IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Enhanced Physical-Cyber Security in IoT by Energy Auditing

[1]E. Satish Babu, [2]B. Sirisha, [3]V. Neha, [4]B. Aadarsh, [5]B. Vijaya Durga,
[2,3,4,5]Final Year – Department of Computer Science and Engineering
[1]Asso. Professor, Jyothishmathi Institute of Technology and Science
Karimnagar, Telangana

ABSTRACT:
Internet of Things (IoT) are vulnerable to both cyber and physical attacks. Therefore, a cyberphysical 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, 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 model system, which adaptively learns the system behaviours 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 analyses 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.

Keywords: IoT Security, Energy Auditing, Cyber-Physical Security, Deep Learning.

I. INTRODUCTION

The Internet of Things (IoT) confronts intricate security challenges, with both cyber and physical attacks posing significant risks. To effectively combat these threats, IoT systems require adaptable measures capable of addressing both online and physical assaults, yet limitations in storage and connectivity options complicate security solutions. Attacks on IoT systems occur at various layers, including physical assaults on the application layer and cyberattacks on the network layer. A robust monitoring mechanism is crucial for IoT security, with energy auditing emerging as a viable solution due to the abundant energy resources available to IoT devices like smartphones. This novel monitoring approach leverages energy consumption rates as a security metric, detecting anomalies in energy profiles indicative of potential attacks. In cases where IoT devices lack native energy auditing capabilities, inexpensive energy meters can be deployed to ensure ongoing security monitoring. Deep learning-based analysis of IoT energy audits is explored to address both cyber and physicalsecurity concerns, enabling the identification and differentiation of attack tactics used in various assault scenarios.

II. LITERATURE SURVEY

In the context of semi-honest public cloud storage, Attribute-based Encryption (ABE) is introduced to enable fine-grained data owner-side access control [1-3], with CP-ABE being a practical scheme [1], [5] where ciphertexts are encrypted under access policies. Several variants and protocols [6-9] aim to enhance CP-ABE's suitability and security for real-world scenarios. However, this cryptography-driven access control doesn't safeguard against attacks like

Distributed Denial of Service (DDoS), which can inflict significant resource consumption in public clouds [10]. Existing works attempt to mitigate DDoS and related attacks [11-16], but challenges remain regarding resource accounting and accountability in cloud computing [17-20]. Our approach focuses on protocol-level resource verifiability, leveraging authorized users and CP-ABE policies to achieve practical and secure covert security.

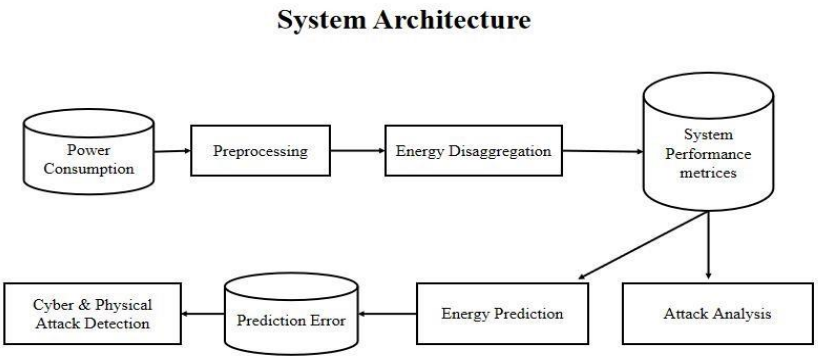
III. EXIXTING SYSTEM

In the existing system 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. Physical attacks are not mainly focused here.

IV. PROPOSED SYSTEM

A dual deep learning model designed for IoT security. It adaptively learns normal system behaviors and can detect both cyber and physical attacks. Unlike previous models, it utilizes a disaggregation-aggregation architecture, allowing it to analyze energy consumption data from system subcomponents to identify attacks. Remarkably, the system relies solely on energy consumption data for attack detection, marking a novel approach in IoT security. Key features include its pioneering use of energy audit data, the introduction of a dual deep learning model system, and its ability to detect and identify attacks based solely on energy audit readings. Preliminary experiments demonstrate promising performance, indicating the system's potential effectiveness in real-world applications.

