Smart Monitor for Enhancing Security in Smart Home Systems

Bhuvana Janita\textsuperscript{1} and Jagadeesh Kannan\textsuperscript{2}

\textsuperscript{1,2} School of Computer Science & Engineering, Vellore Institute of Technology Chennai Campus, \textsuperscript{1}bhuvana.janita2017@vitstudent.ac.in, \textsuperscript{2}jagadeeshkannan.r@vit.ac.in

Abstract. This Smart Home device like smart TV, Refrigerator, Smart Thermostat, Smart bulbs, Smart garage doors are preferred for hassle free life, better ambience and to automate mundane tasks. Smart Home helps in Mindful resource utilization and also in Wellness assisted living. Though there are many advantages, Smart Home devices are basically embedded devices that comes with firmware and limited memory capacity. These devices cannot have an Antivirus installed for preventing Virus, Malware, Worms and other security hazards. The Internet of Things has no standard protocol for communication. This is a serious security threat for Home Automation systems. Proposed Idea is to introduce an edge device that will monitor and manage all the home devices and alert user in the event of their abnormal activity. The proposed idea would mitigate Man-in-the -Middle (MITM) attacks and Denial of service (DOS) attacks.

Keywords: Denial of service attacks, Home Security, Home Monitor, Home Automation, Man-in the –Middle attack.

1. Introduction
There are many Benefits of Remote Monitoring Network including locking / unlocking houses by a long range, getting alerted in case of smoke / burn in the house and optimizing the care of gadgets. It is advantageous to support the disabled who are ill and tend to stay at home, instead of at a clinic. The automation system Internet of Things Home fully optimizes the home life and reduces resources. Depending on the context, the client can adjust the atmosphere. Reading the electric and water meter would be highly useful for careful power use. It is also possible to track the corrosion of the units, which ensures their servicing simple. These apps do carry a lot of protection and security concerns, given the benefits. IOT computers have a configuration with less battery and less processing power. They still haven't developed an anti-virus app. These apps carry apparently massive quantities of data and are most susceptible to protection activities, such as Denial of Service (DOS), intrusion threats and Cyber security threats.

2. Related works
Please to understand the limitations of the Smart home devices, Sukhvir et.al performed an experiment that highlighted the devices’ contact patterns and attempted to examine the transmissions using wire shark \cite{1}. The study which was carried out on certain smart homes devices like Phillips Hue light-bulb, the Belkin WeMo power switch has showcased the ease with which security and privacy can be
compromised in these devices as shown in figure 1. The case study on Samsung smart things Hub conducted by Earlene Fernandes.et.al Showed that there were access privilege escalations in the design of these systems [2]. The permission that is accessed granted the users with the permission to access all the devices that are connected to the Hub even when permission is not sought.

Wei Zhang.et.al exposed Event spoofing done by misbehaving smart apps in Samsung Smart Things. A deceptive SmartApp with the understanding of the host and system descriptors can fake an inappropriate occurrence, which is simple to remember. The Smart Things database will find the event valid and spread it to all Smart Apps that connect to the matching event-related functionality [3]. To detect smartapp mis behavior the Authors have proposed HoMonit that comes close encrypted traffic-induced SmartApps actions with planned actions determined in their files or UI frameworks.

Smart Home devices have heterogeneous protocols and communication pattern. To derive meaningful information from this type of communication will require new techniques. Roberto Morabito et.al have proposed LegIoT (Light weight edge Gateway device) which by integrating the deployment of different constructs with the advantages of container-based scalability, edge gateways are enhanced to allow automated energy management and necessarily show considerations like energy consumption, dual-tenancy and interoperable [4].

3. Smart Home systems

Before A smart home system generally consists of three components, (1) home server, (2) home gateway, and (3) smart home devices. The home server provides storage, integration and distribution function of the information collected from various media in the home. Next, the home gateway interconnects internet and a wired/wireless home network. Home automation systems that illustrated in figure.2 gather data via various sensors and send and receive among systems and gateway products. And it is easily mountable over the environment, and the vendor provide Two specifications: a software development kit (SDK) with specific features and standards to handle larger IoT implementations (e.g., ARM, AVR, PIC) and a tracking system (gateway or web-based platform) to link different instruments to a home automation network. The SDK is not designed specifically for one but for a variety of devices [2] and all the tools do not have a security system.
3.1. **Drawbacks in existing Smart Home systems**

Although the intention of smart home systems is to automate day to day activities in home or to improve better ambience, currently available systems lack security and centralized monitoring capabilities. Security comes with a cost which the different smart home product vendors hesitate to offer. Multiple products and heterogeneous protocols increase the challenge in providing a security solution. Even the smart home users use different products which require them to handle multiple smart apps individually as in figure 3. Not all Smart Home Users control their smart devices with a Hub. A smart Hub is a device which acts a centralized unit through which all the smart home devices in a home are monitored. The user has the privilege to control all the devices via a single smart hub app which makes it easier for the user.

