

Tmp/2020/45

**Sri Lanka Institute of Information Technology**Project Topic Assessment – 2020 Regular**Topic**

Centralized hub for securing a network of IOT devices

Abstract (200 Words Max):

The main purpose of IOT (Internet of Things) is to connect devices with each other which operate over the internet. The biggest challenge in accomplishing this is the risk of security. These devices which are always connected to the internet have access to sensitive information and any security breach is a huge risk.

The IOT environment consists of hardware, software and middleware. As of modern era, cybercrimes have become a well-organized and planned set of actions. Cybercriminals always try to find vulnerabilities of systems. Connecting to the internet means it can send or receive information/data. There are many security frameworks and technologies that are being used in organizations when creating and deploying IOT devices. This area is an ongoing development.

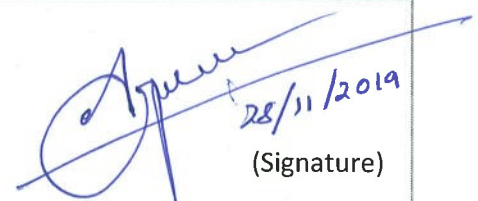
Under the given IOT security circumstance, the proposed solution could be utilized as a better way to mitigate these potential issues, as enabling a connection to the internet without proper security results in devastating vulnerabilities. With the main goal of the Centralized IOT Hub being centrally authenticating all the IoT devices of the network and secure information transmission between the users online, it will also provide device management panel, security updates, sensitive data and privacy protection mechanisms.

Research Area/Group: Select the area by referring to the document uploaded to the Courseweb

Information Security

Supervisor:

Name: Kavinga Yapa Abeywardena

Added to the Project Registration System ☒
28/11/2019
(Signature)

Research Problem:

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.

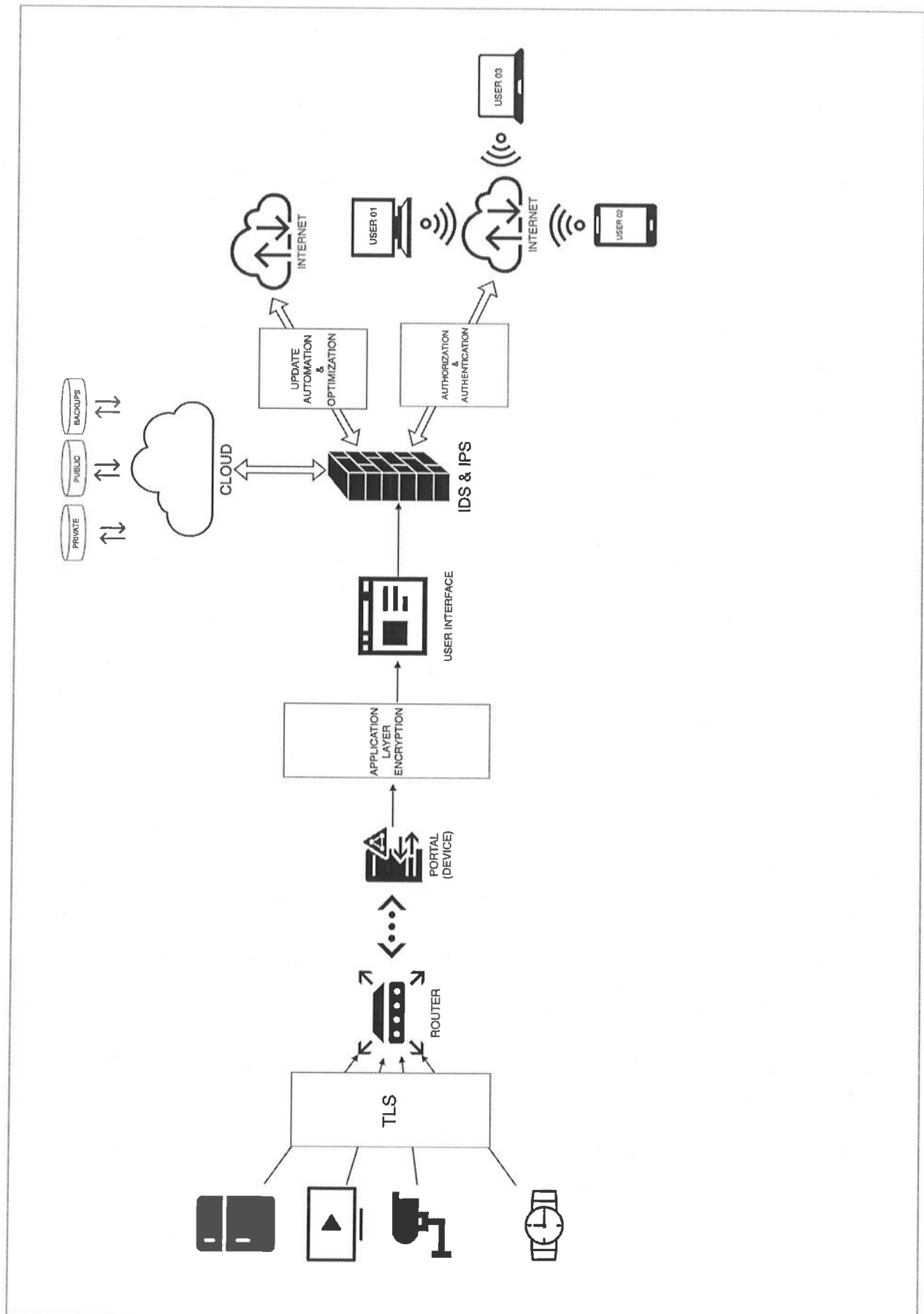
Solution proposed:

