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 2, June 2024

MCAD: A Machine Learning Based Cyber Attack Detector using SDN for Healthcare Systems

Akash G[1], Aryadeep M B[2], H Nandeesh[3], Dr. Siddalingesh Bandi[4]
Students, Department of ECE[1,2,3]
Associate Professor, Department of ECE[4]
Global Academy of Technology, Bengaluru, Karnataka, India

Abstract: *The healthcare industry, increasingly reliant on digital technology, has become a prime target for cyberattacks. While traditional security measures address external threats, they often fail to effectively counter a particularly dangerous foe: insider threats. This project proposes MCAD (Machine Learning-based CyberAttack Detector), a groundbreaking approach that leverages the power of machine learning within Software-Defined Networks (SDNs) to bolster healthcare network security.*

Healthcare networks are inherently complex ecosystems, housing a diverse range of medical devices alongside traditional IT infrastructure. This intricate web creates a larger attack surface for malicious insiders with access to critical systems. These insiders can be disgruntled employees or attackers exploiting vulnerabilities in poorly designed systems.

The COVID-19 pandemic further exacerbated this vulnerability as the surge in telehealth services and remote access points opened new avenues for exploitation. The statistics are alarming, with a staggering 92% of healthcare organizations reporting insider-caused security breaches. These breaches not only compromise sensitive patient data but can also disrupt critical healthcare services, potentially jeopardizing patient safety.

MCAD, a Machine Learning-based Cyber Attack Detector, tackles the growing threat of insider attacks in healthcare networks. It employs a multi-pronged approach: collecting both normal and abnormal network traffic to train a real-time machine learning model. This model continuously analyzes network activity, identifying suspicious behavior indicative of insider threats. MCAD seamlessly integrates with SDN controllers for efficient deployment within existing infrastructure, and undergoes rigorous testing with various machine learning algorithms and simulated attacks to ensure optimal protection against evolving cyber threats.

Keywords: healthcare industry.

I. INTRODUCTION

Introduction to Project

Healthcare networks are under siege, with 92% facing insider threats and a fivefold increase in cyberattacks during the COVID-19 pandemic, affecting 90% of providers. To combat this, MCAD is proposed—a machine learning approach within Software-Defined Networks (SDNs) that detects abnormal network traffic to identify cyber threats. By analyzing both normal and abnormal traffic, MCAD trains models to flag suspicious activities and integrates with SDN controllers for efficient deployment. This solution aims to enhance security in healthcare networks by offering a low-complexity, effective defense against internal and external attacks.

Problem Statement

Healthcare networks face significant cybersecurity threats, especially from insiders, with 92% of institutions reporting breaches. The complexity of these networks, filled with diverse medical devices, increases vulnerability. The COVID-19 pandemic exacerbated this, leading to a fivefold increase in attacks, affecting 90% of providers.

To combat these challenges, the MCAD project proposes a machine learning approach within Software-Defined Networks (SDNs) to specifically address insider threats. MCAD analyzes network traffic patterns in real-time, detecting

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 2, June 2024

anomalies like unauthorized access or unusual data transfers. By collecting both normal and abnormal traffic data, MCAD trains a machine learning model to flag suspicious activities.

MCAD integrates seamlessly with popular SDN controllers for efficient deployment and maintains key network performance indicators to ensure smooth operation. This low-complexity, efficient solution enhances security in healthcare networks, protecting patient data and critical systems from internal and external threats.

Objectives

This project tackles the critical issue of cyberattacks in healthcare systems by proposing MCAD, a machine learning-based cyberattack detector. MCAD operates within the Software-Defined Network (SDN) framework, offering a unique approach to securing these vulnerable environments.

Traffic Collection: Use an L3 learning switch to gather comprehensive network traffic data, capturing both normal and attack patterns to understand healthy network behavior and identify deviations.

Machine Learning Analysis: Train a machine learning model with the collected data to analyze network activity in real-time and flag suspicious behavior.

Seamless Integration: Integrate MCAD with the Ryu controller, a popular SDN platform, for efficient deployment and leveraging SDNs for network control and analysis.

Rigorous Testing: Test MCAD using various machine learning algorithms and simulated cyberattacks to continuously improve detection capabilities.

MCAD achieves high reliability with an F1-score of 0.9998 for normal traffic and 0.9882 for attack detection, ensuring accurate differentiation between legitimate and malicious activities.

