IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205232 |

Signature and Anomaly Based Intrusion Detection in Medical IoT Systems Using Ensemble Learning

Krishna Sajeev, Mahesh Murali

P.G Student, Department of Computer Application, Mount Zion College of Engineering, Kadammanitta, Kerala, India

Head of the Department, Department of Computer Application, Mount Zion College of Engineering, Kadammanitta, Kerala, India

ABSTRACT: The pervasive integration of Internet of Things (IoT) systems in various domains has brought unprecedented convenience and efficiency to everyday life. However, with this ubiquity comes an escalating risk of cyber threats, posing significant challenges to ensuring the security and integrity of IoT infrastructures.Nowhere is this concern more acute than in the realm of Medical IoT, where the stakes are exceptionally high, and the potential consequences of security breaches are dire. In the context of medical IoT, where sensitive patient data and critical healthcare infrastructure are at stake, the imperative to detect and mitigate cyber attacks is paramount. Traditional security measures, while essential, often fall short in adequately safeguarding the complex and heterogeneous landscape of medical IoT devices. The multifaceted nature of healthcare IT environments, coupled with the rapid proliferation of IoT devices, exacerbates the vulnerability of medical IoT systems to a myriad of cyber threats. To address these challenges, machine learning (ML) and deep learning (DL) techniques have emerged as promising approaches for IoT attack detection.However, despite their potential efficacy, traditional ML and DL approaches may still exhibit limitations in terms of accuracy and scalability. This project aims to develop an enhanced and streamlined ML-based intrusion detection system for medical IoT environments, leveraging the power of ensemble learning. The Medical IoT attack dataset will be collected from various resources from the internet and an extensive preprocessing and data analysis will be applied to the data to make it suitable for training algorithms. This data will be used to train conventional Machine Learning models and Ensemble models like Random Forest, XGBoost, and AdaBoost algorithms. The trained models will be tested, evaluated, and compared based on metrics and parameters such as Accuracy, Precision, and Recall. The best model will be deployed at the backend of a web app to test IoT attacks developed in HTML and will be tested in real-time.

KEYWORDS: IDS, IOT Attack, Medical IOT, Ensemble learning

I.INTRODUCTION

The advent of the internet revolutionized the way we communicate, collaborate, and conduct business, ushering in an era of unprecedented connectivity and accessibility. With the proliferation of internet-enabled devices and the advent of the Internet of Things (IoT), this connectivity has extended beyond traditional computing devices to encompass a diverse array of everyday objects, from household appliances to industrial machinery. This interconnected ecosystem holds immense promise for enhancing efficiency, convenience, and productivity across various domains, but it also introduces new challenges and vulnerabilities, particularly in sensitive sectors such as healthcare. As IoT systems permeate every aspect of modern life, the healthcare industry stands at the forefront of this technological transformation, embracing IoT devices to revolutionize patient care, streamline clinical workflows, and improve operational efficiency. The emergenceof Medical IoT (MIoT) has enabled the seamless integration of medical devices, wearables, and sensors into the healthcare infrastructure, empowering healthcare providers with real-time insights, remote monitoring capabilities, and personalized treatment approaches.

II. RELATED WORK

The related work highlights the evolution of intrusion detection systems from traditional methods to advanced machine learning and deep learning techniques. Ensemble learning, in particular, shows great promise in enhancing the accuracy and robustness of IDS in Medical IoT environments. The proposed project aims to build upon these existing works by developing a more scalable and effective ML-based intrusion detection system using ensemble learning, specifically

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205232 |

tailored to the unique challenges of Medical IoT systems.

III. METHODOLOGY

To achieve the objectives of the project, we have to go through all these steps and processes carefully, collect the data, preprocess it well, train and fine-tune the models in order to get the better performance accuray. It starts with the data collection and the dataset research and ends at the final testing of the web app.