3.2. **Attacks on Smart Home systems**

IoT computers have a firmware with little battery and less processing power as in figure 4. They still haven't activated a bashers-virus app. These apps carry apparently large quantities of data and are most susceptible to protection attempts, such as Denial of Service (DOS), ransomware threats and Ransomware attacks.
3.2.1. Baby monitor and CCTV Attacks
A person with an intention to hack a house constantly looks for open ports or Wi-Fi hot spots with weak passwords to hack. Unfortunately, there are many websites and apps available in market that will list down the number of open cameras in a particular neighborhood. The number of Baby Monitor and CCTV attacks [6] reported are on constant increase. The users are completely unaware that they are being exposed as there are no systems to alert them.

3.2.2. Mirai/Ransomware Attacks
Figure 5 shows Mirai Attacks that was reported in 2016 is a typical DDOS (Distributed Denial of services attack) on IoT devices like scanners and cameras. This attack is considered a wake-up call that exposed the vulnerabilities of the smart devices that are in day-to-day use and the importance of creating security measures to prevent them.

The Hacker/Attacker makes use of a compromised system in a network and installs a BOT in the machine. The compromised device then installs the BOT/Malicious code in the connected devices of the network. This group of affected devices in a network is called a BOTNET which are designed to act on the commands of the Attacker. Some BOTNETS totally affects the targeted device while others silently run in the background parallel sending information about the network devices to the Hacker illegally. The User will not have any clue of the BOTNET in the latter scenario as the devices don’t show any abnormality in its daily operations. In case of Ransom Ware Attacks, the malicious code/Malware is installed in the compromised devices and the Attacker demands a ransom amount from the user to return the system to its normal state. In the both the cases early detection is difficult for a normal user and he/she comes to know it only after the damage is done. Hence periodic scanning for any malicious code installed in the devices becomes important.

3.2.3. Weak permission Management
Fernandes.et.al exposed the lack of fine grained security management system in Samsung smart Home system [2]. Smart Things has a priority isolation process called requirements which specifies the set of operates that a Smart-App can problem to a supported smart home unit. A functionality is consisting of a series of orders and characteristics (properties) (method calls). Orders describe the ways to regulate or actuating a system. Qualities reflect the quality of a system such as On / Off mode. These systems issue permission to the user to access either all devices or none. The author has proposed a solution based on Contextual information from devices using a backend cloud system for rule management and a companion smart app that seeks permission from end user in complicated decision making scenarios.

4. Proposed Smart Monitor

Smart Home systems are vulnerable to man-in-the-middle attack (MITM) attacks, Eaves Dropping, DOS Attacks and Malware injection attacks from Misbehaving smart apps. To protect the Home Network, the devices connected in the network has to be monitored on a regular basis. By introducing an edge device, the latency in the network that is exhausted for decision making can be minimized. The agent software that will be running in the edge device will monitor the devices for the network Traffic parameters and abnormal behaviour of devices can be detected well in advance. The User can be alerted using the companion app based on the analysis. This reduces the latency and also effective in memory and resource restrained devices. The proposed edge device/Hub will be a Raspberry Pi based controller with a sniffer agent installed as shown in figure.6. This device will sniff the packets inside the network and the home network information is sent to a cloud backend service that checks for abnormality in the devices.

To decrease the number of transactions, device profiling is done. Device profiling is the basic data about each device connected in the home network. Based on this the devices inside the home network can be given weight age and only the information about the more vulnerable devices can be analysed. For Instance, a smart camera is more vulnerable than a smart Thermometer. Network information of smart camera can be given more importance for analysis rather than analysing all the devices.

The agent software in the edge device also runs a script to monitor the status of all the device connected in the home network and send the details to the backend cloud service for further analysis. As open ports are the main vulnerabilities of smart device that expose sensitive information, scanning for open ports on a periodic basis is a much needed security check that will bring down number of attacks.

4.1. Working Model of Proposed solution

Cloud is the core of every electronic network which focuses mainly on the delivery of software without physical infrastructure as a central repository. The centrally linked system server sends and evaluates the data produced from our homes and sends the status of our smart telephones. The server manages the whole database and also changes if changes are made at home. The key advantage of this program is that it manages some simple operations with telephone or computers as other forms of devices are built in the home worldwide and are considered automatic or intelligent home everywhere in the world. This system is also very useful in the use of energy. The network introduced comprises of modules and controls of WIFI servers. The Controller board, which runs all operations with our sensors connected to the cloud. Systems = Automatic system access built in the house can be remotely operated from any local machine or mobile phone using an internet link. In WIFI network connectivity, WIFI is used and chosen to link sensors to severs with improved coverage, portability, durability and WIFI requirements, improving device versatility and scalability as a protection framework. Data processing cloud service offers a stronger network for web based applications, because data is sent very quickly, even though very reliable, so all information received by computers because sensors is then processed in a central repository, including data storage and computation. Web service is used to store data. The additional smart phone application also requires the user to control devices and systems without triggering the sensor.
4.1.1. Device Registration
All smart home devices must be registered and configured in Smart Hub using the smart app of the Hub or web portal. The smart Hub maintains a database about the devices that are connected. The data is streamlined to the home router through the smart Hub.

