IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, November 2024

Enhanced Security Framework for Multi-Layered Wireless Communication Systems

Vaishnavi Aradhye[1], Aditi Hinge[2], Pratham Ingle[3], Vedang Khutale[4] and Prof. Waghole[5]
Students, Department of Information Technology[1,2,3,4]
Assistant Professor, Department of Information Technology[5]
Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India
Savitribai Phule Pune University, Pune, India

Abstract: *The goal is to predict a Windows machine's probability of getting infected by various families of malware, based on different properties of that machine. The telemetry data containing these properties and the machine infections was generated by combining heartbeat and threat reports collected by Microsoft's endpoint protection solution, Windows Defender. Each row in this dataset corresponds to a ma- chine, uniquely identified by a Machine Identifier. Has Detections is the ground truth and indicates that Malware was detected on the machine. Using the information and labels in train.csv, you must predict the value for Has Detections for each machine in test.csv. The sampling methodology used to create this dataset was designed to meet certain business constraints, both in regards to user privacy as well as the time period during which the machine was running. Malware detection is inherently a time-series problem, but it is made complicated by the introduction of new machines, machines that come online and offline, machines that receive patches, machines that receive new operating systems, etc. While the dataset provided here has been roughly split by time, the complications and sampling requirements mentioned above may mean you may see imperfect agreement between your cross validation, public, and private scores! Additionally, this dataset is not representative of Microsoft customers machines in the wild it has been sampled to include a much larger proportion of malware machines.*

Keywords: Feature Engineering, Imbalanced Learning, Machine learning, Model Selection

I. INTRODUCTION

For the past few years, network has played a significant role in communication. The computer network allows the computing network devices to exchange information among different systems and individuals. The services of various organizations, companies, colleges, universities are accessed throughout computer network. This leads to a massive growth in networking field. The accessibility of internet has ac- quired a lot of interest among individuals. In this context, security of information has become a great challenge in this modern area. The information or data that we would like to send is supposed to be secured in such a way that a third party should not take control over them. When we are talking about security, we have to keep three basic factors in our mind: Confidentiality, Integrity and availability. Confidentiality means privacy of information. It gives the formal users the right to access the system via internet. This can be performed suitably along with accountability services in order to identify the authorized individuals. The second key factor is integrity. The integrity service means exactness of information. It allows the users to have self- assurance that the information passed is acceptable and has not been changed by an illegal individual. An Intrusion Detection System (IDS) is used to watch malicious
activities over the network. It can sort the unfamiliar records as normal or attack class. First monitoring of the network traffic is done, and then the IDS sorts these network traffic records into either malicious class or regular class. It acts as an alarm system that reports when an illegal activity is detected. The exactness of the IDS depends upon detection rate. If the performance is high for the IDS, then the correctness of detection is also high. Some of the intrusion detection systems are marketed with the ability to stop attacks before they are successful. They are used to shield an association from attack. It is a relative concept that tries to identify a hacker when intrusion is attempted. Ideally, such a system will only alarm when a successful attack is made.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, November 2024

II. LITERATURE SURVEY

Network threats and hazards are evolving at a high-speed rate in recent years. Many mechanisms (such as firewalls, anti- virus, anti-malware, and spam filters) are being used as security tools to protect networks. An intrusion detection system (IDS) is also an effective and powerful network security system to detect unauthorized and abnormal network traffic flow. This article presents a review of the research trends in network-based intrusion detection systems (NIDS), their approaches, and the most common datasets used to evaluate IDS Models. The analysis presented in this paper is based on the number of citations acquired by an article published, the total count of articles published related to intrusion detection in a year, and most cited research articles related to the intrusion detection system in journals and conferences separately. Based on the published articles in the intrusion detection field for the last 15 years, this article also discusses the state-of-the-arts of NIDS, commonly used NIDS, citation-based analysis of benchmark datasets, and NIDS techniques used for intrusion detection.

