DL BASED IOT ENERGY AUDIT ANALYTICS FOR DETECTING AND IDENTIFYING CYBER-PHYSICAL ATTACKS

J Prashanthi [1], M. Pravalika[2], B. Savitha[2], Ch. Manikanta[2], M. Balraj[2], M. Haritha[2]

[1,2]Department of Computer Science and Engineering

[1,2] Sree Dattha Group of Institutions, Sheriguda, Telangana.

Abstract: Internet of Things (IoT) are vulnerable to both cyber and physical attacks. Therefore, a cyber-physical security system against different kinds of attacks is in high demand. Traditionally, attacks are detected via monitoring system logs. However, the system logs, such as network statistics and file access records, can be forged. Furthermore, existing solutions mainly target cyber-attacks. This paper proposes the first energy auditing and analytics based IoT monitoring mechanism. To our best knowledge, this is the first attempt to detect and identify IoT cyber and physical attacks based on energy auditing. Using the energy meter readings, we develop a dual deep learning (DL) model system, which adaptively learns the system behaviors in a normal condition. Unlike the previous single DL models for energy disaggregation, we propose a disaggregation-aggregation architecture. The innovative design makes it possible to detect both cyber and physical attacks. The disaggregation model analyzes the energy consumptions of system subcomponents, e.g., CPU, network, disk, etc., to identify cyber-attacks, while the aggregation model detects the physical attacks by characterizing the difference between the measured power consumption and prediction results. Using energy consumption data only, the proposed system identifies both cyber and physical attacks. The system and algorithm designs are described in detail. In the hardware simulation experiments, the proposed system exhibits promising performances.

Keywords: Energy Auditing, Deep Learning, Cyber-Physical Attacks.

1. INTRODUCTION

1.1 Motivation

A cyber-physical security system against different kinds of attacks is in high demand. Traditionally, attacks are detected via monitoring system logs. However, the system logs, such as network statistics and file access records, can be forged. Furthermore, existing solutions mainly target cyber-attacks.

1.2 Problem Definition

IoT devices are exposed to both cyber and physical worlds, so attacks and threats may come from both cyber and physical channels [1]. With diversified and numerous applications, IoT systems require the adaptive adjustment ability to solve not only cyber threats but also physical attacks [2], [3]. However, because of the limited processing, storage and communication resources as well as the unpredictable physical environment, traditional security software solutions are too heavy for IoT devices and often cannot detect physical threats [1], [4]. Thus, the IoT security system design is always challenging. In an IoT system, the perception and application layers have physical attack vulnerabilities, while the network layer is facing possible cyber-attacks [2]. Typically, the IoT system performance data can be used for analyzing the system behavior [5], such as network parameters [6], but those anomaly detection approaches are usually targeting cyber-attacks [7]. When IoT systems carry ubiquitous computing, IoT devices are physically reachable [8], thus physical threats and attacks become possible [9], which should be considered. However, as system logs are also attack targets and can be forged, IoT security should depend on a more "reliable" system monitoring mechanism. Energy auditing has been investigated in the emerging smart grids [10], but has not been known as a major attack target.

1.3 Objective of Project

The proposed energy audit and analytics-based security mechanism for IoT security is original and has not been attempted before. In this section, we first introduce some typical cyber and physical attacks and discuss their characteristics, then the most related works—power disaggregation and prediction, are presented.

2. LITERATURE SURVEY

2.1 A survey of machine and deep learning methods for internet of things (IoT) security

AUTHORS: M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani

The Internet of Things (IoT) integrates billions of smart devices that can communicate with one another with minimal human intervention. IoT is one of the fastest developing fields in the history of computing, with an estimated 50 billion devices by the end of 2020. However, the crosscutting nature of IoT systems and the multidisciplinary components involved in the deployment of such systems have introduced new security challenges. Implementing security measures, such as encryption, authentication, access control, network and application security for IoT devices and their inherent vulnerabilities is ineffective. Therefore, existing security methods should be enhanced to effectively secure the IoT ecosystem. Machine learning and deep learning (ML/DL) have advanced

considerably over the last few years, and machine intelligence has transitioned from laboratory novelty to practical machinery in several important applications. Consequently, ML/DL methods are important in transforming the security of IoT systems from merely facilitating secure communication between devices to security-based intelligence systems. The goal of this work is to provide a comprehensive survey of ML methods and recent advances in DL methods that can be used to develop enhanced security methods for IoT systems. IoT security threats that are related to inherent or newly introduced threats are presented, and various potential IoT system attack surfaces and the possible threats related to each surface are discussed. We then thoroughly review ML/DL methods for IoT security and present the opportunities, advantages and shortcomings of each method. We discuss the opportunities and challenges involved in applying ML/DL to IoT security. These opportunities and challenges can serve as potential future research directions.

2.2 Cyber-entity security in the internet of things

AUTHORS: H. Ning, H. Liu, and L. Yang

A proposed Internet of Things system architecture offers a solution to the broad array of challenges researchers face in terms of general system security, network security, and application security.

2.3 A comprehensive IoT attacks survey based on a building-blocked reference model.

AUTHORS: H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub

Internet of Things (IoT) has not yet reached a distinctive definition. A generic understanding of IoT is that it offers numerous services in many domains, utilizing conventional internet infrastructure by enabling different communication patterns such as human-to-object, object-to-objects, and object-to-object. Integrating IoT objects into the standard Internet, however, has unlocked several security challenges, as most internet technologies and connectivity protocols have been specifically designed for unconstrained objects. Moreover, IoT objects have their own limitations in terms of computation power, memory and bandwidth. IoT vision, therefore, has suffered from unprecedented attacks targeting not only individuals but also enterprises, some examples of these attacks are loss of privacy, organized crime, mental suffering, and the probability of jeopardizing human lives. Hence, providing a comprehensive classification of IoT attacks and their available countermeasures is an indispensable requirement. In this paper, we propose a novel four-layered IoT reference model based on building blocks strategy, in which we develop a comprehensive IoT attack model composed of four key phases. First, we have proposed IoT asset-based attack surface, which consists of four main components: 1) physical objects, 2) protocols covering whole IoT stack, 3) data, and 4) software. Second, we describe a set of IoT security goals. Third, we identify IoT attack taxonomy for each asset. Finally, we show the relationship between each attack and its violated security goals, and identify a set of countermeasures to protect each asset as well. To the best of our knowledge, this is the first paper that attempts to provide a comprehensive IoT attacks model based on a building-blocked reference model.