![Device Registration Diagram]

Figure 6. Data analysis from sensors

4.1.2. Device profiling
The Data traffic network is checked against the usual device behavior for abnormal payloads. Device profiling also reduces the time required for analysis as not all smart devices are risky. Every time a new device is registered the device profile is updated in the edge device profile. The network parameters of those devices that have more risk is sent for further analysis.

Port Scanning: A web service is called periodically to check for open ports in all the devices connected to the home and open ports are closed. This will prevent Hackers using open ports a means to infiltrate home devices.

4.1.3. Fine Grained permission management and conflict resolution
This is provided by the smart Hub. Since such decision making is done locally this will avoid latency-issues. Further the data is analysed for botnets based on network traffic on a periodic basis.

5. Simulation and Results
Micro services are used to facilitate each feature of the Smart Monitor Hub. For simulation Azure simulation portal was identified. As the first step, the new devices are registered in the Hub. The device information like device Id, Status (on/off) etc., is stored as xml file. The devices are connected based on REST Principles. The smart devices expose API that should be programmed to connect to the Smart Monitor Hub. The messages are sent in JSON format and the message telemetry is storage in storage endpoint server for further analysis. The IoT hub can be connected to less than 100 devices (in simulation) and handles MQTT, HTTP protocols. The refresh time to update device state is also set in the configuration file. Home status and system design shown in figure 7 and figure 8.
Figure 7. Home status

Figure 8. System simulation design

private async static Task AddDeviceAsync()
{
    string deviceId = "ParkingLevelOne";
    Device device;
    try
    {
        Console.WriteLine("New device:");
        device = await registryManager.
        AddDeviceAsync(new Device(deviceId));
    }
    catch (DeviceAlreadyExistsException)
    {
        Console.WriteLine("Already existing device:");
        device = await registryManager.
        GetDeviceAsync(deviceId);
    }
    Console.WriteLine("Generated device key: ",
    device.Authentication.SymmetricKey.PrimaryKey);
}
Device probing is done using script run on Kali Linux that looks for all open ports and the log information is periodically sent to the cloud for further analysis.

6. Conclusion and Future works
In this paper the vulnerabilities of Smart Home devices were analyzed. The proposed system can help solve the most obvious issues like eaves dropping, MITM attacks and DOS attacks. Introducing edge device will reduce latency. The existing communication pattern of smart Home devices need not be altered so it is easy to implement in all Homes. Smart Home users with less knowledge on technical details of smart Home systems can also be benefitted with this solution. Based on the data that is communicated between the device app and companion app co further Analysis for malicious activity of misbehaving smart apps can be traced.

References
[1] Sukhvir N, Siddiqiy M, Gharakheiliy HH, Sivaramany V, and Boreli R 2019 An Experimental Study of Security and Privacy Risks with Emerging Household Appliances IEEE conference on communications and network security 79-84
[2] Earlence F, Jung J, and Prakash 2016 A Security Analysis of Emerging Smart Home Applications IEEE Symposium on Security and Privacy 636-654
[3] Wei Z, Meng Y, Liu Y, Zhang X, Zhang Y, and HoMonit HZ Monitoring Smart Home Apps from Encrypted Traffic CCS In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security 15-19
[4] Roberto M, Petrolo R, Loscri V, Mitton N LEGIoT: A Lightweight Edge Gateway for the Internet of Things Future Generation Computer Systems, 81, 2018.
[5] Isa S Implementing Smart Home using Cisco Packet Tracer Simulator International Journal of Engineering Science Invention Research & Development 4
[6] abc NEWS. 2013 Baby Monitor Hacking Alarms Houston Parents.http://goo.gl/LpuJzg
[7] Tatikayala SG, Meerolla M, Jyostna G, Reddy Lakshmi Eswari P and Magesh E Mitigating Mirai Malware Spreading in IoT Environment Centre for Development of Advanced Computing(C-DAC),
[8] Narayanan KL, Ramesh GP and Divya V Robust and brittle secured video for IOT International Journal of Engineering and Technology 7 93
[9] Shahada S, Ahmad A, Mohammed Hreiji S and Shamsudheen S 2019 IoT Based Garbage Clearance Alert System with GPS Location using Arduino International Journal of MC Square Scientific Research, 11 1-8
[10] Badawi I and Ali W 2019 Underground Pipeline Water Leakage Monitoring Based on IoT International Journal of MC Square Scientific Research, 11 01-08