Journal of Information Processing Vol.31 802–811 (Dec. 2023)

[DOI: 10.2197/ipsjjip.31.802]

Regular Paper

The Attacker Might Also Do Next: ATT&CK Behavior Forecasting by Attacker-based Collaborative Filtering and Graph Databases

Masaki Kuwano[1,a)] Momoka Okuma[1,b)] Satoshi Okada[1,2,c)] Takuho Mitsunaga[1,d)]

Received: March 8, 2023, Accepted: September 11, 2023

Abstract: Cyber attacks are causing tremendous damage around the world. To protect against attacks, many organizations have established or outsourced Security Operation Centers (SOCs) to check a large number of logs daily. Since there is no perfect countermeasure against cyber attacks, it is necessary to detect signs of intrusion quickly to mitigate damage caused by them. However, it is challenging to analyze a lot of logs obtained from PCs and servers inside an organization. Therefore, there is a need for a method of efficiently analyzing logs. In this paper, we propose a recommendation system using the ATT&CK technique, which predicts and visualizes attackers' behaviors using collaborative filtering so that security analysts can analyze logs efficiently. We evaluated the proposed method using real-world cyber-attack cases and found that it is able to make predictions with higher recall than our previously proposed method.

Keywords: MITRE ATT&CK, Collaborative Filtering, Attack Prediction, Graph Database

1. Introduction

In recent years, the number of cyber-attacks has been increasing, and various companies and organizations have been affected. According to the FBI [2], in the past five years from 2017 to 2021, the number of reported cybercrimes has increased from 301,580 to 847,376 and the amount of damage from $1.4 billion to $6.9 billion.

In a situation where cyber attacks are increasing rapidly, and the damage is expanding, organizations must fully leverage SOC capabilities to counter cyber attacks. However, according to a survey of 127 organizations conducted in 2021 by SANS [3], a security professional organization, many organizations face the challenges of "the lack of skilled staff in the SOC" and "lack of automation and orchestration". For these reasons, the problem is that it takes some time to respond to attacks. SOC analysts mainly use Security Information and Event Management (SIEM) tools to detect attacks. However, SIEM cannot predict the signs of the next attacks based on the information already acquired. Therefore, they have to analyze huge amounts of logs without any clues.

MITRE began research to detect APTs more quickly, and as part of this research, ATT&CK was published [4]. ATT&CK data contains 133 "groups", 191 "techniques" and 14 "tactics" targeting enterprises (v11, April 25, 2022). It is known from ATT&CK data that each group has attack characteristics. The characteristic is the techniques which are used in combination. When an attack is detected, if the combination of techniques is similar to the combination of techniques used by a particular group, that factor can be used for attack prediction.

Many e-commerce sites have a recommendation system that suggests items and services that may suit users' tastes. A recommendation system can predict future purchasing behavior based on an analysis of the user's purchase history [5]. This system is based on the following idea. Users who have purchased a similar set of products in the past are considered similar users. The system compares products that a user purchased against a similar user's purchase history to suggest an item that is most pertinent to the user.

Replacing with ATT&CK, each group can be considered as a user, and techniques used by that group can be considered as a user's purchase history. Thus, just as with e-commerce sites, it is possible to predict which techniques an attacker may use in the future, based on the techniques already detected. In this paper, we propose a recommendation system for attack forecasting using the results of collaborative filtering. Security logs generally contain data about system and network activity. Visualizing these data improves SOC analysts' ability to analyze individual data and their relationships by using graphs [6]. It also enables them to detect anomalous patterns of attackers' activities. Visualization of security logs makes it easier for SOC analysts to under-

[1] Toyo University, Kita, Tokyo 115–8650, Japan
[2] The University of Tokyo, Bukyo, Tokyo 113–8656, Japan
[a)] s1f101902152@iniad.org
[b)] s1f102000871@iniad.org
[c)] okada-satoshi323@g.ecc.u-tokyo.ac.jp
[d)] takuho.mitsunaga@iniad.org

The preliminary version of this work [1] appeared in the 2nd IEEE Computing Conference 2022 (ICOCO 2022). This paper extends the contribution by adding the improving of collaborative filtering algorithm (Section 4 and Section 5.2) and comparative performance analysis between algorithms with additional test data sets (Section 6).

stand the data and quickly identify anomalous activity for quick response and minimization of damage. Therefore, our proposed system also provides visualization of the attacker's behavior and will assist SOC analysts in their work.

1.1 Our Contribution

In the previous work [1], we proposed a method to predict attacker behavior using ATT&CK and collaborative filtering and quantitatively confirmed that it was able to predict an attacker's behaviour with a high degree of accuracy. In this paper, we further improve this method and confirm its generality through additional experiments. We describe the overview of the main contributions of this paper.

- In the machine learning model implemented within our proposed method, we identified a better value for the hyperparameter to improve the performance of our proposed algorithm.
- By introducing Weighted-k-Nearest-Neighbor (WkNN) instead of k-Nearest-Neighbor (kNN) used in the previous study [1], we succeeded in improving the prediction accuracy of our proposed method.
- We utilized a larger set of test data compared to the previous study [1]. In every case, our method accurately predicted attacks, thereby proving its versatility and broad applicability.

2. Preliminary

2.1 ATT&CK

ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge and is a knowledge base provided by MITRE, a non-profit organization in the U.S. ATT&CK consists of five elements: Adversary Group (Group), Software, Technique, Tactic, and Mitigation, where Group is an attacker, Software is a tool used by the attacker, Technique is the technology used in the attack, Tactic is the objective to be achieved by technique, and Mitigation is a measure to mitigate against the attacks. **Figure 1** visualizes the relationship between these five elements.

2.2 Collaborative Filtering

Collaborative filtering is an inference method often used for recommendation and personalization in e-commerce sites. There are three types of collaborative filtering: memory-based, model-based, and hybrid, with memory-based further divided into user-based and item-based [8]. User-based recommends products based on the similarity of purchase history between users. In this paper, we assume that if an attacker, presumed from an observed technique, is similar to a particular ATT&CK group, then the attacker is likely to use the same technique as that group. **Figure 2** is an example of user-based collaborative filtering for recommendations to User C. Users A, B, and C purchased items 1 and 2, item 3, and item 2 respectively. Since User A and User C have purchased Item 1 in common, the system judged that User A and User C are relatively similar and suggested Item 3 to User C.

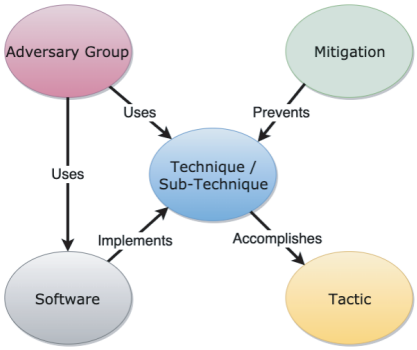


Fig. 1 Components of ATT&CK [7].