III. SOFTWARE AND HARDWARE REQUIREMENT

- Operating System: Windows 7 or later
- Programming Language: Python
- Integrated Development Environment (IDE): Anaconda
- Processor: Intel Core i3 or higher
- Hard Disk: 20 GB or more
- RAM: 8 GB or more

IV. METHODS

The Intrusion Detection System (IDS) proposed by this research is a LightGBM, an efficient gradient boosting framework, aimed at effectively not only recognizing intrusions and other anomalies in a network. The methodology consists of the following phases:

1. Data Gathering as well as Data Cleaning

The IDS system starts with the collection of the network traffic data which consist of normal and some samples of malicious activities. Basically the dataset that can be used in this study is collected from open sources such as the CICIDS or KDD datasets. The data undergoes preprocessing steps such as:

- Data Cleaning: Cleansing of data in which irrelevant, irrelevant or inconsistent records are deleted.
- Feature Selection: Recognition of the most important fields (packet size, protocol type, source IP address, destination port etc.).
- Normalization: Standardizing features so they are on the same scale as each other so that the performance of LightGBM can be enhanced.

2. Feature Engineering

It was noted that feature extraction for effective detection is accretive. In this phase:
Some features include connection duration, packet rate, and anomalies involving ports are generated from the domain specific features.
So correlation analysis is carried for finding out the features which are most discriminant for normal and malicious activities.
But sometimes, there is redundancy in the features, in such cases methods like PCA (Principal Component Analysis) are used.

3. Model Design

This paper focuses on proposing a model and implementing it.
The basic of the system relies on LightGBM that performs effective training through fast learning methods bolstered by gradient boosting through the employment of tree based learning models. Key implementation details include:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, November 2024

Model Architecture:
For the decision tree, LightGBM employs a histogram based approach that is computationally much lighter.
Another mechanism referred to as the boosting technique progressively adjustments for the residual contributions of previous iterations.

Hyperparameter Optimization:
The setting of hyperparameters such as learning rate, number of leaves and the max depth involves using the two following techniques: Grid Search and Random Search.
Best parameters are selected using cross validation method on the training data only.

4. Training and Testing
Training Phase:
The preprocessed dataset is split into training and validation sets using an 80:20 ratio.
LightGBM model is fine-tuned over the labeled data to identify different features of normal and malicious traffic.

Testing Phase:
The model under consideration is tested on independent test data set considered after training had been done.
Evaluation of the system is done by the use of certain points like accuracy, precision, recall, F1 score and AUC-ROC.
Through feature importance scores, the importance of selected features is analysed in order to confirm their relevance.

5. Real-Time Detection Framework
The IDS is designed for real-time deployment with the following components:

Data Capture:
A packet capture tool such as Wireshark or Tcpdump is included to capture and monitor the of traffic in the network continuously.

Anomaly Detection:
The trained LightGBM model takes real time traffic records as input.
Non-routine patterns cause alerts to be raised.

Response Mechanism:
Any intrusion attempts are immediately recorded and responses that may be as simple as banishing the offending IP address or as complex as notifying the relevant administrators are implemented.

6. In this section, the new method presented in this paper is compared to some existing approaches.
The proposed system is of course put up for comparison with other machine learning models like Random Forest, Support Vector Machines (SVM) and other traditional gradient boosting models. The comparison highlights:
The comparative analysis of LightGBM resulted in the faster detection of customers and higher accuracy of their identification.
Its specifically less memory and computation comprehensive which makes it ideal for large scale deployment.

V. DISCUSSION

The "Enhanced Security Framework for Multi-Layered Wireless Communication Systems" research focuses on an exhaustive examination of system functionalities and user interaction by a structured methodology. In extensive analysis, the study defines the significant constituents and their respective roles in the system, with special attention to the two principal factors: **Users** and **System Administrators**.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, November 2024

User Roles and Interactions:

The users are responsible for accessing the system, managing their profiles, and using security features to protect their data.

System Administrators oversee system maintenance, user management, and monitor security protocols to ensure system integrity.

Its primary functionalities are **User Authentication**, **Data Encryption**, and **Intrusion Detection**, which individually will affect the protection of sensitive information. Another important aspect is that they are interrelated; for instance, the ability to give robust user authentication prevents unauthorized access; effective encryption of data ensures that it can be neither read nor written into when intercepted.

The study outlines the importance of an **Intrusion Detection System (IDS)** as a proactive approach against potential threats. Given the constant monitoring of network traffic and the exploitation of very complex algorithms, the IDS is able to identify anomaly patterns that indicate malicious activities. This multi-faceted approach improves security considerably, not only by being able to respond swiftly but also minimizing damage caused by threats.

