

Rapidly Deployed Artificial Intelligence Module Corresponding to Cyber Security Recognition and Learning

Ming-Shen Jian*, Bo-Yi Lee**, Yong-Qing Hsieh*, Chun-He Cheng*, Xing-En Liu*, Rui-Lun Cai*, Pei-Cen Liao*, Ta-Yuan Chou**, Wun-Yuan Huang**

*CCIS Lab., Dept. of CSIE, National Formosa University, Yunlin County, Taiwan 632

**National Center for High-Performance Computing, National Institutes of Applied Research, Taiwan

jianms@nfu.edu.tw, 1203007@narlabs.org.tw, vicky940318@gmail.com, neil990006@gmail.com, usa105032@gmail.com, a0983805812@gmail.com, peiiccx@gmail.com, 1203053@narlabs.org.tw, wunyuanyuan@narlabs.org.tw

Abstract— To protect the services and data of the main servers, Rapidly Deployed Cyber Attack Bait is proposed for the unpredictable cybersecurity attack in this research. Based on Software Defined Network, the data packet and operation of a cybersecurity attack could be redirected to the on demand deployed bait container. By suitable artificial intelligence strategy, the idle bait containers corresponding to the type of cybersecurity attack can be on demand deployed automatically and rapidly. Verification shows the feasibility of the virtualized bait container could be about 1.16 times to 2 times enough for the future coming attacker and also record the all operations of the cybersecurity attack individually.

Keywords— cybersecurity, bait, Software Defined Network, Artificial Intelligence, container

I. INTRODUCTION

Cyber-attacks targeting network services and digital data have been a longstanding concern in the field of information security. These attacks encompass a wide range of malicious activities, including phishing attacks, man-in-the-middle attacks, DNS record forgery, SQL injection, ransomware, password attacks, brute force attacks, insider threats, malware, and cross-site scripting (XSS) attacks, etc. Such threats have the potential to compromise the integrity of local devices by altering files or content. Various forms of cyber intrusions can severely damage information systems. Incidents such as data theft, encryption of files by ransomware, and unauthorized data manipulation or surveillance, highlight the increasing importance of robust cybersecurity measures to safeguard sensitive information. The evolution and diversification of these cyber threats continue to emphasize the critical

need for effective protection mechanisms to secure both digital assets and network infrastructures.

Despite the implementation of various security and protection mechanisms, the continuous monitoring and analysis of hacker behaviors and attack patterns remain essential for identifying emerging security vulnerabilities [1]. In addition to real-time monitoring, the use of deceptive techniques such as baiting attackers has been proposed as a method for uncovering latent security risks [2, 3, 16-18]. This approach, which allows for the collection of valuable data on hacker behavior and attack patterns, can subsequently inform the development of adaptive security responses. Leveraging artificial intelligence to process and analyze the gathered data offers the potential to enhance real-time threat detection and enable dynamic security improvements [4].

In recent years, artificial intelligence (AI) has gained widespread adoption across various industries and information systems. Typically, small-scale AI models or services can be developed and deployed for specific tasks or objectives. One effective approach to optimizing the performance and scalability of AI services is to parallelize and distribute computational tasks across multiple nodes [5,6] with more efficient processing. Moreover, due to the diverse and evolving nature of cybersecurity threats, the development of specialized AI services or modules for specific cybersecurity challenges can significantly improve the accuracy and

responsiveness of threat mitigation efforts. Such targeted AI solutions are better equipped to address particular aspects of cybersecurity.

Artificial intelligence was generally used in data or text vocabulary analysis [19]. According to the proven training data, AI applications could find the corresponding features or keywords instead of the whole content related to the training data. Therefore, according to the possible relationship between the found features and new data, the new coming network risk or attack could be classified. However, the hacker would also mix actual attack instructions with many invalid instructions. It increases difficulty in identifying malicious network attacks. Hence, to improve the prediction accuracy of the possible cyber security risks considering the possible false attack instructions to cause confusion should be the important issue.

Considering the various malicious network attacks, deploying multiple AI modules for the attack identification and prediction would be the possible solution. There were researches proposed for the parallel processing based on the distributed AI modules [6]. In addition, to collect the log data or related information, the cybersecurity baits which could be rapidly deployed as “Security Crisis as a Service” on cloud computing platform can be used [16].

