

Energy Auditing for Improved Cyber-Physical Security in the Internet of Things

Miss. Chandramoulika Nekkanti¹, Mrs. M. Revati²

**#1PG Scholar, Dept Of CSE, Nova College Of Engineering and Technology,
Jangareddygudem.**

**#2 Associate Professor, Dept Of CSE, Nova College Of Engineering and
Technology, Jangareddygudem.**

ABSTRACT_ IoT devices are susceptible to both physical and cyber threats. A cyber-physical security system that can fend off various threats is therefore highly sought after. Attacks are typically found by keeping an eye on system logs. But system logs can be faked, including records of file access and network information. Additionally, current solutions primarily focus on cyberattacks. The first energy auditing and analytics-based IoT monitoring method is proposed in this research. To the best of our knowledge, this is the first effort to use energy auditing to detect and identify IoT cyber and physical threats. We create a dual deep learning (DL) model system using the energy metre readings, which adaptively learns the system's actions under typical conditions. We provide an architecture for energy disaggregation that combines disaggregation and aggregation, in contrast to earlier single DL models. Attacks on both a physical and virtual level can be detected because to the creative design. The aggregation approach detects physical attacks by describing the difference between the measured power consumption and predicted results, whereas the disaggregation model analyses the energy consumptions of system subcomponents, such as CPU, network, disc, etc., to identify cyber attacks. The suggested method recognises both physical and cyber threats using simply energy usage data. In-depth descriptions of the system and algorithm designs are provided. The proposed system displays promising performances in the hardware simulation studies.

1.INTRODUCTION

The Internet of Things (IoT) has faced numerous complex security difficulties. The likelihood of both cyber and physical attacks is high. The IoT system must therefore

have the flexibility to adapt in order to deal with both online threats and physical assaults. But because there are fewer storage and connectivity options, IoT device security problems are harder to solve. Its design is therefore extremely dangerous. Physical attacks on the application layer and cyberattacks on the network layer are both common in IoT systems. The security of the Internet of Things heavily depends on a solid system monitoring mechanism. IoT devices like smartphones have access to energy auditing in large quantities. Therefore, we choose the rate of energy consumption as the security system's source. This brand-new monitoring technique works with the majority of IoT solutions. According to the underlying theory, any physical or digital attack will alter the energy profile. If an attack occurs that has no impact on the energy profile, it can be disregarded. We can create a cheap energy metre if some IoT gadgets do not support energy auditing. so that it may continue performing energy audits and ensuring security. We explore deep learning-based IoT energy audit analysis in this study to confirm both cyber and physical concerns. Here, we differentiate between the use of force, which demonstrates the tactics used in particular types of assaults.

2.LITERATURE SURVEY

2.1 H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, “A comprehensive IoT attacks survey based on a building-blocked reference model,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018.

The definition of the Internet of Things (IoT) is still nebulous. IoT can enable various communication patterns, such as human-to-object, object-to-object, and object-to-object, by employing traditional internet infrastructure. This is how it is generally understood. However, as the majority of internet technologies and communication protocols have been created exclusively for unrestrained items, integrating IoT gadgets into the normal Internet has revealed a number of security challenges. Additionally, IoT items have their own constraints in terms of memory, bandwidth, and processing power. Consequently, IoT vision has been impacted by previously unheard-of attacks that target both persons and businesses. Some examples of these attacks include loss of privacy, organised crime, mental suffering, and the potential to endanger human lives. Therefore, it is essential to provide a thorough classification of IoT attacks and the various defences against them. In this

research, we present a novel four-layered IoT reference model based on the building blocks approach, in which we establish a thorough IoT assault model made up of four essential phases. The first thing we've suggested is an attack surface based on IoT assets, which has four key parts: 1) physical items, 2) protocols covering the entire IoT stack, 3) data, and 4) software. We then go over a number of IoT security objectives. Third, we determine each asset's IoT attack taxonomy. Finally, we demonstrate the connection between each attack and the security objectives it has breached, as well as a number of solutions to safeguard each asset. We believe that this is the first study to make an effort to present a thorough IoT threats model based on a building-blocked reference model.

2.2 M. Zou, C. Wang, F. Li, and W. Song, “Network phenotyping for network traffic classification and anomaly detection,” in Proc. IEEE Int. Symp. Technol. Homeland Security (HST), Woburn, MA, USA, 2018, pp. 1–6.

