Sri Lanka Institute of Information Technology

PROJECT REGISTRATION FORM

The purpose of this form is to allow final year students of the B.Sc. (Hon) degree program to enlist in the final year project group. Enlisting in a project entails specifying the project title and the details of four members in the group, the internal supervisor (compulsory), external supervisor (may be from the industry) and indicating a brief description of the project. The description of the project entered on this form will not be considered as the formal project proposal. It should however indicate the scope of the project and provide the main potential outcome.

PROJECT TITLE	Trust Evaluation of MANETS using Deep Reinforcement Learning
RESEARCH GROUP	Machine Learning
PROJECT NUMBER	(will be assigned by the lecture in charge)

PROJECT GROUP MEMBER DETAILS:

	STUDENT NAME	STUDENT NO.	CONTACT NO.	EMAIL ADDRESS
1	Jayasekara R.A.N.T	IT13023256	0771037870	zantgatsu@gmail.com
2	Priyadarshani T.D.H	IT13067816	0779216686	princesshassi@gmail.com
3	Chathuranga K.B.L.	IT13048624	0774636634	lahiru.chathuranga774@gmail.com
4	Anooj R.	IT13096908	0712898781	anoojaj9@gmail.com

SUPERVISOR

Name	Signature	Date
Lakmal Rupasinghe		

CO-SUPERVISOR (will be assigned by the Supervisor, if necessary)

Name	Signature	Date
Krishnadewa Kesavan		

EXTERNAL SUPERVISOR (if any, may be from the industry)

Name	Affiliation	Contact Address	Contact Numbers	Signature/Date

ACCEPTANCE BY CDAP MEMBER

Name	Signature	Date

PROJECT DETAILS

Brief Description of your Research Problem:

The Internet of Things (IoT) is one of the new emerging technologies. The main limitation that might threaten the growth of IoT will be the difficulties in the Security. Since IoT is composed of various heterogeneous smart devices, the security vulnerabilities in IoT are very high because the number of malware that can affect will also be higher. Although there are many studies carried out on trust evaluation, normal trust evaluation methods will not serve due to the high diversity of the IoT devices. This paper state of a machine learning mechanism to determine the trust of the devices involved in IoT by looking at various aspects that indicate the presence of malware in a device which will ultimately diminish trust. The features we collect are based on Network Information, Application information, Operating System Information and User Information. By considering many parameters from these features, the overall trust of the device is determined. Our ultimate goal is to build a trust network by connecting devices with higher trust values, so that sensitive information can be exchanged through IoT.

Description of the Solution:

Trust or Reputation analysis is looked upon in various angles. Presence of malicious programs affects trust of the device most because most of the time the user is unaware about the presence of malware. We believe that presence of malware can be analyzed and confirmed in various aspects. Various studies are based on malware detection and analysis. There are static analysis techniques, dynamic analysis techniques as well as hybrid approaches. There are multiple ways how malware get installed into devices and several different ways they get activated. They could exploit the vulnerabilities in the user level, network level, operating system and applications installed in the device. Therefore it is necessary to identify the weakness at each of these levels because all of these weaknesses will diminish the trust of the devices and provide many opportunities for malware to get installed in our devices

Main expected outcomes of the project:

- Compute the trustworthiness of the User, in the overlay network
- Compute the trustworthiness of the Nodes, in the network
- Compute the trustworthiness of the Android OS
- Compute the trustworthiness of the Applications installed in the device.

WORKLOAD ALLOCATION

MEMBER 1

- Algorithm designing
- Creating the Reinforcement Model
- Extracting the Network Features

MEMBER 2

- Algorithm designing
- Protocol Implementation
- Extracting the User-Level Features

MEMBER 3

- Algorithm designing
- Extracting the Application S/W Features

MEMBER 4

- Algorithm designing
- Extracting OS Features

DECLARATION

"We declare that the project would involve material prepared by the Group members and that it would not fully or partially incorporate any material prepared by other persons for a fee or free of charge or that it would include material previously submitted by a candidate for a Degree or Diploma in any other University or Institute of Higher Learning and that, to the best of our knowledge and belief, it would not incorporate any material previously published or written by another person in relation to another project except with prior written approval from the supervisor and/or the coordinator of such project and that such unauthorized reproductions will construe offences punishable under the SLIIT Regulations.

We are aware, that if we are found guilty for the above mentioned offences or any project related plagiarism, the SLIIT has right to suspend the project at any time and or to suspend us from the examination and or from the Institution for minimum period of one year".

	STUDENT NAME	STUDENT NO.	SIGNATURE
1	Jayasekara R.A.N.T	IT13023256	
2	Priyadarshani T.D.H	IT13067816	
3	Chathuranga K.B.L.	IT13048624	
4	Anooj R.	IT13096908	