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

TOWARD SECURE AS WELL AS EFFECTIVE COMMUNICATION FOR THE NET OF DETAILS

AYYALASOMAYAJULA NAGA SAILAJA[1] , BVVSKR PAVAN[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:

Internet of Things has been widely applied in everyday life, ranging from transportation and healthcare to smart homes. As most IoT devices carry constrained resources and limited storage capacity, sensing data need to be transmitted to and stored at resource-rich platforms, such as a cloud. IoT applications need to retrieve sensing data from the cloud for analysis and decision-making purposes. Ensuring the authenticity and integrity of the sensing data is essential for the correctness and safety of IoT applications. We summarize the new challenges of the IoT data communication with authenticity and integrity and argue that existing solutions cannot be easily adapted to resource constraint IoT devices. We present two solutions called dynamic tree chaining and geometric star chaining that provide efficient and secure communication for the Internet of Things. Extensive simulations and prototype emulation experiments driven by real IoT data show that the proposed system is more efficient than alternative solutions in terms of time and space.

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

1. INTRODUCTION

Internet of Things (IoT) as defined by the ICT (Information and Communication Technology) as a dynamic global network infrastructure with self configuring capabilities based on standard and inter operable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities use intelligent interface and seamlessly integrated into the information network. IoT is the inter networking of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data [7]. In 2013 the Global Standards Initiative on Internet of Things (IoT GSI) defined the IoT as the infrastructure of the information society [8]. The traditional fields of embedded system, wireless sensor networks, control system, automation systems are together interconnected to form the IoT. That means the internet of things builds over the revolutionary success of mobile and internet network [9, 10]. Even a few decades back, nobody could have imagined having a video chat with their families. Nowadays, it is merely a child’s play. All of this is due to the wide availability of internet and creation of devices with Wi-Fi abilities. Technology costs are going down, and smart-phones are capable of doing almost anything with their inbuilt features and apps. What we have till now is “Internet of Computers (IoC)” and it is gradually growing in size. According to Gartner’s study, “the world will be a more deeply and intimately connected place, with an estimated 7.3 billion tablets, PCs and Smartphone’s, by the end of this decade. By the year 2020, this massively connected system is likely to expand at even more rapid rate to 26 billion connected devices around the globe.” Thus, emerging the huge scope of Internet of Things (IoT). This so called IoT is sitting on a perfect storm. And the storm revolves around five basic areas Sensor technologies, Local processing, Networking models, Data Science and Predictive Technologies, Machine Learning and Security.

2. RELATED STUDY

Motivated by three main points, which align with Zarpelao et al. Who provide a comprehensive literature review on the matter. Firstly, the majority of the proposed systems focus on detecting a limited set of attacks; in particular, routing attacks and DoS. In this case, the proposed system aims to identify a larger set of attacks including multistage attacks that represent complex combinations of attack behaviour, which is significantly more challenging to detect. Specifically, the IDS presented in this paper is evaluated against 12 popular attacks from 6 categories found within the IoT domain, but also against 4 scenarios of scripted multistage attacks with complex chains of events. Secondly, existing literature lack focus on device profiling. Detecting malicious traffic is a challenging task without profiling the ‘normal’ behaviour of devices connected to the network. Therefore, in this paper, the behaviour of 8 different IoT devices is profiled so that unusual behaviour can be detected, and subsequently, so can cyber-attacks. Thirdly, current IDSs fail to identify the type of attack that has occurred. Without this information, significant human effort is needed to respond to alerts and determine the severity of an attack. However, in this paper, a machine learning approach demonstrates that it is possible to address this limitation by not only automatically distinguishing between benign and malicious network traffic, thus detecting whether an attack has been deployed, but also to automatically identify the type of the attack that has occurred and against which device. These two factors provide crucial information that can help determine the severity of the cyber-attack, and subsequently accelerate the launch of countermeasures to defend against it. Thus, these features are implemented as part of the proposed IDS. The experiments conducted in this paper show that the performance of the system’s three core functions result in an average F-measure of: 1) 99.7%, 2) 97.0%, and 3) 99.0%. This demonstrates that the proposed architecture can automatically distinguish between IoT devices on the network, whether network activity is malicious or benign, and detect which attack was deployed on which device connected to the network successfully. To the best of our knowledge, the architecture of the IDS proposed here is novel and addresses most of the aforementioned limitations of the existing systems. The main contributions of the work presented in this paper are:

- Three layer architecture for a lightweight, standalone IDS tailored towards IoT devices within a smart home network.
- An investigation into which attributes best represent packets as features in the context of supervised learning, so that devices, maliciousness, and attacks can automatically be identified.
- Resources that can further support research into automating IoT-based cyber-attack detection, such as benign and malicious network activity datasets and a set of scripts for automatically deploying attacks.

