LAB ASSIGNMENT 5 **SJSU ID**: 012018487 **NAME**: NIVEDHITHA RAMARATHNAM KRISHNA

TASK 1:

Manipulating Event Reporting:

Referring to the paper on "Experiments with Security and Privacy in IoT Networks" (Schurgot), manipulation of data sent from IoT hub to the Hub-Server can significantly impact the cost of the unauthorized users to attack the system. Thus, this ensures privacy and the user's activities cannot be tracked easily.

This can be implemented by using firewall rules such as "DROP" on chains "INPUT, FORWARD and OUTPUT". Manually creating firewall rules such as Dropping TCP packets at a specific time till a particular time will change the timestamp of the actual event occurrence. For example, if the user leaves the home at 9:30 then the sensor in a home automation system might log this event. If Drop TCP rule is inserted in iptables then this exact timestamp is not recorded and the time at which rule is removed is recorded as the event timestamp at the server's end. Hence confusing the attacker.

Similarly inserting events using artificial techniques such as triggering sensors using robots etc., can trick the attacker.

Other manipulating techniques includes blocking only of the "sensor application data" depending upon size of the packet (which can be analyzed by observing network traffic) other firewall rules can be added and hence dropping the main events.

Apart from changing firewall rules other methods such as mobile presence spoofing can help in fake GPS location which would again trick the attacker.

TASK 2:

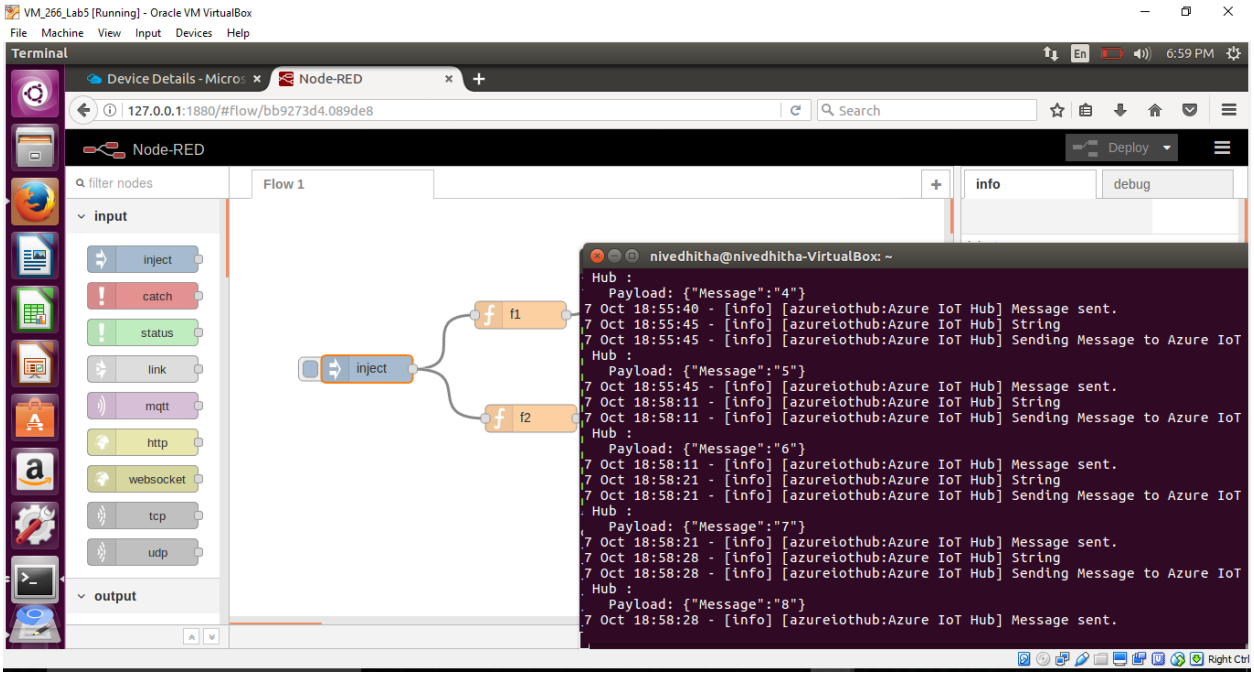

Figure shows initial injection of message successful.

