2024 IEEE 7th International Conference on Advanced Technologies, Signal and Image Processing (ATSIP) | 979-8-3503-5148-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/ATSIP62566.2024.10638911

Enhancing Security and Energy Efficiency in Smart Energy Management Systems through IoT Device Detection and Machine Learning Techniques

Mohammed Ali Algarni[1]
[1]*College of Computer Science, King Khalid University, Abha, 61413, Saudi Arabia*

Naoufel Kraiem[2]
[2]*RIADI Laboratory, ENSI, Manouba University, Campus Universitaire de la Manouba, La Manouba, 2010, Tunisia*

Houneida Sakly[3]
[3]*Center for Research on Microelectronics and Nanotechnology (CRMN), Sousse ,Technopole, Sahloul Sousse, Tunisia*

Abstract— This research endeavors to fortify the security aspects of smart energy management systems (SEMSs) while optimizing energy efficiency by amalgamating Internet of Things (IoT) technologies. By integrating the IoT into the SEMS framework, this study aims to explore and enhance cybersecurity measures by implementing cutting-edge strategies to protect against potential vulnerabilities and threats. This comprehensive approach involves leveraging IoT devices to create a secure and efficient ecosystem within an SEMS, encompassing encryption techniques, authentication protocols, anomaly detection, and other innovative security strategies to ensure the resilience and optimal performance of these interconnected energy management systems.

Keywords— Smart energy management systems (SEMSs), Security, Energy efficiency, Internet of Things (IoT), Cybersecurity, Vulnerabilities, Device detection

1. INTRODUCTION

The smart energy management system is developing remarkably due to ongoing technical advancements.

An intelligent energy management system uses technology to monitor and control energy use in homes, businesses, and buildings. This method aims to lower expenses associated with overconsumption, increase energy efficiency, and protect the environment by lowering carbon emissions.

Improving security becomes essential as smart energy management systems increasingly employ smart devices. A smart energy management system must include wireless sensors and smart devices that can transfer data. Nevertheless, these devices' security flaws might jeopardize the system and have a detrimental effect on energy efficiency [1]. Through the using data packets sent by sensors, this research aims to increase energy efficiency and machine learning may be used to forecast how smart devices will function in the future and implement early corrective measures to increase energy efficiency and lower security threats [1].

By using sensor-transmitted data packets, we expect to increase energy efficiency and create an efficient framework for enhancing security in smart energy management systems. We will discuss the approaches and strategies used to examine and identify security and performance, including machine learning and artificial intelligence methodologies. Case studies and real-world examples that demonstrate how to use packet data in a smart energy management system to increase security and energy efficiency. [2]

To increase the security and effectiveness of smart devices in an intelligent energy management system, our study will offer useful recommendations and assistance to experts in the fields of energy management and IT. Furthermore, by increasing awareness of the importance of incorporating efficiency and safety into the design and operation of smart energy management systems, this research will also help to achieve sustainable development and efficient energy consumption.

Smart energy management systems (EMSs) can help people cope with expenses by using the IoT and big data technologies and promote the more efficient utilization of energy.

To fully examine the cybersecurity efficacy of our suggested methodology, we carried out the following evaluations:

Penetration testing: Since penetration tests require permission from the system owner and in an attempt to ensure that the system's protections are as tight as described, we hired ethical hackers to conduct the penetration test using different hacking methods. The findings showed that we were able to successfully respond to and counter every threatened intruder movement.

Vulnerability Assessment: More specifically, we sought to identify well-documented weaknesses in the software and hardware infrastructure of the system. In the examination, we identified a few problems that were rather small and could be solved immediately.

Attack Simulation: To measure the effectiveness of the system in addressing disasters we simulated real-life instances such as virus attacks and DDos attacks. Commencing from the results acquired through the simulations it was evident how productive the system was with regard to the identification of the violations, the containment of the threats and the recovery time from the assumed attacks without a significant amount of time loss.

Thus, pertaining to cybersecurity assessment, our smart energy management system robustness and reliability were confirmed.