In addition, the analysis presents possible improvement scopes within the framework. For instance, when compared to the conventional design, machine learning can significantly enhance the adaptability of the Intrusion Detection System. Other than that, the invocation of mechanisms for user feedback can provide understanding and user experience, and contribute to iterative improvements in the system design.

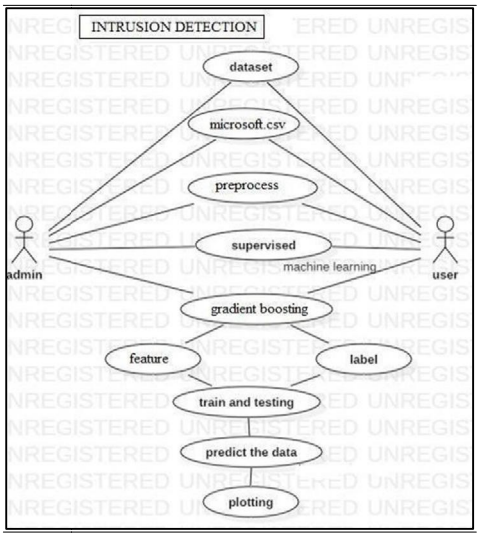
VI. CONCLUSION AND FUTURE SCOPE

This Enhanced Security Framework, therefore, is an almost full answer to issues associated with the security of multi-layered wireless communication systems. These three prime mechanisms of user authentication, data encryption, and intrusion detection combined in powerful ways increase the protection of data considerably, while all cyber-related risks have been significantly alleviated.

Looking forward, several enhancements are envisioned to further bolster the system's capabilities:

Real-Time Threat Detection: With advanced algorithms for real-time monitoring capable of responding immediately to a detected threat, overall security will be enhanced.

Mobile application development entails the creation of a mobile application, which would enable users to manage their accounts and monitor security alerts conveniently from their smartphones.



Advanced techniques for encryption will provide a secure safeguard for sensitive data against emerging cyber threats, and:. Analytics integration would allow comprehensive analytics tools, set to enable administrators with information about network performance, user behavior, and data-driven decisions.

AI Integration: Exploring artificial intelligence applications could lead to personalized security measures that adapt to individual user behaviors and preferences.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, November 2024

This framework will continually evolve to maintain its leadership in respect of cybersecurity solutions for wireless communication systems with regard to emerging threats and technological advancements. The proposed improvement contributions will not only contribute to improving security measures but will also make a major contribution toward advancements in assessment practices in educational contexts and elsewhere.

REFERENCES

[1] SATISH KUMAR, SUNANDA GUPTA, "Research Trends in Network-Based Intrusion Detection Systems: A Review", Received October 26, 2021, accepted November 8, 2021, date of publication November 22, 2021, date of current version December 3, 2021. Digital Object Identifier 10.1109/ACCESS.2021.3129775

[2] Lirim Ashiku1 Cihan Dagli, "Network Intrusion Detection System using Deep Learning", 1877-0509 © 2021 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by- nc-nd/4.0) Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference, June 2021. 10.1016/j.procs.2021.05.025

[3] Anish Halimaa A, Dr. K. Sundarakantham, "MACHINE LEARNING BASED IN- TRUSION DETECTION SYSTEM", Proceedings of the Third International Con-ference on Trends in Electronics and Informatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8

[4] Patrick Vanin 1, Thomas Newe, "A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning", Intrusion Detection Sys- tems Using Artificial Intelligence/Machine Learning. Appl. Sci. 2022, 12, 11752. https://doi.org/10.3390/ app122211752

[5] Mrutyunjaya Panda, Ajith Abraham, Swagatam Das, Manas Ranjan Patra, "Net- work Intrusion Detection System: A Machine Learning Approach", Article in Intelligent Decision Technologies · November 2011 DOI: 10.3233/IDT-2011-0117 Source: DBLP

[6] Manvith Pallepati1, Soujenya Voggu2, Rithesh Masula3, Manisai Konjarla," Network Intrusion Detection System Using Machine Learning with Data Preprocess- ing and Feature Extraction", International Journal for Research in Applied Science Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VI June 2022- Available at www.ijraset.com

[7] Emad E. Abdallah*, Wafa' Eleisah, Ahmed Fawzi Otoom, "Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey', 1877-0509 © 2022 The Authors. Published by Elsevier B.V. This is an open access article un- der the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/) Peer-review under responsibility of the Conference Program Chairs. 10.1016/j.procs.2022.03.029