DATA COLLECTION AND PREPROCESSING

The dataset will be collected from the research titled "A Framework for Malicious Traffic Detection in IoT Healthcare Environment". This dataset contains normal and malicious IoT traffic and is developed by simulating a use case of an IoT-based ICU with the capacity of 2 beds, where each bed is equipped with nine patient monitoring devices (i.e., sensors) and one control unit called Bedx-Control-Unit using a tool called IoT-Flock.

This data is passed through a long preprocessing steps like below:

- Basic statistical analysis.
- Exploratory Data Analysis including column, data type analysis, etc.
- Preprocessing steps like remove unwanted columns, check for missing values, check data types, check types ofvariables, etc.
- Label encoding of categorical variables.
- Feature Engineering to choose only 10 features and drop the rest.
- Remove highly correlated features.
- Train Test split the data at ratio

K-NEAREST NEIGHBOR CLASSIFIER.

The first model is the simplest machine learning classifier available. K-nearest neighbors (KNN) algorithm is a type of supervised ML algorithm which can be used for both classification as well as regression problems. However, it is mainly used for classification problems in the industry.

Following are some important points regarding KNN-algorithms.

- K-Nearest Neighbor is one of the simplest Machine Learning algorithms based on Supervised Learning technique.
- KNN algorithm assumes the similarity between the new case/data and available cases and puts the new case into thecategory that is most similar to the available categories.
- KNN algorithm stores all the available data and classifies a new data point based on the similarity. This means whennew data appears then it can be easily classified into a well suited category by using K- NN algorithm.
- KNN is a non-parametric algorithm, which means it does not make any assumption on underlying data.
- It is also called a lazy learner algorithm because it does not learn from the training set immediately instead it stores thedataset and at the time of classification, it performs an action on the dataset.
- KNN algorithm at the training phase just stores the dataset and when it gets new data, then it classifies that data intoa category that is much similar to the new data.

DECISION TREE CLASSIFIER.

A decision tree is a non-parametric supervised learning algorithm, which is utilized for both classification and regression tasks. It has a hierarchical tree structure, which consists of a root node, branches, internal nodes and leaf nodes.

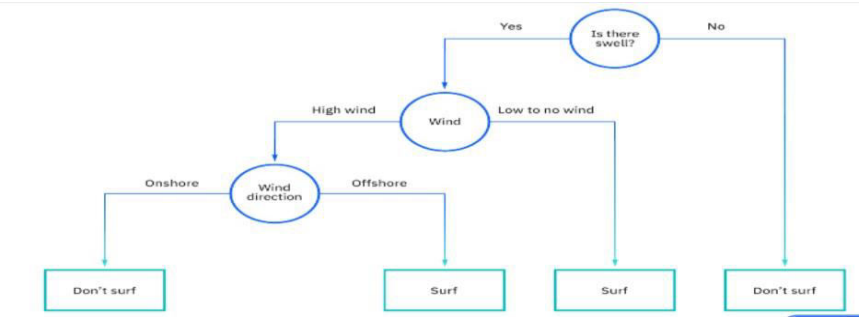


Figure 4.7: Decision Tree

International Journal of Innovative Research in Computer and Communication Engineering