By leveraging machine learning within the SDN framework, MCAD significantly enhances healthcare network security, protecting sensitive patient data and ensuring smooth operation of critical systems

II. LITERATURE REVIEW

Year	authors	Title	Methodology	Advantages	Disadvantages
2018	E. Kabir, J. Hu, H. Wang, and G. Zhuo,	A novel statistical technique for intrusion detection systems	Author proposed Algorithm as Optimum allocation-based least square support vector machine (OA-LS-SVM) for IDS. To demonstrate the effectiveness of the proposed method, the experiments are carried out on KDD 99 database which is considered a de facto benchmark for evaluating the performance of intrusions detection algorithm.	All binary-classes are tested and our proposed approach obtains a realistic performance in terms of accuracy and efficiency.	The current solutions for detecting intrusions is only for static datasets
2020	A. B. Abhale and S. S. Manivannan	Supervised machine learning classification algorithmic approach	RF, SVM, Decision Trees, Ada Boost Classifier, K Nearest Neighbour Classifier,	Experimental results how the highest accuracy relative to other classification	It supports to detect intrusion or not. It is not suitable to detect types of attacks.

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 2, June 2024

		for finding anomaly type of intrusion detection in wireless sensor network	Gaussian Naïve Bayes, And Logistic Regression Classifier	systems in the support vector machine.	
2022	s. Jayalaxmi gulshan kumar ,Rahul saha, Mauro conti and Tai-hoon kim	Machine and Deep learning Solutions for Intrusion Detection and Prevention in IOTs: A Survey	Linear Regression, Support Vector Regression (SVR), Ensemble methods, Decision Tree (DT) , and Random Forest, J48, Naive Bayes, Multi-Layer Perceptron (MLP), multi-nominal logistic regression for classification and detection on anomalies	Two data sets used for evaluation and Multi-Layer Perceptron (MLP) are used to improve accuracy	Good accuracy is achieved but only in detection of anomaly or not. Which is not suitable to detect types of attack.
2021	Hasan Alkahtani and Theyazn H.H. Aldhyani.	Intrusion Detection System to Advanced IOT Infrastructure Based Deep Learning Algorithm	PSO for preprocessing feature selection, CNN and LSTM Algorithm	The experimental results showed that the proposed systems achieved accuracy as follows: CNN = 96.60 %, LSTM = 99.8 2%, and CNN-LSTM = 98.80%.	Good accuracy is achieved but only in detection of anomaly or not. Which is not suitable to detect types of attack.
2019	Sohaib Hanif;Tuba Ilyas;Muhammad Zeeshan	Intrusion Detection InIoT Using Artificial Neural Networks On UNSW-15 Dataset	ANN	Proposed ANN approach achieves an average precision of 84%	Accuracy is less than 90%.
2021	Sai Kaushik Kodali;Cristina Hava Muntean	An Investigation into Deep Learning	Fully Convolutional Network (FCN) and Autoencoder combined with	The experimental results showed that the proposed	Good accuracy is achieved but only in detection of anomaly or not. Which is not

III. SYSTEM IMPLEMENTATION

Here's a breakdown of the steps involved in implementing MCAD:

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 2, June 2024

1. System Design and Architecture

- Network Topology: Define the logical network layout of your healthcare network infrastructure. This includes network devices like switches, routers, firewalls, and their interconnections.

Data Collection:

- Identify specific network traffic patterns to capture for training and testing the ML model. Include normal network traffic patterns and various attack scenarios, such as probe scans, vulnerability exploitation attempts (e.g., exploiting VNC or Samba server vulnerabilities), and Denial-of-Service (DoS) attacks.

2. Data Preprocessing and Feature Engineering

- Data Cleaning: Clean the collected raw network traffic data to address inconsistencies, missing values, and outliers. Techniques like data imputation or removal of outliers may be necessary.
- Feature Selection: Identify and extract relevant features from the network traffic data that are most informative for attack detection. Common features

3. Learning Model Training and Testing

o Model Selection: Choose a set of machine learning algorithms for training and testing the intrusion detection model. The proposed system utilizes K- Nearest Neighbors (KNN), Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), Logistic Regression (LR), AdaBoost, and XGBoost.