This paper aims to fortify the security and increase the efficiency of smart energy management systems (SEMSs) in IoT devices by detecting devices in the network and evaluating the performance to enhance SEMSs and detect potential risks exploited by hackers. Our objective is to unravel how smart energy management systems can be secured and improved by machine learning algorithms that are used to detect devices the IoT connects to the system and evaluates the functional Internet of Things devices.

The reminder of the paper is structured as follows. Section 2 addresses the relevant current work. The strategy used in this study is presented in Section 3. The machine learning technique for data analysis is implemented in Section 4. Future research issues are presented in the paper's conclusion

2. RELATED WORK

[3] presented the paper "Integrating Smart Energy Management System with internet of Things and Cloud Computing for Efficient Demand Side Management in Smart Grids."

It is a complete smart energy management system that combines cloud computing and the IoT for effective demand-side management in smart grids. It focuses on maximizing the energy utilization of buildings' air conditioning systems and shows notable energy savings of 15% to 49%.

The system uses several time-slot (TS) algorithms, such as the Evening Slow Down (TS8) and Close of Business Automation (TS7) algorithms, to optimize energy usage depending on the building operating dynamics and ambient temperature; the researcher discussed how energy management systems must include sophisticated algorithms, real-time monitoring, and user-friendly interfaces. He emphasized how crucial it is to incorporate smart appliances and wireless sensor networks into the design of the energy management system

To monitor and regulate energy use in [2], A. R. Al-Ali and I. A. Zualkernan, proposed an energy management system (EMS) for smart homes that makes use of the IoT and big data analytics. The data collection module is attached to every home device, creating a wireless network of connected devices. Energy use data are gathered and sent for analysis to a centralized server. The suggested EMS manages energy usage and satisfies customer demand using commercially available business intelligence (BI) and big data analytics technologies . The paper was provided by M. S. Abdul Wahab and N. A. Ramli [4]. The management of energy and lighting controllers jointly plays an important role in achieving the purpose of using as much energy as possible in any building for efficiency. This can be achieved through the adaptation of lighting system sensors; occupancy sensors, daylight sensors, and dimming controls can be used to sense place lights, and they can be adjusted accordingly. The power efficiency case study demonstrates that the system has a large environmental gain. The work presented by Asem Alzoubi [5] involved the application of machine-learning techniques to optimize energy usage in smart homes, with a specific focus on data fusion and energy management.

This study emphasizes the significance of precise energy consumption forecasts and suggests a data fusion strategy that outperforms previously published approaches, achieving a prediction accuracy of 92%. In [7] S. Iram etal presented a decision algorithm model that uses fuzzy operators and machine learning to forecast energy usage in smart homes based on meteorological data

In this approach, machine learning algorithms are trained and tested, LASSO regression is used to analyze weather patterns, and a decision matrix is used to aggregate the methods. The findings include details on how much power equipment is used as well as how much energy is used overall in the smart home.

Conclusions were drawn from this study. In a study he investigated on the importance of smart energy management in allowing energy efficiency for internet of Things (IoT)) tools.[8] Future design issues in energy harvesters for the IoT are highlighted, along with an overview of energy harvesting systems, distribution strategies, storage devices, and controllers for IoT networks.

Here is the comparative analysis :

Comparison with Recent Related Works:

This approach comparable to previous works in that employs the Internet of Things (IoT) and analytics to improve energy usage. Specifically, this proposed model seeks to address security and energy efficiency concerns by identifying IoT devices and utilizing machine learning,

while previous studies have focused mainly on the energy saving aspect.

Advantages of the Proposed Model:
This work employs IOT device identification and machine learning for enhanced security as well as energy consumption optimization in smart energy management systems. A more comprehensive approach is proposed for the management of smart energy systems because it encompasses the elements of weaknesses, threats, and risks. By providing real-life scenarios and respective analyses, this paper aims to prove the practicality and effectiveness of the proposed model.

Limitations of the Proposed Model:
The evaluation and case studies are limited to the particular smart energy management system, and its application, and thus may not be applicable to other cases.