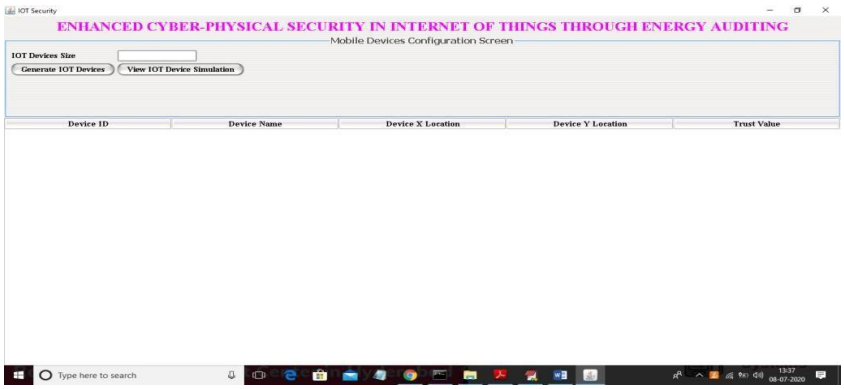
V. SYSTEM ARCHITECTURE



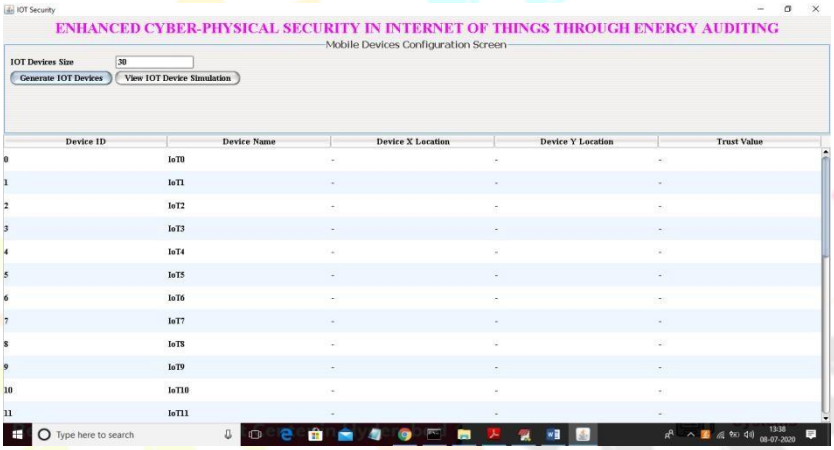
FigWorkflow of the proposed IoT security system. The block in gray indicates the possible attack analytics when the system performance metrics are measured.

VI. RESULTANALYSIS

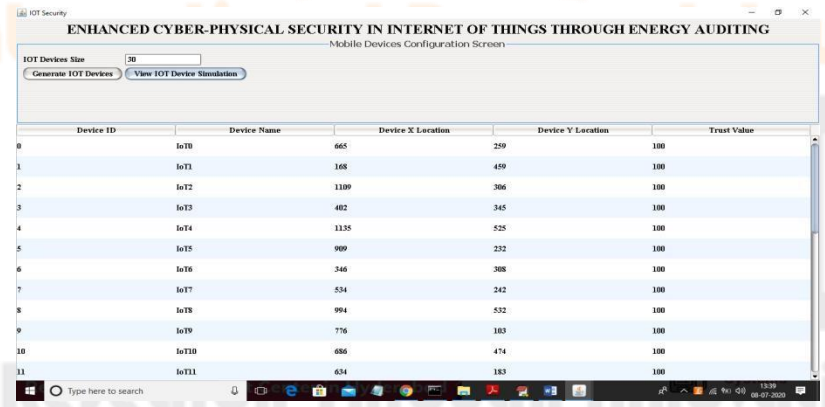
To run this project double click on run.bat file to get below screen