2.4 A new learning Automata-Based pruning method to train deep neural networks

AUTHORS: H. Guo, S. Li, B. Li, Y. Ma, and X. Ren

Deep neural network are one of the most powerful model for machine learning, which can learn the underlying patterns automatically from a large amount of data. So it can be extensively used in more and more Internet-of-Things (IoT) applications. However, the training of deep models is difficult, suffering from overfitting and gradient vanishing problem. Besides, the large amount of parameters and multiplication operations make it impractical for most deep learning models to directly execute on target hardware. In this paper, we propose a method of gradually pruning the weakly connected weights to improve the traditional stochastic gradient descent. And we adopt a reinforcement learning method called learning automata to find the weakly connected weights on account of its strong policy-making ability in stochastic and nonstationary environment. Our proposed method can learn a more effective and sparsely connected architecture during training from the initially fully connected neural networks. The experiments on MNIST show that our method have stronger power to defeat overfitting and can get better generalization performance on test set. Meanwhile, the thin and sparsely connected model we get can be more suitable for IoT applications.

2.5 System statistics learning-based iot security: Feasibility and suitability

AUTHORS: F. Li, A. Shinde, Y. Shi, J. Ye, X. Li, and W. Z. Song

Cyber-attacks and malfunctions challenge the wide applications of Internet of Things (IoT). Since they are generally designed as embedded systems, typical auto-sustainable IoT devices usually have a limited capacity and a low processing power. Because of the limited computation resources, it is difficult to apply the traditional techniques designed for personal computers or super computers, like traffic analyzers and antivirus software. In this paper, we propose to leverage statistical learning methods to characterize the device behavior and flag deviations as anomalies. Because the system statistics, such as CPU usage cycles, disk usage, etc., can be obtained by IoT application

program interfaces, the proposed framework is platform and device independent. Considering IoT applications, we train multiple machine learning models to evaluate their feasibility and suitability. For the target auto-sustainable IoT devices, which operate well-planned processes, the normal system performances can be modeled accurately. Based on time series analysis methods, such as local outlier factor, cumulative sum, and the proposed adaptive online thresholding, the anomalous behaviors can be effectively detected. Comparing their performances on detecting anomalies as well as the computation sources required, we conclude that relatively simple machine learning models are more suitable for IoT security, and a data-driven anomaly detection method is preferred.

3. PROPOSED SYSTEM

we develop a dual deep learning model system, which adaptively learns the system behaviors in a normal condition. Unlike the previous single deep learning models for energy disaggregation, we propose a disaggregation-aggregation architecture. The innovative design makes it possible to detect both cyber and physical attacks. The disaggregation model analyzes the energy consumptions of system subcomponents, e.g. CPU, network, disk, etc. to identify cyber attacks, while the aggregation model detects the physical attacks by characterizing the difference between the measured power consumption and prediction results. Using energy consumption data only, the proposed system identifies both cyber and physical attacks. The system and algorithm designs are described in detail. In the hardware simulation experiments, the proposed system exhibits promising performances.

In this paper, we propose a DL based IoT energy audit analytics for detecting and identifying not only cyber but also physical attacks. Using the proposed DL models, a system is built to detect anomalies in power consumption, which indicate characteristics of certain types of attacks. The contributions of our work are as follows:

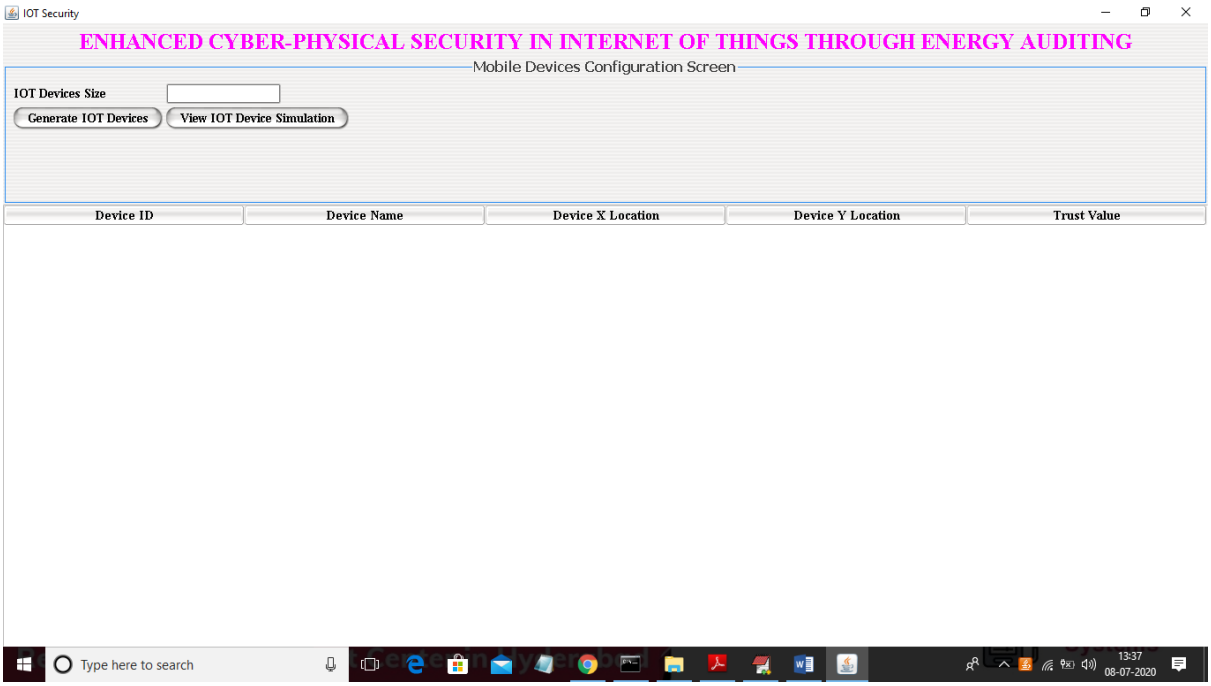
1) To our best knowledge, this is the first attempt to use energy audit data in the IoT security system to detect both cyber and physical threats and attacks; 2) We propose a dual deep learning model system. Unlike the previous deep learning applications, our system has two deep learning models, the disaggregation model and aggregation model

3) Our system detects operation anomalies based on only the energy audit readings without other sources. The dual DL models are pre-trained based on the performance metrics and energy consumption of an IoT device.