3. Research Methodology

Even though using smart devices makes life more comfortable, managing, monitoring, and guaranteeing the efficiency of their operation—as well as addressing power consumption issues in these devices remains a significant challenge because an imbalance in the data flow sent over the network causes a host of issues, such as the following :
Overpowering: A few smart gadgets could have an issue with overpowering, meaning that they keep using power even when they are not truly using it. It is challenging for users to adjust the power settings of gadgets to meet their demands. This project can be used to help control energy consumption based on device detection on the network. The major goal of this project is to extract features and attributes from pcap files to represent the raw data stream in the vector space model. To predict the detection of IoT devices and perform a performance evaluation by classifying whether they will be detected or not.
There are 13138 records in the collection, with 18 attributes per record (miscellaneous:944, camera:8010, assistant:2178, outlet:1802, and mobile: 186). We will extract 18 features from each of the packages from the five devices. In this research, we used **Bayes classifier models and decision tree classifier model**s . [11]

4. Data Visualization and Analysis

Through the enquiry of network packets of IOT units , we can determine the relationships that are conceived as well as the existence of multiple behaviors that are contained within this current network . This approach allows us to improve both the security and efficiency of networks reducing any uncertainty we may encounter.
The 18 features are the data that are delivered by the IoT devices. Therefore, important details can be deduced about data attributes by extracting and categorizing them. The Ack number, label, IPL length, IPHeaderLength, TTL, Protocol, SourcePort, DestPort, TCPHeaderLength, TCPLength, TCPStream, TCPUrgentPointer, IPFlags, IPID, IPchecksum, TCPflags, and TCPChecksum follow next.

the figures below can shows that

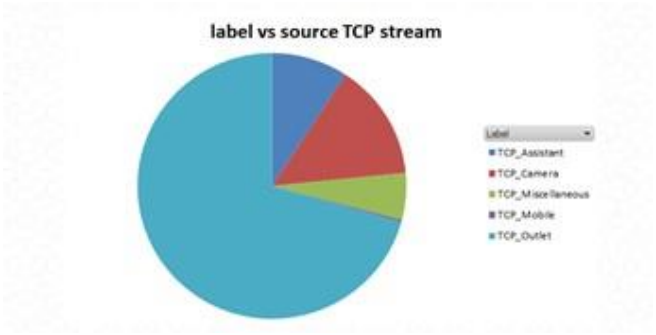


Fig. 1. Distribution of IoT device data

Box plots are helpful tools for displaying the statistical characteristics and distribution of numerical data. employing box plots, for instance: summary of data distribution, which offers a succinct overview of the data distribution and includes metrics such as the median, quartiles, and any outliers. They provide you with a brief summary of the data's skewness, distribution, and central tendency.

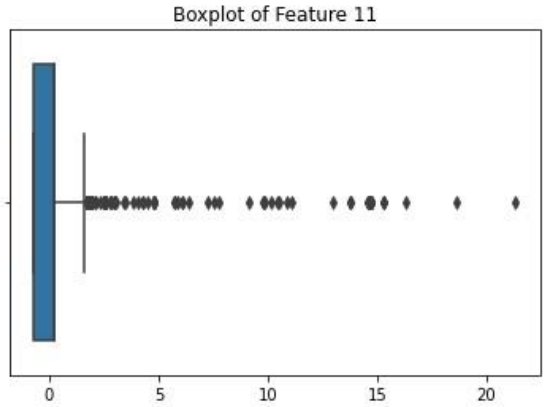


Fig. 2. Box-plot of features

Heatmaps are frequently used to show how values are distributed or correlated in a matrix or table. When working with enormous datasets or attempting to find patterns and links within the data, heatmaps are especially helpful