The contributions of this research can be shown as follows:

1. Based on the container and virtual machine of the cybersecurity bait system, the malicious network attacks could be recorded. The attack data can be used not only as the training data but also the test data. In other words, the deployed multiple AI modules can keep training and prediction.
2. Based on parallel AI modules, the style of malicious network attack could be identified and classified. The features of the attack instruction and timing/sequence can be defined and found. The possible false attack instructions to cause confusion could be ignored by AI modules.
3. According to the prediction results, the possible attack can be found based on the on demand defined threshold. In opposition, if

there exist multiple prediction results, the current attack or network connection could be treated as the new security potential threats. In other words, a new possible malicious network attack could be found.

4. Voting mechanisms are proposed for separating the normal users and malicious connections. The possible new high security risk connection could be redirected to the bait system for monitoring.

In the following, section 2 provides the related works. The proposed system is introduced and verified in section 3. The conclusion is given in section 4.

II. RELATED WORKS

Due to the high performance of computing and huge computing resources, network security issues or malicious network attacks [1] become important issues or research topics. To redirect the malicious network attack connection and reduce the security risk of the services, some security systems would deploy the bait for the network connection with high security risk [2,3,16-18]. Considering the known types of attack or system vulnerability, the corresponding bait virtual machines or containers on cloud would be built for the malicious user. However, to define or detect the possible malicious attacks, collecting and detecting the data packets passed through the network is important.

To detect and gather the data packets, the SNORT, a popular open source network intrusion prevention software and network intrusion detection software, was generally used [12-15]. The data packet which matches the rules of malicious attack could be found or detected. In other words, to enhance the dataset of the malicious attack rules could improve the performance of the possible malicious attack defence.

Considering the malicious attack would be various anytime, anywhere, to automatically detect and analyze the data packets is the issue. Dealing with the huge data related to the network packets, Artificial intelligence (AI) could be the possible solution for the services or applications [4,5,11,15]. Based on the assistance of the software defined network (SDN) [8-11], the malicious network

connection could be blocked [11,15] or redirect to the bait system [16-18].

However, considering the possible malicious attacks, multiple attack methods or strategies would be chosen. Furthermore, the unknown malicious attack strategies would also happen. To parallel estimate and classify the possible attack methods will be the basic requirement. In addition, without suitable defence strategies, the latency of the malicious attacks would not be enough for the AI recognition and detection. Hence, how to rapidly prepare and deploy the AI system corresponding to the current coming connection for both malicious connection detecting and unknown attack recognition would be an important issue.

III. PROPOSED SYSTEM

In this research, three partitions are proposed for the Cyber Attack Auto Recognition and Learning based on Rapidly Deployed Artificial Intelligence Module: rapidly artificial intelligence module deployment, parallel classification and recognition framework, and bait system.

Figure 1 presents the concept of the proposed system. Based on the SDN, the network data packet could be obtained and redirected. In addition, all the log data with the access information or command operation could be delivered from the servers or baits.

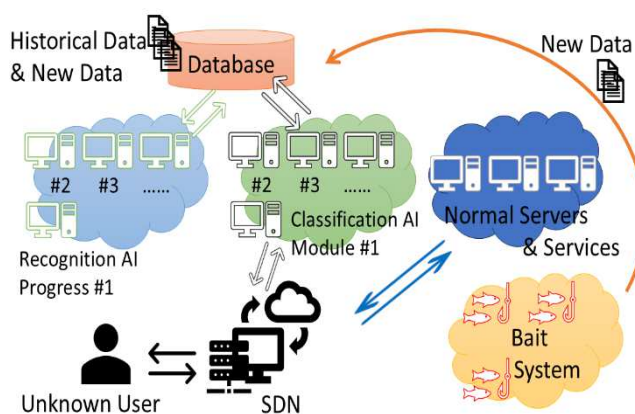


Figure 1. The concept of the proposed system

In the parallel classification and recognition framework, there will be classification AI modules and recognition AI progresses. Suppose that the operation historical data can be collected from the

server or bait system. In this research, the data or login information would be analysed.