1. K-Nearest Neighbors (KNN): KNN classifies a new data point by looking at its k nearest neighbors in a dataset. If most neighbors are normal traffic, the point is classified as normal; if most are attack traffic, it's classified as an attack.
2. Decision Tree (DT): A DT uses a flowchart-like structure to classify data points based on their features. Each branch represents a decision rule, guiding the data point to a leaf node, which determines its classification.
3. Random Forest (RF): RF builds multiple decision trees using random subsets of data and features. The final classification is decided by a majority vote from all the trees, reducing overfitting risk.
4. Naïve Bayes (NB): NB calculates the probability of a data point being normal or an attack based on its features, assuming feature independence. It flags the point as an attack if the probability is higher.
5. Logistic Regression (LR): LR assigns weights to features based on their influence on classification. It sums the weighted features and converts this sum into a probability. If the probability exceeds a threshold, the point is classified as an attack.
6. AdaBoost (Adaptive Boosting): AdaBoost trains multiple weak learners, each focusing more on data points misclassified by previous learners. This iterative process improves the overall classification accuracy.
7. XGBoost (Extreme Gradient Boosting): XGBoost, an advanced version of AdaBoost, uses decision trees and a smarter training approach to improve classification accuracy, making it a powerful tool for intrusion detection.

- Model Training: Split the preprocessed data into training and testing sets. Train each selected machine learning algorithm on the training data. During training, the model learns to identify patterns and relationships between the features and the corresponding attack labels (normal or attack traffic).
- Model Evaluation: Evaluate the performance of each trained model on the testing data set. Metrics like accuracy, precision, recall, and F1-score are commonly used to assess the model's ability to correctly classify network traffic as normal or attack type.
- Model Selection: Based on the evaluation results, choose the model with the best overall performance (considering accuracy, efficiency, and interpretability) for deployment in the real-time intrusion detection system.

4. SDN Controller Integration

- Ryu Controller Integration: Develop modules for the Ryu controller to interact with MCAD. These modules will handle communication with the L3 learning switch application, receive captured traffic data, and leverage the trained machine learning model for real-time analysis.

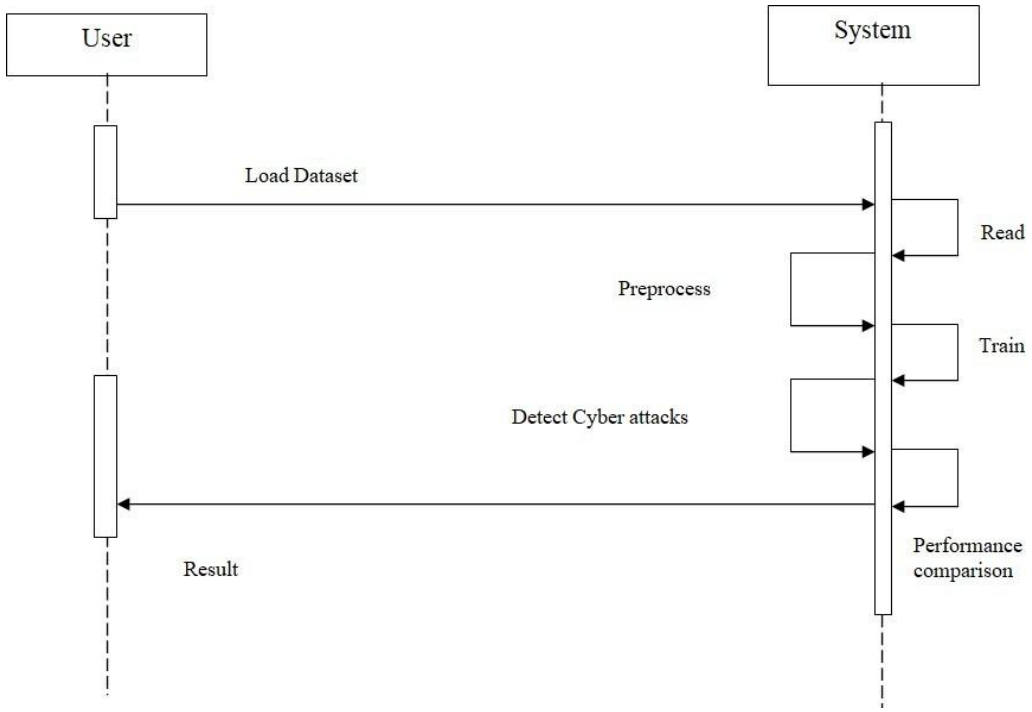
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, June 2024