2.3 k-nearest-neighbor and Weighted-k-nearest-neighbor

Since the k-nearest neighbor (kNN) was first introduced by Fix and Hodges [10], it has become a widely used classifier in pattern classification. The basic idea of kNN is that an unclassified object is assigned to the class, represented by a majority of its k nearest neighbors in the training set. **Figure 3** shows an example for k=4. The unknown data is classified into Class A because the class is the highest percentage of the four nearest data belonging to it. The distance-weighted k-nearest neighbor (WkNN), which weighs more heavily close neighbors based on their distances to the query object, was proposed by Dudani [11].

WkNN considers distance as a weight in the majority vote process, giving more weight to those that are closer in distance. Depending on the target data, WkNN can produce better results than kNN [12]. When using kNN and WkNN, careful attention must be paid to choosing an appropriate value of k. While research has

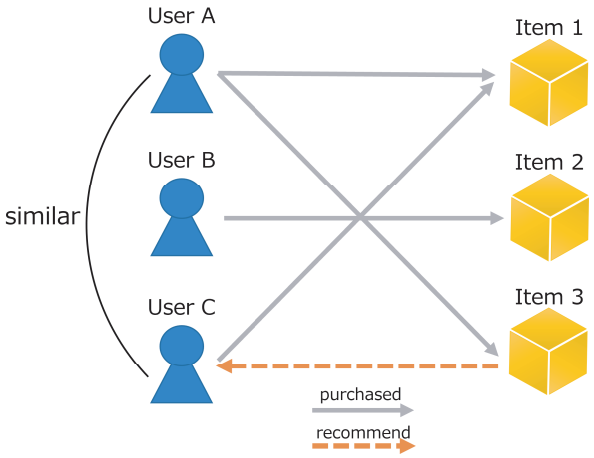


Fig. 2 User-based collaborative filtering example.

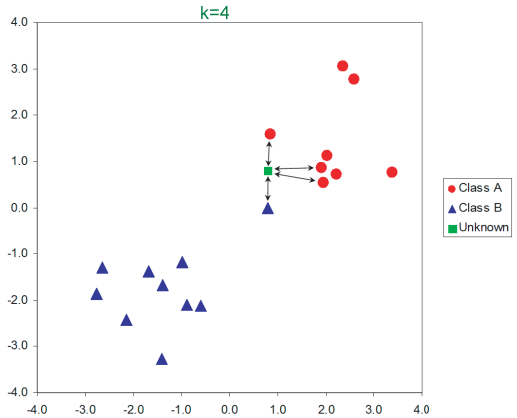


Fig. 3 kNN example [9].

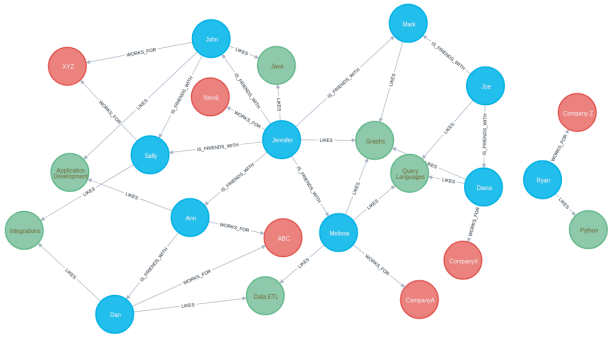


Fig. 4 Graph database example [17].

been conducted on how to determine the optimal k for any kind of data, it is yet to be resolved to determine it. For instance, k from 20 to 50 is appropriate in the real world [13], on the other hand, the square root of the data size is appropriate for k [14]. Overfitting and underfitting occur depending on the value of k. If k is too large, it will be affected by data with low similarity and noise [13]. It becomes more sensitive to values and can reduce the quality of predictions [13].

Similarity measures for k-Nearest-Neighbor include Sorensen-Dice coefficient (SDC), Jaccard index (JI) and Overlap coefficient (OLC). JI may not give the correct value when there is a large difference in the number of elements in the given set [15]. In this paper, JI is not suitable since the analysis is intended to cover from 1 to 25 elements. OLC takes a high value such as 1.0, if one set is a true subset of the other. All attackers using an observed particular technique result in a similarity of 1.0. Therefore, OLC is unsuitable for our research because it is difficult to calculate the similarity among attackers. Based on the suitability, we use SDC as a similarity measure. SDC(A, B) for sets A and B is defined by the following equation.

$$SDC(A, B) = \frac{2|A \cap B|}{|A| + |B|} \tag{1}$$

2.4 Graph Database

A graph database is based on a graph structure consisting of three elements: nodes, edges, and properties. Nodes represent entities, edges represent relationships among nodes, and properties represent attribute information of nodes and edges. Graph databases can visualize data relationships. In this paper, neo4j [16] is used to create the graph database. **Figure 4** is an example of a graph database.

3. Related Works

There are various types of attack prediction methods in cyber security. Husák et al. [18] classified prediction methods into four categories based on theoretical background: discrete models, continuous models, machine learning and data mining, and others in their survey. A graphical representation of an attack scenario is called an attack graph, which is classified as a discrete model.

Polatidis et al. [19] applied a recommendation system to the attack graph. They used collaborative filtering to predict attacks on attack graphs created based on information provided by the maritime supply chain infrastructure, Common Weakness Enumeration (CWE), and Common Vulnerabilities and Exposures (CVE). Sadlek et al. [20] and Cho et al. [21] conducted research on cyber attack prediction, combining the cybersecurity framework Cyber Kill Chain and ATT&CK. Sadlek et al. [20] proposed the kill chain attack graph, which combines the cyber kill chain and attack graph. The proposed approach can predict the sequence of actions of an attacker in a network. This allows administrators to check the kill chain phases and decide on countermeasures to mitigate possible cyber threats. They combine not only the cyber kill-chain to create the attack graph but also ATT&CK and STRIDE, a threat analysis model. However, the problem is the complexity of the multiple types of data that are input to create the graph. Cho et al. [21] proposed a new cyber kill chain model and developed Cyber Common Operational Picture (CyCOP), which is based on the model and visualizes the situation in cyberspace in real time. The proposed model uses MITRE CAPEC and MITRE ATT&CK to classify threats into attack tactics and techniques at each phase in the cyber kill chain. Their proposed method can aid in the prediction of cyber attacks. These two studies did not evaluate the forecasting results, and their accuracy is not known.