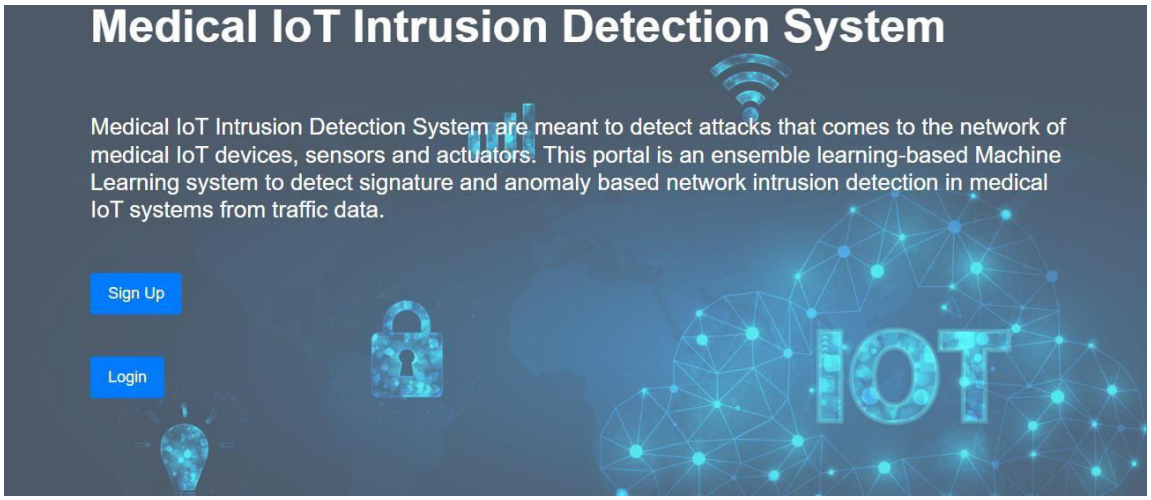
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205232 |

As you can see from the diagram above, a decision tree starts with a root node, which does not have any incoming branches. The outgoing branches from the root node then feed into the internal nodes, also known as decision nodes. Based on the available features, both node types conduct evaluations to form homogenous subsets, which are denoted by leaf nodes, or terminal nodes. The leaf nodes represent all the possible outcomes within the dataset. As an example, let's imagine that you were trying to assess whether or not you should go surf, you may use the following decision rules to make a choice: Types of Decision Trees Types of decision trees are based on the type of target variable we have. begins with the original set S as the root node. On each iteration of the algorithm, it iterates through the very unused attribute of the set S and calculates Entropy(H) and Information gain(IG) of this attribute. It then selects the attribute which has the smallest Entropy or Largest Information gain. The set S is then split by the selected attribute to produce a subset of the data. The algorithm continues to recur on each subset, considering only attributes never selected before.

IV. EXPERIMENTAL RESULTS



Fig(a)

Fig(b)

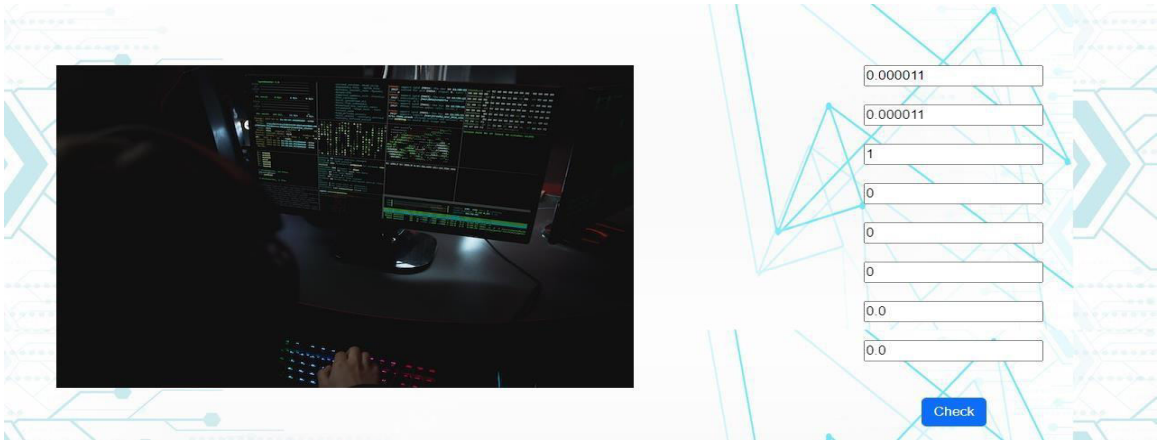
International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205232 |

Fig(c)



Fig(d)

.

