Cyber Security for Consumer Internet of Things

Yu-Chiang Wang*, Chiung-Fang Hsu*, Yu-Pin Shen*, Yu-Ting Lu*, Jiann-Liang Chen*,

Han-Hung Hsu**

** Department of Electrical Engineering, National Taiwan University of Science and Technology Taipei, Taiwan*

*** Auray Technology Corp. Taoyuan, Taiwan*

M11207509@gapps.ntust.edu.tw, M11207524@gapps.ntust.edu.tw, M11207508@gapps.ntust.edu.tw, M11207516@gapps.ntust.edu.tw, lchen@mail.ntust.edu.tw, hayes.hsu@auray.com.tw

***Abstract*—With the increasing prevalence of handheld devices in daily life, routers have become essential for connecting devices to the Internet while also becoming prime targets for hacker attacks. Currently, the cybersecurity testing of these devices primarily relies on manual processes. Testing engineers are required to thoroughly understand various regulations, such as EN 303 645 and TS 103 701, and to develop specific testing procedures for different devices. This paper proposes a semi-automated AI system for testing Internet of Things (IoT) devices. The system uses standardized procedures and AI-driven regulatory interpretation to rapidly generate test reports, significantly reducing engineers' time searching for relevant regulations and improving testing efficiency and accuracy. This study evaluates multiple open-source embedding models and the Llama 3.1 70B large language model to develop an Advanced Retrieval-Augmented Generation (Advance-RAG) framework. This framework automatically retrieves test items from cybersecurity regulations and generates preliminary assessments based on self-declarations provided by device manufacturers. It quickly determines whether a device's functionalities comply with specified testing standards. Testing engineers can then upload supporting evidence through the report generation system, providing a comprehensive test report.**

***Keyword*—Large Language Model, Embedding Model, Advance RAG, EN 303 645, TS 103 701**

Yu-Chiang Wang was born in Taiwan in 2000. He received the B.S. degree in 2023. He is currently pursuing an M.S. degree in electrical engineering at the National Taiwan University of Science and Technology, Taipei. His main research interests include artificial intelligence and penetration testing.

Chiung-Fang Hsu was born in Taiwan in 2001. She received her B.S. degree in 2023 and is currently pursuing an M.S. degree in Electrical Engineering at the National Taiwan University of Science and Technology. Her main research interests include applications of artificial intelligence.

Yu-Pin Shen was born in Taiwan in 1999. He received a B.S. degree in Electronic Engineering in 2022. He is currently pursuing an M.S. degree in Electrical Engineering at the National Taiwan University of Science and Technology (NTUST), Taipei. His main research interests include Artificial Intelligence, the Internet of Things (IoT), AI Image Detection, and Cybersecurity.

Yu-Ting Lu was born in Taiwan in 1999. He received the B.S. degree in 2022. She is currently pursuing an M.S. degree in electrical engineering with the National Taiwan University of Science and Technology, Taipei. Her main research interests include artificial intelligence and computer Vision.

Jiann-Liang Chen (Senior Member, IEEE) was born in Taiwan on December 15, 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 of National Dong Hwa University, where he is a professor and Vice Dean of Science and Engineering College. Prof. Chen joins the Department of Electrical Engineering, National Taiwan University of Science and Technology, as a Distinguished Professor and Dean. His research interests are cellular mobility management, cybersecurity, personal communication systems, and the Internet of Things (IoT).

Han-Hung Hsu is a master's student at the Defense University Institute of Technology (CCIT) and an engineer at Auray Technology. He is mainly responsible for research on topics related to AI and information security.