Journal of Advanced Research in Technology and Management Sciences
Volume: 01 Issue: 02 ISSN: 2582-3078 November 2019
Available online at: http://www.jartms.org

OVERSEE ASSAULT DISCOVERY SYSTEM FOR SMART HOME IOT DEVICES

NARAHARISETTY SHASHANK REDDY[1], NAGARAJU P[2]
[1]M.TECH ES, DEPT OF E.C.E, KAKINADA INSTITUTE OF ENGINEERING AND TECHNOLOGY-2, KORANGI, ANDHRAPRADESH, INDIA, 533461
[2]ASSOSIATE PROFESSOR, KAKINADA INSTITUTE OF ENGINEERING AND TECHNOLOGY-2, KORANGI, ANDHRAPRADESH, INDIA, 533461

ABSTRACT:

Cyber-attacks on the Internet of Things (IoT) are growing at an alarming rate as devices, applications, and communication networks are becoming increasingly connected and integrated. When attacks on IoT networks go undetected for longer periods, it affects availability of critical systems for end users, increases the number of data breaches and identity theft, drives up the costs and impacts the revenue. It is imperative to detect attacks on IoT systems in near real time to provide effective security and defense. In this paper, we develop an intelligent intrusion-detection system tailored to the IoT environment. Specifically, we use a deep-learning algorithm to detect malicious traffic in IoT networks. The detection solution provides security as a service and facilitates interoperability between various network communications protocols used in IoT. We evaluate our proposed detection framework using both real-network traces for providing a proof of concept, and using simulation for providing evidence of its scalability. Our experimental results confirm that the proposed intrusion-detection system can detect real-world intrusions effectively.

Keywords: IOT data, smart homes, high efficient data communication.

1. INTRODUCTION

The popularity of Internet of Things (IoT) devices has significantly increased over the past few years. This is due to their ubiquitous connectivity, allowing them to communicate and exchange information with other technologies, their intelligence, and their decision making capabilities to invoke actions [1]. This provides seamless user experiences which significantly enhance people's everyday lives, and is demonstrated by how prominent such devices are today. However, the proliferation of smart devices is not only within the domestic environment, but it is also the driving force behind the development of an interconnected knowledge-based world; our economies, societies, machinery of government, and Critical National Infrastructure (CNI) [2]. More specifically, CNI concepts such as smart homes, smart cities, intelligent transport, smart grids, and health care systems are heavily dependent on smart technologies and IoT devices. Nevertheless, although these concepts support the tasks of everyday life, their dependency on Information Communication Technology (ICT) and IoT devices come with tremendous security risks [3]. A survey by Synopsys in May 2017 revealed a lack of confidence in the security of medical devices with 67% manufacturers believing that an attack on a medical device is likely to occur within 12 months, and only 17% of manufacturers taking steps to prevent them [4]. The insufficient security measures and lack of dedicated anomaly detection systems for these heterogeneous networks make them vulnerable to a range of attacks such as data leakage, spoofing, disruption of service (DoS/DDoS), energy bleeding, insecure gateways, etc. These can lead to disastrous effects; causing damage to hardware, disrupting the system availability, causing system blackouts, and even physically harms individuals [5], [6]. Therefore, it is clear that the scale of impact of the attacks

performed on IoT networks can vary significantly. For example, a relatively simple and seemingly harmless deauthentication attack can cause no significant damage, but if performed on a device with critical significance, such as a steering wheel in a wireless car, it can pose a threat to human life. Consequently, it is obvious that there is a major gap between security requirements and security capabilities of currently available IoT devices. Two of the main reasons that make these devices insecure include restriction in computational power and heterogeneity in terms of hardware, software, and protocols [7]. More specifically, it is generally not feasible for IoT devices with restricted computational power, memory, radio bandwidth, and battery resource to execute computationally intensive and latency sensitive security tasks that generate heavy computation and communication load [8]. As a result, it is not possible to employ complex and robust security measures. Additionally, given the diversity of these devices, it is very challenging to develop and deploy a security mechanism that can endure with the scale and range of devices [9]. A traditional IT security ecosystem consists of static perimeter network defenses (e.g. firewalls, IDS), ubiquitous use of end-point defenses (e.g. anti-virus), and software patches from vendors. However, these mechanisms cannot handle IoT deployments due to the heterogeneity in devices and of their use cases, and device/vendor constraints.