Considering the new or unknown data, the recognition AI progress would be used for the feature finding or extracting. In this research, the TF-IDF (Term Frequency–Inverse Document Frequency) is deployed for the evaluation of individual vocabulary in the document or text [8]. The term frequency and inverse document frequency of each vocabulary can be calculated. Due to the possible terms or vocabularies would be huge, the PCA (Principal Component Analysis) is used. Therefore, if there exist multiple features corresponding to the new coming unknown data, the recognition AI progress would possibly find the features. In addition, the data of the known malicious attacks can be also recognized by finding the corresponding features. In other words, various types of the malicious attacks can be separated or differentiated into independent malicious attack definitions based on the found features. Figure 2 presents the flowchart of the multiple recognition AI progress.

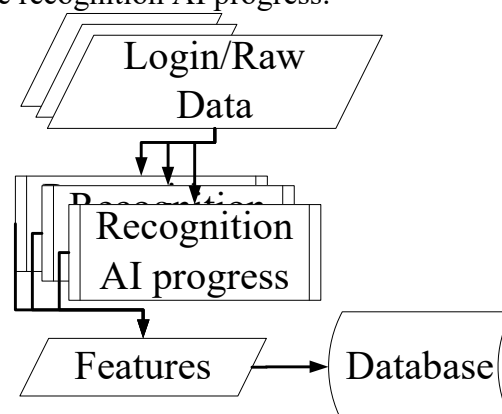


Figure 2. The flowchart of the multiple recognition AI progress

With the found features of the raw data, the classification AI module is proposed. To reduce the risk of blocking the normal network connection, we propose the “voting mechanism”. In this research, we deploy the classification methods such as K-means, DBSCAN (Density-Based Spatial Clustering of Applications with Noise), SVM (support vector machine), and CNN-LSTM (Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM)). According to the found features, the malicious attacks can be classified or separated into the corresponding attack modes. However, the

malicious operation may have similar features with multiple attack modes. Therefore, we propose the threshold α about the classification prediction accuracy for the recognition and classification. Based on the classification results from various classification methods, the malicious operation would be classified into specific attack mode with the accuracy rate value. If the classification accuracy rate value is larger than the on demand given threshold α , the malicious operation is classified. In opposition, the operation is not clearly defined as the specific mode. Since we have multiple classification methods, the possible malicious mode classified by different methods may be different. Hence, in this research, the classification AI module will count the vote corresponding to each possible malicious mode. The mode with the highest vote number will be the malicious mode which the system classifies.

In addition to the malicious operation, the normal operation to the network service or server could be also recognized. Corresponding to the network services, the normal or regular operation commands could also extract the features. Different purposes to the related services would have various and different features. Hence, the normal mode can be also defined by the proposed recognition AI progress. The normal operation could be identified by the classification AI module.

In this research, the features corresponding to various operations will be recorded in the database. In other words, in addition to the historical data, the real time data or packet related to the network connection can be also identified. According to the current command or data packet, via classification methods voting mechanism, the possibility of the malicious attack can be decided. If the connection is decided as the malicious attack after voting, the bait system will be deployed for the operation recording. Figure 3 presents the flowchart of the multiple classification AI module. Considering the possible hybrid malicious attack connections, the classification or grouping mechanism may not classify the current connection clearly. Therefore, we would provide the two steps of voting mechanism: Normal Connection Voting and Malicious Type Voting.

Since the services provided to the customers or remote users are known, we assume that the

operations or commands of the normal users which indicate the safe connections could be known and defined as the features of the safe connection. Therefore, the first step, Normal Connection Voting would be used to decide whether the connection is normal or with high security risk. According to the variance in each classification algorithm, the probability of the group that the current connection belongs to can be defined. According to the decision and the corresponding probability, the vote of individual classification algorithm is also decided. Therefore, the first step of voting could decide the current connection as the possible normal or possible attack connection. If the connection is defined as the attack connection, it means that the operations or commands of this connection are unusual. Then, the second step, Malicious Type Voting would start to classify the current connection. Considering the rapid changing of the malicious attack, there will be always some new types or operations of attack not defined yet. Hence, to exclude the un-normal users or possible malicious connections in the services would be the first step.