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 one of the emerging technologies that have grabbed the attention of researchers from academia and industry. The idea behind Internet of things is the interconnection of internet enabled things or devices to each other and to humans, to achieve some common goals. In near future IoT is expected to be seamlessly integrated into our environment and human will be wholly solely dependent on this technology for comfort and easy life style. Any security compromise of the system will directly affect human life. Therefore security and privacy of this technology is foremost important issue to resolve. In this paper we present a thorough study of security problems in IoT and classify possible cyber attacks on each layer of IoT architecture. We also discuss challenges to traditional security solutions such as cryptographic solutions, authentication mechanisms and key management in IoT. Device authentication and access controls are an essential area of IoT security, which is not surveyed so far. We spent our efforts to bring the state of the art device authentication and access control techniques on a single project.

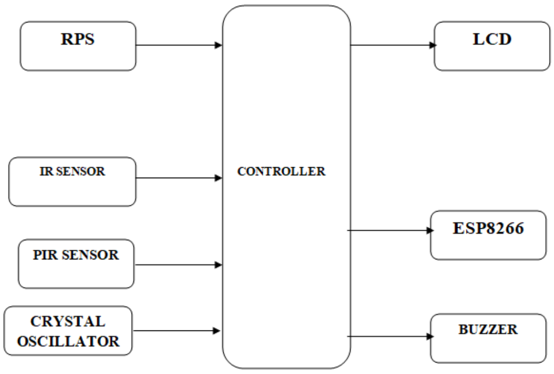


Fig.3.1. Proposed system.

Basics of IR transmitter and receiver transmitter and receiver are commonly used in engineering projects for remote control of objects. In particularly, in Robotic system uses transmitter and receiver. Here i would like to describe the basics if IR transmitter and receiver

Basics of IR transmitter:

An electroluminescent IR LED is a product which requires care in use. IR LED's are fabricated from narrow band hetero structures with energy gap from 0.25 to 0.4 eV. Infra red transmitter emits IR rays in planar wave front manner. Even though infra red rays spread in all directions, it propagates along straight line in forward direction. IR rays have the characteristics of producing secondary wavelets when it collides with any obstacles in its path. This property of IR is used here.

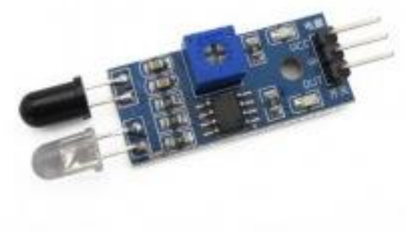


Fig.3.2. IR Sensor.

PIR SENSOR:

The PIR Sensor detects motion up to 20 feet away by using a Fresnel lens and infrared-sensitive element to detect changing patterns of passive infrared emitted by objects in its vicinity. Inexpensive and easy to use, it's ideal for alarm systems, motion-activated lighting, and holiday props. The PIR Sensor is compatible with all Parallax microcontrollers. BASIC Stamp and SX/B code is available under Downloads below, and Spin code is posted to the Propeller Object Exchange.
PIR sensors allow you to sense motion, almost always used to detect whether a human has moved in or out of the sensors range. They are small, inexpensive, low-power, easy to use and don't wear out. For that reason they are commonly found in appliances and gadgets used in homes or businesses.

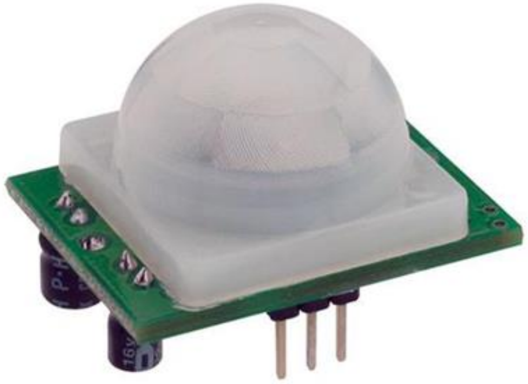


Fig.3.3. PIR Sensor.

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.

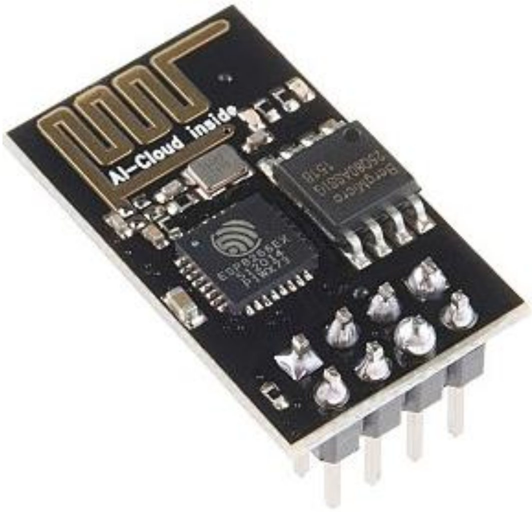


Fig.3.4. ESP8266 module.