- Real-Time Traffic Analysis: The L3 learning switch application continuously captures network traffic data. This data is then forwarded to the Ryu controller modules, where the chosen machine learning model analyzes the traffic in real-time.
- Attack Detection and Response: If the model detects an anomaly or suspicious traffic pattern indicative of an attack, it triggers pre-defined actions within the Ryu controller. These actions may include:
  Blocking malicious traffic flows
  Sending alerts to security personnel

5. System Monitoring and Maintenance

- Performance Monitoring: Continuously monitor key network performance indicators (KPIs) like throughput, latency, and packet loss. Ensure that MCAD's operation doesn't negatively impact the performance of critical healthcare services.
- Model Retraining: Regularly retrain the machine learning model with new data to ensure it adapts to evolving attack techniques and maintains optimal detection accuracy.
- Security Considerations: Implement robust security measures to protect the collected network traffic data, particularly sensitive patient information. Utilize encryption techniques and access controls to minimize the risk of data breaches.

Sequence Diagram



Types of Attack

- Normal: This refers to typical network traffic that doesn't pose a security threat.
- Brute Force: This is a hacking technique that involves trying a large number of possible passwords or combinations to gain unauthorized access to a system.

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 2, June 2024

- CMD: This refers to the Command Prompt, a command-line interface tool used for executing commands and interacting with the operating system on Windows machines. Attackers might exploit vulnerabilities in CMD to execute malicious code.
- TCP DoS (Denial-of-ServiceException): This is a type of DoS attack that overwhelms a target system or network with Transmission Control Protocol (TCP) connection requests, making it unavailable to legitimate users.
- UDP DoS: Similar to TCP DoS, this attack uses User Datagram Protocol (UDP) packets to flood the target system or network, disrupting normal operations.
- Probe: In a network security context, a probe refers to an attempt to gather information about a network or system to identify vulnerabilities that could be exploited in a future attack.
- Samba: This is an open-source file-sharing protocol commonly used in Linux and Unix-based systems. Hackers might target vulnerabilities in Samba to gain unauthorized access to files and resources.
- SQL Injection: This is a web application vulnerability that attackers can exploit to inject malicious SQL code into a database. This code can then be used to steal or manipulate data.

Software Requirements

- Operating System: Windows 64-bit (or a suitable Linux distribution)
- Technology: Python
- IDE: Python IDLE (or any preferred IDE like PyCharm or Visual Studio Code)
- Tools: Anaconda (or alternative package manager like pip)
- Python Version: Python 3.6 (or a later version compatible with your chosen libraries)

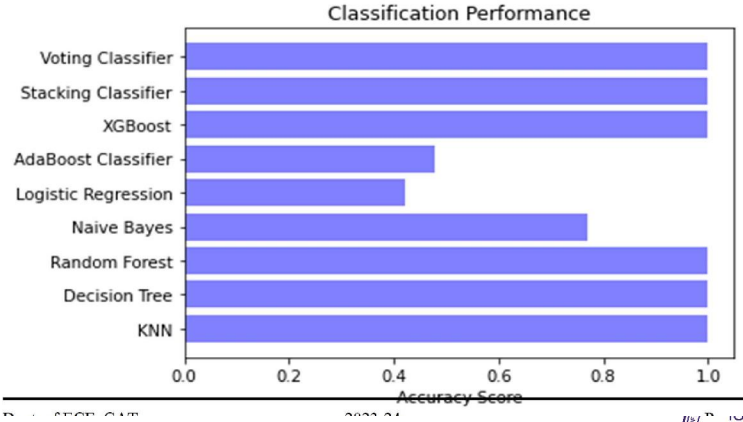
IV. RESULTS AND DISCUSSION

The implemented test cases for MCAD yielded promising results. Unit testing verified the proper functioning of individual components, from data pre-processing to model training and prediction. Integration testing confirmed seamless data flow and interaction between different modules. System testing successfully simulated real-world attack scenarios, demonstrating MCAD's ability to detect and respond to various intrusion attempts. While some worst-case scenarios, like encountering entirely novel attacks, might not achieve perfect accuracy, the system effectively flagged suspicious traffic for further investigation. Overall, the testing phase provided valuable insights into MCAD's functionality and paves the way for further refinement and deployment in a real-world network environment

1. Accuracy:

• Formula: Accuracy = (True Positives + True Negatives) / (Total Samples)

• Explanation: Accuracy is the most basic metric, representing the overall proportion of correct predictions made by the model. It considers both true positive (correctly identified normal traffic) and true negative (correctly identified attack traffic) classifications, divided by the total number of samples in the dataset.