In order to identify aberrant network traffic, this study suggests creating a network phenotyping system based on network resource utilisation analysis. Different metrics, such as resource and network consumption monitoring and physical state estimation, may be used for network phenotyping in a cyber-physical system (CPS). Through sophisticated image processing and machine learning techniques, the group of devices will jointly determine a comprehensive perspective of the entire system. The methodology described in this paper can be used for classification and anomaly detection based on various resource metrics, however we use the network traffic pattern as a study example to show how effective it is. On the basis of network resource utilisation, we utilise image processing and machine learning to identify and extract communication patterns. Four decentralised applications from the actual world are used to test the phenotypic technique. The overall accuracy of recognition is around 99 percent when using the right length of sampled continuous network resources. The anomalous network traffic is also found using the recognition error. We simulate anomalous network resource utilisation that is equal to 10%, 20%, and 30% of the typical network resource usage. The results of the experiment demonstrate the effectiveness of the suggested anomaly detection strategy in identifying each level of abnormal network resource utilisation.

2.3 J. Pacheco and S. Hariri, “IoT security framework for smart cyber infrastructures,” in Proc. IEEE Int. Workshops Found. Appl. Self* Syst., 2016, pp. 242–247.

The Internet of Things (IoT) will link not only computers and mobile devices, but also intelligent cities, houses, and buildings, as well as gas and water networks, automobiles, aeroplanes, and other transportation systems. As a result of IoT, a wide range of cutting-edge information services will emerge that must be processed in real-time and call for data centres with ample storage and processing capacity. In addition to providing the necessary processing and storage capacity, the integration of IoT with cloud and fog computing enables IoT services to be widely available, affordable, and accessible from any location using any device (mobile or stationary). However, because of the enormous growth in the attack surface, complexity, heterogeneity, and amount of resources, IoT infrastructures and services will present significant security challenges. An IoT security architecture for smart infrastructures, such as Smart Homes (SH) and smart buildings, is presented in this study (SB). Additionally, we provide a general threat model that may be applied to the creation of a security protection approach for Internet of Things services against cyberattacks (known or unknown). Furthermore, we demonstrate how the Anomaly Behavior Analysis (ABA) Intrusion Detection System (ABA-IDS) can recognise and categorise a variety of assaults on IoT sensors.

3.PROPOSED SYSTEM

The first IoT monitoring system based on energy audits and analytics is proposed in this study. To the best of our knowledge, this is the first effort to use energy auditing to detect and identify IoT cyber and physical threats. We create a dual deep learning model system using the energy metre readings that adaptively learns the behaviours of the system under typical conditions. We suggest a disaggregation-aggregation architecture as opposed to the prior single deep learning models for energy disaggregation. Attacks on both a physical and virtual level can be detected because to the creative design. The aggregation approach detects physical attacks by describing the difference between the measured power consumption and predicted results, whereas the disaggregation model analyses the energy consumptions of system subcomponents, such as CPU, network, disc, etc., to identify cyber attacks.

The suggested method recognises both physical and cyber threats using simply energy usage data. In-depth descriptions of the system and algorithm designs are provided. In hardware simulation tests, the suggested system displays encouraging performances.