2. RELATED STUDY

Knowledge-driven, adaptive, and lightweight IDS. It collects knowledge about features and entities of the monitored network and leverages it to dynamically configure the most effective set of detection techniques. It can be extended for new protocol standards, whilst at the same time providing a knowledge sharing mechanism that enables collaborative incident detection. Results showed that the system had a high accuracy in detecting mainly DoS and routing attacks. Furthermore, Thanigaivelan et al. Proposed a hybrid IDS for IoT. In this system, each node on the network monitors its neighbor. If abnormal behavior is detected, the monitoring node will block the packets from the abnormally behaving node at the data link layer and reports to its parent node. Oh et al, implemented a distributed lightweight IDS for IoT, which is based on an algorithm that matches packet payloads and attack signatures. They evaluate the IDS by deploying conventional attacks and by using attack signatures from traditional IDSs such as SNORT. The results demonstrated that this system's performance is promising. Finally, Ioulianou et al. Proposed a hybrid lightweight signature-based IDS, in an attempt to mitigate two variations of denial of service attacks; "Hello" flood and version number modification. Few approaches to classifying attack types currently exist. Such approaches, however, have only been employed and evaluated in traditional networks. Therefore, as these approaches were not designed to consider the specific requirements and computational capabilities of IoT, it is challenging to employ them in such environments. Bolozoni et al. Propose a machine learning approach to classify the difference types of cyber-attacks detected by Alert Based Systems (ABS). To achieve this, byte sequences were extracted from alert payloads triggered by a certain attack. Sequences were compared to previous alert data. Although this technique is effective in traditional systems, such approach relies on the alerts produced by the ABS, which are not effective in IoT environments, for reasons discussed in Section I. Additionally, as the detection method uses payload values to detect attacks, attacks which IoT systems are vulernable to and which do not alert the payload (e.g. DoS) are not detected. Subba et al. Implemented a model that uses feed forward and the back propagation algorithms to detect and classify cyber-attacks in desktop networks. However, to evaluate their system they used the NSL-

KDD dataset and attempted to classify probe, DoS, User to Root, and Remote to User attack. Nevertheless, there is no evidence that this system would be as effective if deployed in a heterogeneous IoT environment, which consists of many more protocols, devices, and network behaviors.

EXISTING SYSTEM:

Technology is a never ending process. To be able to design a product using the current technology that will be beneficial to the lives of others is a huge contribution to the community. This paper presents the design and implementation of a low cost but yet flexible and secure cell phone based home automation system. The design is based on a standalone Micro controller BT board and the home appliances are connected to the input/ output ports of this board via relays. The communication between the cell phone and the Micro controller BT board is wireless. This system is designed to be low cost and scalable allowing variety of devices to be controlled with minimum changes to its core. Password protection is being used to only allow authorized users from accessing the appliances at home.

3. AN OVERVIEW OF PROPOSED SYSTEM

The Internet of Things (IOT) is an ever-growing network of smart objects. It refers to the physical objects capable of exchanging information with other physical objects. Nowadays safety and security has always become a basic necessity for metropolitan society. Our project proposes security system for IOT environment. Which prevent intrusion in Home, Bank, Airports, Offices, University or any location with security system? The primary objective of our project is to reduce human work by designing and implementing a security system. System that offers controllability through a hand held mobile phone and PC by means of IOT. To detect for malicious activity or policy violation we use Intrusion Detection System (IDS), which detect any intrusion or violation and typically report to the administrator. The project includes Anomaly based technique for intrusion detection and signature analysis using haar algorithm to differentiate between legitimate person and intruder and thus raising accuracy in authorizing the legitimate person and provide access to private/personal zone, therefore risk of sending false alerts/alarm is reduced.

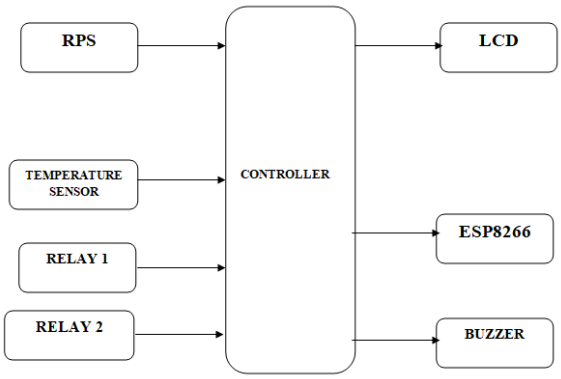

Fig.3.1. Proposed system.