OPERATION:

From the experimental results, we can know that a pair of PIR-based modules mounted on opposite walls facing each other could classify the direction of movement, the distance of the body from the PIR sensors and the speed level of movement during two-way, back-and-forth walking and even identify the walking subjects. A ceiling-mounted PIR-based module could also classify the direction, distance and speed of walking subjects, but does not perform subject identification well. Accordingly, we can imagine extensions to this study adapted to building a smart environment, where a set of PIR sensors are attached on opposite walls facing each other at the entrance to the room and multiple PIR-based modules are distributed in a square grid across the ceiling in the room. In the smart environment, the wall-mounted PIR sensors at the entrance could identify the user entering the room, and the ceiling-mounted PIR-based modules could detect the user’s movement, including direction, distance and speed, robustly tracking the user and, thus, helping the system build a rich model of the user’s context.

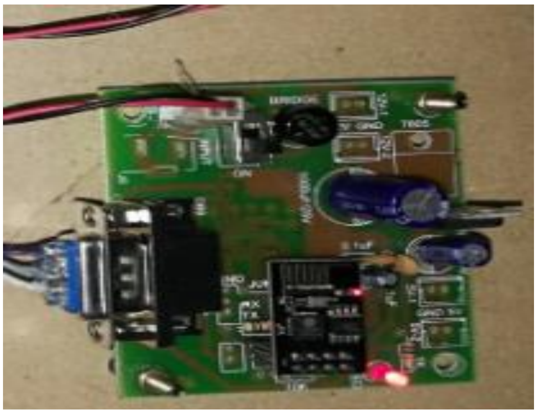
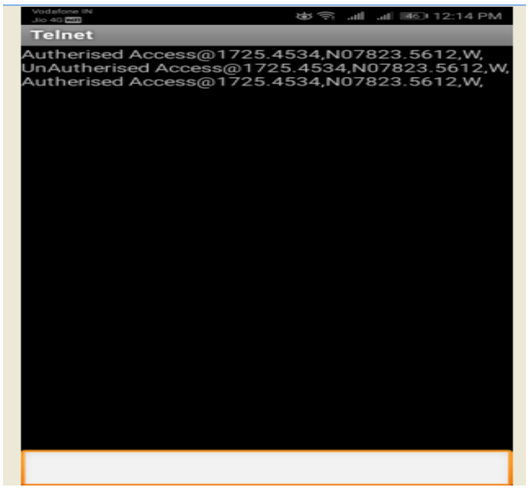


Fig.3.5. Hardware of wifi module.

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.



```
Autherised Access@1725.4534,N07823.5612,W,
UnAutherised Access@1725.4534,N07823.5612,W,
Autherised Access@1725.4534,N07823.5612,W,
```

Fig.3.6. Output results.

4. CONCLUSION

We summarize the new challenges of the IoT data communication with authenticity and integrity and argue that existing solutions cannot be easily adopted. We design a system aimed to address these challenges. This system is able to uniformly sample data from sensing devices and then securely store the data in the cloud while respecting resource budget constraint. The sub-systems in our paper symbiotically operate together and this system is efficient in terms of space and time, as is validated by extensive simulation and prototype emulation experiments.

REFERENCES

[1] X. Li, H. Wang, Y. Yu, and C. Qian, “An IoT data communication framework for authenticity and integrity,” in Proc. IEEE/ACM 2nd Int. Conf. Internet Things Design Implement. (IoTDI), Apr. 2017, pp. 159–170.

[2] eHealth. Accessed: Jan. 2019. [Online]. Available: http://www.who .int/topics/ehealth/en/

[3] World Health Organization. MHealth: New Horizons for Health Through Mobile Technologies. Accessed: Jan. 2019. [Online]. Available: http://www.who.int/goe/publications/goe_mhealth_web.pdf

[4] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds,” in Proc. IEEE World Internet Things (WF-IoT), Mar. 2014, pp. 241–246.

[5] G. Wang et al., “Verifiable smart packaging with passive RFID,” IEEE Trans. Mobile Comput. to be published, doi: 10.1109/TMC.2018.2852637.

[6] Nest. Accessed: Jan. 2019. [Online]. Available: https://nest.com

[7] HVAC Monitoring System. Accessed: Jan. 2019. [Online]. Available: https://www.sensaphone.com/industries/hvac.php

[8] T. Gupta, R. P. Singh, A. Phanishayee, J. Jung, and R. Mahajan, “Bolt: Data management for connected homes,” in Proc. USENIX NSDI, Apr. 2014, pp. 243–256.

[9] Y. Kim et al., “Design of a fence surveillance system based on wireless sensor networks,” in Proc. 2nd Int. Conf. Autonomic Comput. Commun. Syst., Sep. 2008, pp. 23–25.
[10] A. J. Brush, J. Jung, R. Mahajan, and F. Martinez, “Digital neighborhood watch: Investigating the sharing of camera data amongst neighbors,” in Proc. Conf. Comput. Supported Cooperat. Work, Feb. 2013, pp. 639–700.