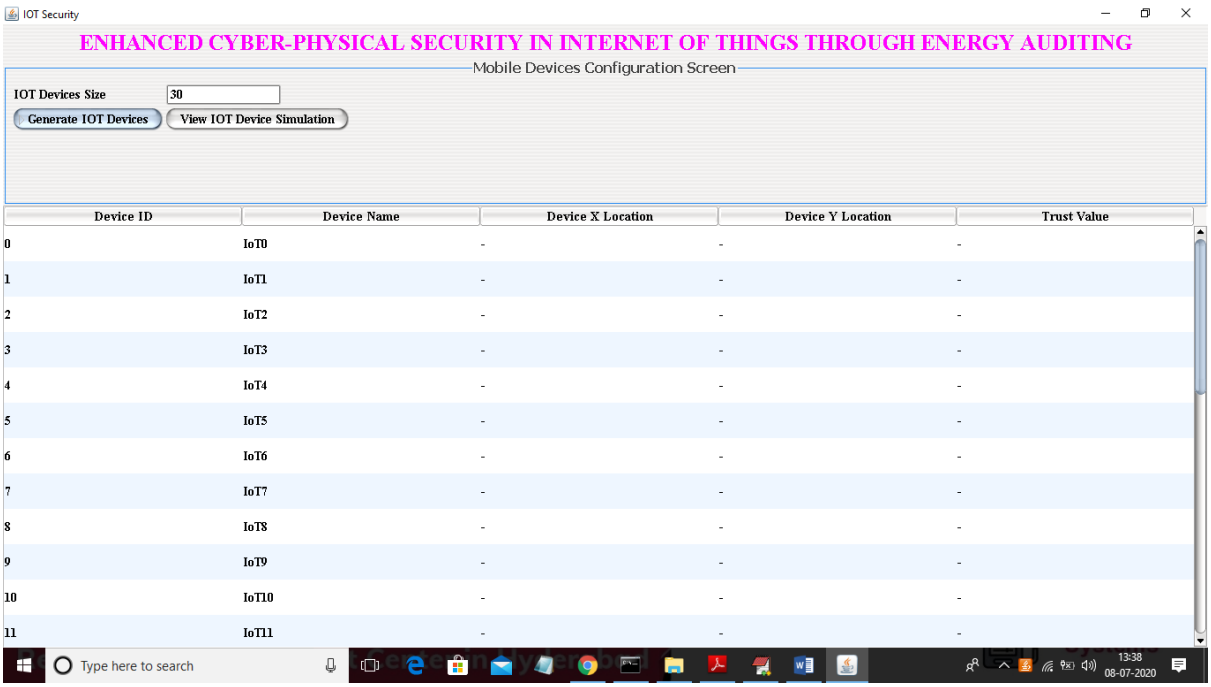
4) Based on the disaggregated system performance metrics and energy consumption prediction, the attacks can not only be detected but also identified.

4. RESULTS

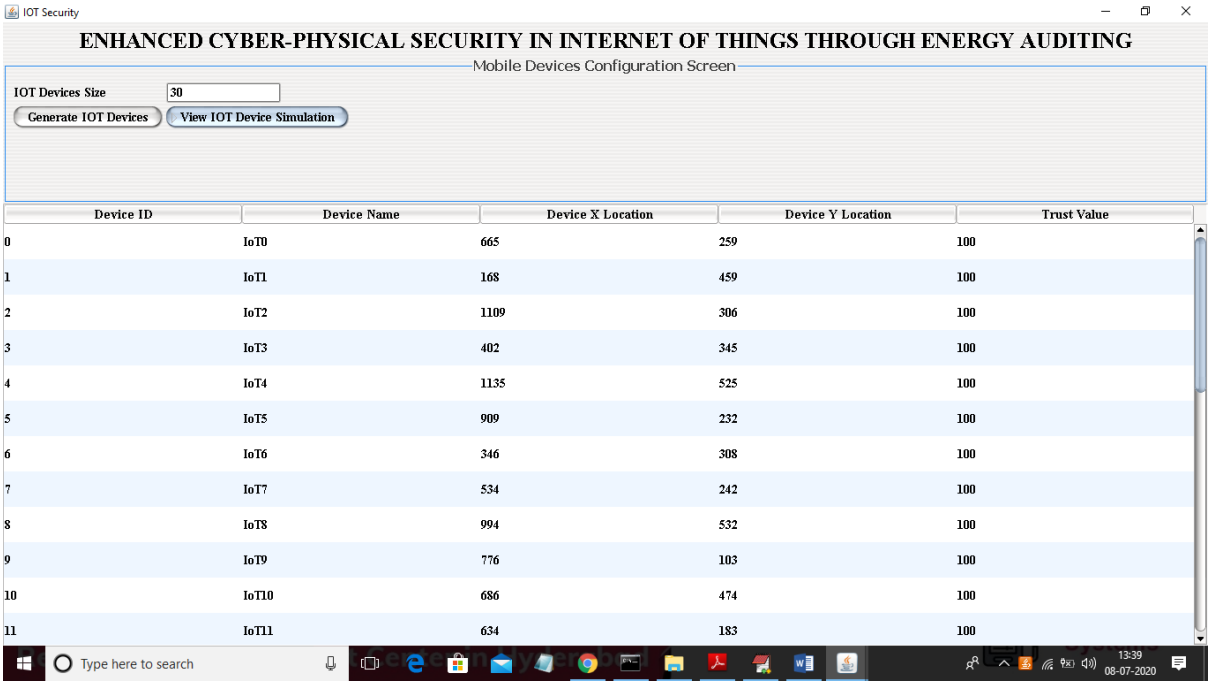
To run this project double click on run.bat file to get below screen