Studies [22] and [23] use ATT&CK data for collaborative filtering, with the aim of assisting SOC analysts in their analysis. Elitzur et al. [22] proposed an approach to improve analysts' hypotheses about ongoing attacks by using a recommendation algorithm on the Cyber Threat Intelligence (CTI) graph and the ATT&CK knowledge graph. First, the analyst creates attack hypotheses based on the ATT&CK technique and the tools attacker used. Subsequently, recommendations made from the hypothesis and past attack cases are used to modify the hypotheses. However, since the analyst-created hypotheses are used as input for the recommendations, the results may be affected by the analyst's skill in creating the hypotheses. Brisse et al. [23] have developed a visualization system based on knowledge-based recommendations called KRAKEN. They intended to add function to a tool called ZeroKit [24] that enables analysts to visualize data during log analysis and incident response. ATT&CK technique and tactic are used as the knowledge base, but they are reclassified into items on Zerokit. Both of these two studies incorporate ATT&CK knowledge into the recommendation system. However, they include CTI and tool data not only ATT&CK technique.

Al-Shaer et al. [25] focused on the ATT&CK technique and proposed a novel approach using hierarchical clustering to show the relationships among techniques from attack data in the ATT&CK. Their study shows that it is possible to predict adversarial behavior from observed techniques, which can be directly applied to attack diagnosis and threat mitigation. However, there are no specific methods of real-world application. Katano et al. [26] proposed a method to find secondarily infected devices by lateral movement from an initially infected device using the quantification theory type 3 and the ATT&CK technique. Lateral movement is one of the ATT&CK tactics. This method connects the logs of each device to the ATT&CK technique and determines the infected device based on the similarity of the logs. The results show that it is possible to characterize the devices by using the ATT&CK technique. Munaiah et al. [27] conducted a research aimed at helping developers and system administrators develop an offensive security perspective in penetration testing.

In this research, the approach used by attackers to find and exploit vulnerabilities was systematized using ATT&CK. The study showed that an attacker's campaign can be characterized as a time series of ATT&CK tactic and technique. Studies Al-Shaer et al. [25], Katano et al. [26], and Munaiah et al. [27] showed that the ATT&CK technique can be used for characterization and that there is a relationship between techniques.

Kuwano et al. [1] proposed a recommending and predicting system for ATT&CK techniques based on attacker characteristics, with the purpose of assisting the SOC analyst. The system recommends a technique by collaborative filtering based on the similarity between the techniques used by the attacker who is currently conducting an ongoing attack and the techniques used in the past by the ATT&CK group. The recommended techniques can be considered as the techniques that the attacker is likely to use in the later stage of the attack flow. Their approach was able to predict techniques with high recall, specificity, and accuracy.

However, their research has some problems. The first is that verification of k in kNN is insufficient. The second is that they have only one data set to evaluate their proposed method. In addition, their test data contains only 12 different techniques, so it is not clear whether their method has general applicability.

4. Preliminary Experiment

Kuwano et al. (2022) were about predicting attacks based on ATT&CK and achieving high detection accuracy, however, there were two issues to be solved as mentioned in the previous section. In this paper, we first conduct a preliminary experiment on the issues to solve the issue (1) to clarify the appropriate value k with the dataset of Kuwano et al. (2022) in this section, and we will propose an improved method to solve the issue (2) with additional datasets in Section 5.

(1) Kuwano et al. (2022) use a value of 40 for k of kNN. However, they have not verified whether this 40 is appropriate. Therefore, it is necessary to verify which value is appropriate for k in the proposed method.

(2) They perform performance evaluations based on a single data set using 13 different techniques. It has not been shown whether their proposed method is effective against large-scale attacks (eg. an attack case that contains over 20 Techniques).

4.1 Evaluation Method

The method proposed by Kuwano et al. (2022) is the following. Groups and techniques from the ATT&CK data are used as training data for collaborative filtering. The input is a set of techniques that have already been detected in the ongoing attack, and the output is a set of techniques recommended by collaborative filtering. We refer to the ongoing attackers using those techniques as "adversary" here. If a technique is newly detected, predicting a technique in the previous stage's tactics, that is, a technique in the previous stage of the attack flow does not help detect subsequent attacks. Therefore, attack predictions and analysis targets are assumed to be included after the most late-stage tactics observed at that time.

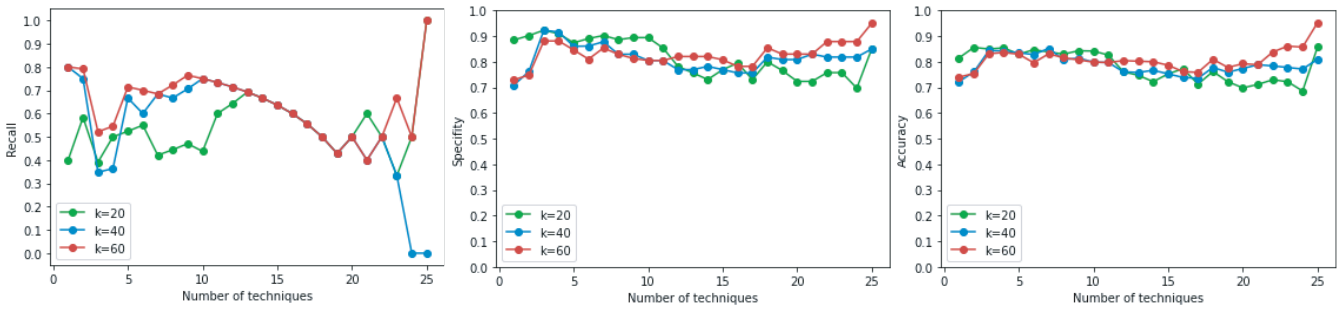
For the evaluation, Kuwano et al. (2022) used an attack scenario described in the Security Alert published by Cyber security and Infrastructure Security Agency (CISA), a U.S. government agency, for two reasons. The first reason is that the scenario has been used by attackers in the wild, and is designed to be neutral in evaluating the research. The second reason is that it is not included in the training data of research, ATT&CK v11 (April 25, 2022) since the Alert.

As well as them, we use a report [28] published by CISA that describes a large-scale attack as our evaluation data. This report was published on October 4, 2022, when CISA responded to APT attack against the enterprise network of an organization in the Defense Industrial Base sector for three months. It lists 26 different techniques and is considered a sufficiently large cyber attack. In addition, in order to find the appropriate k, we also try the case where the k values are set to 20, which is about 1/6, 40, which is 1/3, and 60, which is 1/2, of the 133 groups registered in the ATT&CK. Using that report, we predict with Kuwano et al. (2022) method and calculate recall, specificity, and accuracy from the results.