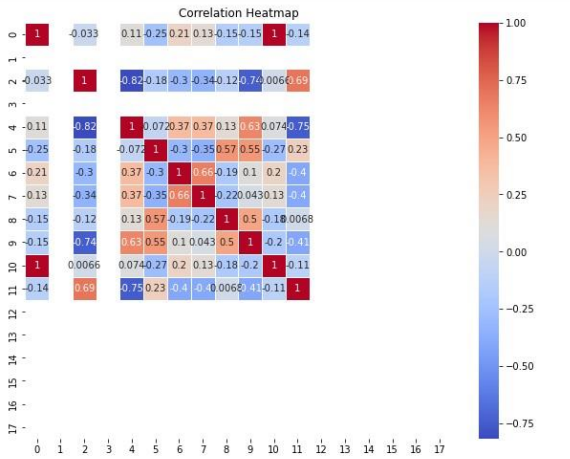


Fig. 3. Heatmap of coronation variables

5. METHODS AND MATERIALS

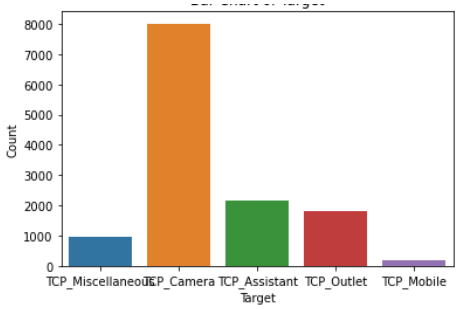
To understand feature extraction and data cleaning , use Python code is used as an essential process to extract , clean , create vector space model
The figure below shows python cod to define labels to store the features for each device to filter

```
ip_filter = {}
ip_filter['TCP_Mobile'] = "'tcp && (ip.src==192.168.1.45)'"
ip_filter['TCP_Outlet'] = "'tcp && (ip.src==192.168.1.222) || (ip.src==192.168.1.67)'"
```

The labels and features are stored in csv files, and 18 features are extracted from each package from the five devices. The figure below shows some of these features:

```
0   Label           13138 non-null  object
1   IPLength        13138 non-null  int64
2   IPHeaderLength  13138 non-null  int64
3   TTL             13138 non-null  int64
4   Protocol        13138 non-null  int64
5   SourcePort      13138 non-null  int64
6   DestPort        13138 non-null  int64
7   SequenceNumber  13138 non-null  int64
```

These features are used to determine the dimensions of the data. With 18 attributes per record (miscellaneous:944, camera:8010, assistant:2178, outlet:1802, and mobile:186), the collection consists of 13138 records. The figure below shows the distribution of the x_ axis of the IoT devices
We used Anaconda platform to construct the training and prediction models



The following is a more concise summary of the Bayes classifier and decision tree classifier models used in the research:

Bayesian Classifier Model:
The Bayes classifier is a form of probabilistic ML algorithm that is used in identifying the IoT devices on the smart energy management system network based on Bayes theory.

Key steps:

1. The filtering of data for extracting attributes such as the type of device, network traffic, and protocols.

2. This involves training the model with prior probabilities of device types and conditional probabilities of feature values.

3. For a newly seen network packet for instance, the posterior probabilities of the various device types which packet could belong can be determined.

Advantages: Efficiency in handling uncertainty, ease of implementation, and computational for real-time detection.

Decision Tree Classifier Model:

Decision trees divide the data into subsets according to the most significant attributes to construct a tree structure for classification.

In this research, it would be generally employed to assess the traffic in a network and to discover trends or irregularities that would suggest security breaches or performance concerns

Key steps:

1. Data cleaning was performed to remove irrelevant attributes before defining the set of variables to be included in the analysis.

2. The decision tree is constructed by recursively partitioning the data based on the maximum information gain.

3. To apply the above steps, the trained model will be is used to classify fresh network traffic as either normal or anomalous.

Advantages: can work with both numerical and categorical data, the rules are understandable, and the model is capable of handling nonlinear relations.

This provides a brief overview of how the two machine learning models may have been developed and why they can be helpful in improving the security and energy efficiency of the smart energy management system.

6. RESULTS :

By applying the model to the machine learning platform the results show that the overall weighted F-measure = 91% using **Bayes classifier models** [10]. The **decision tree classifier model**[11] yielded a 99%
When we compare the confusion matrix between Naieve Bayes and the deception tree, we can see that the diction tree is much more able to predict devices than the Naieve Bayes. The overall weighted average of the F-measure is = 99%

F-Measure	MCC	ROC Area	PRC Area	Class
1.000	1.000	1.000	1.000	TCP_Miscellaneous
1.000	1.000	1.000	1.000	TCP_Camera
0.996	0.995	1.000	1.000	TCP_Assistant
1.000	1.000	1.000	1.000	TCP_Outlet
0.943	0.943	1.000	0.987	TCP_Mobile
0.998	0.998	1.000	1.000	

Only two missed classifications of the confusion matrix

```
=== Confusion Matrix ===

   a    b    c    d    e   <-- classified as
 270    0    0    0    0 |    a = TCP_Miscellaneous
   0 2406    0    0    0 |    b = TCP_Camera
   0    0  671    0    2 |    c = TCP_Assistant
   0    0    0  538    0 |    d = TCP_Outlet
   0    0    4    0   50 |    e = TCP_Mobile
```

determine which features are the most important for determining and detecting types of IoT devices.