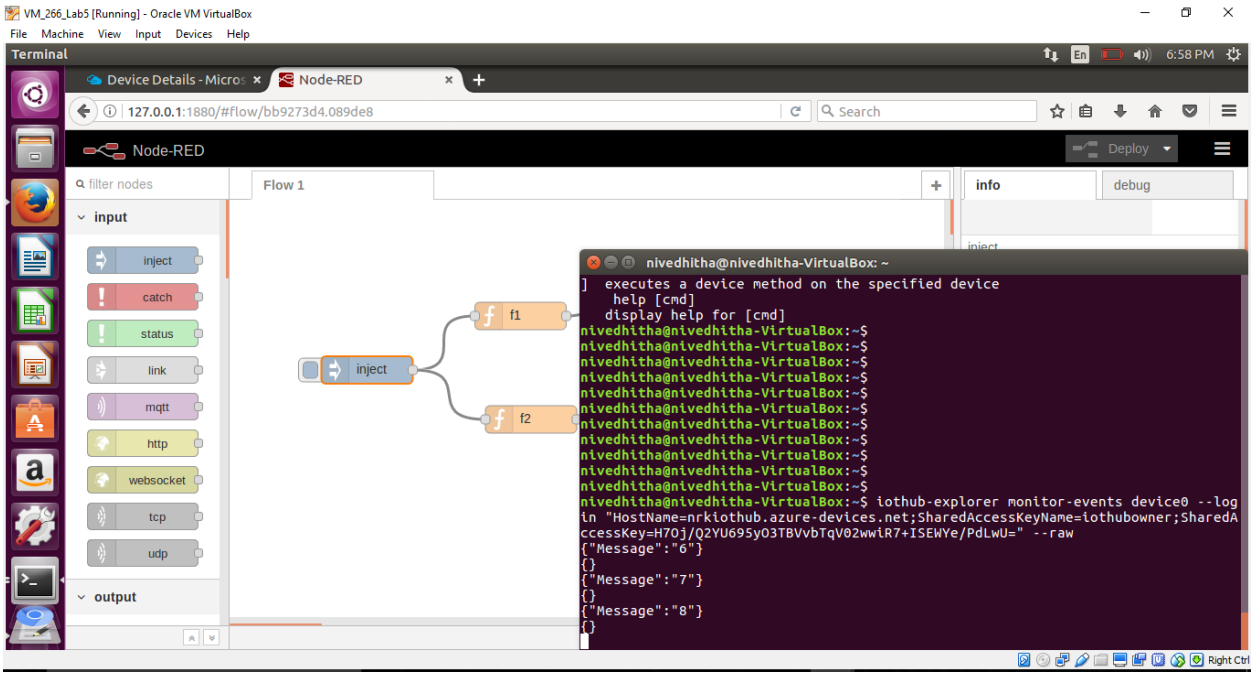

Figure shows successful reception of message.

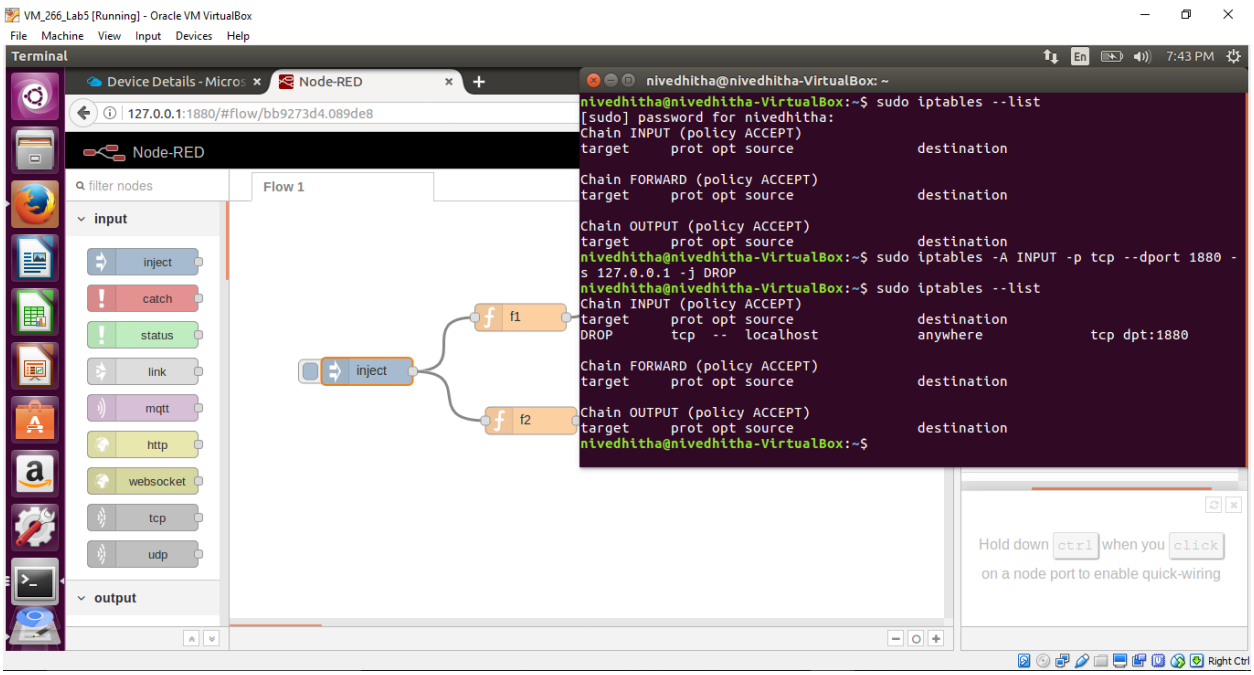

Figure shows adding DROP rule on INPUT chain at particular IP and port to “iptables”.