4.2 Results and Discussion

Figure 5 shows a graph representing the relationship between the number of techniques inputted and the recall, specificity, and accuracy.

First, we focus on recall. The best value is at k=60 until the number of inputted techniques is fourteen. After that, the number of inputted techniques is lowered to almost twenty for any value of k. Then it rises again at k=20 and k=60, decreases at k=40, and finally, the recall is zero. However, any k value will have a



(a) Recall (b) Specificity (c) Accuracy

Fig. 5 Result of Preliminary experiment.

lower recall value after the middle of the attack, decreasing its usefulness.

Next, about specificity and accuracy. When k=40 and k=60, the values of specificity and accuracy are extremely low when the number of inputted techniques is one and two. In the method of Kuwano et al. (2022), k groups with similarity will sometimes not be gathered depending on the inputted techniques. Therefore, if the number of inputs is a few, recommendations will be made based on groups that are not similar, which increases FPs.

The results show that k=60 is appropriate for increasing recall, and Kuwano et al. (2022) method is not applicable to large-scale attacks. They used user-based collaborative filtering as a recommendation engine and used the standard kNN algorithm. Therefore, by changing the value of k and using WkNN, which uses similarity, we assumed that recall would increase after the midpoint of the attack. That would also reduce the number of recommendations when sufficient similarity is not calculated, thereby reducing the number of FPs and increasing specificity and accuracy.

5. Proposed Method

In this paper, we propose a method to recommend undetected techniques based on the result of the preliminary experiment. How we predict the adversarial behavior is described in Section 4.1. Generally, collaborative filtering does not consider the order of items. However, in our case, we use ATT&CK techniques as the items, and these techniques belong to ATT&CK tactics. Since tactics represent the sequence of attacks, even though our collaborative filtering is performed on techniques, we can still interpret the results with consideration for the attack sequence.

Furthermore, in our proposed method, techniques recommended by the proposed method are considered attack predictions and visualized as a graph database. They can assist the SOC analyst in log analysis. The flow from techniques recommendation to visualization is shown in **Fig. 6**. The proposed method is an improvement of the method of Kuwano et al. (2022) based on the experiments in the previous section. WkNN is used as the algorithm for user-based collaborative filtering, and the value of k is set to 60, and the threshold is changed accordingly.

5.1 Data Set

We obtained data on the groups and the techniques which they have used in the past from the ATT&CK website [29]. From the obtained data, we created a table with rows for the group name and columns for the technique name and set 1 if the group used that technique and 0 if it did not. **Table 1** shows a part of the dataset.

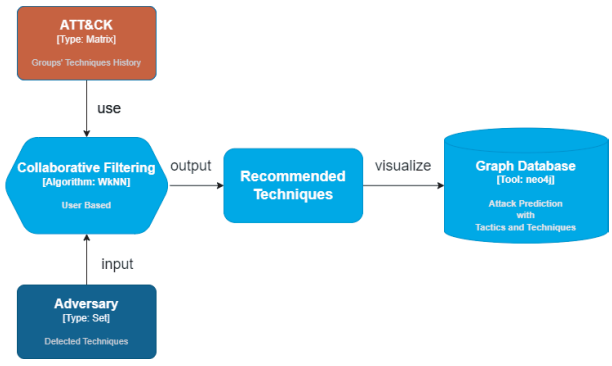


Fig. 6 Recommendation Flow.

5.2 Recommendation System

Technique recommendations we implemented are follows. We show the pseudocode of our proposed method in Algorithm 1. In the following, we explain the overview of this algorithm.

(1) For newly detected techniques, prepare a dataset with used techniques set to 1 and unused techniques set to 0. The dataset represents the behavior of the adversary with shapes corresponding to each row of the ATT&CK dataset (Table 1). **Table 2** shows a part of the adversary dataset.

(2) The similarity (mentioned as $Similarity$ in Algorithm 1) between the adversary and each group is calculated by SDC.

(3) The top k groups (k=60 in this case) with high SDC are considered similar to the adversary.

(4) Support rate ($SupportRate$ in Algorithm 1) is calculated by

Table 1 Some of the data sets used (excerpt).

	T1059	T1583	T1203	T1531	T1083
G0018	1	0	1	0	1
G0006	0	1	0	0	0
G0026	1	0	0	0	1
G0007	1	1	1	0	1
G0060	1	0	1	0	1

Table 2 An example of the adversary dataset (excerpt).

	T1059	T1583	T1203	T1531	T1083
Adversary	1	0	1	0	0

Algorithm 1 Our recommendation algorithm

```
Gall ← DataSetRowsList
Tall ← DataSetColumnsList
Adversary ← AdversaryDataSet
K ← N                                   {K is an arbitrary natural number.}
KSimilarGroups[] ← NIL
GroupsSimilarity[] ← NIL                {This is key-value data.}
RecommendedTechniques[] ← NIL
for group in Gall do
    Similarity ← SDC(Adversary,group)
    GroupsSimilarity[group] ← Similarity
end for
KSimilarGroups ← List of the Top k groups with the highest Similairty
from the result of sorting GroupsSimilarity.
for technique in Tall do
    Score ← 0
    for group in KSimilarGroups do
        Similarity ← GroupsSimilarity[group]
        if Similarity ≠ 0 then
            d ← 1 - Similarity
            Score ← Score + (1/d)(technique[group])
        end if
    end for
    SupportRate ← (1/K)(Score)
    if SupportRate ≥ threshold then
        RecommendedTechniques.add(technique)
    end if
end for
```

summing the product of the binary values in the dataset (Table 1) and the corresponding "weights", and then dividing by k. In WkNN, one of the weighting functions is $\frac{1}{d}$ when d means the distance of a pair of neighbors [11]. In our algorithm, we calculate d by $1-Similarity$. That is because when neighbors are similar to each other (the value of *similarity* is large) their distance should be small. Furthermore, the weight($=\frac{1}{d}$) becomes much larger as $Similarity$ closer to 1. On the other hand, when neighbors are not similar to each other at all ($Similarity = 0$), we set the weight to 0. By setting weights in this way, we can more effectively reflect the values of the similarity in the weights.

(5) Techniques with a support rate higher than a threshold (0.17 in this case) are selected as the recommended techniques.