In this research, all the AI modules are developed in the individual Docker container. Each recognition or classification AI module is independently imaged. In other words, rapid artificial intelligence module deployment is implemented based on modularized AI containers. Therefore, the recognition AI module can be triggered when any new record or data analysis is required. In addition, the new classification AI module can be deployed and embedded by Docker container before the voting mechanism. In other words, not only the computing resource could be reserved by reducing the execution of the recognition AI module but also the voting result could be elastically changed corresponding to the tuning of the classification AI module. By establishing the registry of docker engine, the modularized AI modules can be deployed rapidly.

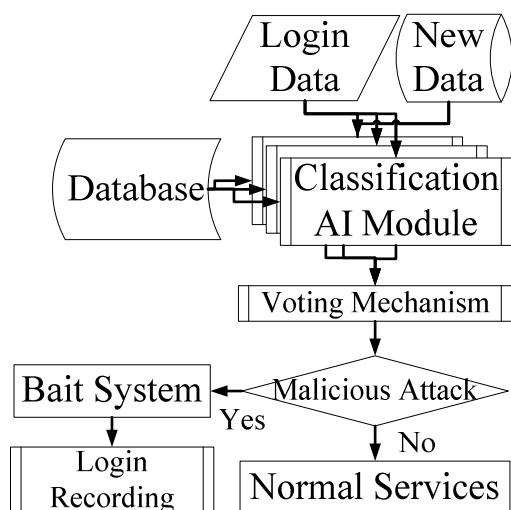


Figure 3. The flowchart of the multiple classification AI module

After voting mechanism, the connection can be decided as the normal or malicious accessing. The malicious connection will be redirected to the bait system [16]. To on demand prepare various baits for the unpredictable types of cyber-attack in advance is unfeasible. Similar to the multiple AI modules of Docker containers, the different types of baits are also pre-deployed as the container images. Hence, when needed, the bait could be rapidly and quickly deployed for the possible malicious connection decided by the voting mechanism. In other words, the SDN could redirect the network connection to the bait instead of the service server. Finally, the malicious connection which classified into the specific type of security risk can be clustered. In addition, due to the two steps voting, even the attack operations or commands are new or not defined yet, the current connection would be defined as the high security risk connection and redirected to the bait. In other words, even the current connection is a new type of malicious attack, now the bait system can deal with and record the operations.

IV. VERIFICATION AND RESULTS

To verify the proposed Rapidly Deployed Artificial Intelligence Module Corresponding to Cyber Security Recognition and Learning, we develop the independent container corresponding to each AI module.

First, the normal network service including File Transfer Protocol (FTP) application and Web service is established. The login file and accessing

information is recorded as the text file for the AI module. According to the TF-IDF and PCA feature recognition AI modules, the features about the status of the server with the same data are found with its own weight value. Figure 4 presents the feature recognition results where (a) is the result based on PCA and (b) is the result of TF-IDF.

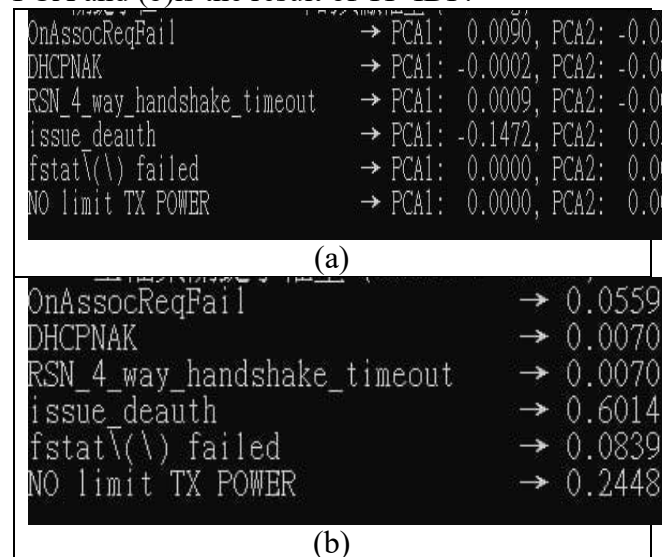


Figure 4. (a) the result based on PCA and (b) the result of TF-IDF.