The LM35 series are precision integrated-circuit LM35 temperature sensors, whose output voltage is linearly proportional to the Celsius (Centigrade) temperature. The LM35 sensor thus has an advantage over linear temperature sensors calibrated in ° Kelvin, as the user is not required to subtract a large constant voltage from its output to obtain convenient Centigrade scaling. The LM35

sensor does not require any external calibration or trimming to provide typical accuracies of ±¼°C at room temperature and ±¾°C over a full -55 to +150°C temperature range. Low cost is assured by trimming and calibration at the wafer level. The LM35's low output impedance, linear output, and precise inherent calibration make interfacing to readout or control circuitry especially easy. It can be used with single power supplies, or with plus and minus supplies. As it draws only 60 µA from its supply, it has very low self-heating, less than 0.1°C in still air. The LM35 is rated to operate over a -55° to +150°C temperature range, while the LM35C sensor is rated for a -40° to +110°C range (-10° with improved accuracy). The LM35 series is available packaged in hermetic TO-46 transistor packages, while the LM35C, LM35CA, and LM35D are also available in the plastic TO-92 transistor package. The LM35D sensor is also available in an 8-lead surface mount small outline package and a plastic TO-220 package.

Fig.3.2. LM35 Sensor.

RELAY:

A relay is an electrically operated switch. It consists of a set of input terminals for a single or multiple control signals, and a set of operating contact terminals. The switch may have any number of contacts in multiple contact forms, such as make contacts, break contacts, or combinations thereof. Relays are used where it is necessary to control a circuit by an independent low-power signal, or where several circuits must be controlled by one signal. Relays were first used in long-distance telegraph circuits as signal repeaters: they refresh the signal coming in from one circuit by transmitting it on another circuit. Relays were used extensively in telephone exchanges and early computers to perform logical operations. The traditional form of a relay uses an electromagnet to close or open the contacts, but other operating principles have been invented, such as in solid-state relays which use semiconductor properties for control without relying on moving parts. Relays with calibrated operating characteristics and sometimes multiple operating coils are used to protect electrical circuits from overload or faults; in modern electric power systems these functions are performed by digital instruments still called *protective relays*. Latching relays require only a single pulse of control power to operate the switch persistently. Another pulse applied to a second set of control terminals, or a pulse with opposite polarity, resets the switch, while repeated pulses of the same kind have no effects. Magnetic latching relays are useful in applications when interrupted power should not affect the circuits that the relay is controlling.

Fig.3.3. Module

ESP8266:

Modules made with the ESP8266 by the third-party manufacturer Ai-Thinker and remains the most widely available. They are collectively referred to as "ESP-xx modules". To form a workable development system they require additional components, especially a serial TTL-to-USB adapter (sometimes called a USB-to-UART bridge) and an external 3.3 volt power supply. Novice ESP8266 developers are encouraged to consider larger ESP8266 Wi-Fi development boards like the NodeMCU which includes the USB-to-UART bridge and a Micro-USB connector coupled with a 3.3 volt power regulator already built into the board. When project development is complete, those components are not needed and these cheaper ESP-xx modules are a lower power, smaller footprint option for production runs.

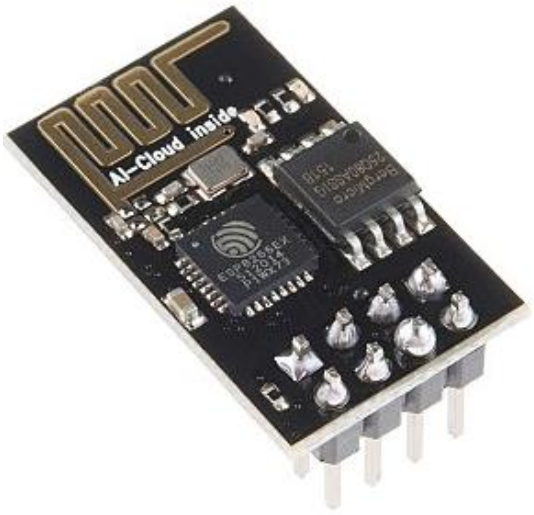

Fig.3.4. ESP8266 module.

OPERATION:

When profiling devices, the classifier demonstrated a high percentage of correct predictions, thus less often misclassifying devices. For example, Lifx Smart Lamp, Samsung Smart Things Hub, and Belkin Net demonstrated few confusion and were generally correctly classified. This may be explained by the fact that such devices are distinct, and thus, so are their network behaviours. In this case, features may exist in some packets from one device, but are missing in packets from others. For example, the behaviour of the TP-Link NC200 is notably different in comparison to the behaviour of the TP-Link SmartPlug as the tasks they exist to perform are different. In this case, a

feature within the TPLink NC200 packets include the connectionless protocol, User Datagram Protocol (UDP), whereas the TP-link SmartPlug packets use Transmission Control Protocol (TCP). However, in some cases, confusion often occurred where Belkin Net and Hive Hub, were misclassified. These confusions may be explained by the fact that such devices may have incurred similar network behaviour during data collection, such as when firmware updates were deployed. Detecting whether network packets are malicious or benign and identifying the type of wireless attacks demonstrated very little confusion. This could be explained by the fact that the attacks that were performed during data collection were off the shelf attacks, i.e. resources which include attacks that are freely available, such as hping, nmap, iot-toolkit, etc., and are unsophisticated. In this case, the features of malicious and benign packets are distinct, and thus, few classification confusions occurred. For instance, malicious packets may contain different flag values which indicate an attack has occurred as explained earlier.

