International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

# IoT Argos-Multi-layer Smart Home Security System

**Mrs.P.Sheela Rani[1], K.Prathana[2], Tarugu Divyasree[3], Shaveetha. K[4]**

*[1]Assistant Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India*

*[2, 3,4Student], Department of Information Technology and Electronics and Communication Engineering, Panimalar institute of Technology, Chennai,India*

---

**Abstract -** The development of IoT has made our lives easy but there is an increase in cybercrimes day by day so providing security for this devices is a great task. IoT Argos incorporates unsupervised learning algorithms to discover unusual or **suspicious behavior** of IoT devices at a precision of 0.9876 and a recall of 0.9763. This has been evaluated on wide range of **COTS smart home devices**. Its a two stage machine learning based intrusion model. To overcome this problem we have IoT Argos that monitors communication of **heterogenous IoT devices via programmable routers.**

## 1.INTRODUCTION

The weakness of IoT systems due to security design flaws, weak password management, vague trust management, lack of IoT security standards, and resource constraints for cryptographic functions have enabled cyber attacks . Thus, securing IoT systems in smart homes calls for security frameworks and standards that consider the weakness and vulnerabilities in all IoT protocol layers. Towards this end, this paper introduces IoTArgos, a security monitoring system that collects, analyzes, and characterizes multi-layer data communications of all IoT devices in smart homes via programmable home routers. IoT Argos leverages home routers powered by OpenWrt, an embedded Linux operating system, to automatically collect TCP/IP-based network flow records via softflowd and nfcapd utilities and wireless packets captured by off-the-shelf wireless sniffers plugged into the routers. The combination of network flows and wireless packets offers a wide range of multi-layer features which capture behavioral patterns of data communications for heterogeneous IoT systems in smart homes and explain what, when, how, if, and why IoT devices communicate with other end systems including remote cloud servers or local IoT hubs in the same home. . Our extensive experimental results based on synthetic IoT data communication traffic demonstrate the effectiveness of the ML-based intrusion detection method in capturing known or new attack behaviors towards smart home IoT devices. Specifically, the two-stage method in IoTArgos, using a combination of random forest (RF) in the classification stage and principal component analysis (PCA) in the anomaly detection stage, achieves a high area under the curve (AUC) value of 0.9678 and 0.9876, 0.9763, 0.9818, 0.9819 of precision, recall, accuracy, F1 score in detecting IoT attacks.

## SYSTEM REQUIREMENT

### Hardware Requirement

- Sensors module
- Arduino Mega 328
- 4 Relay switch board
- Male to female connecting wires
- Android mobile

### Software Requirement

- Operating system windows 10
- Arduino 1.6.7
- Android studio

## 2. TECHNOLOGIES

- Sensor technology
- Zigbee scheme

### ZIGBEE SCHEME:

Zigbee communication is specially built for control and sensor networks on IEEE 802.15.4 standard for wireless personal area networks (WPANs), and it is the product from Zigbee alliance. This communication standard defines physical and Media Access Control (MAC) layers to handle many devices at low-data rates. These Zigbee's WPANs operate at 868 MHz, 902-928MHz, and 2.4 GHz frequencies.

The data rate of 250 kbps is best suited for periodic as well as intermediate two-way transmission of data between sensors and controllers.

**MODULES:**

**CONTROL PANEL:**

The control panel of the whole security system is connected to the mobile of the owner. All sensing alarms are connected to the mobile. If the security system breached the alarms are ON in the owners mobile.

**DOOR AND WINDOW SENSOR**:

Door and Windows are connected with sensing objects.one is installed on the top and other is installed in door frontside.If they closes the door the message is send to the mobile of the house owner ,the home is secured.if someone force to open the door the message is send to the owner of the home.

**MOTION SENSOR**:

It is one of the main protecting invisible sensors to protect the rooms and the valuables in the lockers. if the security is breached the high decibal alarm is send to the owner.