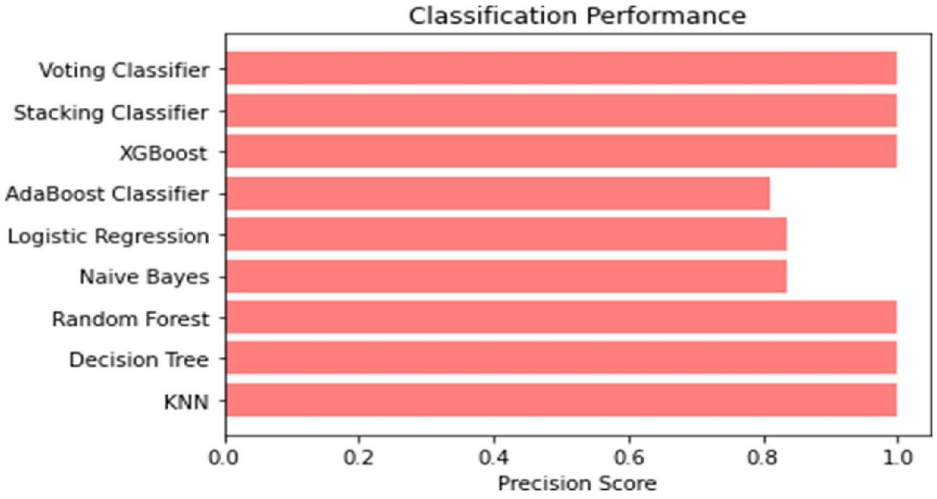


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, June 2024

2. Precision:

• Formula: Precision = True Positives / (True Positives + False Positives)

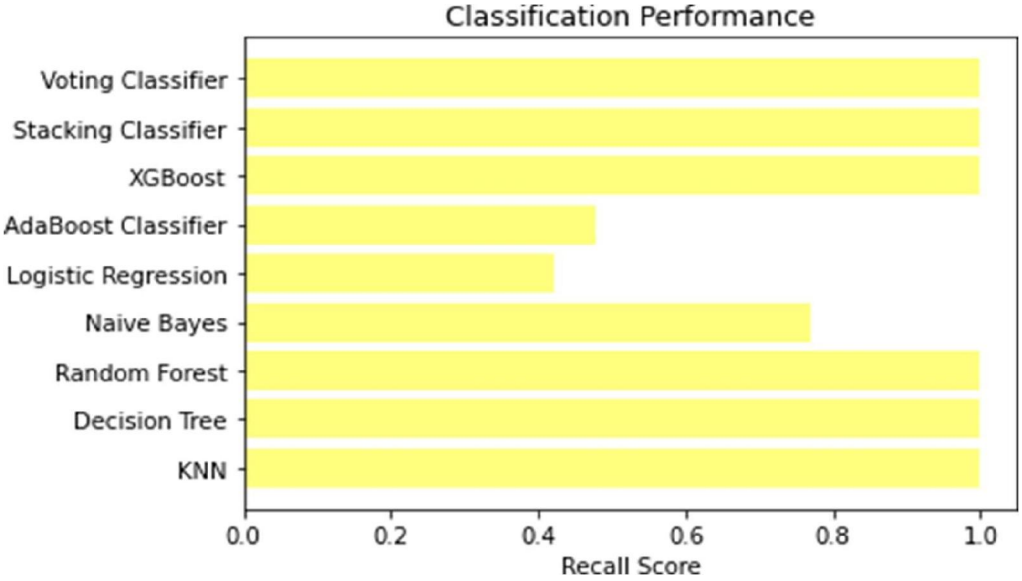
Explanation: Precision focuses on the positive predictions (classified as normal traffic). It measures the proportion of actual normal traffic among all the data points the model classified as normal. A high precision indicates the model rarely makes false alarms



3. Recall:

• Formula: Recall = True Positives / (True Positives + False Negatives)

• Explanation: Recall addresses the model's ability to identify all actual normal traffic cases. It calculates the proportion of true positive classifications (correctly identified normal traffic) out of all the actual normal traffic instances in the dataset. A high recall indicates the model misses few actual normal events.