RULE USED:

1. sudo iptables -A INPUT -p tcp –dport 1880 -s 127.0.0.1 -j DROP

This rule drops TCP packets at port 1880 (port given). Other rules as mentioned in the paper such as FORWARD can also be implemented to delay TCP packets by dropping them.

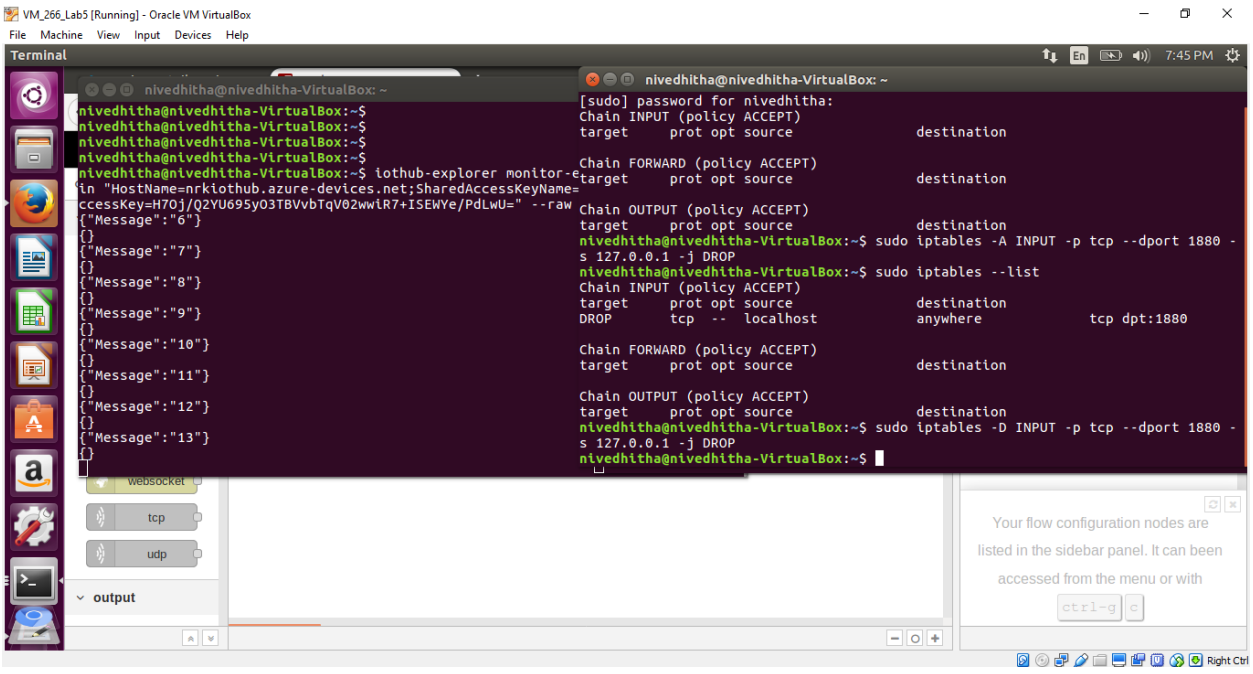

Figure shows as soon as the rule is dropped the messages are received.