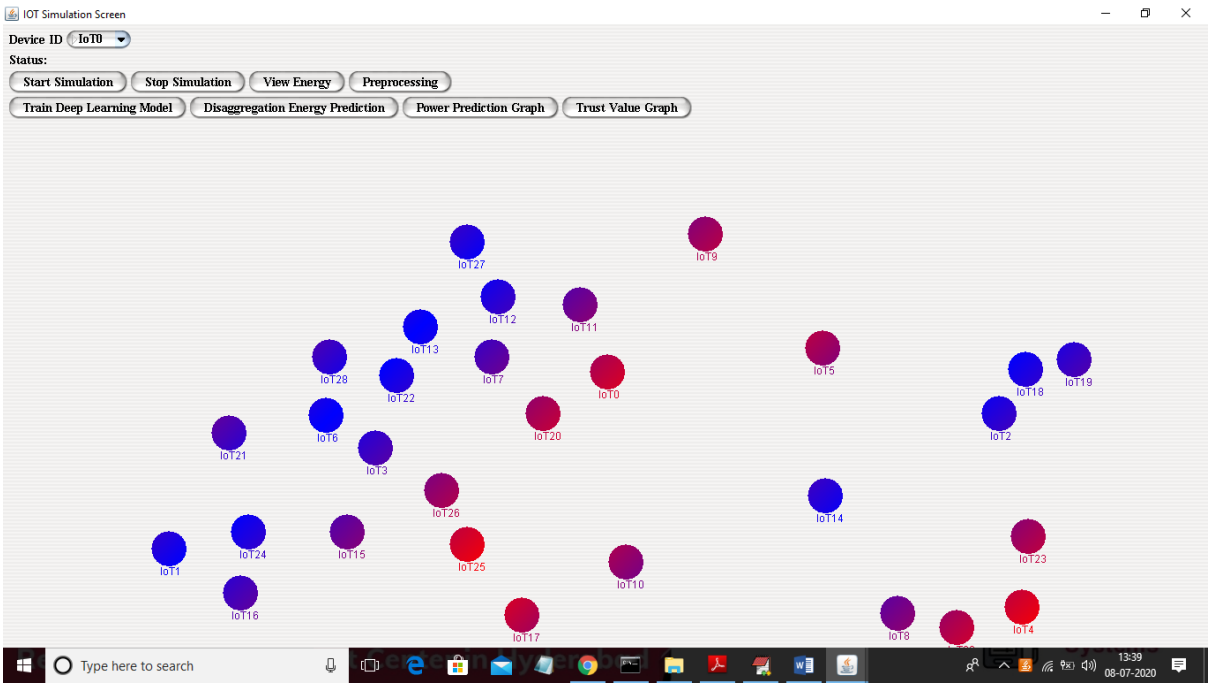
In above screen enter IOT Devices Size and then click on 'Generate IOT Devices' button to get below link



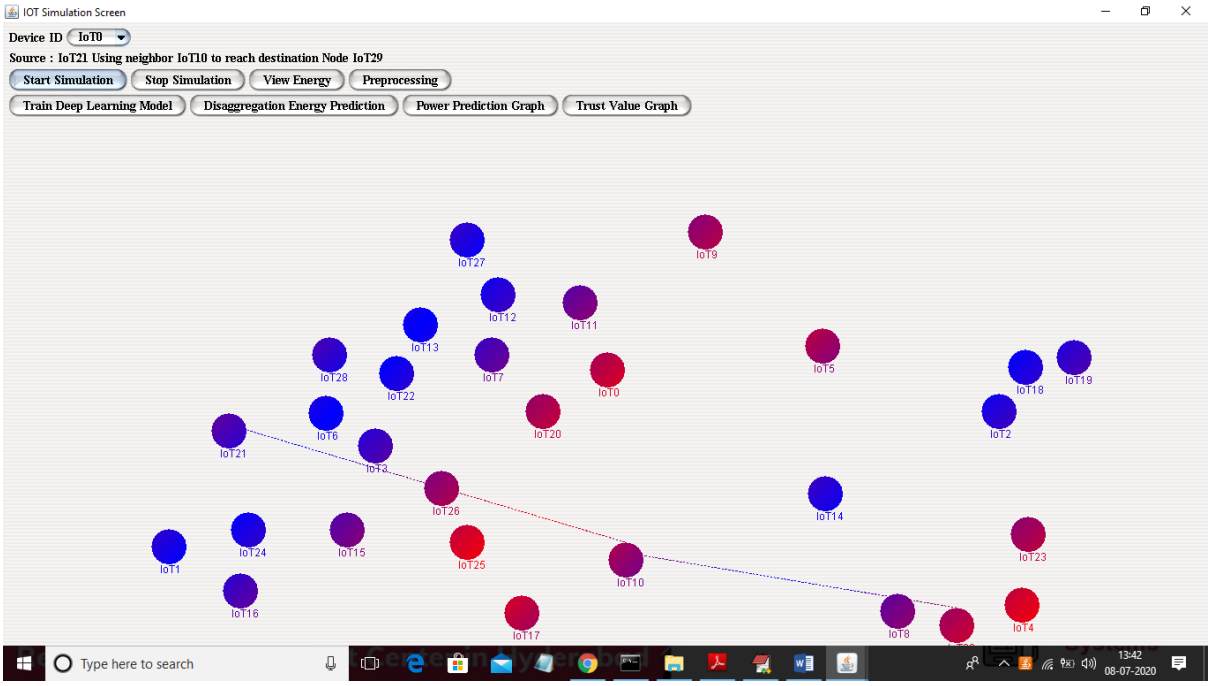
In above screen I entered IOT size as 30 and in above screen we can see each device id and now click on 'View IOT Device Simulation' button to get each IOT X, Y and Trust value