By analyzing the historical malicious attack log data, the corresponding operation can also be found by the proposed system. Since these historical data would be pre-defined and divided into multiple attack type groups. Therefore, to find the corresponding features of the related group or attack type is possible. In addition, Via estimating the weight and the relationship to the whole data, various combinations of the single feature word could be evaluated. In other words, the proposed system would find the most possible features instead of a single word as the main feature of the group.

Due to different types of status corresponding to the server, the classification AI module would cluster or group the information based on the possible features. Based on the K-mean and SVM modules, the data could be clustered into three groups. According to the DBSCAN, there are only two groups. Figure 5 shows the grouping results.

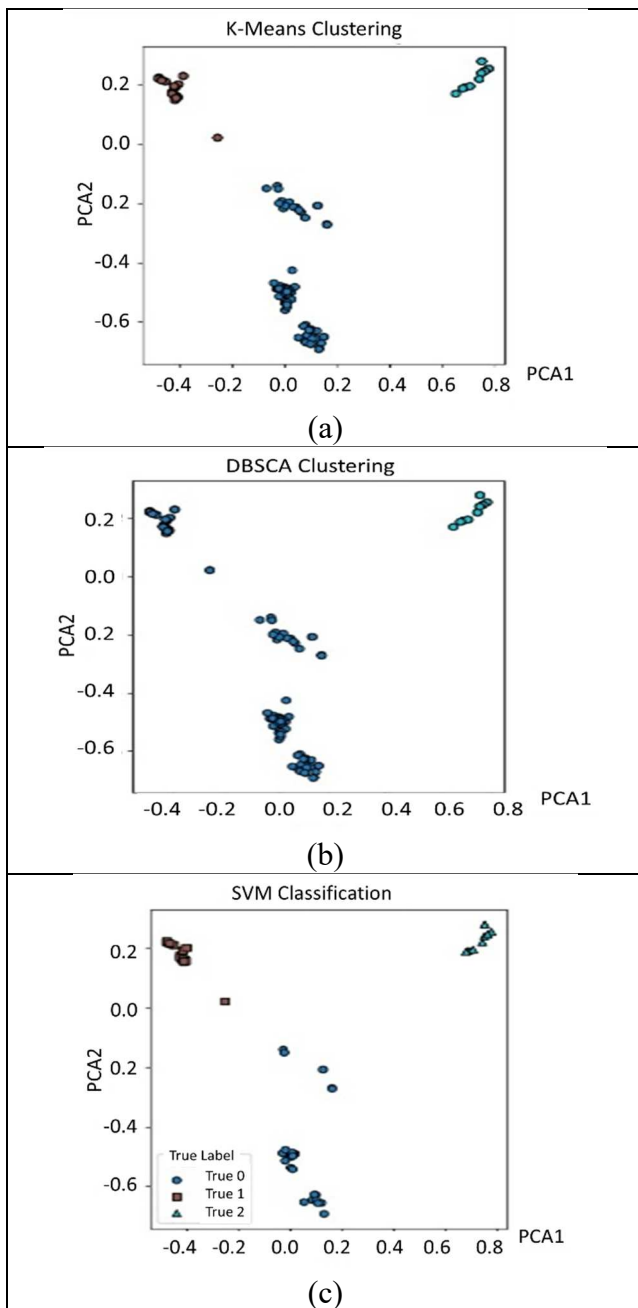


Figure 5. The grouping results of (a) K-Mean, (b) DBSCAN, and (c) SVM

Hence, when a new connection is grouped, different classification AI modules would find and vote the group it belongs to. In other words, the possible type of the connection or operation can be classified. In addition, after grouping, the distance between the current connection and the group center could be estimated. Hence, we could define the threshold value as the vote for voting mechanism between various classification AI modules. Only the distance is smaller than the threshold which means more closer to the group center, the higher

probability of the malicious attack that the current connection would belong to. According to the verification, a single type of the attack could be found by the proposed multiple AI modules.

In this research, the AI modules could be used for cyber security risk learning and detection. However, currently, the data of various risks comes from the existing or known database and operation. It means that the unknown or ungrouped network connection would still probably attack.

V. CONCLUSIONS

According to the proposed Rapidly Deployed Artificial Intelligence Module Corresponding to Cyber Security Recognition and Learning, the AI module can be extended and deployed rapidly and easily. Based on the voting mechanism, we could collect the classification results from multiple AI modules and conclude the most possible type of connection or operation. The verification result shows the reality of parallel classification and recognition framework for various AI modules.