5.3 Visualization

There are two graph databases that represent attack predictions, group-based and tactic-based. An example of the visualization of attack predictions is shown in **Fig. 7** and **Fig. 8**. In the report used in the previous chapter, four techniques T1078 (Valid Accounts), T1047 (Windows Management Instrumentation), T1059 (Command and Scripting Interpreter), T1129 (Shared Modules) were inputted. Group-based is shown in Fig. 7. Figure 7 shows the detected techniques (inputs) in the red circle and the recommended techniques (outputs) in the yellow circle, as shown in the **Table 3**. In addition, the attacker groups are shown in the blue circle as reference information for the analysis. Figure 8 shows the tactic-based prediction. It is made from Fig. 7 and contains techniques included after the most late-stage tactic observed, tactics, and detected techniques. Tactics are represented in the cyan circle. 29 techniques were predicted to be used later, and 136 techniques were predicted not to be used.

Table 3 Description of nodes.

Node Color	Type
Red	Detected Techniques (Input)
Blue	ATT&CK Groups
Yellow	Recommended Techniques (Output)
Cyan	ATT&CK Tactics

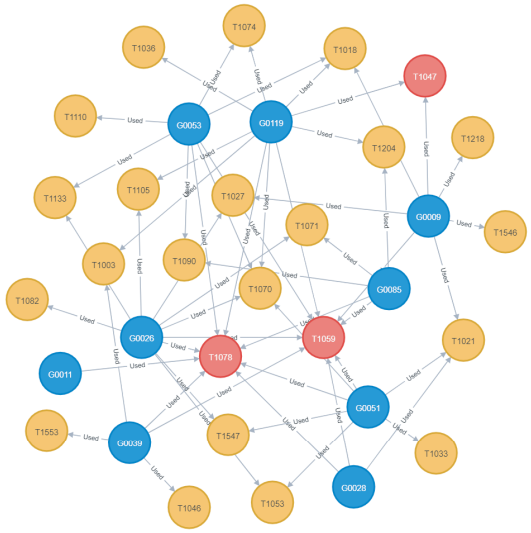


Fig. 7 Group-based attack prediction (exerpt).

6. Evaluation

We use report (AA22-174A) [30] as test data in addition to the report used in Section 4 (AA22-277A) [31] and the report used in Kuwano et al. (2022) (AA22-138B) [28]. Although AA22-138B lists 13 techniques, one of them is classified as a tactic prior to initial access, which is before the attacker enters the organization's network and cannot be handled by the SOC operator. 12 techniques are used for the forecast, excluding that one. The details of the report are summarized in **Table 4**. For each test data set, we perform predictions using Kuwano et al. (2022) and the proposed method and compare the results.

6.1 Performance Metrics

The evaluation results are categorized as follows.

- True Positive (TP): Number of techniques predicted to be used in the attack and actually used.

Table 4 CISA alert used as test data.

Alert	title	total techniques
AA22-277A [28]	Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization	26
AA22-138B [31]	Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control	13(12)
AA22-174A [30]	Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems	13

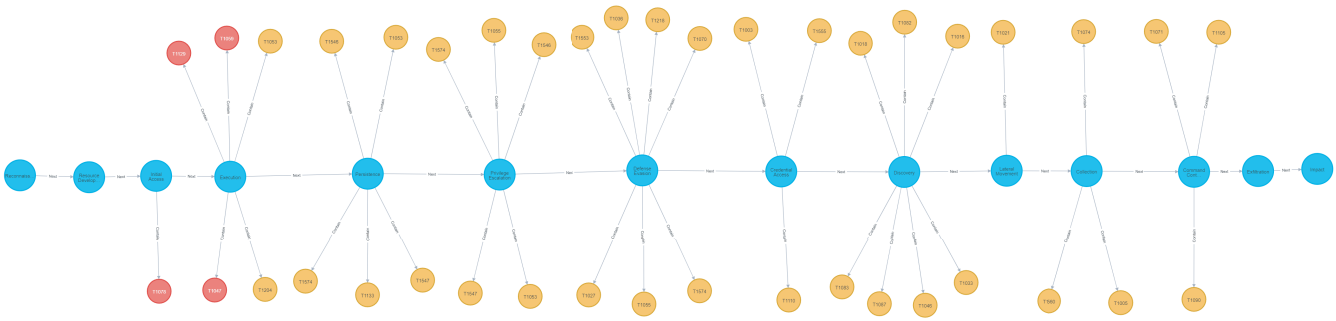
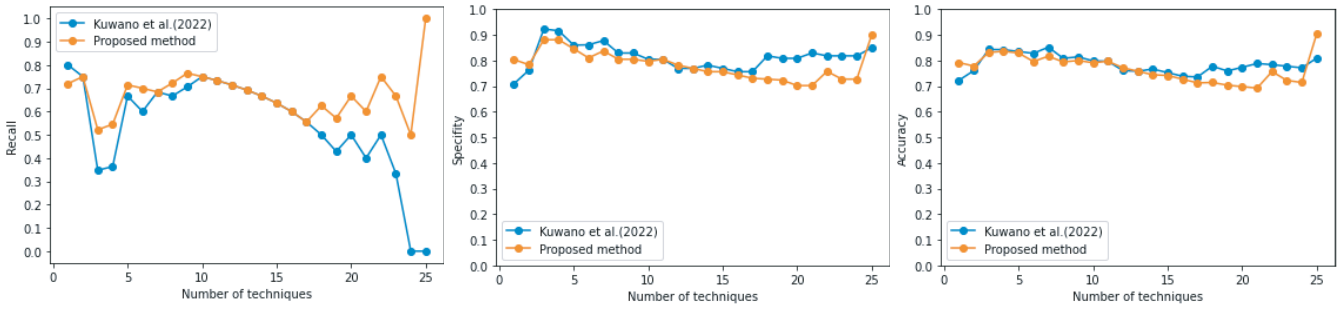
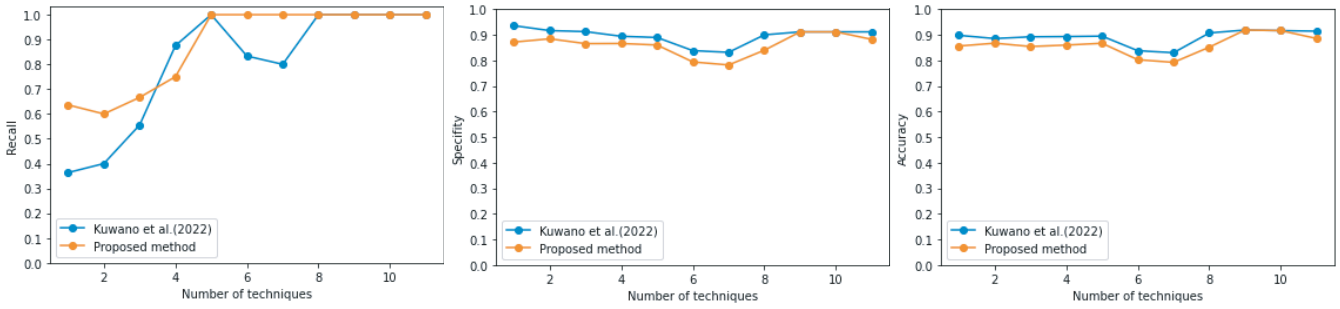


Fig. 8 Tactic-based attack prediction.