This topic comes in to 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.

System Overview Diagram for the solution proposed (Clearly indicate the main four components of the proposal)



Objectives (1 main objective and 4 sub objectives):

Main Objective: -

To ensure the security of user and device communication in an IoT enabled environment

Sub Objectives: -

1. To ensure the user privacy protection
2. To IoT attack detection and mitigation
3. To Secure communication between P2M and M2M
4. To mitigate IoT security risks

Task List divided among the members

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
- Create a way to simulate attack type and gather data and develop machine learning algorithm and train it using gathered information.

Member 3

- Security updates automation and optimization
- Using blockchain the hash value and the timestamp of the update will be stored, and that hash value can be checked against the one prior to the update

Member 4

- Authenticating user using multi-factor authentication and device access authorization
- OTP will be used in addition to the use of user credentials to authenticate a user
- Check for pending updates and push necessary updated automatically

Technologies to be used:**Software Components**

1. Blockchain for secure communication encryption.
2. Machine learning for anomaly and signature based detection of Intrusion prevention system.
3. OPNET/ CISCO packet tracer for simulation.
4. Python as server side scripting language and for signature based and anomaly based algorithm creation.
5. HTML, CSS, JavaScript as client side scripting languages.

Hardware Components

6. Raspberry Pi 4 4GB Starter Kit including Power Supply with Noise Filter, Set of Heat Sinks, Micro HDMI to HDMI Cable.
7. Amazon AWS Cloud Storage.
8. IOT devices.

Team Members:

Student Name	Student ID
Leader: A.M.I.S Abeykoon	IT17009614
Member 2: A.M.S.P.B Atapattu	IT17127356
Member 3: H.N Jayawardhane	IT17078306
Member 4: C.N Samarasekara	IT17126816

For official use only

Acceptable: YES/NO

Minor Corrections (if necessary)

Any other Comments:

Approved by the review panel:

Member's Name	Signature

--	--

Important:

1. According to the comments given by the panel, do the necessary modifications and get the approval by the **same panel**.
2. If the project topic is rejected, find out a new topic and inform the CDAP Group for a new topic pre-assessment.
3. A form approved by the panel must be attached to the **Project Charter Form**.