Combination of Virtual Private Network and Wireless Sensor Network: Protection Against The Interference Problem of IOT

Pramathesh Majumdar
pramathesh@outlook.com
ASET, Amity University
Uttar Pradesh, Noida, India

Ayushi Pandey
ayushi.pandey26@gmail.com
ASET, Amity University
Uttar Pradesh, Noida, India

Sunil Kumar Khatri
skkhatri@amity.edu ,
Amity Institute of Information Technology
Amity University Uttar Pradesh,

Rachna Jain
jain.rac16@gmail
Amity Institute of Information Technology
Amity University Uttar Pradesh, Noida, India

Rana Majumdar
rana.majumdarwb@gmail.com
ASET, Amity University
Uttar Pradesh, Noida, India

Ved Prakash Mishra
mishra.ved@gmail.com
Amity University Dubai, UAE

Abstract - As the era of the Internet of Things (IoT) is emerging rapidly, the interference problem is also increasing at the same pace. In IoT based connections, as we know that devices share a common communication channel to interact with each other, the interference problem arises as all the devices are connected. Once an attacker gains access to any of the devices in an IoT enabled network, the whole IoT network becomes susceptible to breach. The biggest example of it is the IoT enabled CCTV hacking. In this work, we are proposing the usage of Virtual Private Network (VPN) and Wireless Sensor Network (WSN) to create a virtual environment and to protect each device from IP address breach that is connected to an IoT network. Using VPN, each IoT device will gain their own virtual environment which will enable it for using a dynamic IP address to connect to another IoT device's virtual environment. Using WSN, the virtual environments will be able to identify any signal interference that can cause any security breach.

Keywords – Internet of Things (IoT), , Virtual Private Network (VPN), Wireless Sensor Network (WSN).

INTRODUCTION

The main and foremost basic behind the technologies of any field in today's age is how devices can talk to each other. Keeping this in mind, several inventions were and are being made to enable devices to communicate. Internet of Things (IoT) is the filed which makes this attempt possible. But, as it shows the way how to make the devices talk to each other, it introduces some new kind threats as well. As we know, in IoT all the devices are interconnected, hence the chance of security breach increases drastically as a hacked device may lead to security shut down of all the other connected devices.

While a relatively few connected gadgets will use wireline communications, the bulk of these devices ranging in applications from farming to medical to toasters to pets - will connect wirelessly over Bluetooth, Wi-Fi, or cellular. Some will be designed to limit EMI emissions to the proper channels and reject out-of-band power, but many won't.

Cyber-criminals are trying to find ways to breach the IoT security. As much devices are interconnected, the chances of vulnerability increase at the same pace. For e.g., back in 2016, the largest IoT attack of the history was launched on service provider "Dyn" using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN.

By utilizing thousands of insecure associated gadgets, hackers can create DDoS assaults that can handicap the foundation, frameworks, and lifestyle. Or then again, assailants can specifically misuse a gadget and utilize it as a portal to further levels of a system where they assemble important private information.

The following figure shows the increased threat to data privacy of connected devices in IoT (based on the study done by ISACA [13]).

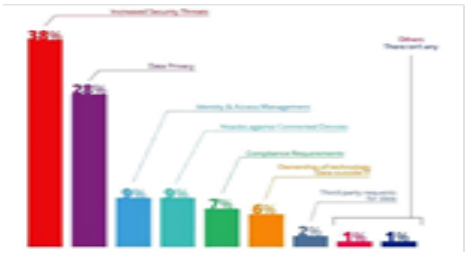

Fig. 1: An Increased threat to data privacy in IoT[13]

In this work, we are introducing the concept of combining Virtual Private Network (VPN) with Wireless Sensor Network (WSN) to secure each interconnected device in a network.

Here, we assume each device as a node (n1, n2, …, nX). Every node will be assigned a VPN setup which will provide the device a designated way to interact with other nodes' VPN setup. Using wireless sensors network, we will be able to track the number of attempts that took place for a security breach. This record will then be used to further improve the VPN setup according to the depth of the vulnerability level.

RELATED WORK

At this moment, the most crucial detriments in IoT is the shortcoming of this meta-system to different sorts of ambushes. Obliged limit and dealing with restricting in IoT contraptions influences the execution of sensible to confirmation parts incredibly troublesome IoT gadgets are slanted to ambushes, their lacking level of security makes them astoundingly fragile concentrations for being vulnerable [2].

The rapid development of new applications using smartphones in the world caused all users of the IoT community to be faced with one major challenge of security in the form of side channel attacks against highly intensive 3D printing systems. The smartphone formulated Intellectual property (IP) of side channel attacks investigate against 3D printer in the physical domain through reconstructed G-code file through primitive operations [3].