(a) Recall (b) Specificity (c) Accuracy

Fig. 9 Comparison of proposed method and Kuwano et al. (2022) forecasting results (AA22-277A).



(a) Recall (b) Specificity (c) Accuracy

Fig. 10 Comparison of proposed method and Kuwano et al. (2022) forecasting results (AA22-138B).

- False Positive (FP): Number of techniques predicted to be used in the attack but not actually used.
- True Negative (TN): Number of techniques not predicted to be used in the attack and not actually used.
- False Negative (FN): Number of techniques not predicted to be used in the attack but actually used.

In this paper, We used recall, specificity, and accuracy to evaluate the prediction. They are defined by the following equations.

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$Specificity = \frac{TN}{TN + FP} \tag{3}$$

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{4}$$

- Recall: Percentage of techniques used in attacks that could be predicted to be used in attacks.
- Specificity: Percentage of techniques that could be predicted not to be used in attacks that were not used in attacks.
- Accuracy: Percentage of techniques that are correctly predicted to be used or not.

6.2 Evaluation Method

The following procedures were used to evaluate the results.

(1) Create the adversary dataset with all technique columns set to 0.
(2) Select one technique in the CISA report in tactic order and set its technique column in the adversary dataset to 1.
(3) Create attack predictions from techniques recommended by collaborative filtering.
(4) Calculate TP, FP, TN, FN, recall, specificity and accuracy from prediction results.
(5) Repeat steps (2) through (4) until the number of technique inputs reaches the number of techniques in each report minus one.
(6) Recall, specificity and accuracy are plotted as a graph along with the number of techniques inputted.

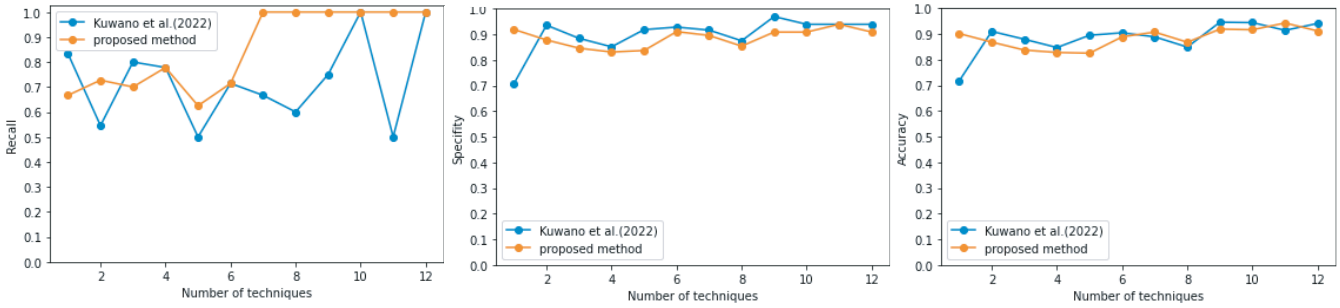
Furthermore, we compare the results of our proposed method with those of Kuwano et al. (2022). The reason why we compare our method with only Kuwano et al.'s method is as follows: the previous studies listed in Section 3 (except Kuwano et al. (2022)) that made some predictions about cyber attacks have a different combination of input data and output results than ours. Therefore, we cannot fairly compare our proposed method with them.

6.3 Results

Figures 9, **10** and **11** show the relationship between the number of input techniques and recall, specificity, and accuracy respectively. Furthermore, **Tables 5**, **6** and **7** show the number of input techniques, predicted techniques, TPs, FPs, TNs, and FNs by using the proposed method.

6.4 Discussion and Future works

In Fig. 9, the proposed method shows better recall values than Kuwano et al. (2022), especially in the later stages of the attack flow. As shown in Section 4, a higher number of k tends to increase the number of recommended techniques. WkNN is a distance weighting method, and techniques with high similarity are assumed to be preferentially recommended by using WkNN. For example, T1567 (Exfiltration Over Web Service) is rarely recommended by Kuwano et al. (2022) because there are only a few groups using it. However, it is appropriately suggested by the proposed method based on WkNN. The recommendation of



(a) Recall (b) Specificity (c) Accuracy

Fig. 11 Comparison of proposed method and Kuwano et al. (2022) forecasting results (AA22-174A).

Table 5 Confusion matrix (AA22-277A).

Input	Prediction	TP	FP	TN	FN
1	47	18	29	119	7
2	49	18	31	112	6
3	29	12	17	126	11
4	29	12	17	126	10
5	37	15	22	121	6
6	40	14	26	111	6
7	33	13	20	103	6
8	37	13	24	99	5
9	37	13	24	99	4
10	37	12	25	98	4
11	35	11	24	99	4
12	27	10	17	61	4
13	27	9	18	60	4
14	27	8	19	59	4
15	26	7	19	59	4
16	26	6	20	58	4
17	26	5	21	57	4
18	20	5	15	40	3
19	17	4	13	34	3
20	18	4	14	33	2
21	17	3	14	33	2
22	11	3	8	25	1
23	11	2	9	24	1
24	10	1	9	24	1
25	3	1	2	18	0

Table 6 Confusion matrix (AA22-138B).

Input	Prediction	TP	FP	TN	FN
1	27	7	20	136	4
2	24	6	18	138	4
3	26	6	20	129	3
4	25	6	19	123	2
5	26	7	19	117	0
6	34	6	28	108	0
7	27	5	22	79	0
8	12	4	8	42	0
9	6	3	3	31	0
10	5	2	3	31	0
11	5	1	4	30	0

Table 7 Confusion matrix (AA22-174A).

Input	Prediction	TP	FP	TN	FN
1	21	8	13	148	4
2	27	8	19	137	3
3	31	7	24	132	3
4	32	7	25	123	2
5	27	5	22	113	3
6	10	5	5	51	2
7	11	6	5	43	0
8	12	5	7	41	0
9	7	4	3	30	0
10	6	3	3	30	0
11	4	2	2	31	0
12	4	1	3	30	0

techniques with high similarity improves the recall value. Recall means how correctly we predicted "positive" as "positive"; in other words, how correctly we predicted the techniques used by attackers and how little we overlooked. High recall is required in the fields of medical and cyber security, where positive data should not be overlooked. It covers a wide range of techniques likely to be used by attackers and can reduce the scope of logs to be analyzed.