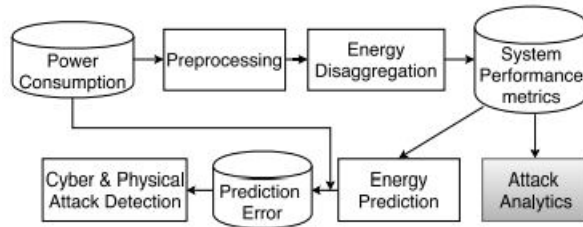
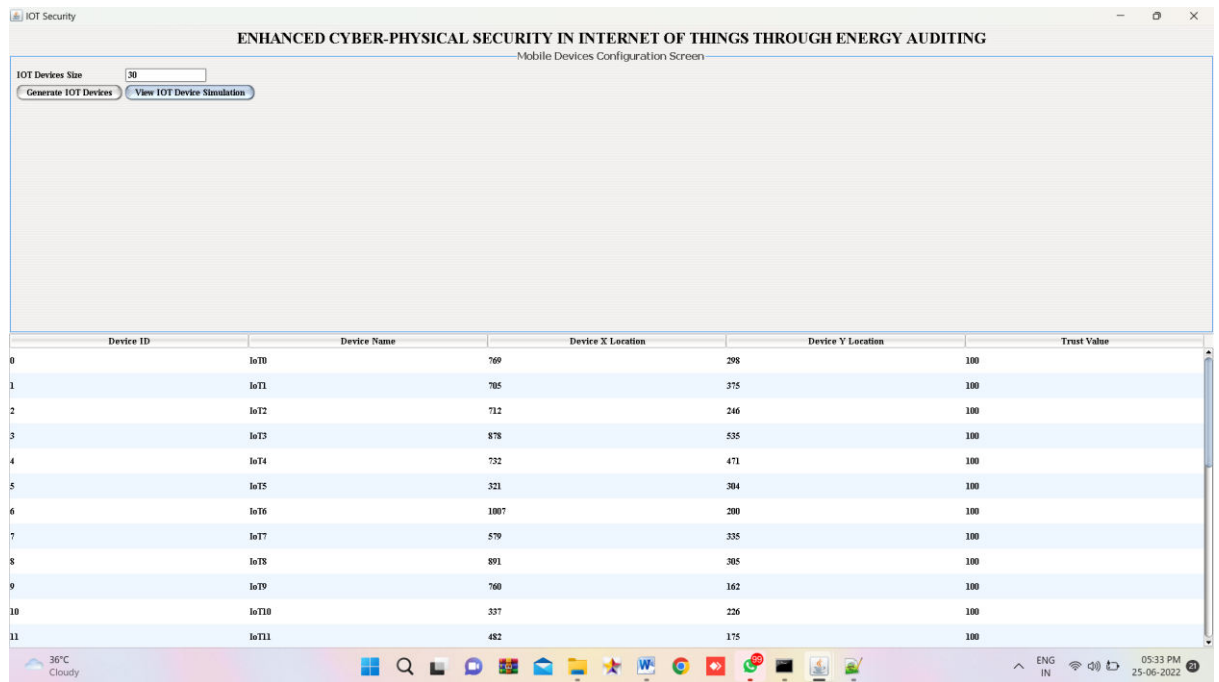


Fig 1:Architecture

3.1 IMPLEMENTATION

- 1) Power consumption: actually we don't have any IOT devices so we are generating random energy consumption values for various IOT devices using simulation.
- 2) Pre-processing: sometime IOT devices will report noisy negative energy value and such values will be replaced with median values by using median filtering algorithm. Using pre-processing steps will remove out all noisy values.
- 3) Energy Disaggregation: Using this module we will store all energy values consume during simulation.
- 4) System Performance Metrics: Using this module we will audit energy model using deep learning algorithm to predict whether system is in attack or normal state.
- 5) Trust value: Each IOT device will have trust value associated with and if IOT device sending DOS attack request (huge size request) to other IOT then deep learning predict it as abnormal IOT and its trust value will be degraded. For all IOT's by default I gave trust value as 100. Upon predicting it as abnormal IOT then its trust value will be deducted.

4.RESULTS AND DISCUSSION



ENHANCED CYBER-PHYSICAL SECURITY IN INTERNET OF THINGS THROUGH ENERGY AUDITING
Mobile Devices Configuration Screen

IOT Devices Size:

Device ID	Device Name	Device X Location	Device Y Location	Trust Value
0	IoT0	769	298	100
1	IoT1	705	375	100
2	IoT2	712	246	100
3	IoT3	878	535	100
4	IoT4	732	471	100
5	IoT5	321	304	100
6	IoT6	1007	200	100
7	IoT7	579	335	100
8	IoT8	891	305	100
9	IoT9	760	162	100
10	IoT10	337	226	100
11	IoT11	482	175	100