Specifically, hackers make use of these devices in coordination to make botnets and make Distributed Denial of Service (DDoS) strikes against a pariah. Such disturbance can turn an IoT orchestrate improving the assignment of an industry or an organization into a security chance itself. Henceforth, the deal of these structures by malicious experts don't simply harm these substances, yet what's more the general ICT condition [3].

The unfortunate use of covering channels among neighboring APIs may provoke extended essentialness usage because of the ensuing re-transmissions. Covering channels among neighboring APs can decrease the execution of preliminary Wi-Fi– based arranging. The correspondence goes for an AP is considered as the cell. By distributing non-covering channels among neighboring cells, the block issue between channels among the APs can be settled [4-6].

The attack basically spreads by first debasing devices, for instance, webcams, DVRs, and switches that run some variation of BusyBox. It by then finds the definitive capabilities of other IoT contraptions by strategies for a mammoth drive, contingent upon a little word reference of potential username– watchword sets. It causes DDoS against a game plan of target servers by continually inducing to weakly composed IoT devices [7-8].

Most remote frameworks are demonstrated as layer 2 (L2), or data interface tradition. Starting late, IoT and huge data dealing with have propelled the use of remote sensor frameworks to interface and send data to server cultivate applications using the Internet. To do in that capacity, the execution of an IP stack on the remote center point, or the section of the IP and remote L2 mastermind, has been proposed.

They are made to allow the application of the IP framework to get to L2 remote framework center points [9].

In the other work, IoT was deciphered using an IP just to endure data made by non-IP center points. Thusly, we display another novel sort of VPN for partner PANs to server ranches, which has three features. The first is that it is a traverse framework instead of an entryway. The remote sensor orchestrates data interface diagrams are transported direct end-to-end through the IP spine [10-12].

INTERFERENCE PROBLEM IN IoT: OVERVIEW

The Internet of Things is the most recent in a long queue of progressively vital advancements, and the quantity of associated protests inside this web is developing at an exponential rate. Gartner anticipated that the quantity of "things" being used in 2019 would grow 22 percent and by 2020, the IT investigate firm anticipated that there would be upwards of 20.8 billion associated protests being used. Organizations and purchasers alike are finding the advantages of the IoT to surprise, and numerous are amped up for its future.

In any case, sadly, IoT gadgets still experience the ill effects of fundamental security vulnerabilities and it is accurately this absence of security that makes them so appealing to programmers. Be that as it may, it's not only a secret word issue any longer. Assailants comprehend that makers and clients are awakenings to the issue of passwords on IoT gadgets, as are looking for more intricate approaches to get to them. As this pattern proceeds, and programmers turn out to be progressively innovative while hunting down new gadgets and approaches to enroll them, there is extremely no restriction to the size and size of future DDoS assaults driven by IoT botnets.

All things considered, any gadget that has an Internet association and a processor can be abused. In a perfect world, all gadgets ought to be compelled to experience a type of system design before being utilized, as opposed to being exploitable from a default position.

Computerized Enterprises can shield their systems from DDoS assaults fuelled by IoT-driven botnets by sending continuous, the robotized arrangement at the system edge, which can quickly distinguish and alleviate DDoS action and kill dangers from entering a system. Similarly, as with all DDoS dangers, clear permeability is a significant advance in distinguishing and protecting against assaults.

Ransom Denial of Service (RDoS) assaults additionally returned in Q3 2017, the report found, as this strategy permits cybercriminals to blackmail cash from their casualties. In these assaults, the criminal will normally

make an impression on the casualty requesting a payment, frequently extending from five to 200 bitcoins, as indicated by a current Kaspersky Lab report. On the off chance that the casualty declines to pay, the assailants debilitate to sort out a DDoS assault on one of the casualty's imperative online assets.

As IoT botnets keep on rising, we may soon observe programmers put on more sensational RDoS presentations to exhibit the quality of their digital capability, with the goal that their future requests for payoff should be considered more important," Stephenson said. "Paying the payment is infrequently the best guard, as it just urges these requests to spread like fierce blaze.