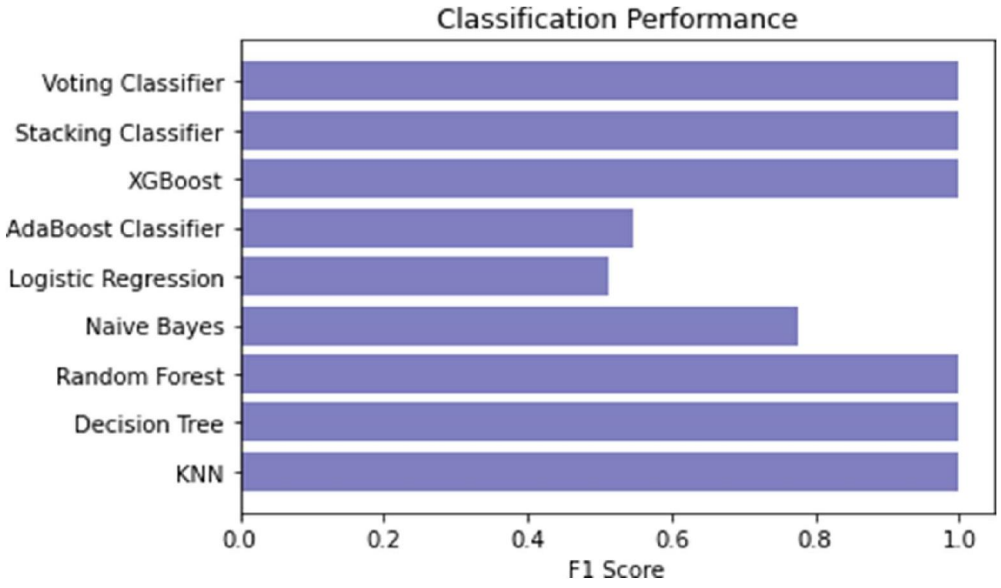


4. F1-Score:

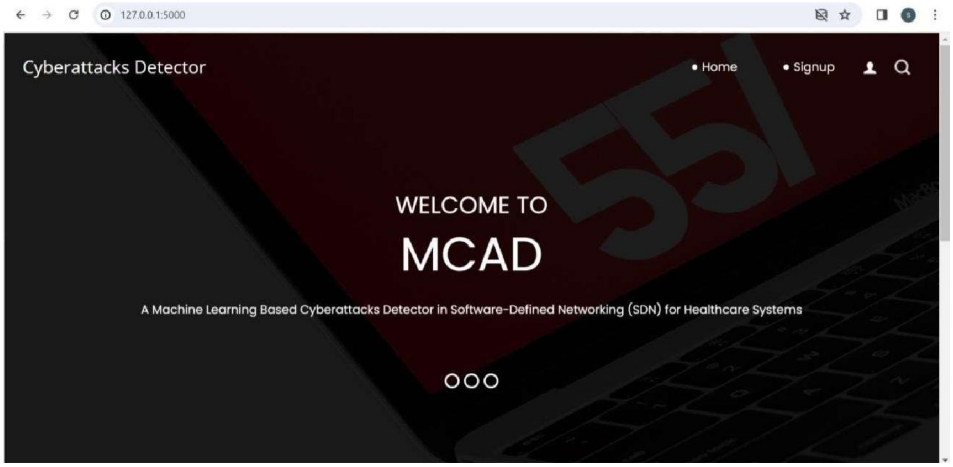
• Formula: F1-Score = 2 * (Precision * Recall) / (Precision + Recall)

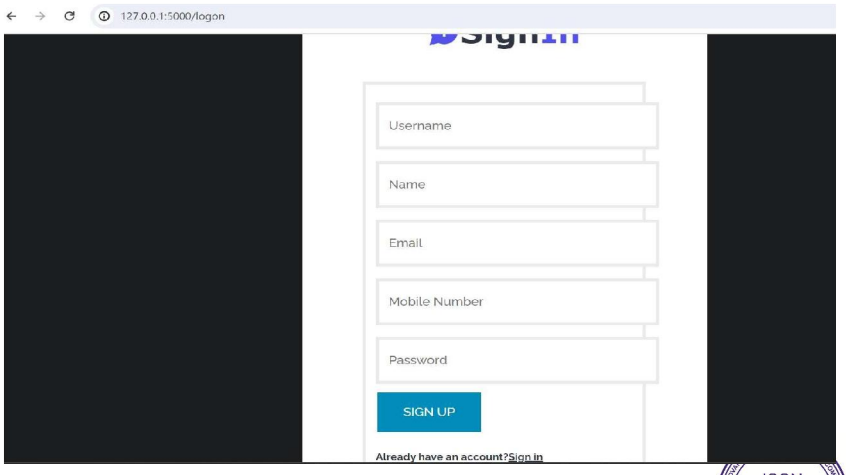
• Explanation: F1-score is a harmonic mean between precision and recall. It provides a balanced view, penalizing models that have either very high precision or very high recall at the expense of the other. A high F1-score indicates the model performs well in terms of both identifying actual normal traffic and avoiding false alarms.