Fig 2: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

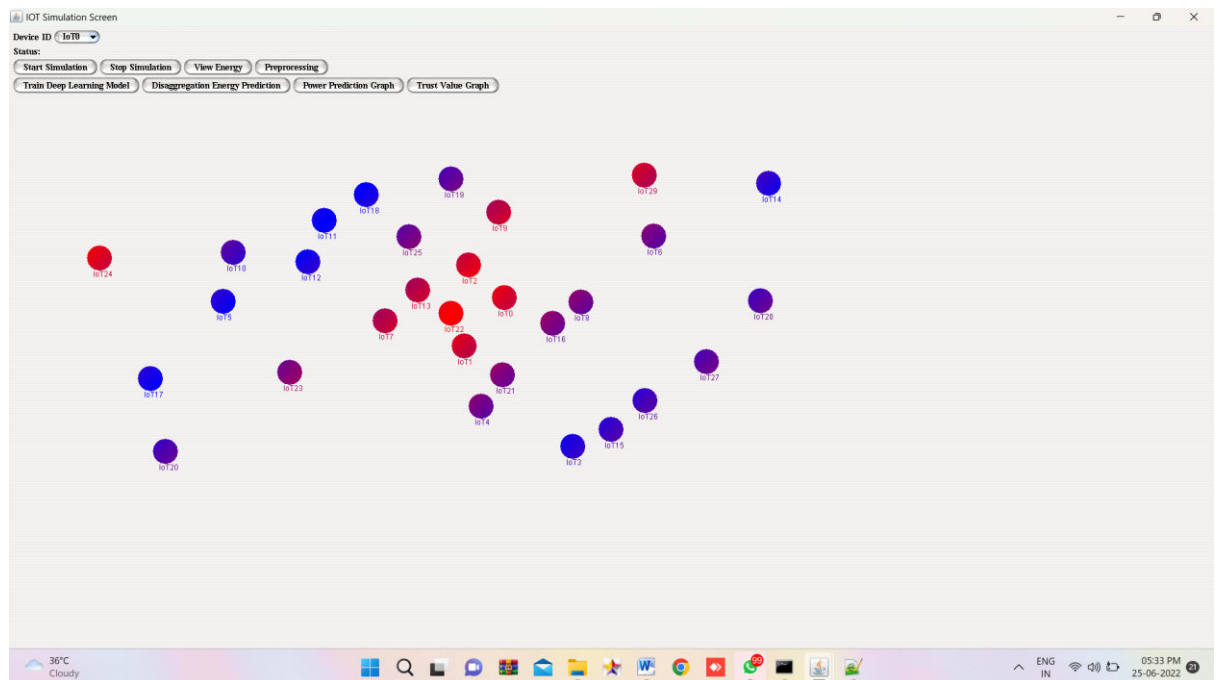


Fig 3:In above screen click on ‘Start Simulation’ button to allow each device to send data to other IOT devices. While sending data application will monitor its energy value. Let this simulation run for 2 to 3 minutes and application will choose random source and destination to send data to each other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