Considering the known types of malicious network attack, the features could be found by analyzing the corresponding log data. Different attack models would show its own features. However, hybrid network attack based on multiple attack types would cause the voting mechanism confused. To set the suitable threshold for the voting and decision making is still important issue. Furthermore, time for the decision making of the connection blocking is still difficult. The key operation for the decision making should be defined.

ACKNOWLEDGEMENT

This research is also guided by the National Center for High-Performance Computing. Also, thanks for the support from Cloud Computing and Intelligent System Lab. of National Formosa University.

REFERENCES

- [1] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 2016, pp. 77-82, doi: 10.1109/W-FiCloud.2016.30.
- [2] S. Vasylyshyn, I. Opirskyy and V. Susukailo, "Analysis of the use of software baits as a means of ensuring information security," 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), Zbarazh, Ukraine, 2020, pp. 242-245, doi: 10.1109/CSIT49958.2020.9321925.
- [3] P. Bajaj and M. Edwards, "Automatic Scam-Baiting Using ChatGPT," 2023 IEEE 22nd International Conference on Trust, Security and

- Privacy in Computing and Communications (TrustCom), Exeter, United Kingdom, 2023, pp. 1941-1946, doi: 10.1109/TrustCom60117.2023.00264.
- [4] Y. Sharma, V. Kumar and H. Chaudhary, "Attack Detection on Internet of Things Devices using Machine Learning Techniques," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 281-287, doi: 10.1109/ICICCS56967.2023.10142701.
- [5] M. -S. Jian, J. -T. Gui, X. -M. Wu, "Uncentralized Artificial Intelligence Computing Agent with the Distributed Training and Computing Tasks Based on Open Source Cloud Proxy," CSCE 2023 - ICAI, Las Vegas, USA, p.93. (ISBN:1-60132-518-5)
- [6] M. -S. Jian, Y. -Z. Luo, P. -W. Wang and T. -Y. Lai, "Cloud and Edge Computing Based Movable 3D Dynamic Image Recognition and Analysis Layer System for Remote Biological Laboratory," 2023 25th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, Republic of, 2023, pp. 429-436, doi: 10.23919/ICACT56868.2023.10079325.
- [7] Ming-Shen Jian, Jun-Hong Shen, Kuan-Wei Lee, Yi-Chen Jhou, Chien-Tang Mai, "Cloud Based Software Computing as a Service in Hybrid Evolution Algorithm with Feedback Assistance" Journal of Electronic Science and Technology, Vol.14, Issue 4, pp.362-369, 2016.
- [8] A. H. Abdi et al., "Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions," in IEEE Access, vol. 12, pp. 69941-69980, 2024, doi: 10.1109/ACCESS.2024.3393548.
- [9] H. Liang, H. Liu, F. Dang, L. Yan and D. Li, "Information System Security Protection Based on SDN Technology in Cloud Computing Environment," 2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2021, pp. 432-435, doi: 10.1109/AEECA52519.2021.9574276.
- [10] Z. Fatehi and A. Montazerolghaem, "DDoS Detection in SDN using Deep Learning," 2024 8th International Conference on Smart Cities, Internet of Things and Applications (SCIoT), Mashhad, Iran, Islamic Republic of, 2024, pp. 201-206, doi: 10.1109/SCIoT62588.2024.10570129.
- [11] N. P. M. T, B. M. J. M, S. M. D. R and K. V. M., "Protecting Healthcare Systems Through an ML-Powered Cyberattack Detection Within Software-Defined Networking (SDN)," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560593.
- [12] <https://www.snort.org/> (available 2024/07/03)
- [13] Y. Kaushik, A. Athmaraman, A. M. John and S. Sridhar Raj, "Signature-based Intrusion Prevention System for Software Defined Networks using SNORT," 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT), Vellore, India, 2024, pp. 1-6, doi: 10.1109/AIIoT58432.2024.10574719.
- [14] M. Sheeraz, M. Hanif Durad, S. Tahir, H. Tahir, S. Saeed and A. M. Almuhaideb, "Advancing Snort IPS to Achieve Line Rate Traffic Processing for Effective Network Security Monitoring," in IEEE Access, vol. 12, pp. 61848-61859, 2024, doi: 10.1109/ACCESS.2024.3395123.
- [15] T. Preethi, P. R. Reddy, L. Likhitha, P. P. Kumar and A. Kamani, "A Novel Approach for Anomaly Detection using Snort Integrated with Machine Learning," 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2024, pp. 796-801, doi: 10.23919/INDIACom61295.2024.10498401.
- [16] Ming-Shen Jian, Bo-Yi Lee, Xing-En Liu, Rui-Lun Cai, Zhong-Wei Cai, Pei-Cen Liao, Ta-Yuan Chou, Wun-Yuan Huang, "Rapidly Deployed Cyber Attack Bait Based on Software Defined Network Corresponding to Artificial Intelligence Strategy," 2025 27th International Conference on Advanced Communications Technology (ICACT), Pyeong Chang, Korea, Republic of, 2025, pp.169-174, doi: 10.23919/ICACT63878.2025.10936784
- [17] A. Albaseer, M. Hamood and M. Abdallah, "Adaptive HoneyPot Defense Deployment: A Stackelberg Game Approach with Decentralized DRL for AMI Protection," 2024 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 2024, pp. 1-5, doi: 10.1109/ICNC59896.2024.10556285.
- [18] T. Shivaprasad, A. S. Moulya and N. Guruprasad, "Enhancing Network Security through a Multi-layered HoneyPot Architecture with Integrated