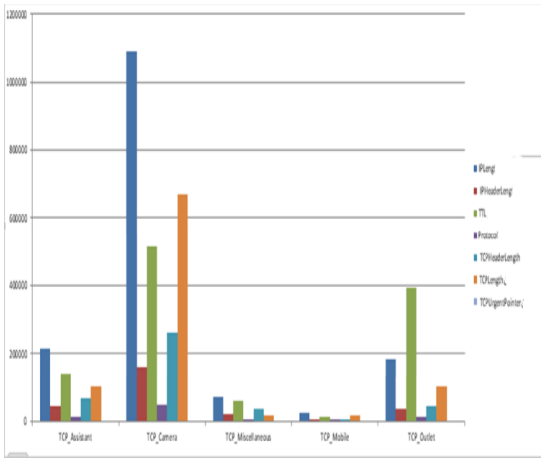


Figure: Rank of IoT features

7. Discussion

This paper presents a strong R framework that has been improved with explainable AI and shows how well it can identify IoT devices. This noteworthy improvement in performance above that of conventional machine learning models such as random forests and naive Bayes highlights is essential for detecting device identification because they extract complicated characteristics from network packets.
The proposed model performs exceptionally well, scoring 99% accuracy on IoT datasets features packets .Transparency and reliability are raised by the model's use of explainable AI, which offers vital insights into the classification choices made by the system. Such openness is essential to IoT security operations, as it greatly improves the ability to respond to cyber threats by knowing the foundation of alarms. This method advances device detection while simultaneously advancing the creation of more complex, adaptive security measures tailored to the evolving landscape of industrial cybersecurity threats . Here some examples

1. IoT Device Detection: This involves the use of intelligent algorithms for recognizing various IoT devices connected to the SEMS network to create a list of such devices and control their activity.

2. Anomaly Detection: The proposed system should regularly monitor the output from the specified IoT devices to identify instances of behavior that point to anomalies such as security threats or inefficient energy usage.

3. Energy Optimization: Taking into consideration some of the features from the identified device profiles and the anomalies that the SEMS is capable of detecting, the system can provide more focused energy optimization, including the detection of rogue/compromised devices that consume far more energy than necessary, as well as the optimization of various energy-related set-ups and schedules connected with devices that have higher energy consumption.

Key Outcomes:
- Improved Cybersecurity: In this case, identification of all connected IoT devices and monitoring for any kind of suspicious activity would enable one to prevent cyberattacks on the SEMS.

IoT device detection is a key feature that fundamental for the SEMS to start acquiring perception, safety, and management of insights on newly connected devices to transform insights into energy efficiency enhancements by using optimization approaches. This approach involves the IoT environment and machine learning to enhance the energy management of structures

8. Conclusion:

The implementation of the classification ML in this project does not directly affect energy optimization, but improving energy efficiency through IoT device detection can be achieved by following these steps:
Power consumption analysis: This analysis of the power consumption of the IoT devices within the system.
Unused Device Detection and Sleep Mode Optimization: Optimize the efficiency of energy utilization in IoT devices by providing them with a power management feature.
Advanced Power Management: Smart power management measures such as optimal utility planning, scheduling, and power control could be employed to improve energy performance in a system that interfaces with IoT devices. Among its features, it enables fixing times when energy is needed, and consumption occurs during those necessary minutes only.
Appropriate Wireless Communication Technologies: Indeed, the power consumption of the IoT device types can be impacted by the wireless technologies that are selected for communication between them, such as those techs with low power consumption and amazing functioning.
Hardware Design Optimization: Improve energy use efficiency by means of better hardware designs for IoT devices. Moreover, being energy conscious in each

component and operational aspect of the device contributes significantly to energy efficiency.