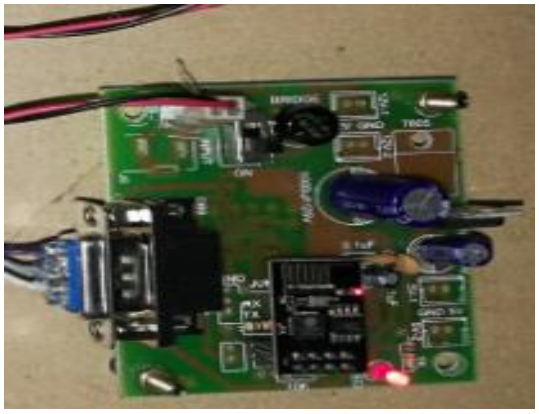

Fig.3.5. Hardware of wifi module.

The experimental results using only a single PIR sensor (i.e., PIR1) embedded in each module have shown good performance in classifying directions, distances and speeds, and this is probably because the walking samples we have used in our experiments are collected from two-way, back-and-forth walking, and PIR1 (and thus, its sensing elements) that each of the PIR-based modules is equipped with, is well aligned with the motion plane, i.e., the walking directions.

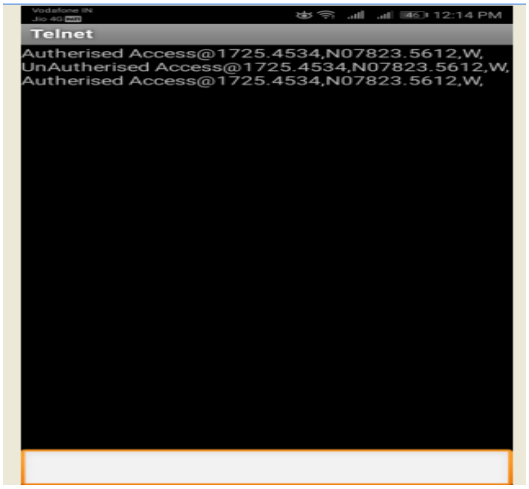

Fig.3.6. Output results.

4. CONCLUSION

We investigated the feasibility of deploying machine-learning-based intrusion detection for resource-constrained IoT networks. To that end, we developed intelligent IDS that tactfully combine network virtualization and DL algorithm to detect anomalous behavior on insecure IoT networks. We investigated the optimal solution for deep-learning-based IDS by evaluating the performance of our scheme against five different attack scenarios, including black hole attack, opportunistic service attack, DDoS attack, sinkhole, and wormhole attacks. Through analysis of precision-recall curves, we obtained an average precision rate of 95% and recall rate of 97% for different attack scenarios. Our experiments also demonstrate higher F1-scores for all attack scenarios indicating better overall detection performance by the proposed system.

REFERENCES

[1] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology (FIT), 2012 10th International Conference on, pages 257–260. IEEE, 2012.

[2] Tobby Simon. Chapter seven: Critical infrastructure and the internet of things. Cyber Security in a Volatile World, page 93, 2017.

[3] Eirini Anthi, Lowri Williams, and Pete Burnap. Pulse: An adaptive intrusion detection for the internet of things, 2018.

[4] Cybersecurity executive: Medical devices a 'bulls-eye' for cyber-attacks. https://www.digitalhealth.net/2017/12/ medical-device-functionality-vs-cybersecurity/. (Accessed on 02/05/2018).

[5] Eirini Anthi, Amir Javed, Omer Rana, and George Theodorakopoulos. Secure data sharing and analysis in cloud-based energy management systems. In Cloud Infrastructures, Services, and IoT Systems for Smart Cities, pages 228–242. Springer, 2017.

[6] Cyber hackers can now harm human life through smart meters — smart grid awareness. https://smartgridawareness.org/2014/12/30/ hackers-can-now-harm-human-life/. (Accessed on 02/05/2018).

[7] Securing the internet of things: A proposed framework - cisco. https://www.cisco.com/c/en/us/about/security-center/ secure-iot-proposed-framework.html. (Accessed on 07/13/2018).

[8] Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. Iot security techniques based on machine learning. arXiv preprint arXiv:1801.06275, 2018.

[9] Eirini Anthi, Shazaib Ahmad, Omer Rana, George Theodorakopoulos, and Pete Burnap. Eclipseiot: A secure and adaptive hub for the internet of things. Computers & Security, 78:477–490, 2018.

[10] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks, page 5. ACM,2015.