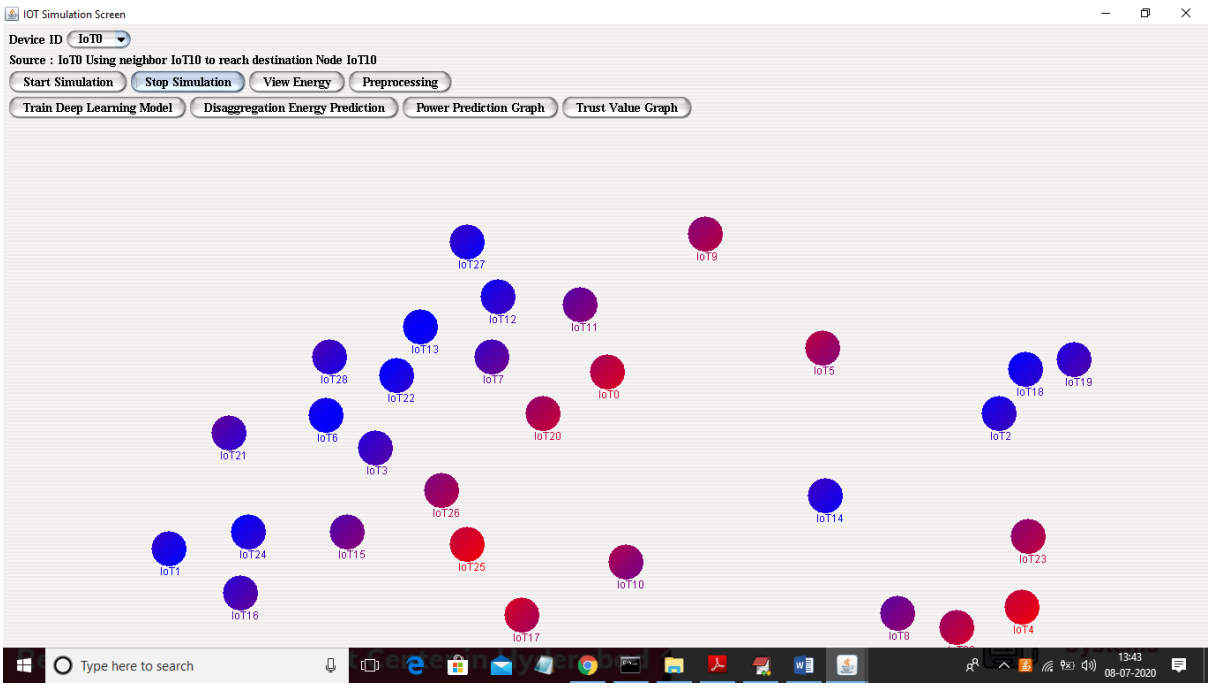
In above screen we can see each device X and Y location and all devices has trust value as 100. Now see below simulation screen



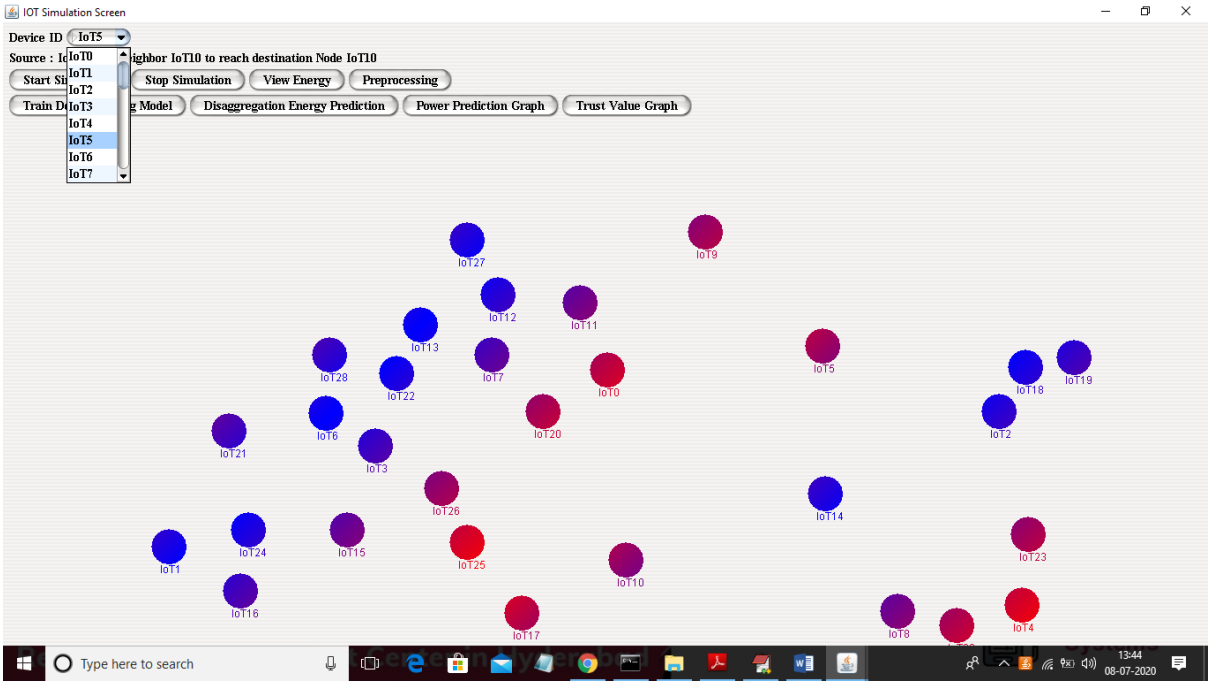
In above screen click on 'Start Simulation' button to allow each device to send data to other IOT devices. While sending data application will monitor its energy value. Let this simulation run for 2 to 3 minutes and application will choose random source and destination to send data to each other using neighbour IOT devices.



