	E
Risk	*low*	*low*	*low*	*high*
Reason	No similarity	No similarity	No similarity	Satisfy requirement (possibly)

```
{
    "CVE-2024-6387":[
        {"192.168.0.15":"medium"},
        {"192.168.0.17":"low"},
        {"192.168.0.20":"high"},
        {"192.168.0.25":"high"}
    ],
    "CVE-2022-21661":[
        {"192.168.0.15":"low"},
        {"192.168.0.17":"low"},
        {"192.168.0.20":"low"},
        {"192.168.0.25":"high"}
    ]
}
```


Figure 6. Output file after evaluation

used OpenSSH. Because the version was unknown, there was a possibility that E satisfied the requirements for vulnerability. So the risk was *high*.

Regarding the vulnerability CVE-2022-21661, the prototype is thought to assess the risk of each terminal for the following reasons.

- D: This terminal didn't use the WordPress that was a requirement, so the risk was *low*.
- E: From the information about open ports and softwares of A, B and C, the prototype estimated that E used WordPress. Because the version was unknown, there was a possibility that E satisfied the requirements for vulnerability. So the risk was *high*.
- Other terminals: They used WordPress but these version were more than 5.8.3. B and D didn't satisfied requirements and the similarities only existed at the OS and software, so the risk was *low*.

As a result, it was confirmed that proposed the system can assess the risk of attacks with clear requirements, such as vulnerabilities that depend on specific softwares and versions. Even when the software used on the terminal is unknown, the system was able to assess the risk by estimating from the service operating status of other terminals. It's thought that this is because there were many terminals providing similar services on the same port in this evaluation. Even when there are few terminals opening the same port, it is necessary to estimate the provided services and the software of the terminal. As a future work, we are planning to make use of well-known ports and etc. to enable such estimation.

In addition, the current prototype only assesses security risks based on user login history, service operation status, etc., for vulnerabilities and attack techniques that do not have clear requirements. In this case, the prototype can only assess risks as *medium* or *low*. As a future work, we will consider improving the prototype so that it can assess the risk of such attacks by adding up the similarity of each element.

V. DISCUSSION

This system evaluation showed that the proposed system is effective in assessing risk from external attacks. However, we have not conducted a quantitative evaluation and have not been able to show how effective the proposed system compared to previous studies. There are two problems in comparing the proposed system with previous studies.

- The previous studies focused on risk assessment before attacks. The proposed system cannot be simply evaluated because it is assumed to be used while responding to attacks.
- The previous studies on attack detection do not cover the steps after the detection of an attack. This system is expected to be effective in response after detection.

Based on these issues, we consider the following comparisons.

- Risk assessment: Evaluation of how close to the accuracy of previous studies in the short time available during response to an attack.
- Attack detection: Comparison of the time required to respond to an attack using the proposed system with that of the previous studies.

In addition, we define a neighboring terminal as a terminal with a number of network hops from the victim that is less than or equal to a threshold, in order to specify the range of assessments by the user. However, in actual network configurations, there are many cases where users don't know how many hops there are from the victim in the range they want to check. On the other hand, the more huge the network becomes, the more difficult it becomes to investigate everything within the network. In future work, we will improve the definition of neighboring terminals so that users can more easily set the range they want to search.

Furthermore, the proposed system omits the aspect of ease of access to the equipment in assessing the security risk. Since this paper only focuses on external attacks, we assumed that all targets are accessible from the outside (i.e., easily accessible). When this system assesses the risk of lateral movement in

internal network, ease of access will be an important metric. (e.g.: The system evaluates only the risk of lateral movement for terminals that can only be accessed from the internal network. This evaluates both external attack and lateral movement risks for terminals that can be accessed externally.)

VI. Conclusion and Future Work

In this paper, we propose a system for assessing the security risk of neighboring terminals using the similarity to the victim. This system can assess the scope of the intrusion from the beginning of the investigation, and it is possible to minimize the damage compared to existing IP address and IoC-based methods. In addition, we evaluated the prototype and demonstrated its potential and effectiveness. As a result, when there were many terminals providing similar services on the same port, it was confirmed that proposed system can assess the risk of attacks with clear requirements. However, there are some issues on the following.

- When there are few terminals opening the same port, the system can't accurately assess the risk for terminals that lack information.
- The system cannot assume that the risk is high for vulnerabilities and attack techniques that do not have clear conditions.

In order to solve these issues, we will work on the following for the Risk Assessment module.

- Use well-known ports, etc. to estimate the services provided by the terminal.
- Improve the prototype so that it can accurately assess the risk of vulnerabilities and techniques that don't have clear requirements.

In addition, this paper only focuses on external attacks and does not consider lateral movement. There are two possible routes of compromise to the terminal in a real attack: external attack and lateral movement. This system should be able to handle both of these attack tactics. In addition to the topics in the Discussion section, there are the following issues.

- Comparison with previous studies in terms of accuracy and time required
- Improve the definition of neighboring terminals so that users can more easily set the range they want to check
- Implement other modules and conduct evaluations in a form that is more suited to the system architecture
- Development of a risk assessment that includes lateral movement

In future work, we will solve the above issues.

Acknowledgement

This work was partially supported by JSPS KAKENHI Grant Number JP24K14959.

References

[1] N. Kumar, V. Poonia, B.B. Gupta and M.K. Goyal, "A novel framework for risk assessment and resilience of critical infrastructure towards climate change," Technological Forecasting and Social Change, Vol. 165, 2021.

[2] I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," Business Horizons, Vol. 64, No. 5, pp. 659-671, 2021.

[3] R. A. Caralli, J. F. Stevens, L. R. Young, and W.R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," Hansom AFB, MA, 2007.

[4] A. Ashok, M. Govindarasu, "Cyber-physical risk modeling and mitigation for the smart grid using a game-theoretic approach," 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1-5,2015

[5] A. A. Ganin, P. Quach, M. Panwar, Z.A. Collier, J.M. Keisler, D. Marchese, and I. Linkov, "Multicriteria decision framework for cybersecurity risk assessment and management," Risk Analysis, Vol. 40, No. 1, pp. 183-199, 2020

[6] A. Sugimoto, Y. Isobe and H. Nakakoji, "Risk Assessment Based on Intrusion Routes of Cyber Attacks," Journal of Information Processing (JIP), Vol. 57, No. 9, pp. 2077-2087, 2016. (In Japanese)

[7] H. N. Mohsenabad and M. A. Tut, "Optimizing cybersecurity attack detection in computer networks: A comparative analysis of bio-inspired optimization algorithms using the CSE-CIC-IDS 2018 dataset," Applied Sciences, Vol. 14, No. 3, 2024.

[8] A. Raza, K. Munir, M. S. Almutairi, and R. Sehar, "Novel class probability features for optimizing network attack detection with machine learning," IEEE Access, 2023.

[9] R. Marri, S. Varanasi, and S. V. K. Chaitanya, "Integrating Next-Generation SIEM with Data Lakes and AI: Advancing Threat Detection and Response," Journal of Artificial Intelligence General science (JAIGS), Vol. 3, No. 1, pp. 446-465, 2024.

[10] A. R. Muhammad, P. Sukarno and A. A. Wardana, "Integrated security information and event management (siem) with intrusion detection system (ids) for live analysis based on machine learning," Procedia Computer Science, Vol. 217, pp. 1406-1415, 2023