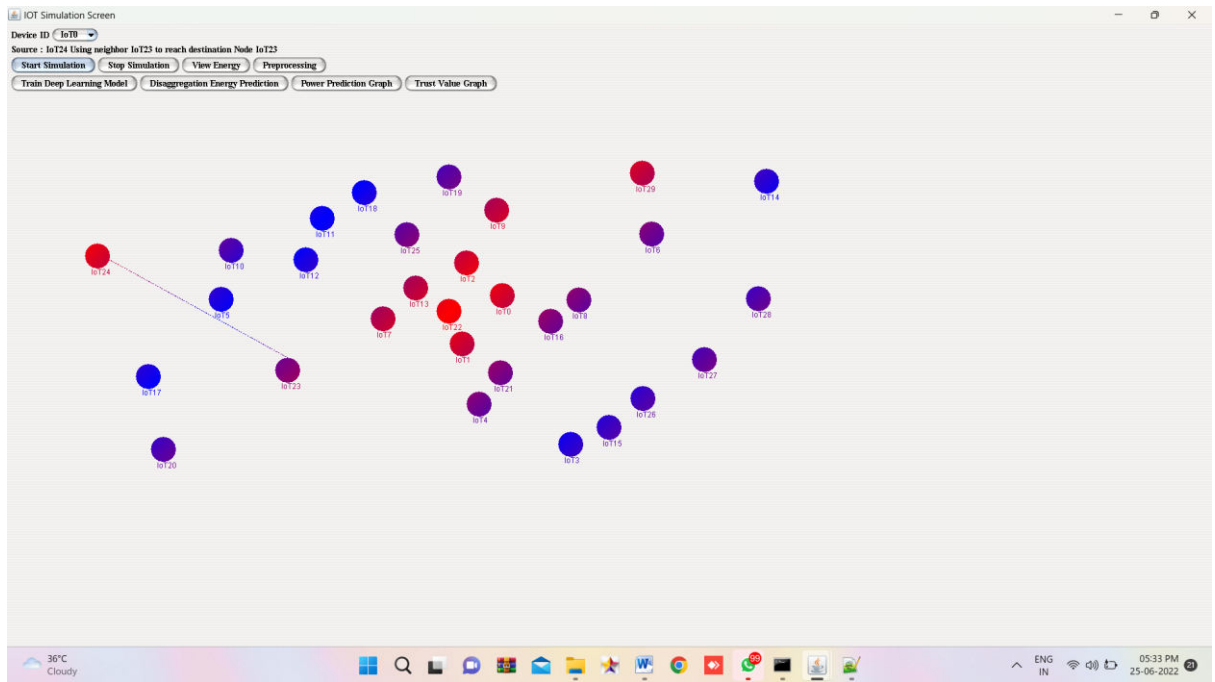


Fig 4:In above screen line from source to destination via neighbour indicates data transmission and after some time click on ‘Stop Simulation’ button to stop sending data.

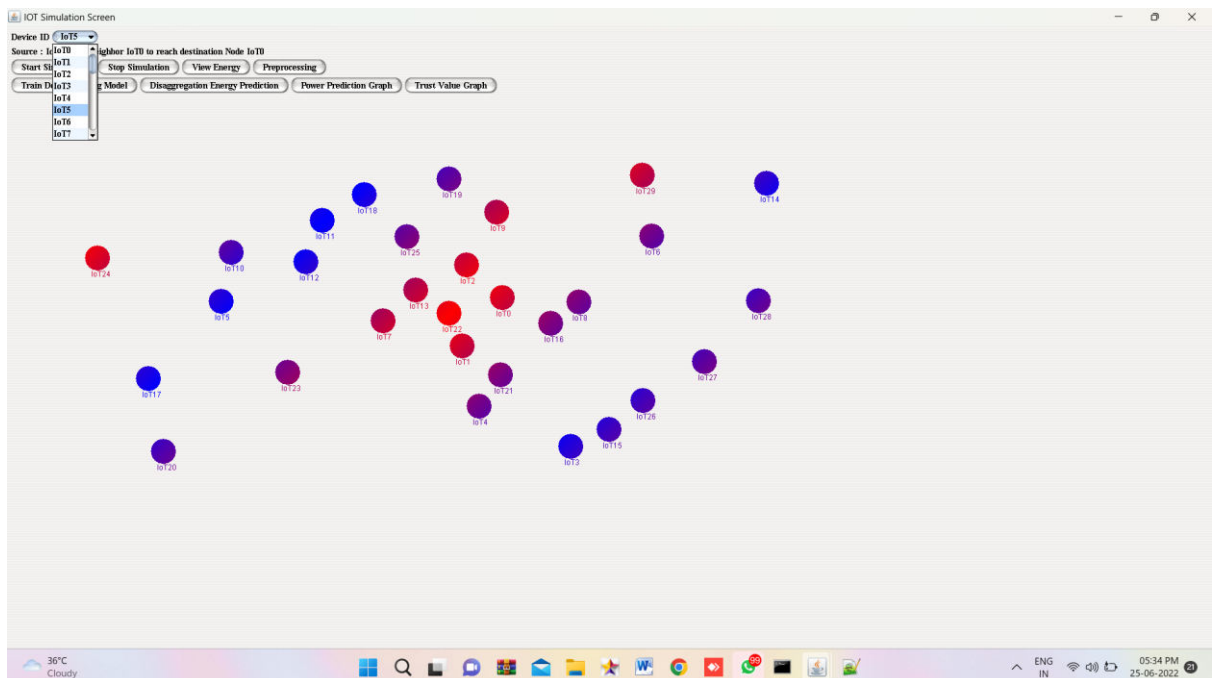


Fig 5:In above screen I am selecting IoT5 and now click on ‘View Energy’ button to get below screen