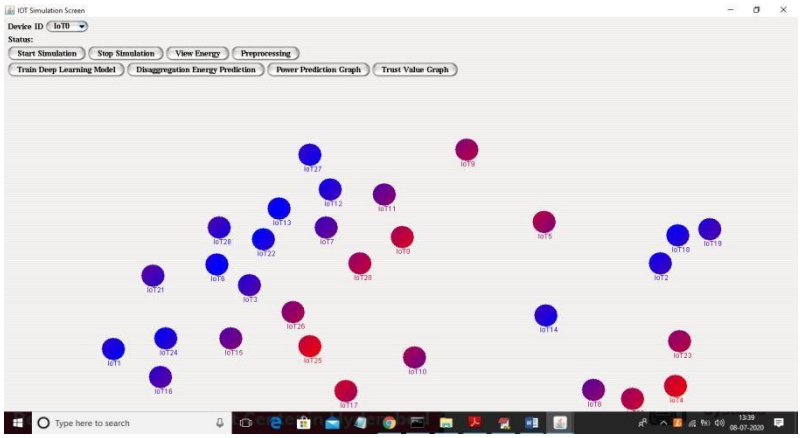
In above screen enter IOT Devices Size and then click on 'Generate IOT Devices' button to get below link



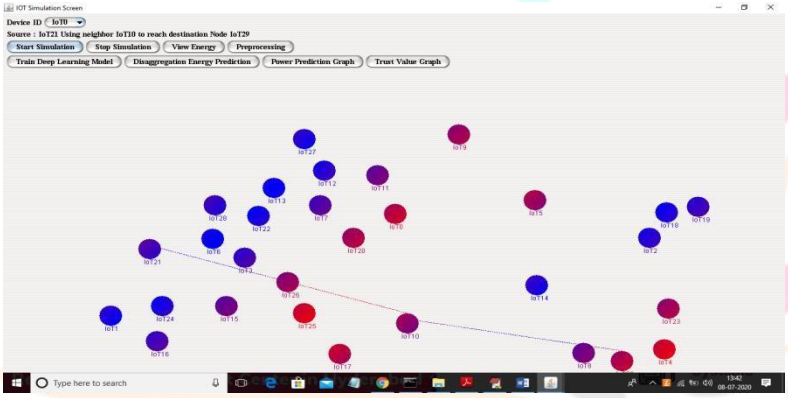
In above screen I entered IOT size as 30 and in above screen we can see each device id and now click on 'View IOT Device Simulation' button to get each IOT X, Y and Trust value



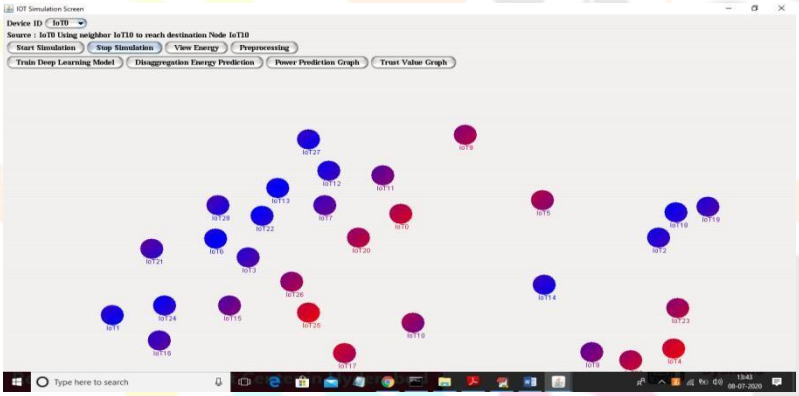
In above screen we can see each device X and Y location and all devices has trust value as 100. Now see below simulation screen



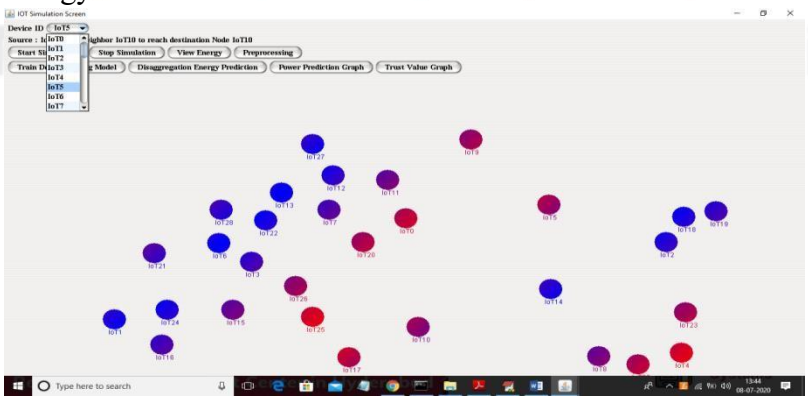
In above screen click on 'Start Simulation' button to allow each device to send data to other IOT devices. While sending data application will monitor its energy value. Let this simulation run for 2 to 3 minutes and application will choose random source and destination to send data to each other using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