4. PROPOSED MODEL

In our work, we are proposing the concept to combine the Virtual Private Network (VPN) with the concept of Wireless Intrusion Detection System

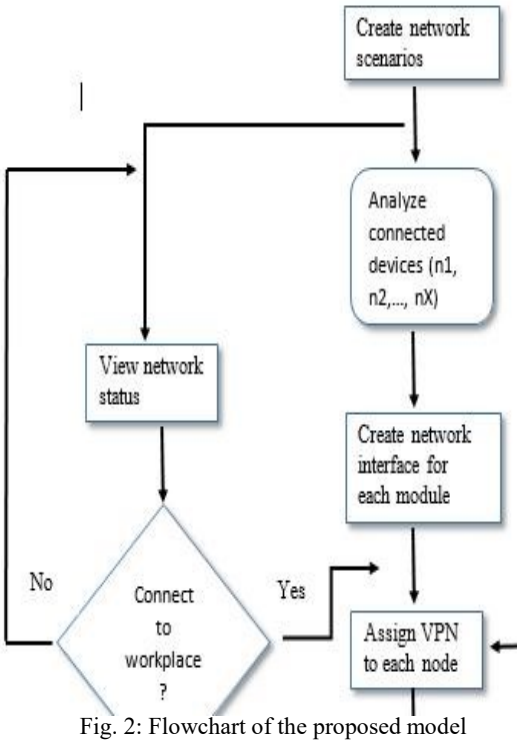

Fig. 2: Flowchart of the proposed model

(WIID) to secure each node that is interconnected to each other in an IoT network. Here we are assuming every device as interconnected nodes which represent a module of the IoT network. The nodes are presented as n1, n2, nX, where X is the maximum number of nodes.

The steps that are followed in our proposed model are as follows –

Step 1: Create network scenarios

Devices are interconnected using an IoT network to create a network scenario. This is the combination of all the devices that communicate to each other via a physical or a wireless network and acts as a framework.

Configure the IP interfaces and IP addresses, and also include a determined default course for the framework. Moreover, we can arrange any framework wide system administrations, for example, naming and index administrations. The accompanying cases accept that we are utilizing the settled mode for arrange setup.

Step 2: Analyze connected devices

As billions of gadgets are added to the Internet of Things, organizations require an approach to increase one of a kind bits of knowledge from their IoT information.

IoT Connection Service empowers organizations to reveal new information-driven bits of knowledge that can change their generation procedure, make one of a kind client encounters, increment operational effectiveness and enhance ecological stewardship.

Each device needs to be analyzed for the IP address configuration in order to set up a VPN. The analysis is done using the network framework created earlier with the help of NS2 tool.

Step 3: Create network interface for each module

For communicating one VPN with other VPNs, there have to be some dedicated interfaces to the VPNs. These interfaces help in talking with the other networks and work as a gateway. The following code was generated to create a network interface –

Create-network-interface
[--description <effective-point>]
[--testing | --no-testing]
[--groups <effective-point>]
[--ipv6-address-count <effective-point >]
[--ipv6-addresses < effective-point >]
[--private-ip-address < effective-point >]
[--private-ip-addresses < effective-point >]
[--secondary-private-ip-address-count <value>]
--subnet-id < effective-point> [--client-input-json < effective-point>]
[--generate-client-skeleton < effective-point >] --desc (double)

Explanation of the interface –
---testings | --no-testing (Boolean)

Checks whether you have the required assents for the action, without making the request, and gives a botch

response. In case you have the required assents, the slip-up response is Testing Operation. Else, it is Unauthorized Operation.
--groups (list)

Step 4: Assign VPN to each network

Once the interfaces are created for each node, the VPNs are configured for the nodes to create the private_network_modules. These processes are done using the following steps –

- Enter into Network and sharing center of the system.
- Manage the network connections and change the adapter settings.
- Now enter into file option and click on a new incoming connection.
- Now mark which nodes have to be given VPN connections and click next.
- Choose which protocols need to be started. Generally, TCP/IPv4 needs to be started to access the network.
- Once done, click on close.

Now the properties of the new nodes have to be well-defined and for that, IP address ranges have to be setup.

- Enter incoming connections section in the network connection window.
- Select the TCP/IPv4 option.
- Now enter the required IP addresses in a manner that they should not conflict with the DHCP ranges.
- Now click OK.

Step 5: Enter CISCO ASA 5500 firewall IP address

In our work, we are utilizing the CISCO ASA 5500 design benchmarks to setup the earth for the VPN firewall.

The ASA programming depends on Linux. It runs a solitary Executable and Linkable Format program called lina. This timetables forms inside instead of utilizing the Linux offices. In the boot grouping, a boot loader called ROMMON begins, stacks a Linux portion, which at that point stacks the lina_monitor, which at that point loads lina.

The ROMMON likewise has a charge line that can be utilized to stack or select other programming pictures and arrangements. The names of firmware records incorporate a form indicator, - smp implies it is for a symmetrical multiprocessor (and 64 bit design), and diverse parts

additionally demonstrate if 3DES or AES is bolstered or not.