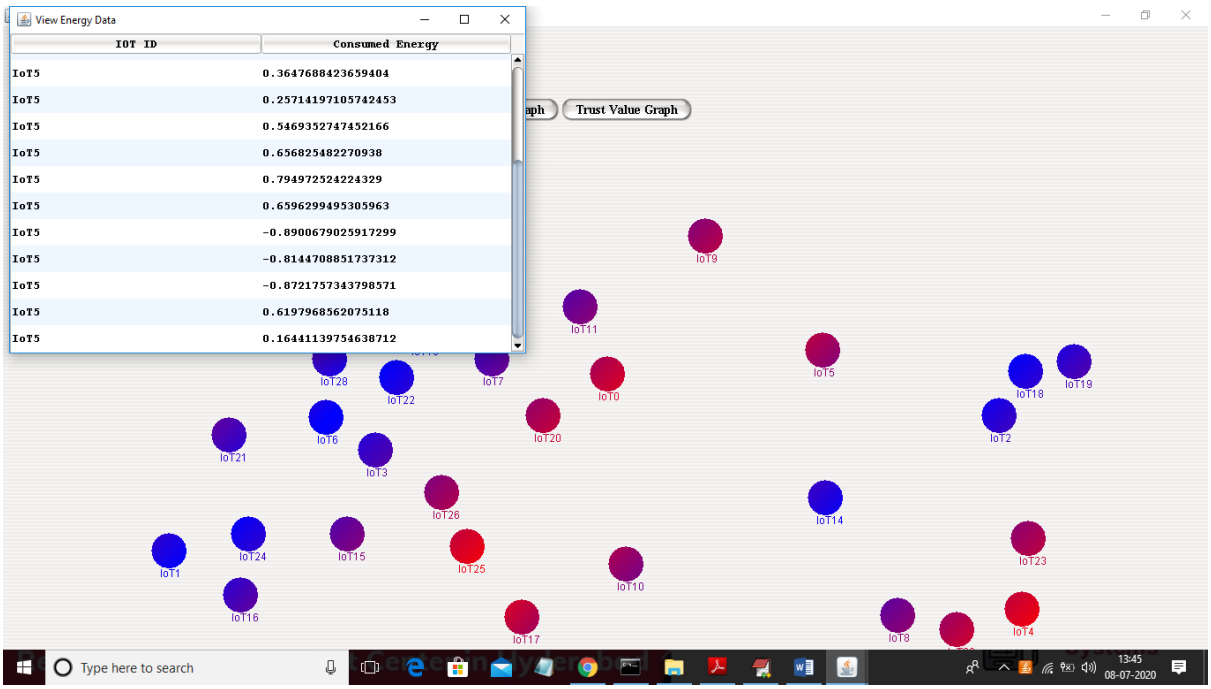
In above screen line from source to destination via neighbour indicates data transmission and after some time click on 'Stop Simulation' button to stop sending data.



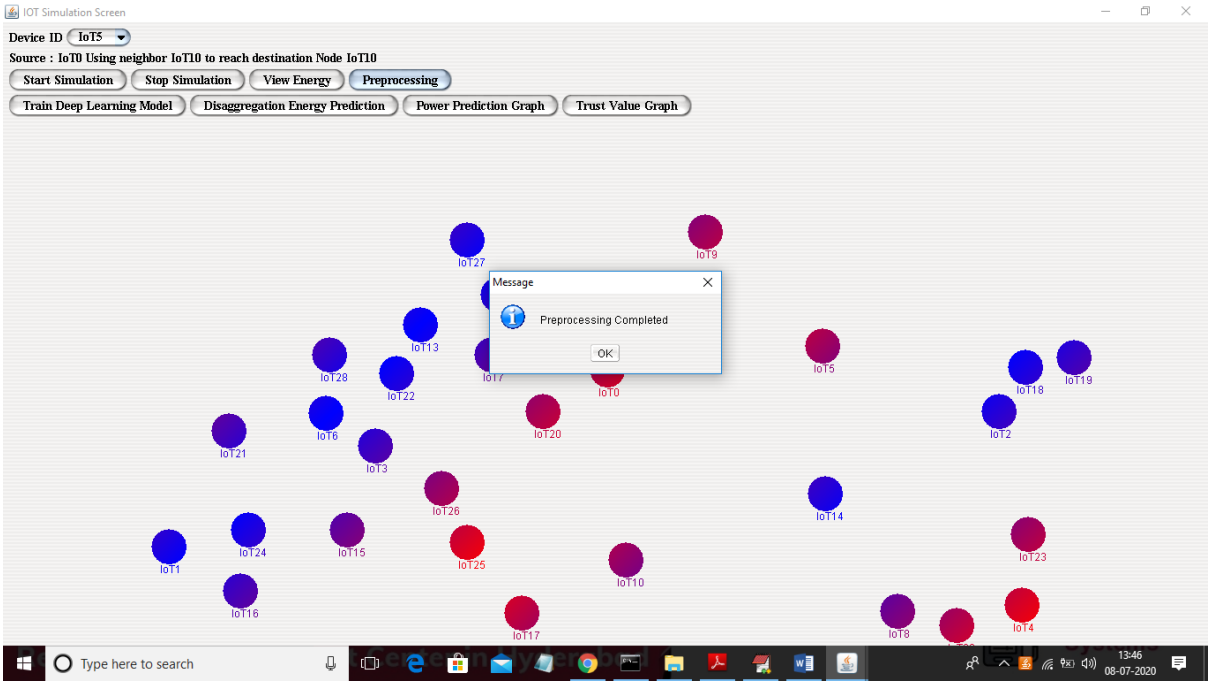
In above screen simulation stop and now select any IOT device from drop down box and click on 'View Energy' button to get its energy consumed information for each transmission