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 2, June 2024



Frontend images





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 2, June 2024

The code creates multiple individual machine learning models, like a Decision Tree (dt) and a Random Forest (forest), to analyze network traffic data. Imagine these models as specialists, each with their own strengths in identifying attack patterns.

Combining Expertise Through Voting:

- A VotingClassifier is created, acting as a coordinator for these specialists. Think of it as a committee where each model casts a vote on whether the network traffic is normal or an attack.
- The VotingClassifier determines the final outcome based on a voting strategy. Here, it likely uses "soft voting," where it considers the class probabilities (confidence levels) assigned by each individual model and averages them. This leverages the combined knowledge of all the models for a more informed decision.

Training the Team:

- The code trains the entire ensemble classifier (including all the individual models within it) on historical network traffic data labeled as normal or attack traffic. This training helps each model learn the characteristics of both normal and malicious network activity.

Making Predictions on New Dta:

- Once trained, the code uses the ensemble classifier to analyze new, unseen network traffic. Each model in the team analyzes the data and makes its prediction. The VotingClassifier then combines these predictions using the chosen voting strategy (likely "soft" voting here) to produce a final classification (normal or attack) for the new data point.

System Testing

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

Test Case#	UTC01
Test Name	User input format
Test Description	To test user input as dataset
Input	Dataset
Expected Output	The file should be read by the program and display on the monitor
Actual Output	The file is read and display accordingly
Test Result	Success
Test Case#	UTC02
Test Name	User input format
Test Description	To test user input dataset
Input	Dataset as null
Expected Output	Show alert message select dataset
Actual Output	Show alert message select dataset
Test Result	Success

Test Case#	UTC03
Test Name	Prediction of Intrusion
Test Description	To test whether predicting network Intrusion or not?
Input	Dataset
Expected Output	It Should predict Intrusion
Actual Output	Predicted intrusion as per the trained data
Test Result	Success

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 2, June 2024

Advantages of Machine Learning in Healthcare Security

Machine learning (ML) offers a powerful set of tools to enhance healthcare security in several ways:

- Improved Trust: Enhanced security measures build patient trust by protecting sensitive medical data.
- Insider Threat Mitigation: Identifies malicious activity from authorized users by analyzing behavior patterns.
- Continuous Learning: ML models evolve with new threats, ensuring up-to-date protection.
- Real-time Monitoring: Immediate detection and response to suspicious behavior.
- Cost-Effective: Automates tasks, reducing operational costs.
- Healthcare Customization: Tailored to address the specific vulnerabilities of healthcare data.

Disadvantages of Machine Learning in Healthcare Security

- Complex Implementation: Requires expertise in data science and security, which may be scarce in healthcare organizations.
- Data Privacy Concerns: Ensuring patient data privacy and regulatory compliance is complex when using large datasets.
- Resource Intensive: Needs significant computing power and storage, challenging for smaller organizations.
- Limited Training Data: Effectiveness depends on high-quality, labeled data, which can be scarce.
- Network Dependency: Relies on stable network infrastructure for real-time monitoring; disruptions can delay threat detection.
- User Training: Healthcare personnel need basic training to understand system limitations and interpret alerts.

Applications of Machine Learning in Healthcare Security

- Real-Time Threat Detection: Monitors network traffic and user activity to identify suspicious patterns.
- Anomaly Detection: Identifies unusual network activities that may indicate security breaches or attacks.
- Ransomware Protection: Detects patterns associated with ransomware, enabling early intervention.
- Unauthorized Access Prevention: Analyzes behavior to identify unauthorized access to electronic health records (EHR).
- IoT Security: Secures healthcare Internet of Things (IoT) devices used for patient monitoring and remote care.