The ASA programming has a comparable interface to the Cisco IOS programming on switches. There is a charge line interface (CLI) that can be utilized to question work or arrange the gadget. In config mode, the design proclamations are entered. The design is at first in memory as a running-config yet would regularly be spared to streak memory.

Step 6: Apply Wireless Infrared Intrusion Detection System (WIID)

The WIID framework is an infrared-based border security checking framework that comprises of multi-beam infrared sensors coordinated with double band (2.4 GHz and Global System for portable correspondence) remote specialized gadget. These are put on the assigned edge.

Remote infrared sensors can work in such the double radio band, which thus ensures that there is positively no loss of data. Multibeam remote infrared sensors likewise distinguish break viably progressively to create spot caution and remote alarm.

The brutal idea of nature/territory around the border makes it troublesome for fiber optic sensors and weight sensor strips to work viably and create fitting alarms. Subsequently, there emerges a huge window for false caution age. On account of ultrasonic sensors, they don't bolster a wide range for identification of a hindrance or interloper. In spite of the fact that, the working rule of photoelectric sensors is to some degree like that of infrared (IR) sensors, their working precision is much lower contrasted with infrared sensors and their arrangements.

The WIID System produces visual alarms at the local security office with the end goal of crisis notice. Messages are additionally sent by means of SMS to the no-obligation security officers and watching staffs with respect to the episode.

The framework produces spot alarms through hooter and concentrates light so as to caution the closest security staff and after that guide them to the area of occasion at the suitable time. This framework additionally incorporates a reconnaissance camera framework that gives data about the idea of the risk.

There is negligible human intercession required, in this manner influencing it to fall flat evidence to human mistakes and makes funds in the enlisting of security workforce.

CONCLUSION AND FUTURE SCOPE

This model provides a systematic way to further provide security to each device connected to an IoT network by protecting them from external unauthorized interference using VPN technology. Wireless sensor technology is used to track the security breach attempts to further improvise the security level using the records gathered from the tracking system i.e. WIID. This work can be further extended to the next level using advanced VPN system using IPv6 configuration to deploy extra security level in the IoT framework

REFERENCES

[1] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), pp.80-84.
[2] Özçelik, M., Chalabianloo, N., & Gür, G. (2017,). IEEE International Conference on Software-Defined Edge Defense Against IoT-Based DDoS. In Computer and Information Technology (CIT), pp. 308-313.
[3] Bilal, M. (2017). A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers. arXiv preprint arXiv:1708.04560.
[4] Wiklundh, K., & Stenumgaard, P. (2017). International Symposium on EMC challenges for the internet of things. In Electromagnetic Compatibility-EMC EUROPE, pp. 1-6.
[5] Bakshi, A., Chen, L., Srinivasan, K., Koksal, C. E., & Eryilmaz, A. (2016,). EMIT: An efficient MAC paradigm for the Internet of Things. IEEE International Conference on In Computer Communications, INFOCOM pp. 1-9.
[6] Stankovic, J. A. (2014). Research directions for the internet of things. IEEE Internet of Things Journal, 1(1), pp.3-9.
[7] Khalil, N., Abid, M. R., Benhaddou, D., & Gerndt, M. (2014,). IEEE Ninth International Conference on Wireless sensors networks for Internet of Things. In Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 1-6.
[8] Mynster, A. P., & Jensen, P. T. (2016). International Symposium on EMC for the IoT. In Electromagnetic Compatibility-EMC EUROPE, pp. 144-149.
[9] Tsitsigkos, A., Entezami, F., Ramrekha, T. A., Politis, C., & Panaousis, E. A. (2012). A case study of internet of things using wireless sensor networks and smartphones. In Proceedings of the Wireless World Research Forum (WWRF) Meeting: Technologies and Visions for a Sustainable Wireless Internet, Athens, Greece pp.23-25.
[10] Zin, H., Kim, C., Wu, M., & Kim, S. (2017). Avoidance of channel interference in polygonal IoT networks. Concurrency and Computation: Practice and Experience, 29(11).
[11] Hata, H. (2017). A bridging VPN for connecting wireless sensor networks to data centers. Journal of Reliable Intelligent Environments, 3(4), pp.211-219.
[12] Dhar, S. K., Bhunia, S. S., & Mukherjee, N. (2014,). Fourth International Conference of Interference aware Scheduling of Sensors in IoT enabled Health-care monitoring system. In Emerging Applications of Information Technology (EAIT), pp. 152-157.