Ministry of Science and ICT

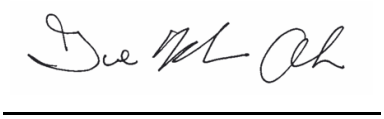
IITP Institute of Information & Communications Technology Planning & Evaluation

APPLICATION FORM
(JOINT RESEARCH)
HIGH POTENTIAL INDIVIDUALS GLOBAL TRAINING PROGRAM)

AGREEMENT

As stated above, I submit this application form to IITP that conducts "High Potential Individuals Global Training Program" supported by Ministry of Science, ICT in South Korea. IITP may disclose the information below to the public for the purpose of providing information and matching a research partnership between your institute and a Korean university.

* IITP : Institute for Information & communications Technology Planning & Evaluation

Printed Name of Chief of Research	Tae Hwan Oh	Date(mm-dd-yyyy)	02-16-2020
Signature of Chief of Research			

☞ ***(Note)*** *This application is to identify the willingness to participate in this research and to find a research partnership for research institutes in Korea. Therefore, in its sole discretion, it is acceptable to contain only minimal information. (max. 3 pages)*

1. Research Title	Design and Develop Malware Detection System for Industry IoT (IIoT) networks using Machine Learning Approaches.						
2. Research Area	**A.I.**	**Big Data**	**Cloud Computing**	**Block Chain**	**AR/ VR**	**ICT/SW Convergence**	**Other ICT /SW**
	X	**X**	**X**				
3. Chief of research	Title	Associate Professor		Contact	E-mail : thoics@rit.edu		
	Name	Tae Hwan Oh			Tel : +1-585-475-7642		
4. Affiliation	Name	Rochester Institute of Technology		Classification	(X) University ( ) Research Institute ( ) Industry ( ) ETC.		
5. Capacity for students (5 or less)	2		**Support for students** ***(all necessary)***		(X) Visa support (X) Research Mentoring (X) Research Space (X) Accessibility to Research equipment		

6. Research Objective	The focus of this research is to protect industry IoT (IIoT) devices using acloud-based machine learning infrastructure with a dynamic on-site firewall. Machine learning is used to profile each IoT device based on network trace from the observed on the firewall. This network trace is then piped to a remote infrastructure where machine learned is used to detect abnormal behavior. Network trace is continuously monitored and classified by the cloud infrastructure which makes necessary adjustments on the firewall to provide protection in near real time. The project will cover the following areas: -Evaluate malware detection methodology for IIoT. -Design malware detection system using machine learning approaches. -Setup prototype development environment- Use tools and setup the development system. -Collect data set and feature extractions. - Build malware detection prototype. -Debug and test the prototype. -Perform the prototype evaluation and analysis
7. Research Summary	We have done a funded research in IoT Malware Detection System for Home Network. Our work was focused on a system which is designed for tackling the problem of detecting IoT specific botnet, malware, intrusion activity in home network using machine learning approaches. The intensive machine learning processes are done in the cloud to reduce the processing overhead on the home network. The IoT malware detection system was developed while incorporating several new ideas (published in conferences). This system operates by extracting relevant features from both malicious and benign network track with a low powered in-line device that is placed between the modem and the devices themselves. After extraction, the features are forwarded to a Using the current result of the research, the system could be adjusted for industry IoT. Current system has positive results for detecting any malware activity for home network using behavior-based approach using machine learning. The internal IoT activities, network activities, packet types and flow were used to detect the malware. However, industry IoT has different requirements and malware activities to compared to home network. The following objectives should be achieved for building a efficient and effective IoT malware detection system. 1. Determine the goals and objectives of the malware detection system for industry IoT. 2. Explore and evaluate different machine learning approaches for industry IoT. 3. Design the system based on behavior detection, machine learning and scalable approach. 4. Setup prototype development environment- Purchase tools and setup the development system. -Purchase necessary software and hardware. 5. Setup computer and software for the malware detection development environment 6. Collect data set and feature extractions. The feature extractor serves as a utility for analyzing the network trace and creating a set of features that will be used in machine learning. This component is split between the node were the specified network trace is extracted and the remote machine learning infrastructure where the bulk of the individual features are extracted/computed happens. Previously the solution consisted of a full feature extractor written from scratch using Python and several useful libraries. This provided very fine-tuned control of the entire process and may be the way some implementors choose to move forward with the design.

	7. Build malware detection prototype using machine learning approach. The Machine Learning Infrastructure depicted in Figure 2 is a remote site which handles all of the heavy processing that comes with machine learning. As the node collects trace owing through the IoT devices it sends it to this remote infrastructure. The process of getting the tra_c to the infrastructure was somewhat challenging as it needed to be quick and efficient so the solution could properly detect an attack and react to it in a timely manner. In past, our team have modified and adjust the existing algorithms to fit the current application. Therefore, the algorithm will be tested and modified to meet the industry IoT requirements. 8. Debug and test the prototype. a. Create test cases and environment to test the basic functionalities and performance of the system. 9. Perform the prototype evaluation and analysis a. Perform extensive test and gather performance data. b. Evaluate the prototype using performance metrics. My collaborator does not require to understand security. Our team can handle the security related research and has already established security expertise. Most of our collaboration will be focused on artificial intelligence and cloud structure of the security system. RIT has been making major investment of $25 million by alumnus and New York State. We are in the process of building 50,000 sq feet for Global Cybersecurity Institute. One of focus to investigate industry IoT and we have relationship with manufacturing companies and industries to explore and develop AI for detection and mitigating intrusion detections and malware.
8. Need for funding from Korean government	$100,000
9. Request for Korean Universities	The selection of students studying abroad should be conducted after mutual consultation, and please cooperate as much as possible to prepare for VISA.