**HIGH-FREQUENCY ALARM:**

Loud enough for neighbors to hear, home security alarms serve a few different purposes. First, they alert the people inside the house that a problem occurred. They're also shrill enough to send a burglar running while also notifying nearby neighbors to the situation.

**DESIGN:**

The security system is always monitoring by the security installment company if some problems arrives in security they will sent the messages to the owner and they also sets the alarms in the buildings. if the owner are not responding to the messages they call the owners and passes the information about security issues. they set alarms which also works during the power shutdown.so the alarms will always work properly it will alterts neighbours too. In our project we are using the android phone as the control panel. if the door and window sensor become breaches they instantly call to the owner to intimate the message of the security issues.it should more fast to avoid the theft.

The security system communicates to owners in different ways:

- If someone arms the home or forces the door or window, the security systems immediately send the message to the owner the door is not in the security zone so they send alert message
- Someone arms the home, the high frequency alarm starts to ring and alerts the neighbor.
- If the owner not responding to the message, the security system company calls the owner directly to alert them or else they directly call the police inform about the illegal entry of the home.

**IMPLENTATION:**

We are connecting the raspberry pi and elegoo to communicates the sensor to the other devices. Once the door is open ,the sensors which is attached is release ,instantly sensor the alerts to the owner by the reed switch when gets activated. Likewise they always sent the each opening of the door. that system software of raspberry and elegoo got continuously connected.the security systems company set the alarm on the top corner of that building which is also connected through the reed switch. They uses the transmitter to passes the updations of the door. The security system sets range of the particular house which covered with sensor installed doors and windows.that range value is always connected to the software.the binary code is transmitted to the receiver which is attached by the raspberry pi.if the security system zone is breached immediately they sent alerts through which is connected to the raspberry pi and sends the alerts to the owner.the company also monitoring the secureness of the home,if they finding something fishy about the protection they intimate the message using the software installed for customers. They are using the sql database to store the data about the opening and closing of the door and windows.they gives updation continuously to the owner about the door and windows.the owner can check the updation of the home via their requested mobile phone.if they get lost their mobile they can see the information from the extra authorized phone of the family.

**ALGORITHMS:**

In this section, we discuss the algorithms corresponding to the different programs running in different portion of the system. The Raspberry Pi required a Python script for updating the information about the doors and a C++ program for receiving the code transmitted by Arduino through the 433 MHz RF antenna . The program in Arduino for sensing door opening and transmitting code to Raspberry Pi was written in C++. The Android application was implemented using Java.

IoTArgos characterizes and models data communication behaviors of heterogeneous IoT devices with a broad range of communication and traffic features. To detect intrusions towards IoT devices, IoTArgos develops a two-stage method to first explore supervised classification algorithms for identifying known attacks based on trained labelled data-sets and then rely on unsupervised anomaly detection algorithms for capturing emerging attacks without prior attack labels or signatures. Our extensive experiments based on synthetic IoT data traffic with normal communications collected from a smart home sandbox and simulated attacks have shown the two-stage method is very effective in detecting a wide range of IoT attacks. Our future work will focus on implementing and deploying IoTArgos across a large number of smart homes and small businesses to monitor the security of IoT systems in these edge networks and correlating the security monitoring of distributed homes for discovering coordinated and large scale cyber attacks towards IoT devices with similar vulnerabilities. We plan to further investigate the mitigation techniques for efficiently identifying and filtering attacks. Our efforts will be also centered on balancing the trade-off between accuracy and false possible rate and looking deep into the data to differentiate between the legitimate and illegitimate accesses of the IoT devices.

**RESULT:**

In the olden method ,they are only using the computer to control the home and security system but now we are using the mobile phones to protect our houses to be secured.it is simple to control and easy to handle and install the software. The companies also continuously monitoring the sendors and security issues.

