

Detection of Oddity using User Behavior Patterns and Home Conditions for Home Automation of IOT Devices

Mr.V.R.Vimal¹, BijjamVineetha², Chandra Dinusha³ and Mummadi Venkata Naga Madhuri⁴

¹⁻⁴Dept of Computer Science and Engineering, Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College.Chennai,India.

Email: vrvimal@veltechmultitech.org, mvnmadhuri@gmail.com

Abstract—In this today's generation, Everyone is using electrical appliances in our homes such as refrigerator, Air Conditioner etc... For security purpose all these were connected to internet. Cyber attacks is one of the main problem in these days. These appliances are targets of cyber attacks which cause harm to users as well as it also a problem in compromising safety. The attacks include volume up air conditioners, automatic operations etc... To overcome this problem we deal with Anomaly Detection. We have proposed a model for detecting such abnormal conditions based on user Behavior patterns. As this is already exists only for single user by using Hidden Markov Model[HMM]. This is an evaluation of HMM model. Smart home consists of multiple users we will be implementing this proposed method even in case on multiple users. This method mainly based on user condition sequences as well of home conditions such as temperature and time. This method obtained detection ratios exceeding 90% anomalous operations with less than 10% of misdirection when our method observed event sequences related to operations.

Index Terms— Anomaly Detection, cyber Security, User behaviors, Hidden Markov Mode.

I. INTRODUCTION

Home Appliances such as refrigerators, heaters, and air conditioners are being increasingly integrated with Internet connections to expand connectivity beyond personal computers and smart phones. These devices are collectively devices. Users can obtain information from devices and operate them using smart phones, tablets, or smart speakers. Currently, seven billion devices are connected to the Internet, with a substantial increase to 215 billion devices expected by 2025 As the number of devices connected to the Internet increases, the risk for these devices to be targeted by cyber attacks also increases. Most of the current attacks targeting IoT devices aim to create botnets. Such attacks are detectable by methods based on analyses of attacker behaviors or through usual traffic comparisons. However, as IoT devices are closely included in our routine, attacks may cause immediate and personal harm to users. To improve user protection, we proposed a method to detect the anomalous operation of home IOT devices by learning user behaviors during operation.

II. LITERATURE SURVEY

[1] Blindness is a more severe problem among the disabilities of Human. It is difficult to lead a normal life for blind like a sighted person. Because they cannot feel their surroundings. So, most of the blind peoples require travel aids to travel freely in an unknown environment. Researchers were invented several devices to make independent navigation for blinds. But most of them are invented for a specific task or the devices do not cost friendly. To gain independent navigation, a device with more features is required. For this purpose, "Design and Implementation of a Blind Assistive Robot" is designed to fulfill the goal. The device eliminates the requirement of human assistance for blind while traveling outside. It is made of reliable parts and has a relatively low cost compared to industrial bots.

[2] Two-way communication facilities and advanced metering infrastructure enable residential buildings to be capable of actively participating in demand side management schemes. This paper proposes a new home energy management system (HEMS), which optimally schedules the operation of home energy resources, with the aim to minimize the home's one-day electricity cost charged by the real-time pricing while taking into account the monthly basis peak power consumption penalty, charged by the demand charge tariff. To better ensure the user's lifestyle requirements, the HEMS also models lifestyle-related operational dependencies of household appliances.

[3] Smart home is a term that is commonly used to refer to homes where the appliances, lightning, air-conditioning, TVs etc. are capable of communicating with each other and can be controlled remotely via some kind of interface. In this project presents a Home automation system using Wireless Fidelity as communication interface. The idea behind this project was to develop a home automation system which is a cheaper alternative to commercial options of home automation and at the same time could be seamlessly integrated with the commercial products.

III. PROPOSED SYSTEM

In this proposed method, we introduce a method to detect the anomalous operation of home devices attributed to attackers. The proposed method considers specific patterns of user behavior depending on diverse conditions. For example, when users return home it will check for a climate condition, it is summer or winter based on that loads will be operated. In a family each person has separate rooms which are allocated by them and loads will be operated using that. Each room has a camera using that persons will be recognized and loads will be turn on using there access of room loads. In this section, we describe the proposed model of user behavior. The proposed method learns these types of condition dependent operation sequences to establish behavior patterns, and it classifies deviations from these learned patterns as anomalies Then, we explain the learning of user behaviors and the detection of anomalous operations.

IV. WORKING OF PROPOSED SYSTEM

The figure 1 represents architectural diagram of our proposed system. As shown in the diagram we have used the software PYCHARM as data for the experiment is stored.

Training Side

A. Image input

The image element having the image value in its type attribute, represents a graphical submit button, which is a regular image that when pressed, submits the form it belongs to... This can be useful for example to allow the user to select an area of the image while submitting the form.

B. Gray Scale Conversion

Grayscale is a range of monochromatic shades from black to white... Many image editing programs allow you to convert a color image to black and white, or grayscale. This process removes all color information leaving only the luminance of each pixel.

C. Segmentation

Segmentation is the technique of dividing or partitioning an image into parts, called segments. It is mostly useful for applications like image compression or object recognition, because for these types of applications, it is inefficient to process the whole image.