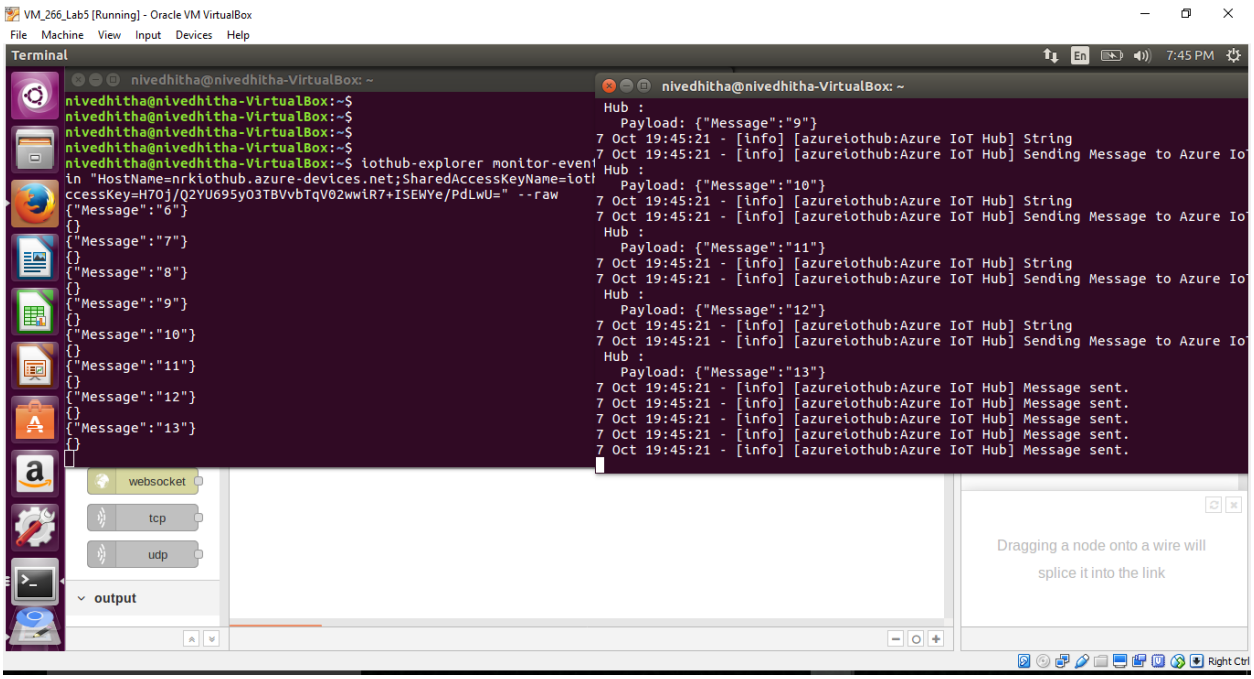

Figure shows that after removing rule from iptables messages are sent and received continuously.

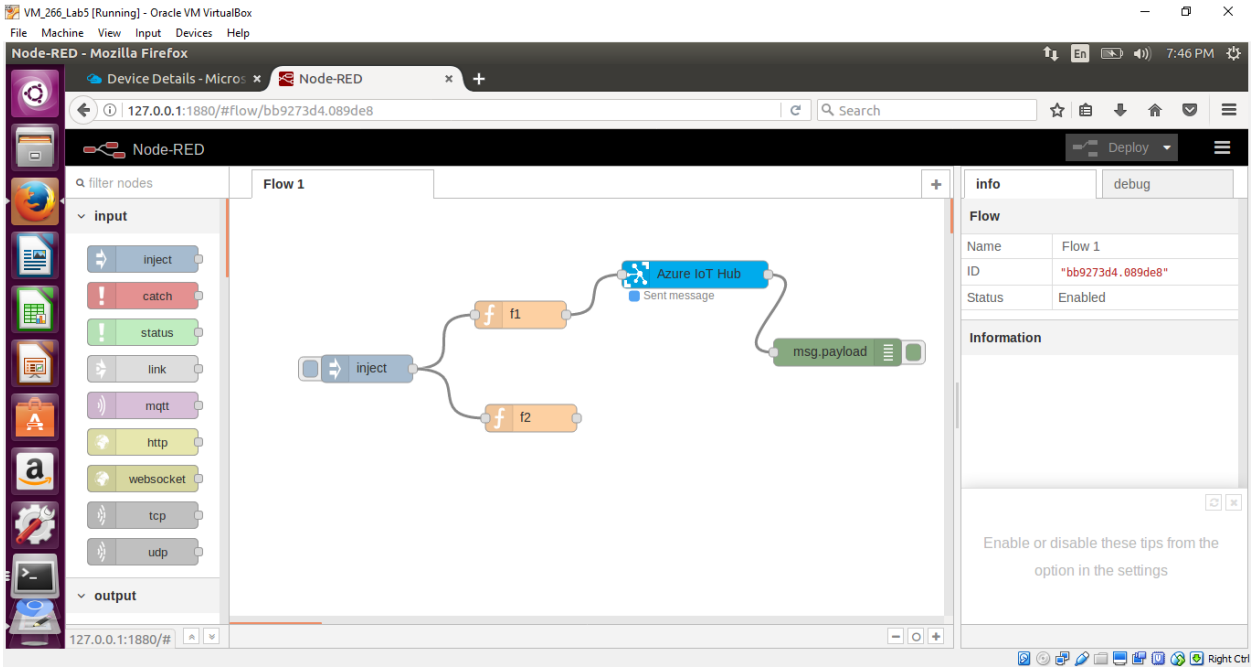

Figure shows the workflow established.