Network Monitoring Tools," 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2024, pp. 473-477, doi: 10.23919/INDIACom61295.2024.10498895.

- [19] Hsiu-Ying Wang, Chun-Ho Cheng, Bo-Yuan Huang, Ming-Shen Jian, "Artificial Intelligence Model for Fake News Detection in Traditional Chinese," 11th IEEE International Conference on Applied System Innovation 2025



Ming-Shen Jian was born in Kaohsiung City, Taiwan in 1978. He received the B.S. from the National Chiao Tung University, HsinChu, and Ph.D degrees in Computer Science and Engineering from the National Sun Yat-sen University, Kaohsiung, Taiwan in 2007. From 2018, he was an Associate Professor and director with the National Formosa University Cloud Computing and Intelligent System Laboratory. Currently he is also an IEEE Senior Member.. His research interests include IOT development and application, Big Data, Optimal Solution, Intelligent System, and Cloud Computing. He was a Secretary of the Taiwan Association of Cloud Computing.



Bo-Yi Lee is a Ph.D. candidate in the Department of Information Management at National Sun Yat-sen University and has served as a senior engineer at the National Center for High-Performance Computing. He possesses extensive experience in various fields, including cyber security architecture design, malware analysis, and intrusion detection. His primary research interests focus on network threat detection through data-driven threat intelligence and machine learning techniques.



Yong-Qing Hsieh currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. Her current research interests are in the area related to artificial intelligence and cybersecurity. She joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2023.



Chun-He Cheng currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to artificial intelligence and Docker container services, digital twins, and IoT system. He joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2022.



Xing-En Liu currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Cloud Computing and Docker container services, security, and intelligent system. He joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2022.



Rui-Lun Cai currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Cloud Computing and Docker container services, and security services. He joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2022.

Pei-Cen Liao currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. Her current research interests are in the area related to security and Docker

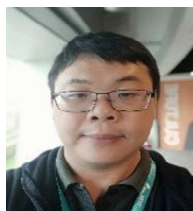


container services, and intelligent bait system. She joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2023.



Ta-Yuan Chou received the Ph.D. degree at the department of computer science and engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan, R.O.C in 2008. He is an assistant researcher in National Center for High-Performance Computing. His doctoral research mainly focuses on evolutionary computation, multiobjective optimization, and scheduling problems. His current research interests include various open networking technologies, such as software defined

network, and P4 programming.



Wun-Yuan Huang received his BS degree in Information and Computer Engineering from Chung Yuan Christian University, Taiwan, in 2006, and his MS degree in Computer Science and Information Engineering from National Dong Hwa University, Taiwan, in 2009. He is currently an associate researcher at the National Center for High-Performance Computing. His primary research focuses on SDN, threat deception, and the deployment

of honeypots.