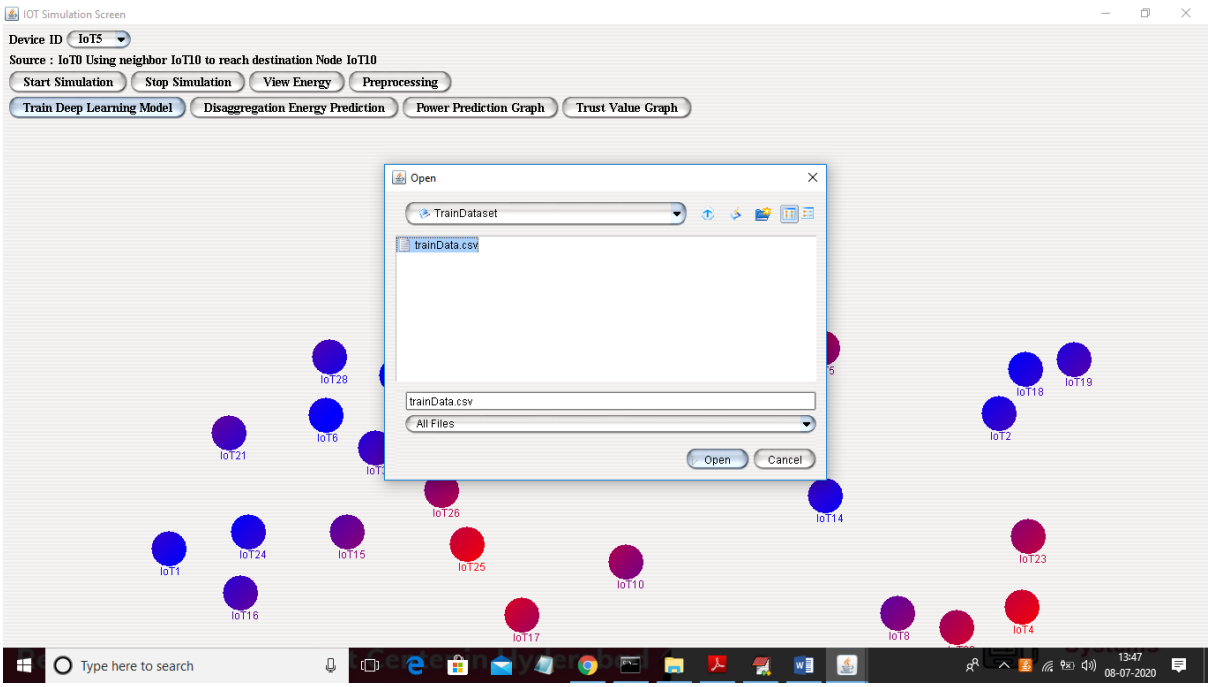
In above screen I am selecting IoT5 and now click on 'View Energy' button to get below screen



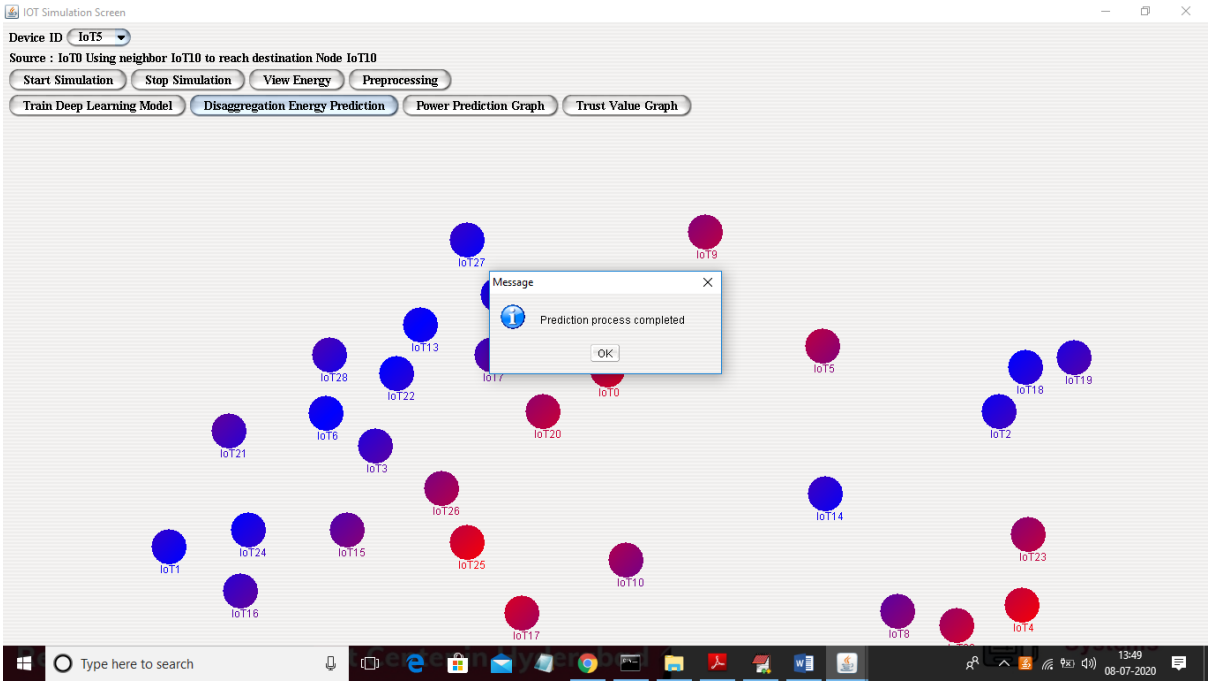
In above screen IOT5 energy consumed values we can see and sometime IOT reports negative energy and to clean such values click on "Preprocessing' button



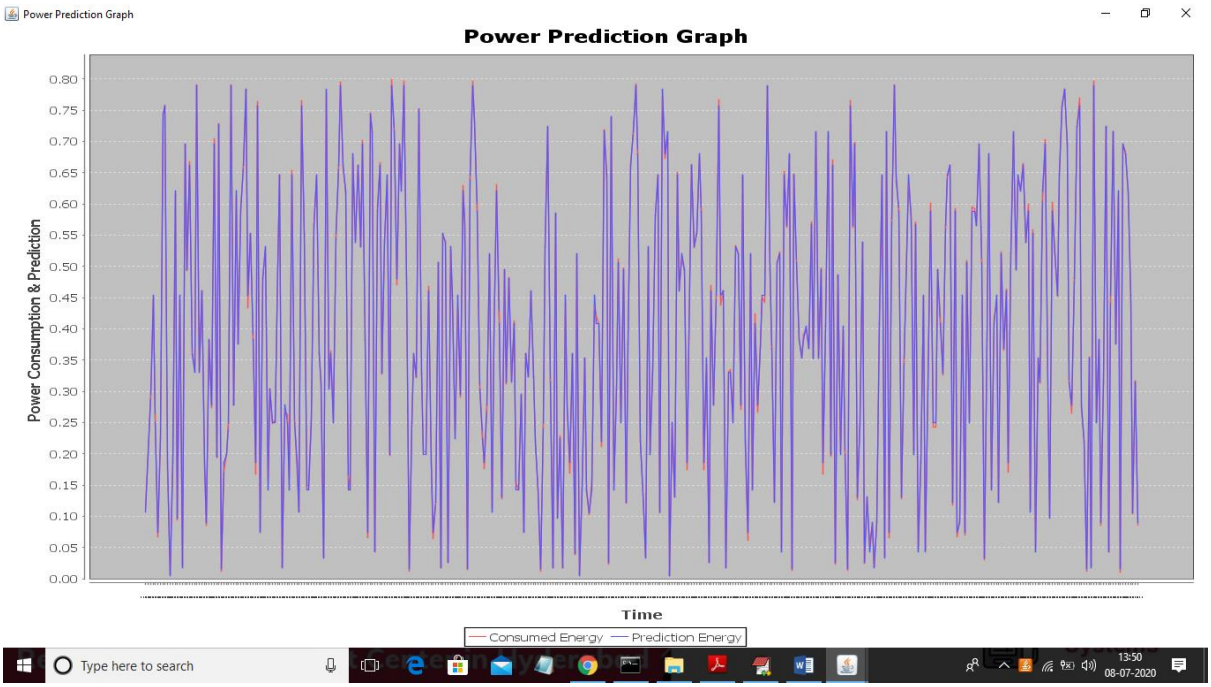
In above screen Preprocessing done and after Preprocessing no such negative values we can see. Now click on 'Train Deep Learning Model' button to upload train dataset and to train model