FIG(E)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205232 |

V. CONCLUSION

project delved into the exploration and evaluation of machine learning (ML) and Ensemble ML algorithms for the detection of attacks in IoT networks. Through rigorous experimentation, it was observed that Ensemble Models exhibited commendable performance, particularly when coupled with meticulous feature engineering and extraction techniques. Notably, the XGBoost algorithm emerged as a standout performer, showcasing impressive results during real-time testing scenarios.

While the findings underscore the efficacy of Ensemble Models, there remains room for further enhancement. One avenue for improvement lies in the expansion of the dataset to encompass more relevant features, thereby enriching the learning process and enhancing model robustness. Additionally, the adoption of advanced deep learning (DL) algorithms, such as Long Short-Term Memory (LSTM), holds promise for achieving even greater performance gains. The inherent capacity of LSTM networks to capture temporal dependencies and sequential patterns suggests that leveraging such algorithms could yield substantialimprovements in attack detection accuracy and efficacy.

REFERENCES

1. Ekolle, Zie & Ochiai, Hideki & Kohno, Ryuji. (2023). Collabo: A Collaborative Machine Learning Model and its Application to the Security of Heterogeneous Medical Data in an IoT Network. 10.36227/techrxiv.22714864.
2. A. A. Hady, A. Ghubaish, T. Salman, D. Unal and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," in IEEE Access, vol. 8, pp. 106576- 106584, 2020, doi: 10.1109/ACCESS.2020.3000421.
3. Ghourabi, "A Security Model Based on LightGBM and Transformer to Protect Healthcare Systems From Cyberattacks," in IEEE Access, vol. 10, pp. 48890-48903, 2022, doi: 10.1109/ACCESS.2022.3172432.
4. N. T. Bhutia, H. Verma, N. Chauhan and L. K. Awasthi, "DDoS Attacks Detection in 'Internet of Medical Things' Using Machine Learning Techniques," 2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2022, pp. 1-6, doi: 10.1109/IATMSI56455.2022.10119428.
5. A. Sharma, H. Babbar and A. K. Vats, "Detection of Attacks in Smart Healthcare deploying Machine Learning Algorithms*," 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 2023, pp. 1-6, doi: 10.1109/INCET57972.2023.10170367. A. Sharma, H. Babbar and
6. K. Vats, "Detection of Attacks in Smart Healthcare deploying Machine Learning Algorithms*," , Belgaum, India, 2023, pp. 1-6, doi: 10.1109/INCET57972.2023.10170367.
7. Abdulwahid Al Abdulwahid, "Detection of Middlebox-Based Attacks in Healthcare Internet of Things Using Multiple Machine Learning Models", Computational Intelligence and Neuroscience, vol. 2022, Article ID 2037954, 15 pages, 2022. https://doi.org/10.1155/2022/2037954
8. Rabie, O.B.J., Selvarajan, S., Hasanin, T. et al. A novel IoT intrusion detection framework using Decisive Red Fox optimization and descriptive back propagated radial basis function models. Sci Rep 14, 386 (2024). https://doi.org/10.1038/s41598-024-51154-z
9. Hosseinzadeh, M., Yoo, J., Ali, S. et al. A fuzzy logic-based secure hierarchical routing scheme using firefly algorithm in Internet of Things for healthcare. Sci Rep 13, 11058 (2023). https://doi.org/10.1038/s41598-023-38203-9
10. Vijayakumar, K.P.; Pradeep, K.; Balasundaram, A.; Prusty, M.R. Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network. Processes 2023, 11, 1072. https://doi.org/10.3390/pr11041072
11. J. Alanya-Beltran, J. Padilla-Caballero, R. Pant, S. Jagadish, R. K. Ibrahim and M. B. Alazzam,"Identification of Cyber-Attacks in IoT-based Healthcare," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 2692-2696, doi: 10.1109/ICACITE57410.2023.10183349.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details