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	Shahram Shah Heydari	Date(mm-dd-yyyy)	01-30-2020
Signature of Chief of Research	Shahram S. Heydari 2020.01.31 01:21:26 -05'00'		

☞ ***(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	Application of Generative Adversarial Networks in handling unknown security attacks						
2. Research Area	**A.I.**	**Big Data**	**Cloud Computing**	**Block Chain**	**AR/ VR**	**ICT/SW Convergence**	**Other ICT /SW**
	X					X	
3. Chief of research	Title	Associate Professor		Contact	E-mail : shahram.heydari@ontariotechu.ca		
	Name	Shahram Shah Heydari			Tel : +1-905-721-8668		
4. Affiliation	Name	University of Ontario Institute of Technology		Classification	(X) University ( ) Research Institute ( ) Industry ( ) ETC.		
5. Capacity for students (5 or less)	3 (three)		**Support for students *(all necessary)***		(X) Visa support (X) Research Mentoring (X) Research Space (X) Accessibility to Research equipment		

6. Research Objective	To develop a training framework for an intrusion detection system based on Generative Adversarial Networks (GAN) for the purpose of detecting and mitigating network attacks with unknown or dynamically-changing profiles.
7. Research Summary	Machine Learning and Deep Learning techniques have been used successfully for detecting network-based security attacks with known feature profiles. However, they usually fail when applied to attacks with feature profiles even slightly different from what they have been trained with. This issue creates a vulnerability in dealing with attacks that dynamically change certain features (e.g. packet rate, message length or IAT). The objective of this research is to create a training framework in which a defender and an attacker both deploy Machine Learning techniques to adjust their feature profile to overcome the other side. We are looking at the possibility of deploying Generational Adversarial Networks (GAN) for this purpose, and to evaluate its efficiency in dealing with dynamically-changing attack profiles.
8. Need for funding from Korean government	$75000 total as following: $25000/Student to cover the university overhead, cost of equipment and space, and personnel salaries.
9. Request for Korean Universities	The selection of students studying abroad should be conducted through mutual consultation. Intellectual property and publication rights to be negotiated between the institutions.