According to the measured active power of the IoT device and detection of unused devices, energy can be saved by taking actions that can lead to more efficient energy use. For example if devices are not in use, then they can be powered off, or their sleep mode can be set up in to reduce electricity waste when the devices are not functional. Locating unused gadgets, tweaking sleep modes, deploying top notches, taking advantage of the power network, utilizing suitable wireless communication technology, and designing crue hardware are the reasons why the efficient energy usage of IoT devices can be supported. This enables the proper production of energy and power sources to improve the ecological system. These devices, by sensing and reporting about energy efficiency issues, are working positively in all dimensions of sustainability. The conservation of energy and the mitigation of negative emissions from the environment are the benefits.

In summary, using IoT device detection on the web has become an essential way for automation to increase energy efficiency. There are various ways of improving the energy consumption of connected devices, such as power consumption monitoring , the optimization or disabling of unneeded devices, better powering modes, energy management techniques, the use of suitable network technologies in wireless communication, and hardware design optimization. This results in a significant reduction in the power consumption of the connected devices; thus, the environment is saved.

REFERENCES

[1] T. Ahmad and D. Zhang, "Using the internet of things in smart energy systems and networks," *Sustain. Cities Soc.*, vol. 68, p. 102783, May 2021, doi: 10.1016/j.scs.2021.102783.

[2] A. R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar, "A smart home energy management system using IoT and big data analytics approach," *IEEE Trans. Consum. Electron.*, vol. 63, no. 4, pp. 426–434, Nov. 2017, doi: 10.1109/TCE.2017.015014.

[3] U. Tariq, I. Ahmed, M. A. Khan, and A. K. Bashir, "Fortifying IoT against crimpling cyber-attacks: a systematic review," *Karbala Int. J. Mod. Sci.*, vol. 9, no. 4, Oct. 2023, doi: 10.33640/2405-609X.3329.

[4] M. Saleem *et al.*, "Integrating Smart Energy Management System with Internet of Things and Cloud Computing for Efficient Demand Side Management in Smart Grids," *Energies*, vol. 16, no. 12, p. 4835, Jun. 2023, doi: 10.3390/en16124835.

[5] M. S. Abdul Wahab and N. A. Ramli, "Lighting Control System for Energy Management System and Energy Efficiency Analysis," *J. Phys. Conf. Ser.*, vol. 1529, no. 5, p. 052022, May 2020, doi: 10.1088/1742-6596/1529/5/052022.

[6] Asem Alzoubi, "MACHINE LEARNING FOR INTELLIGENT ENERGY CONSUMPTION IN SMART HOMES," *Int. J. Comput. Inf. Manuf. IJCIM*, vol. 2, no. 1, May 2022, doi: 10.54489/ijcim.v2i1.75.

[7] S. Iram *et al.*, "An Innovative Machine Learning Technique for the Prediction of Weather Based Smart Home Energy Consumption," *IEEE Access*, vol. 11, pp. 76300–76320, 2023, doi: 10.1109/ACCESS.2023.3287145.

[8] S. Zeadally, F. K. Shaikh, A. Talpur, and Q. Z. Sheng, "Design architectures for energy harvesting in the Internet of Things," *Renew. Sustain. Energy Rev.*, vol. 128, p. 109901, Aug. 2020, doi: 10.1016/j.rser.2020.109901.

[9] Y. Chen, L. Lu, X. Yu, and X. Li, "Adaptive Method for Packet Loss Types in IoT: An Naive Bayes Distinguisher," *Electronics*, vol. 8, no. 2, p. 134, Jan. 2019, doi: 10.3390/electronics8020134.

[10] M. Aljabri *et al.*, "Machine Learning-Based Detection for Unauthorized Access to IoT Devices," *J. Sens. Actuator Netw.*, vol. 12, no. 2, p. 27, Mar. 2023, doi: 10.3390/jsan12020027.

[11] J. Lavanya, M. Ramesh, J. S. Kumar, G. Rajaramesh, and S. Shaik, "Hate Speech Detection Using Decision Tree Algorithm," *J. Adv. Math. Comput. Sci.*, vol. 38, no. 8, pp. 66–75, Jun. 2023, doi: 10.9734/jamcs/2023/v38i81791.