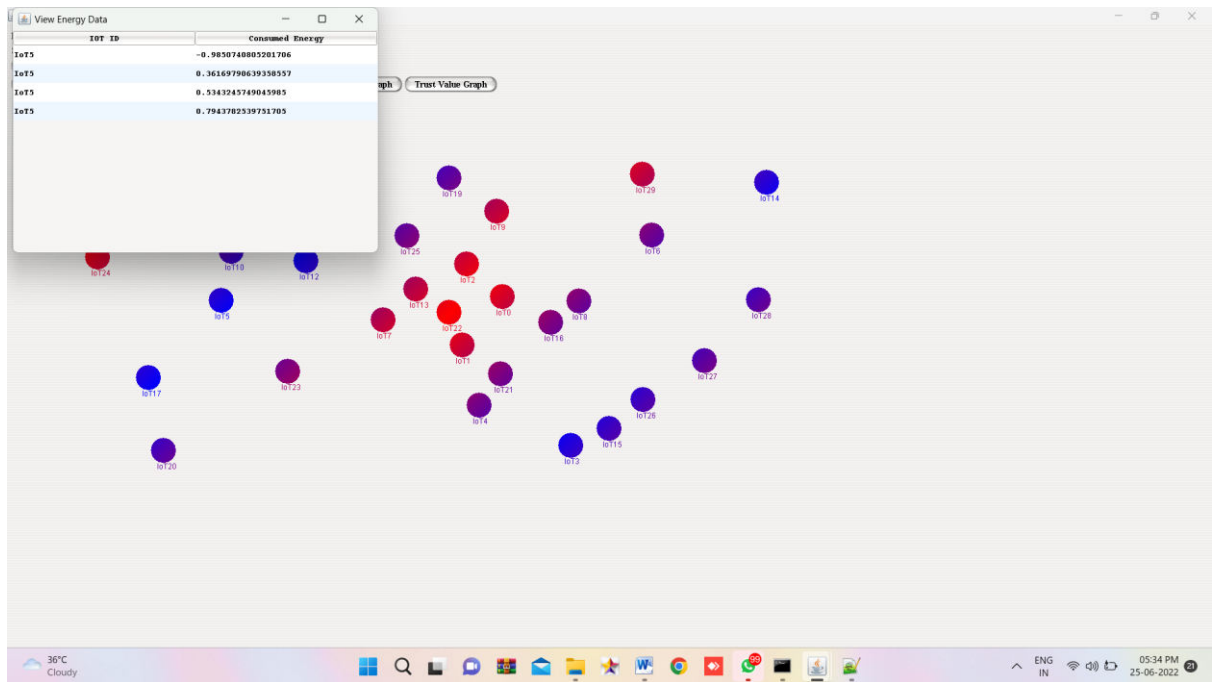


Fig 6:In above screen IOT5 energy consumed values we can see and sometime IOT reports negative energy and to clean such values click on “Preprocessing” button