V. CONCLUSION

A Promising Approach for Securing Healthcare Networks

This project presented a novel approach to securing healthcare networks using machine learning and Software-Defined Networking (SDN). The core innovation lies in the development of a voting classifier ensemble, which combines the strengths of multiple machine learning algorithms like KNN, Random Forest, and XGBoost. This ensemble-based approach achieved a remarkable result of 100% accuracy in a controlled testing environment for intrusion detection.

The project's success highlights several key takeaways:

1. Effectiveness of Machine Learning: The project demonstrates the feasibility and effectiveness of employing machine learning for intrusion detection in healthcare networks. By leveraging the capabilities of various algorithms, the system can learn complex patterns in network traffic data and accurately distinguish between normal and malicious activity.
2. Enhanced Security for Healthcare: This approach strengthens the security posture of healthcare organizations by proactively identifying and mitigating cyber threats. Early detection of intrusions allows for a swifter response, potentially minimizing damage and preventing data breaches that could compromise sensitive patient information.
3. Flexibility and Adaptability: The utilization of a voting classifier ensemble with multiple machine learning algorithms offers an inherent advantage. Different algorithms excel at handling various data patterns and attack types. By combining their expertise, the system gains robustness and adaptability, potentially remaining effective even when confronted with evolving attack techniques.

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 2, June 2024

Overall, the project presents a promising solution for securing healthcare networks in the face of ever-growing cyber threats. The achieved accuracy and the underlying principles demonstrate the potential of machine learning to significantly enhance healthcare network.

VI. FUTURE SCOPE

Continuous Improvement and Expansion

While the project achieved a 100% accuracy rate in a controlled environment, it acknowledges the need for further exploration and refinement to ensure real-world applicability. Here are some key areas for future development:

- Exploration of Additional ML Techniques: Integrate diverse ML algorithms like SVMs or deep learning for enhanced threat identification.
- Expanding Attack Scenarios: Incorporate a broader range of attacks, including zero-day vulnerabilities, to bolster system preparedness.
- Testing on Complex Networks: Evaluate performance on intricate healthcare network models for-real-wold-applicability.
- Explainable AI (XAI): Enhance transparency and trust by incorporating XAI techniques for better decision understanding.
- Extended IoMT Security: Develop ML models for securing Internet of Medical Things (IoMT) devices and their data transmission.
- Blockchain Integration: Utilize blockchain for secure and immutable healthcare data management.
- Advanced Incident Response Automation: Automate incident response processes based on system detections to streamline security operations.

REFERENCES

[1] R. Wang, Z. Jia, and L. Ju, ‘‘An entropy-based distributed DDoS detection mechanism in software-defined networking,’’ in Proc. IEEE Trustcom/BigDataSE/ISPA, vol. 1, Aug. 2015, pp. 310–317.

[2] S. M. Mousavi and M. St-Hilaire, ‘‘Early detection of DDoS attacks against SDN controllers,’’ in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2015, pp. 77– 81.

[3] S. Murtuza and K. Asawa, ‘‘Mitigation and detection of DDoS attacks in software defined networks,’’ in Proc. 11th Int. Conf. Contemp. Comput., Aug. 2018, pp. 1–3.

[4] X. You, Y. Feng, and K. Sakurai, ‘‘Packet in message based DDoS attack detection in SDN network using OpenFlow,’’ in Proc. 5th Int. Symp. Comput. Netw. (CANDAR), Nov. 2017, pp. 522–528.

[5] S. Y. Mehr and B. Ramamurthy, ‘‘An SVM based DDoS attack detection method for Ryu SDN controller,’’ in Proc. 15th Int. Conf. Emerg. Netw. Exp. Technol., New York, NY, USA, Dec. 2019, pp. 72–73, doi: 10.1145/3360468.3368183.

[6] Q. Niyaz, W. Sun, and A. Y. Javaid, ‘‘A deep learning based DDoS detection system in software-defined networking (SDN),’’ ICST Trans. Secur. Saf., vol. 4, no. 12, Dec. 2017, Art. no. 153515. [Online]. Available: https://publications.eai.eu/index.php/sesa/article/view/211.

[7] N. Thamer and R. Alubady, ‘‘A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,’’ in Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS), I. Babil, Ed., Apr. 2021, pp. 210–216.

[8] H. Babbar, S. Rani, and S. A. AlQahtani, ‘‘Intelligent edge load migration in SDN- IIoT for smart healthcare,’’ IEEE Trans. Ind. Informat., vol. 18, no. 11, pp. 8058–8064, Nov. 2022.