CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

Research Progress Report

Record/Log of Contact Sessions between the Student and the Guide

Register No.: 1747230	**Name of Student: Lakshay Grover**
Class: 3-MCA	**Paper Code : MCA381**
Name of the Research Guide: Nandhakumar K G	

Date	Contact Mode (Email / in person)	Duration (Hours)	List of Interaction
Week_1 Session 1	**Email**	02 Hrs	Domain Introduction and discussion on work done.
Week_1 Session 2	**In Person**	02 Hrs	Process of Research, how to identify a problem, techniques of research progress.
Week_2 Session 1	**Phone**	02 Hrs	Study of Onion Routing and ToR Network
Week_2 Session 2	**In Person**	02 Hrs	Discussed the techniques, difficulties, and challenges in ToR Network and IoT Network.
Week_3 Session 1	**Phone**	02 Hrs	Study of Different Attacks in IoT Network
Week_3 Session 2	**In Person**	02 Hrs	Discussion on Problem Identification and pursuing the challenges/ flaws in current method.
Week_4 Session 1	**Phone**	02 Hrs	Study the various option to overcome the challenges faced in current method.
Week_4 Session 2	**In Person**	02 Hrs	Discussion on Month Progress and implementation plan.
Additional Session (If so)			

Activities Done (for a Month – June 2017)	
Activity Plan for the next one month commencing from the close of the current Report Period.	To start with writing paper and implementation work.

Student Comments:
Gained knowledge on security breaches and flaws in networks of IoT. To start with literature review writing.

Research Guide Comments:

Signature of Student:	**Signature of Guide:**

MCA381 - RESEARCH PROBLEM IDENTIFICATION

Progress Report Submission

Submitted by

LAKSHAY GROVER

Under the Guidance

NANDHAKUMAR K G

July 2018

Department of Computer Science
CHRIST (Deemed to be University)
Hosur road, Bengaluru 560 029

Research Domain – Problem Statement Title

Reg. Number : 1747230
Student Name : LAKSHAY GROVER
Guide Name : NANDHAKUMAR K G

# Introduction to topic, existing scenario and applications :

Sending the data over a network is prone many attacks and it the primary medium for IoT devices to interact. In order to ensure the security of data and privacy of the devices interacting, it has become necessary to have a secured protocol for data transfer.
The existing scenario uses IEEE 802.15.5 protocol which offers basic
authentication and security . The IoT threat model changed dramatically after WSNs gained the ability to access the public internet as attackers can reach WSNs
ubiquitously where sensor nodes are the most vulnerable due to scarce computational resources.
The existing application majory uses HTTP as a transfer protocol. The packets from the gateway are secured using Hypertext Transfer Protocol Secure (HTTPS), which makes use of a Secure Sockets Layer (SSL) certificate to ensure the authenticity of the sender/receiver.

# Problem Statement :

The problem with the existing system is that all the packets are sent openly on the internet. An adversary with malicious intent and sufficient computational resources can easily perform an attack to extract and manipulate the packets being sent/received. A Key Reinstallation Attack (KRACK) can compromise all packets in a wireless network without breaking the encrypted authentication key . An
IoT network connected and controlled through the public internet is exposed to a huge number of malicious users.

# Necessity of Defining the Problem (Research Gap) :

The need to securely transfer data over wireless network is must since, if there’s a data breach, all the devices connected to target device can be compromised leading to illegal access and extraction of any information that is confidential, personal, or financial in nature.

# Literature Review and Analysis : Phase I (Minimum 03 articles)

Sl.No	Author and Title	Objectives of the paper	Methodology Proposed	Result Analysis	Tools used	Student observation on this paper (Remark)
1.	**Ajay Mishael and Joy Paulose**	**To make the data transfer between IoT devices secure.**	**The data is sent through a onion network where 7 layers of encrypted data is sent over a randomly selected path of relays that**	**Data Transferred is more secure and prone to MITM, DoS, Replay attack and Key Reinstall**	**Raspberry Pi model 3, Arduino Uno, Python, Tor Network**	**Data transferred over ToR has more Response time as compared to data transferred over HTTP protocol.**

			provides anonymity	ation Attack(KRACK)		
2.	Security and Privacy Challenges in the Internet of Things	Abha Kiran Rajpoot, Mukul Varshney, Aparajita Nailwal	The paper is focused on attacks during the operational phase. These attacks can vary from eavesdropping to active routing attacks to denial-of-service attacks. These attacks can be separated into a few categories, physical capture, disrupt, degrade, deny, or destroy a part of the network, manipulation attacks, and eavesdropping attacks.	The ultimate difference between IoT and Internet is the networks in which they are deployed. IoT ha low power lossy networks which complicates security issues. Protocols like ROLL secure lower layers which conserving resources.	----	In order to gain more security, there is a need to have and IoT device that has more processing power and capability to handle the algorithms and protocols that can ensure security, integrity and privacy.
3.	Tor: The Second-Generation Onion Router	Roger Dingledine, Nick Mathewson, Paul Syverson	Tor is a circuit-based low latency anonymous communication service. Tor works on the real world Internet and requires no Kernel modification. It is an overlay network; each onion router (OR)	The data sent over a TOR network uses a random chosen relay where it will have 7 layers of encryption by the first node and decryption is	----	ToR network is slow but reliable. An increasing number of nodes would ensure an increase in bandwidth of the data.

			runs as a normal user-level process without any special privileges. It makes use of empheral keys to communicate between next nodes.	**possible only by the last node. Each node only the the former and latter node where the data passes through.**		

# Objectives of Research Domain Based :

- **Primary Objective**

-> To secure the IoT network so that data transferred over the network either locally, or using the Internet is secured and immuned to various attacks like Man In the middle Attack, Krack, Dos , etc.

- **Secondary Objectives**

-> The increase the speed over which data travels through ToR Network by distributing the data into smaller chunks or find an alternative way to transfer data over the network more securely.

#References :

1. R. Dingledine, M. Nick, and P. Syverson, “Tor : The Second-Generation Onion Router,” 13th USENIX Secur. Symp., 2004.
2. T. Borgohain, U. Kumar, and S. Sanyal, “Survey of Security and Privacy Issues of Internet of Things,” arXiv Prepr.
3. Securing IoT Networks Using and Onion Routing Based Approach - International Journal of Mechanical Engineering and Technology (IJMET)
4. N. P. Hoang, D. Pishva, and R. Asia, “A TOR-Based Anonymous Communication Approach to Secure Smart Home Appliances,” vol. 3, no. 5, pp. 517–525, 2014.