Intrusion Detection System for AI Box Based on Machine Learning

Jiann-Liang Chen, Zheng-Zhun Chen, Youg-Sheng Chang,

Ching-Iang Li, Tien-I Kao, Yu-Ting Lin, Yu-Yi Xiao, Jian-Fu Qiu

Department of Electrical Engineering, NTUST (National Taiwan University of Science and Technology), Taipei, Taiwan

ITRI (Industrial Technology Research Institute), Hsinchu, Taiwan

Lchen@mail.ntust.edu.tw, LambertChen@itri.org.tw, itriA60429@itri.org.tw, ci@itri.org.tw, kaoti@itri.org.tw, M11007501@gapps.ntust.edu.tw, M11007512@gapps.ntust.edu.tw, M11007513@gapps.ntust.edu.tw.

***Abstract*—This paper presents an integrated application of network intrusion detection. The intercepted packets are first analyzed using a machine learning algorithm, the HistGradient Boosting classifier, to detect network traffic as abnormal or normal. If the network traffic is unnatural or disruptive, the system will immediately notify the information security expert whether to disrupt the network traffic. We propose an information security application combined with hardware and software. The application system can secure IoT devices or any field that needs to use the network environment, including abnormal network traffic, system outages, betrayals, and other cyber threats. The system is scalable and can easily port to other devices or platforms. This study will introduce datasets and pre-processing methods, machine learning model building, abnormal packet handling, and operating system environment building of the AI BOX device. Two public datasets were used to train and test the model, and our model obtained 99.9% prediction accuracy. The system has been successfully tested on the Yocto Project operating system of the AI BOX device.**

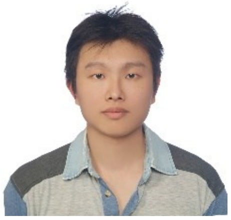
***Keyword*—Artificial Intelligence, Confidentiality of Data Transfer, Feature Selection, HistGradient Boosting Classifier Algorithm, Information Security, IoT Device Security, Machine Learning, Packet Capture Analysis.**

Jiann-Liang Chen (Senior Member, IEEE) was born in Taiwan in December 1963. He received a Ph.D. in electrical engineering from the National Taiwan University, Taipei, Taiwan, in 1989. Since August 1997, he has been with the Department of Computer Science and Information Engineering, National Dong Hwa University, where he is a Professor and the Vice Dean of the Science and Engineering College. He joins the Department of Electrical Engineering, National Taiwan University of Science and Technology, as a Distinguished Professor. His current research interests include cellular mobility management, cyber security, personal communication systems, and the Internet of Things (IoT).

Zheng-Zhun Chen received the M.S. degree in Department of Electrical Engineering from National Taiwan University of Science and Technology, Taipei, Taiwan, ROC in 2017. Since 2017, he joined Industrial Technology Research Institute, served as software engineer. His research interests include Smart Healthcare and Smart Factory.

Yung-Sheng Chang received the M.S. degree in Department of Electrical Engineering from National Yunlin University of Science and Technology, Yunlin, Taiwan, R.O.C. in 2017. Since 2017, he joined Industrial Technology Research Institute, served as hardware engineer. His research interests include Smart Factory and Edge AI platform.

Ching-Iang Li received the Ph.D. degree in the Department of Computer Science and Information Engineering in the National Central University, Taiwan. He is currently an engineer in the Heterogeneous Integration Technology & Intelligent System Division of Industrial Technology Research Institute, Taiwan. His research fields include control system, embedded system integration, and VLSI design.



Tien-I Kareceived the A.S. degree in Electrical Engineering from Kuang Wu Institute of Technology, Taipei, Taiwan, ROC in 2004 and the M.S. degree in Automation Technology from Automation Technology, Taipei, Taiwan, ROC in 2009. Since 2021 he joined Industrial Technology Research Institute, served as software engineer. His current research interests are system integration and Artificial Intelligence.

Yu-Ting Lin is a student at National Taiwan University of Science and Technology. He received a bachelor’s degree in Electrical Engineering from National Taiwan University of Science and Technology. His research interest includes information security.

Yu-Yi Xiao is currently studying the M.S. degree in Electrical Engineering of National Taiwan University of Science and Technology, Taipei, Taiwan. Her research interests include open radio access network, information security, and tactile internet.

Jian-Fu Qiu is currently studying the M.S. degree in Electrical Engineering of National Taiwan University of Science and Technology, Taipei, Taiwan. His research interest includes information security.