However, as described in Section 5, it is important to note that the population of expected attacks and expected targets, the data on which Figs. 9, 10 and 11 are based, are assumed to be included after the most late-stage tactic observed at that time.

In specificity and accuracy, when the number of inputted techniques is one or two, the values are higher than those in Kuwano et al. (2022). This is because the use of W*k*NN eliminates recommendations from non-similar groups among the k groups.

In Figs. 10 and 11. Overall, we can see that the recall values are higher than those of Kuwano et al. (2022). The specificity and accuracy values are a little lower than Kuwano et al. (2022), but are consistently higher than 0.8. We explain why we did not see improvements in specificity and accuracy. We focused on improving recall and actually succeeded in doing so. As a result, we observed a few cases where FP values were slightly larger than with the Kuwano et al. (2022) method. However, we also succeeded in increasing TN values in some cases. Thus, despite the increase in FP, the values of accuracy and specificity remain high without a significant decrease compared to the previous work. Although there are some problems, our newly proposed method is general and can predict the ATT&CK technique with high recall. Therefore our recommendation system enables analysts to perform log analysis efficiently.

A limitation exists in the proposed method. Five techniques, T1129 (Shared Modules), T1497 (Virtualization/Sandbox Evasion), T1039 (Data from Network Shared Drive), T1095 (Non-Application Layer Protocol), and T1029 (Scheduled Transfer) in AA22-277, could not be predicted by either Kuwano et al. (2022) nor by the proposed method. This is because these techniques were used in fewer of the 133 groups: 0 groups for T1129, 6 groups for T1497, 7 groups for T1039, 7 groups for T1095, and 1 group for T1029. That is called the cold-start problem in collaborative filtering, where appropriate recommendations cannot be made when there are no previous evaluations of items or users. According to Ref. [32], the cold start problem occurs in the following three cases.

(1) Recommending existing items for new users
(2) Recommending new items for existing users
(3) Recommending new items for new users

As a solution to (1), it may be possible to solve this problem by combining rules related to techniques that are often used in advance. (2) and (3) are difficult to solve with the proposed method. However, it may be possible to predict these problems if the data in ATT&CK is updated and more information on groups and techniques is available.

There are three challenges for future work. The first is to reduce the number of FPs. The solution to this depends on the early stage of the attack and the middle or late stage of the attack. In the early stages of the attack, there is a high probability that techniques with high original utilization will be recommended. Therefore, instead of using collaborative filtering in such a case, we can improve the prediction results by recommending a combination of frequently used techniques based on a rule that is determined in advance. For FPs that occur in the middle or later stages of the attack, it may be possible to improve the results by recommending not only user-based collaborative filtering but also a combination of different algorithms, such as item-based collaborative filtering. In fact, according to the results of Ref. [33], the prediction error of combining User-based and Item-based recommendations is smaller than that of the two algorithms alone.

The second is to optimize the parameters dynamically. In the proposed method, there are two parameters: k and threshold in WkNN. The k determines how many groups to recommend based on, and the threshold determines the number of technique recommendations. By using WkNN, if the number of techniques to be input increases and the similarity increases, the number of recommendations may become too large if the threshold is constant. Therefore, it is necessary to dynamically optimize the threshold, and the optimal k value may change accordingly.

The third is the practical use of the proposed method by SOC analysts. When using the proposed method in practice, it is necessary to correlate the logs with the ATT&CK techniques. For example, a tool like Atomic Red Team [34] can be used to associate a log with a technique, but it must be done manually. This task is highly dependent on the analyst's skill and can be time-consuming. Although the proposed method can predict attacks, we could not evaluate the analysis time in this paper. It is necessary to experiment whether the results of this paper can be used in practice when considered in the time of the entire analysis, including techniques associations.

7. Conclusion

SOCs are required to respond quickly to cyber attacks. However, PCs and servers generate a huge number of logs, and analyzing them without any clues takes a lot of time. Attack prediction has the potential to reduce the time required for log analysis by identifying logs.

In this paper, We proposed a recommendation system for the ATT&CK technique, which is an improvement of Kuwano et al. (2022). We apply user-based collaborative filtering to the observed ATT&CK techniques and the techniques used by the ATT&CK group in the past, perform technique recommendation, predict attacker behavior using the results, and visualize the results as a graph database.

We evaluated the proposed method using publicly available ATT&CK analysis reports and confirmed that the proposed method can predict techniques with high recall when a certain number of techniques are inputted. We also confirmed that the proposed method is general by using multiple test data. The results are better than our previously proposed method. The proposed method enables analysts to predict attacks by inputting ongoing attacks and to analyze logs efficiently.

However, there is still room for improvement. It could be improved by optimizing the k and threshold parameters of the WkNN, changing the weighting method, or combining different recommendation algorithms. This research has not been evaluated from the SOC analyst's point of view. We would like to verify such things in the future. Ultimately, we would like to enhance the real-world usefulness of the proposed method by creating a tool that automatically maps ATT&CK techniques from logs and by developing a system that recommends techniques by inputting logs in combination with the tool.

References

[1] Kuwano, M., Okuma, M., Okada, S. and Mitsunaga, T.: ATT&CK Behavior Forecasting based on Collaborative Filtering and Graph Databases, *2022 IEEE International Conference on Computing* (*ICOCO*), pp.191–197 (2022).

[2] Abbate, P.: Internet Crime Report, Technical Report 1-33, Federal Bureau of Investigation, NY (2021).

[3] Crowley, C. and Pescatore, J.: A SANS 2021 Survey:Security Operations Center (SOC), Technical Report 1-22, SANS, NY (2021).

[4] Strom, B.E., Battaglia, J.A., Kemmerer, M.S., Kupersanin, W., Miller, D.P., Wampler, C., Whitley, S.M. and Wolf, R.D.: Finding Cyber Threats with ATT&CK™-Based Analytics, Technical Report 1-53, The MITRE Corporation, MA (2017).

[5] Schafer, J.B., Konstan, J. and Riedl, J.: Recommender Systems in E-Commerce, *Proc. 1st ACM Conference on Electronic Commerce*, pp.158–166 (1999).

[6] Gove, R.: Automatic Narrative Summarization for Visualizing Cyber Security Logs and Incident Reports, *IEEE Trans. Vis. Comput. Graph.*, Vol.28, No.1, pp.1182–1190 (2022).

[7] Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G. and Thoma, C.B.: MITRE ATT&CK®: Design and Philosophy, Technical Report 1-46, The MITRE Corporation, MA (2020).

[8] Su, X. and Khoshgoftaar, T.M.: A Survey of Collaborative Filtering Techniques, *Advances in Artificial Intelligence*, Vol.2009, pp.1–19 (2009).