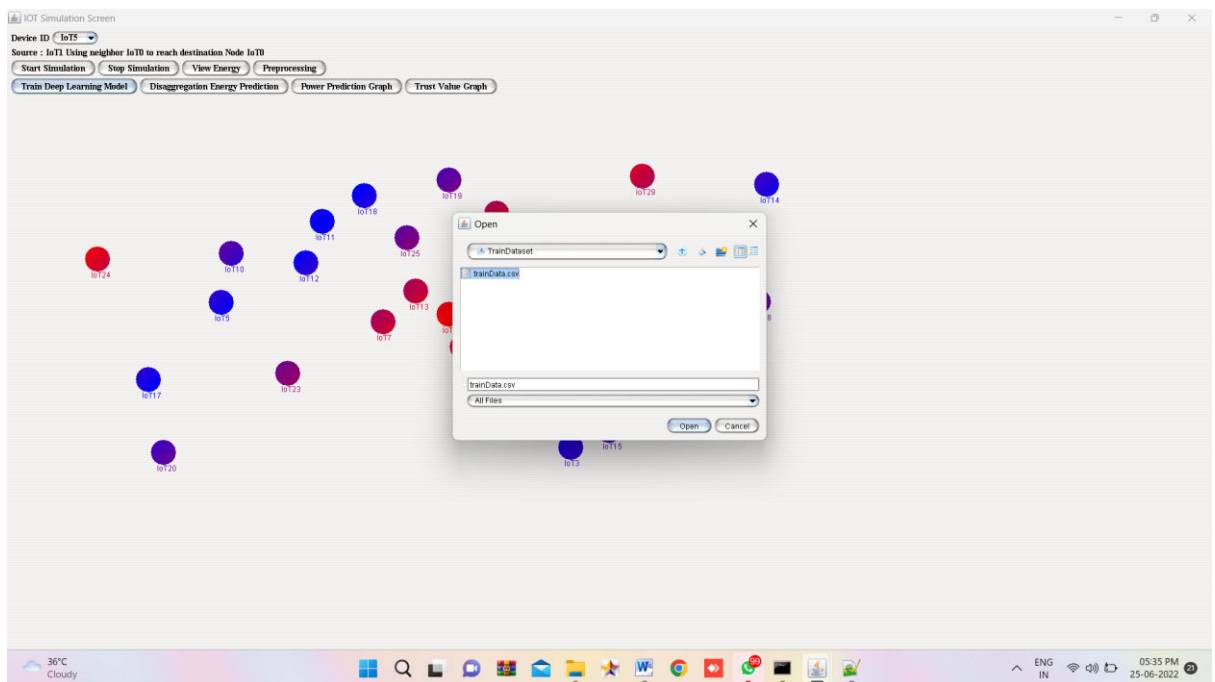


Fig 8:In above screen uploading train dataset to train deep learning model and now click on ‘Disaggregation Energy Prediction’ button to predict energy consumption as normal or abnormal

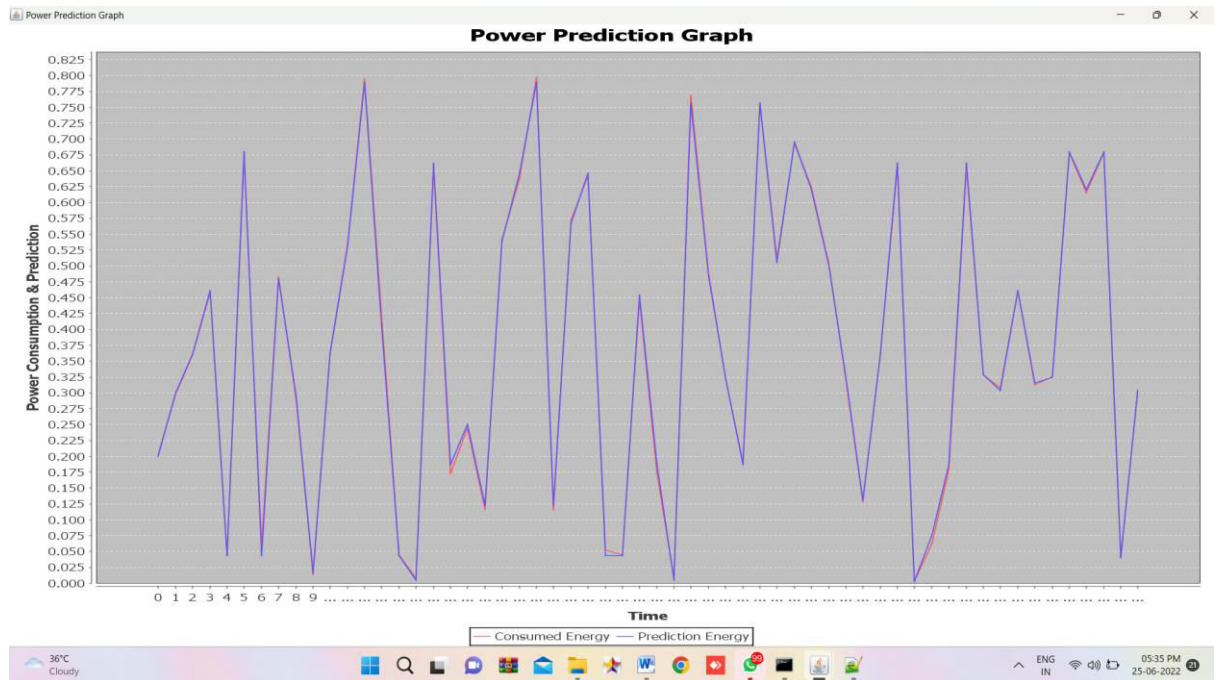


Fig 9:In above graph x-axis represents Time and y-axis represents power consumption and blue line indicated predicted energy and red line indicates consumed energy. In above graph we can see consumed energy red line is little bit out of predicted energy and those energy consumption can be predicted as abnormal. To get all normal and abnormal IOT's click on 'Trust Value Graph' button