**3. CONCLUSIONS**

It can be very easy handle because IoTargos security systems.it can be more develop in future in many ways better than this.the technology keep developing now a days.you may get the better idea about this smart home security systems.we may get the more updation of this security system in future if we are go for it.

**REFERENCES**

[1] IEEE journal paper about IoTArgos-multi layer monitoring systems.

[2] smart home security system paper by Mr.Mohammed

[3] J. Dunning, "Taming the Blue Beast: A Survey of Bluetooth Based Threats," IEEE Security & Privacy, vol. 8, no. 2, 2010.

[4] H. Jafari, O. Omotere, D. Adesina, H.-H. Wu, and L. Qian,"IoT Devices Fingerprinting Using Deep Learning," in Proc. of IEEE MILCOM, 2018.

[5] E. Fernandes, A. Rahmati, K. Eykholt, and A. Prakash, "Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?" IEEE Security & Privacy,vol. 15, no. 4, pp. 79–84, 2017.

[6] Z.-B. Celik, P. McDaniel, and G. Tan, "Soteria: Automated IoT Safety and Security Analysis," in Proc. of USENIX ATC, 2018.

[7] J. Dahmen, D. Cook, X. Wang, and H. Wang, "Smart Secure Homes: A Survey of Smart Home Technologies that Sense,Assess, and Respond to Security Threats," Journal of Reliable Intelligent Environments, vol. 3, no. 2, pp. 83–98, 2017.

[8] S. Demetriou, N. Zhang, Y. Lee, X. Wang, C. Gunter, X. Zhou, and M. Grace, "HanGuard: SDN-driven Protection of Smart Home WiFi Devices from Malicious Mobile Apps," in Proc. Of ACM WiSec, 2017.

[9] J. Obermaier and M. Hutle, "Analyzing the Security and Privacyof Cloud-based Video Surveillance Systems," in Proc. of ACM IoTPTS, 2016.

[10] E. Ronen and A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights ," in Proc.of IEEE EuroS&P, 2016.

[11]Samsung,"SmartThings,"https://www.smartthings.com/.

[12] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing:Vision and Challenges," IEEE Internet of Things Journal,vol. 3, no. 5, pp. 637–646, 2016.

[13] S. Siby, R. Maiti, and N. Tippenhauer, "IoTScanner: Detecting Privacy Threats in IoT Neighborhoods," in Proc. of ACM IoTPTS, 2017.

[14] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-PhonesAttacking Smart-Homes," in Proc. of ACM WiSec, 2016.

[15] Y. Tian, N. Zhang, Y.-H. Lin, X.-F. Wang, B. Ur, X. Guo, and P. Tague, "SmartAuth: User-Centered Authorization for the Internet of Things," in Proc. of the USENIX Security, 2017.

[16] A. Wang, A. Mohaisen, and S. Chen, "XLF: A Cross-layer Framework to Secure the Internet of Things (IoT)," in Proc. IEEE ICDCS, 2019.

[17] Q. Wang, W. Hassan, A. Bates, and C. Gunter, "Fear and Logging in the Internet of Things," in Proc. of NDSS, 2018.

[18] R. Want, B. Schilit, and S. Jenson, "Enabling the Internet of Things," Computer, vol. 48, no. 1, pp. 28 – 35, 2015.

[19] D. Wood, N. Apthorpe, and N. Feamster, "Cleartext Data Transmissions in Consumer IoT Medical Devices," in ACM Workshop on IoT S&P, 2017.

[20] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41 – 49, 2018.

[21] K. Xu, Y. Wan, G. Xue, and F. Wang, "Multidimensional Behavioral Profiling of Internet-of-Things in Edge Networks," in Proc. of IEEE/ACM IWQoS, 2019.

[22] K. Yang, J. Ren, Y. Zhu, and W. Zhang, "Active Learning for Wireless IoT Intrusion Detection," IEEE Wireless Communications, vol. 25, no. 6, pp. 19 – 25, 2018.