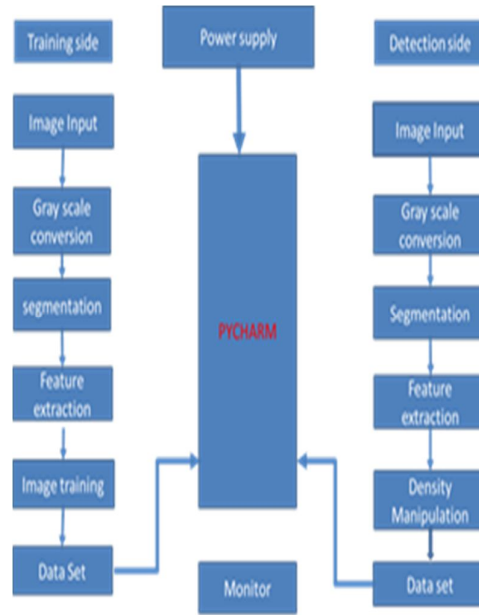


Fig.1:Architecture Diagram

D. Feature Extraction

Feature extraction is a part of the dimensionality reduction process, in which an initial set of the raw data is divided and reduced to more manageable groups. These features are easy to process but still able to describe the actual dataset with accuracy and originality

E. Image Training

It is a form of training performed on the mental level, using images in one's mind to perform that training exercise. It is also called image battle.

F. Data Set

Collection of related set of information that is composed of separate elements in training side but it can be manipulated as a unit by a computer.

Detection Side

As the process is same as in training side, the detection side includes:

A. Density Manipulation

Density manipulation is the ability to control the density of objects and begins, possibly including one's self. This power can be used to make objects denser, heavier, and more durable, or to lower their density to become lighter and more agile, or even to make them disperse and lose their solidity.

The power supply is given to the software, the data from the training side is obtained to the pycharm and by that data whether the given image is detected or not can be shown in detection side.

IV. EXPERIMENTAL RESULT

We should also discuss the possibility that attackers change their attacks so as to avoid detection by our method. The attackers might mimic the behaviors of legitimate users. In this case, our method cannot detect the command sent by the attackers. To mimic the behavior of legitimate users, the attackers require the knowledge of the behavior of legitimate users and the ability to control the devices included in the legitimate event sequence. Especially if many users use a device in the same manner, the attackers may easily infer the behavior of legitimate users. To avoid such attacks, we need to (1) protect learned user behaviors so that attackers cannot obtain the information, (2) make the model complicated so that the attacker cannot infer the behavior by adding more sensors, including more events and so on, and (3) include the devices that are difficult to be operated by the

attackers in the model. Another point to be discussed is the number of users in a home. Our method considers the case that multiple users in a home, and avoids misdetection by learning essential behaviors of all users. By doing so, our method avoids misdetections even if many users are in a home and behave differently from each other. However, as the number of users who behave differently from each other increases, more event sequences are stored as legitimate sequences. Even if a large number of event sequences are stored, it is difficult for attackers to operate the home IoT devices so that the event sequence including the attack matches the learned event sequences, if the model of the event sequence is complicated enough to avoid the inference of the legitimate behavior.



Fig.2:Image detection

As shown in the above figure , It represents the face identified by a person from where the data of a person is already obtained in the data set. The dataset contains the data obtained from the user behaviors.

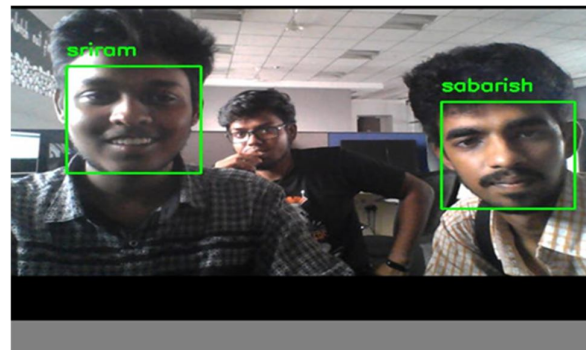


Fig.3:Detection of images from data set

The data set contains the related sequence of user behaviours ,The dataset generates the users learned sequences. If the data is matched with the learned sequence then that is considered as detected,otherwise it is considered as misdetection.

V. CONCLUSION

The proposed method can learn sequences of user behaviors according to conditions such as time of day, temperature, and humidity. Then, when an operation command arrives, the method compares the current sequence with learned sequences for the current condition. If the sequences do not match, the operation is considered as anomalous. We evaluated the detection and misdetection rates of the proposed method and its variants considering only the condition or without removing spurious events. The proposed method can detect over 90% of anomalous operations with less than 10% of misdetections if the events related to legitimate operations can be monitored. The proposed method achieves a higher accuracy by learning sequences executed multiple times than by using only condition information. However, the proposed detection method can produce a high rate of misdetections, especially when single or rare operations occur. Mitigating the misdetection of rare legitimate operations is another challenge, as we cannot obtain sufficient training data to accurately identify such rare operations in each home. To obtain more training data, we will

usedata from several homes in future work. However, some problems remain to be solved before achieving this type of data collection. For instance, different homes and environments and varying user behaviors may render the collected data useless. Thus, we need to gather data from several homes whose users exhibit similar behaviors. Moreover, as privacy is a major concern, we should use anonymized data from different homes to preserve information privacy.

REFERENCES

- [1] B. Mocanu, R. Tapu and T. Zaharia, "Single object tracking using offline trained deep regression networks," In IPTA, 2017, pp. 1-6.
- [2] H Jiang and E. G. Learned-Miller, "Face detection with the faster RCNN," 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), pp. 650-657, 2017.
- [3] J. Deng *et al.*, "ImageNet: A large-scale hierarchical image database," In CVPR, 2009, pp. 248-255.
- [4] K. Simonyan and A. Zisserman. "Very deep convolutional networks for large-scale image recognition". In ICLR, 2015.
- [5] M. Kristan *et al.*, "The Visual Object Tracking VOT2017 Challenge Results," 2017 In ICCV Workshops, 2017, pp. 1949-1972
- [6] R. Tapu, B. Mocanu, T. Zaharia, "*DEEP-SEE*: Joint Object Detection, Tracking and Recognition with Application to Visually Impaired Navigational Assistance", Sensors 2017, vol. 17.