Sri Lanka Institute of Information Technology

PROJECT REGISTRATION FORM

(This form should be completed and submitted on or before 11.55 PM, Friday 17th January, 2020)

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 (As per the accepted topic assessment form)	Centralized hub for securing a network of IOT devices

RESEARCH GROUP **(as per the Topic assessment Form)**	Information Security

PROJECT NUMBER	2020-086	(will be assigned by the lecture in charge)

PROJECT GROUP MEMBER DETAILS: (Please start with group leader's details)

	STUDENT NAME	STUDENT NO.	CONTACT NO.	EMAIL ADDRESS
1	A.M.I.S Abeykoon (GROUP LEADER)	IT17009614	077 0833305	isuru.srimal258@gmail.com
2	A.M.S.P.B Atapattu	IT17127356	077 4441004	supushpitha@live.com
3	H.N Jayawardhane	IT17078306	077 6851553	helanij@gmail.com
4	C.N Samarasekara	IT17126816	076 9426460	chamath96@outlook.com

SUPERVISOR Details

Kavinga Yapa Abeywardena		
Name	Signature	Date

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

Tharika Munasinghe		
Name	Signature	Date

EXTERNAL SUPERVISOR Details (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: (extract from the topic assessment form)

IoT devices connected to a specific network is accessed by the user through a home router where each device will be assigned a port individually and there will be no proper mechanism to authenticate if the user is legitimate or if it is an attacker trying to gain access to the devices by compromising the network. In case of a compromise, the whole network of devices can be taken down. When considering the information security, it can create different levels of impact based on the level of sensitivity of the information that the devices contain the information can be disclosed to unwanted/ unauthorized parties. Which can later be used for other purposes by them for financial means etc. When taking the storage capacity of IoT devices into consideration it will be considerably less, therefore updates aren't don't successfully which will in return create loopholes for an attacker to exploit the network of devices.

Description of the Solution: (extract from the topic assessment form)

This topic comes into light with the goal of protecting a small office/home office or a home network of IoT devices.

The proposed method here is to authenticate the users online using a centralized hub. This hub/portal will be placed between the router and the internet that the user will use to communicate with the IoT devices. Hence will add an additional layer of security to the network. The hub will be centrally authenticating users that will be trying to access the network and giving access to the legitimate user. All the devices will be connected through the portal and each port will be assigned to a device. And the devices will be given access rights to certain features. For example, a television might not require access to the store, but the refrigerator does, therefore the refrigerator will be provided with the required access rights.

The portal will consist of an attack detection mechanism and an attack mitigation mechanism to mitigate the attacks that were identified by the attack detection mechanism. For example, if one of the devices will found to be compromised. The mitigation mechanism will block that port from the portal to make sure that it doesn't take down the other devices of the network as well. The information that the devices hold will be of various sensitivity levels hence the protection required will be different. Hence, the information will be classified into different levels as public and private. When taking the device updating process, rather than doing a full update only needed updates can be done so that both the memory and security problems will be resolved hence the updating process can be optimized the portal will search for pending updates and push it if considered necessary. Hence the portal will also help optimize the process of updating the devices in a secure manner. The portal will act as a SSO (single sign on) in order to access all IOT components from one authenticated session. As much as SSO makes things easier for the user it can also cause a single point of failure. In order to tackle this issue a multi factor authentication process will be in use to enhance security upon user authentication.

Main expected outcomes of the project: (extract from the topic assessment form)

Ensure the security of the user over IoT devices

WORKLOAD ALLOCATION (extract from the topic assessment form)

(Please provide a brief description about the workload allocation)

MEMBER 1 ....

- Implementation of a mechanism to prevent Botnet attacks.
- Implementing Host-Based intrusion prevention to keep botnets from taking root in a system. Concentrate additional protections on specific network layer-based vulnerability, such as at point contact between specific IoT devices. Botnets typically establish communication with one or more remote servers that hackers use to retrieve private information. Prohibit unwanted traffic from leaving the network and filter data leaving the network

MEMBER 2 ....

- Implement method to detect and mitigate DoS attacks for IoT devices
- A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts and All devices and users would use public key cryptography. Key pairs will be stored on Blockchain to enable a device to lookup when any login request and hash value can be checked.

- Create a way to simulate attack type and gather data and develop machine learning algorithm and train it using gathered information.
- Use blockchain technology to support the creation of secure P2P network where all IoT devices would interconnect in a reliable way while avoiding DDos threats.

MEMBER 3

- Security updates automation and optimization by checking for new/pending updates and download suitable updates and install them automatically.
- Enable mechanism to rollback update in case of system instability.
- Using blockchain, the hash value and the timestamp of the update will be stored, and that hash value will be checked against the one prior to the update in order to determine if the update has been successfully.

MEMBER 4

- Authenticating user using multi-factor authentication and device access authorization
- Use of user credentials to authenticate a user along with basic security features such as login attempt restrictions and account lockout mechanisms.
- Develop a mobile application which authenticates the user based on a biometric fingerprint scanner.
- Create a mechanism that identifies user behavioral traits in order to identify illegitimate users and blacklist them.

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	A.M.I.S Abeykoon (GROUP LEADER)	IT17009614	
2	A.M.S.P.B Atapattu	IT17127356	
3	H.N Jayawardhane	IT17078306	
4	C.N Samarasekara	IT17126816	