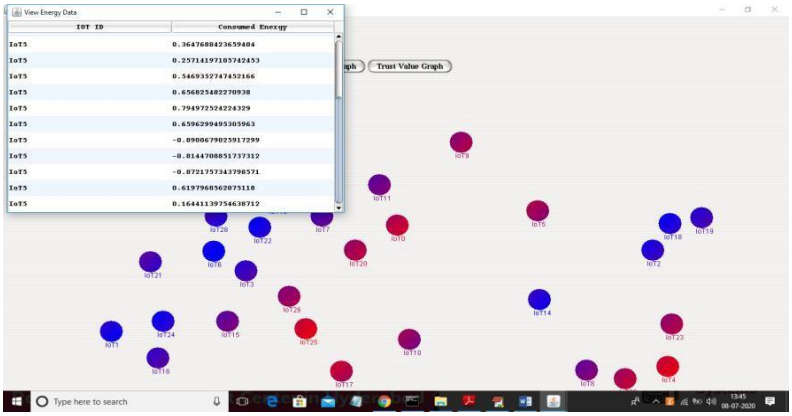
In above screen line from source to destination via neighbour indicates data transmission and after some time click on 'Stop Simulation' button to stop sending data.



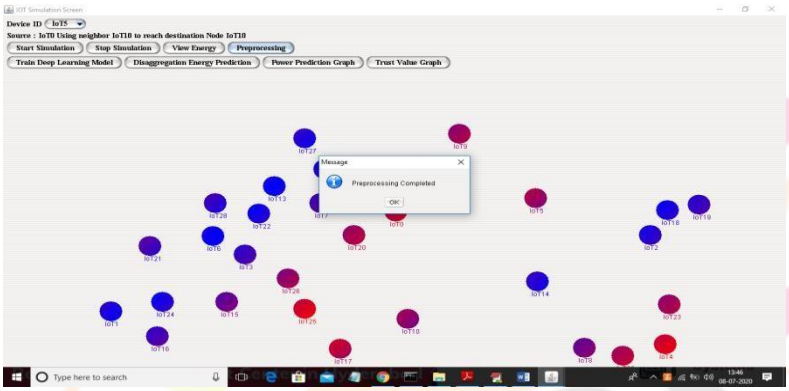
In above screen simulation stop and now select any IOT device from drop down box and click on 'View Energy' button to get its energy consumed information for each transmission



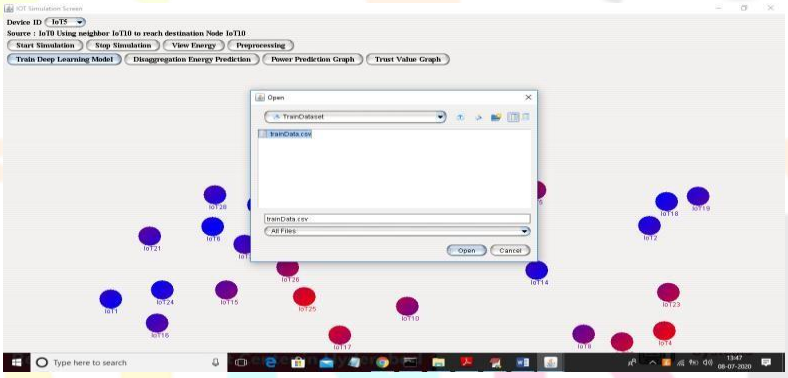
In above screen I am selecting IoT5 and now click on 'View Energy' button to get below screen