[9] Peterson, L.E.: K-nearest neighbor, *Scholarpedia*, Vol.4, p.1883 (2009).

[10] Fix, E. and Hodges, J.L.: Discriminatory Analysis, Nonparametric Discrimination: Consistency Properties, Technical Report 238-247, Air Force School of Aviation Medicine, TX (1951).

[11] Dudani, S.A.: The Distance-Weighted k-Nearest-Neighbor Rule,

IEEE Trans. Systems, Man, and Cybernetics, Vol.SMC-6, pp.325–327 (1976).
[12] Mladenova, T. and Valova, I.: Comparative analysis between the traditional K-Nearest Neighbor and Modifications with Weight-Calculation, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (*ISMSIT*), pp.961–965 (2022).
[13] Jannach, D., Zanker, M., Felfernig, A. and Friedrich, G.: *Recommender Systems: An Introduction*, p.18, KYORITSU SHUPPAN (1964).
[14] Zhang, S., Li, X., Zong, M., Zhu, X. and Cheng, D.: Learning k for KNN Classification, *ACM Trans. Intell. Syst. Technol.*, Vol.8, pp.1–19 (2017).
[15] Verma1, V. and Aggarwal, R.K.: A comparative analysis of similarity measures akin to the Jaccard index in collaborative recommendations: Empirical and theoretical perspective, *Social Network Analysis and Mining*, Vol.10, pp.43–58 (2020).
[16] Neo4j, Inc.: neo4j, Neo4j, Inc. (online), available from ⟨https://www.neo4j.com/⟩ (accessed 2023-01-31).
[17] Neo4j, Inc.: Subqueries, Neo4j, Inc. (online), available from ⟨https://neo4j.com/docs/getting-started/current/cypher-intro/subqueries/⟩ (accessed 2023-01-31).
[18] Husák, M., Komárková, J., Bou-Harb, E. and Čeleda, P.: Survey of Attack Projection, Prediction, and Forecasting in Cyber Security, *IEEE Communications Surveys & Tutorials*, Vol.21, pp.640–660 (2019).
[19] Polatidis, N., Pimenidis, E., Pavlidis, M., Papastergiou, S., Haralambos and Mouratidis: From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks, *Evolving Systems*, Vol.11, pp.479–490 (2018).
[20] Sadlek, L., Čeleda, P. and Tovarňák, D.: Identification of Attack Paths Using Kill Chain and Attack Graphs, *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pp.1–6 (2022).
[21] Cho, S., Han, I., Jeong, H., Kim, J., Koo, S., Oh, H. and Park, M.: Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture, *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment* (*Cyber SA*), pp.1–8 (2018).
[22] Elitzur, A., Puzis, R. and Zilberman, P.: Attack Hypothesis Generation, *2019 European Intelligence and Security Informatics Conference* (*EISIC*), pp.40–47 (2019).
[23] Brisse, R., Boche, S., Majorczyk, F. and Lalande, J.-F.: KRAKEN: A Knowledge-Based Recommender system for Analysts, to Kick Exploration up a Notch, *International Conference on Security for Information Technology and Communications*, pp.1–17 (2021).
[24] Inria: ZeroKit, the innovative toolkit from Malizen start-up that visualizes intrusions into IT systems, Inria (online), available from ⟨https://www.inria.fr/en/zerokit-innovative-toolkit-malizen-start-visualizes-intrusions-it-systems⟩ (accessed 2023-01-31).
[25] Al-Shaer, R., Spring, J.M. and Christou, E.: Learning the Associations of MITRE ATT & CK Adversarial Techniques, *2020 IEEE Conference on Communications and Network Security* (*CNS*), pp.1–9 (2020).
[26] Katano, Y., Kozai, Y., Okada, S. and Mitsunaga, T.: Prediction of Infected Devices Using the Quantification Theory Type 3 Based on MITRE ATT&CK Technique, *2022 IEEE International Conference on Computing* (*ICOCO*), pp.198–203 (2022).
[27] Munaiah, N., Rahman, A., Pelletier, J., Williams, L. and Meneely, A.: Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition, *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement* (*ESEM*), pp.1–6 (2019).
[28] CISA: Alert (AA22-277A) Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization, CISA (online), available from ⟨https://www.cisa.gov/uscert/ncas/alerts/aa22-277a⟩ (accessed 2023-01-31).
[29] The MITRE Corporation: ATT&CK, The MITRE Corporation (online), available from ⟨https://attack.mitre.org/⟩ (accessed 2023-01-31).
[30] CISA: Alert (AA22-174A) Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems, CISA (online), available from ⟨https://www.cisa.gov/uscert/ncas/alerts/aa22-174a⟩ (accessed 2023-01-31).
[31] CISA: Alert (AA22-138B) Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control, CISA (online), available from ⟨https://www.cisa.gov/uscert/ncas/alerts/aa22-138b⟩ (accessed 2023-01-31).
[32] Seung-Taek, P. and Wei, C.: Pairwise Preference Regression for Cold-Start Recommendation, *Proc. 3rd ACM Conference on Recommender Systems*, pp.21–28 (2009).
[33] Priyank, T., Krunal, V., Vijay, U., Sapan, M. and Sudeep, T.: Combining User-Based and Item-Based Collaborative Filtering Using Machine Learning, *Information and Communication Technology for Intelligent Systems*, pp.173–180 (2019).
[34] Canary, R.: Explore Atomic Red Team, Red Canary (online), available from ⟨https://atomicredteam.io/⟩ (accessed 2023-01-31).

Masaki Kuwano graduated from Information Networking for Innovation and Design at Toyo University in Japan. He majored in computer science, especially cyber security. His interest includes how to utilize MITRE ATT&CK.

Momoka Okuma is an undergraduate student at Information Networking for Innovation and Design at Toyo University in Japan. Her research focuses on cyber security, especially log analysis.

Satoshi Okada received his B.E. and M.E. degrees in engineering from The University of Tokyo, in 2020, 2022. His research interests include cybersecurity (especially, IoT Security, Network Security, and Post-quantum Cryptography) and Digital Transformation.

Takuho Mitsunaga is an Associate Professor at Toyo University. He is also a senior fellow at The Tokyo Foundation for Policy Research and a security expert at the Information-technology Promotion Agency in Japan. He received his B.Ec. degree from Osaka University in 2008 and M.E. and Ph.D. degrees from Kyoto University in 2010 and 2016, respectively. He worked at the front line of incident handling and penetration testing at a security vendor and JPCERT/CC, where he is engages in cyber attack analysis including APT cases. He has also contributed in some cyber security related books as coauthor or editorial supervisor including "Fundamentals of Control System Security (NTT Publishing)".