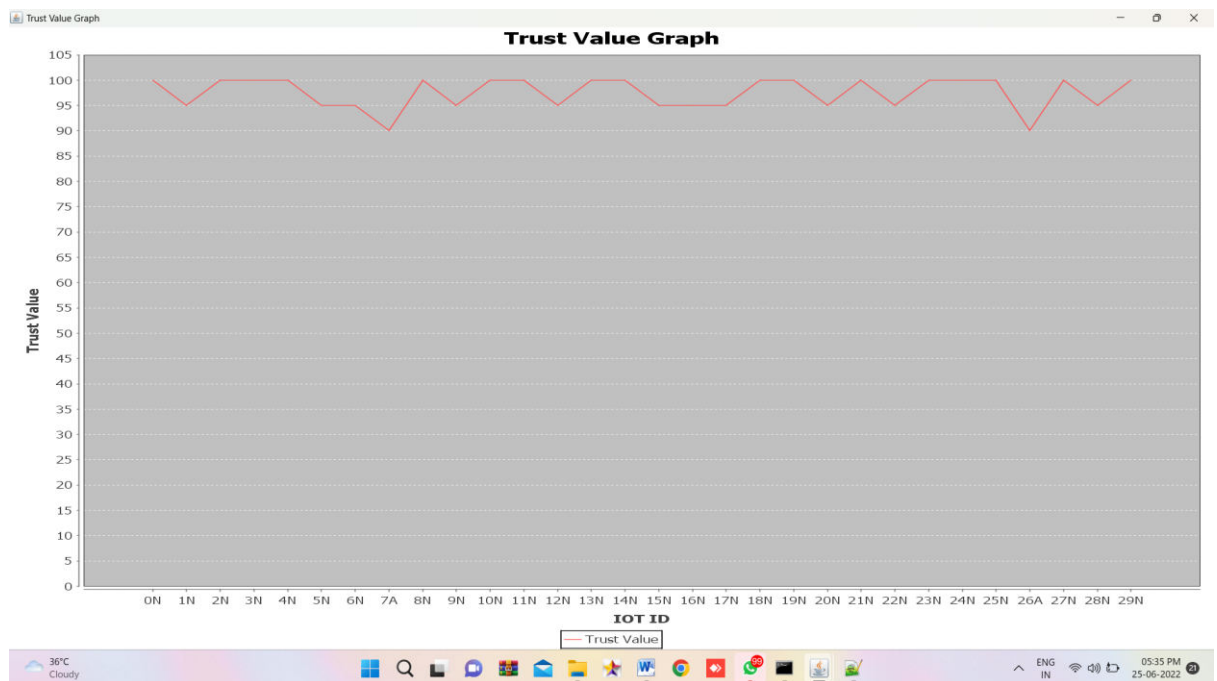


Fig 10:In above graph x-axis represents IOT ID and Y-axis represents trust values. In X-axis with IOT ID if we see character 'A' then that IOT ID is abnormal and 'N' means normal. In above graph we can see all IOT whose trust value less than 100 is marked as abnormal. I make all IOT's whose trust value drops lower than 95 to be marked as abnormal.

4.CONCLUSION

In this study, we suggest an IoT security solution based on DL that makes use of energy auditing data. The suggested system has the ability to identify physical as well as cyberattacks and threats thanks to the side-channel energy metre readings. In contrast to data from other sources, energy auditing data is very difficult to tamper with. The dual disaggregation and aggregation deep learning models learn the typical IoT system performance indicators and, if necessary, can additionally offer in-depth analytics of specific system performance metrics. The prediction errors-based anomaly detection system keeps track of both cyber- and physical-anomalous behaviours. The suggested method will improve IoT system security and monitoring.

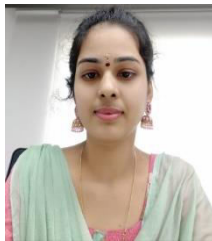
REFERENCES

- [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. [Online]. Available: <http://dx.doi.org/10.1109/JIOT.2017.2711426>
- [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.



Miss. Chandramoulika Nekkanti pursuing M.Tech in department of Computer Science and Engineering at Nova College Of Engineering and Technology, Jangareddygudem. She has completed B.Tech from Kakinada Institute of Engineering and Technology.



Mrs. M. Revati, well known Author and excellent teacher Received M.Tech (SE) from Jawaharlal Nehru Technological University Hyderabad ,she is working as Associate Professor ,Department of computer science engineering , Nova college of Engineering and Technology, She has 11 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals.

Her area of Interest includes Data Warehouse and Data Mining, information security, computer organization, flavors of Unix Operating systems and other advances in computer science.