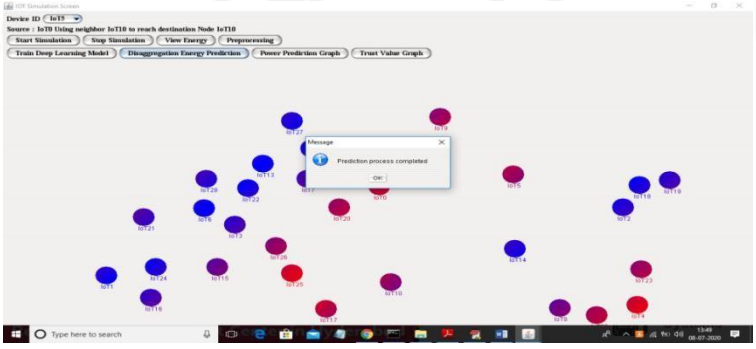
In above screen IOT5 energy consumed values we can see and sometime IOT reports negative energy and to clean such values click on “Preprocessing’ button



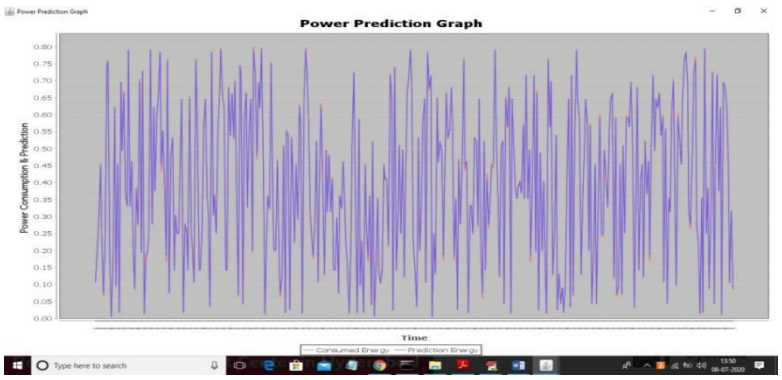
In above screen Preprocessing done and after Preprocessing no such negative values we can see. Now click on ‘Train Deep Learning Model’ button to upload train dataset and to train model



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.

VII. CONCLUSION AND FUTURE SCOPE

"In this paper, we propose a DL-based IoT security system using energy auditing data. The side-channel energy meter readings enable the system to detect both cyber and physical attacks. The dual deep learning models learn normal IoT system performance and track anomalies. This approach enhances IoT system monitoring and security. The use of dual deep learning models in energy auditing for enhanced cyber physical security in the IoT has promising future applications. One potential future direction is the integration of this approach with blockchain technology to further enhance security and ensure data integrity.Additionally, the use of multiple sensors and data sources can increase the accuracy and reliability of the system. The development of more advanced anomaly detection techniques and real-time monitoring can also improve the system's ability to quickly identify and respond to attacks. Finally, the proposed system can be extended to other industries such as manufacturing, transportation, and healthcare to provide enhanced security in various IoT applications.

VIII. REFERENCES

1. Cyber-entity security in the internet of things.AUTHORS: H. Ning, H. Liu, and L. Yang

2.System statistics learning-based iot security: Feasibility and suitability AUTHORS: F. Li, A. Shinde, Y. Shi, J. Ye, X. Li, and W. Z. Song

3. 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.

4.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.

5. 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.

6. PerukaPriyavarshini, R Jegadeesan, Thatla Vaishnavi, KampellySahithi, Boga Shivani, P.Balakishan, 2021 & June, "Cyber Money Laundering Detection Using Machine Learning", Zeichen Journal, Volume 7, Issue 6, 2021, Page No.231-238,ISSN No: 0932-4747. DOI:15.10089.ZJ.2021.V7I6.285311.2422 (UGC Care Group II Journal)

7. R Jegadeesan, Dava Srinivas, N Umapathi, G Karthick, N Venkateswaran "Personal Healthcare Chatbot For Medical Suggestions Using Artificial Intelligence And Machine Learning", European Chemical Bulletin, Eur. Chem. Bull. 2023, 12 (S3), 6004 – 6012, DOI: 10.31838/ecb/2023.12.s3.670. (Scopus)

8. R Jegadeesan, Dava Srinivas, N Umapathi, G Karthick, "Utilizing Ensemble Learners Help Prevent Unauthorized Access Into Iot Networks", European Chemical Bulletin, Eur. Chem. Bull. 2023, 12 (S3), 5994 – 6003, DOI: 10.31838/ecb/2023.12.s3.669. (Scopus)

9. 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.