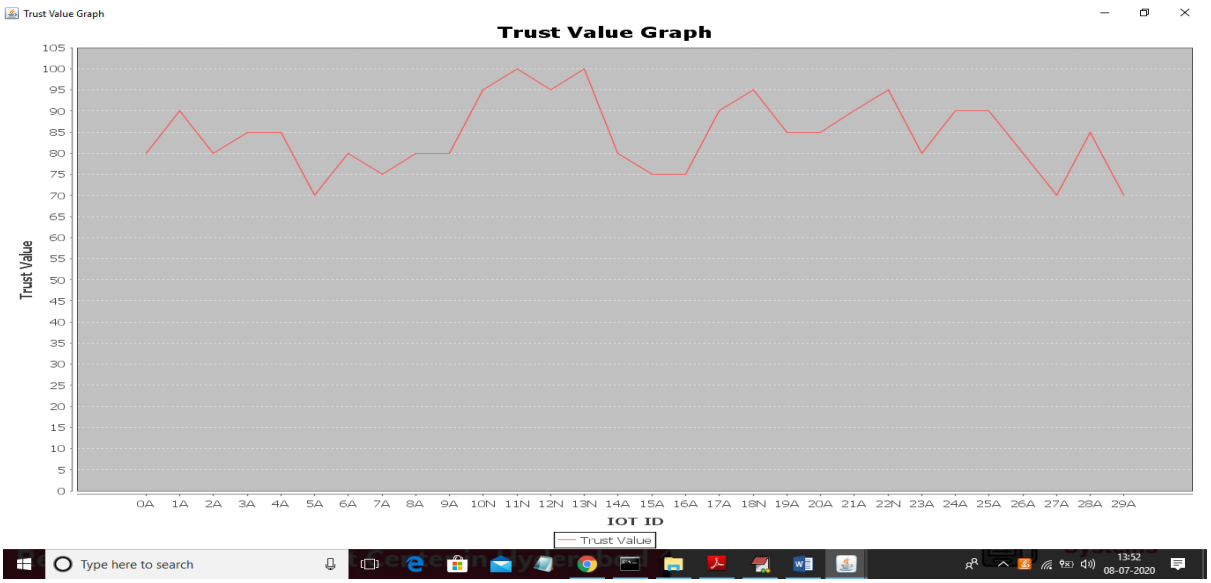
In above screen uploading train dataset to train deep learning model and now click on 'Disaggregation Energy Prediction' button to predict energy consumption as normal or abnormal



In above screen prediction process completed and now click on 'Power Prediction Graph' button to get below graph



In above graph x-axis represents Time and y-axis represents power consumption and blue line indicated predicted energy and red line indicates consumed energy. In above graph we can see consumed energy red line is little bit out of predicted energy and those energy consumption can be predicted as abnormal. To get all normal and abnormal IOT's click on 'Trust Value Graph' button



In above graph x-axis represents IOT ID and Y-axis represents trust values. In X-axis with IOT ID if we see character 'A' then that IOT ID is abnormal and 'N' means normal. In above graph we can see all IOT whose trust value less than 100 is marked as abnormal. I make all IOT's whose trust value drops lower than 95 to be marked as abnormal.

5. CONCLUSION

In this paper, we propose a DL based IoT security system using energy auditing data. The side-channel energy meter readings enable the proposed system to detect not only cyber but also physical attacks and threats. In addition, the energy auditing data are hard to be compromised compared with other sources. The dual disaggregation and aggregation deep learning models learn the normal performances of the IoT system, and can also provide detailed analytics of individual system performance metrics, if applicable. The anomaly detection based on the prediction errors tracks both cyber and physical anomalous behaviors. With the proposed approach, IoT system will be better monitored and secured.

REFERENCES

[1] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," arXiv preprint arXiv:1807.11023, 2018.
[2] H. Ning, H. Liu, and L. Yang, "Cyber-entity security in the internet of things," Computer, p. 1, 2013.
[3] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," International Journal of Advanced Computer Science and Applications(IJACSA), vol. 9(3), 2018.
[4] H. Guo, S. Li, B. Li, Y. Ma, and X. Ren, "A new learning Automata-Based pruning method to train deep neural networks," IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3263–3269, Oct. 2018.
[5] F. Li, A. Shinde, Y. Shi, J. Ye, X. Li, and W. Z. Song, "System statistics learning-based iot security: Feasibility and suitability," IEEE Internet of Things Journal, pp. 1–8, 2019.
[6] .M. Zou, C. Wang, F. Li, and W. Song, "Network phenotyping for network traffic classification and anomaly detection," in IEEE International Symposium on Technologies for Homeland Security (HST), 2018.
[7] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in Foundations and Applications of Self* Systems, IEEE International Workshops on. IEEE, 2016, pp. 242–247.
[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
[9] .A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber-physical systems," Proceedings of the IEEE, vol. 100, no. 1, pp. 283–299, 2012.
[10] D. E. Phillips, R. Tan, M.-M. Moazzami, G. Xing, J. Chen, and D. K. Y. Yau, "Supero: A sensor system for unsupervised residential power usage monitoring," in 2013 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE, 2013, pp. 66–75.