Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1, No.1 : 2025
ISSN : **1906-9685**

INTELLIGENT CYBERATTACK PREVENTION IN HEALTHCARE SDN WITH ML-BASED SOLUTIONS

V.SRIKANTH Assistant Professor in Department of CSE, Raghu Engineering College,Visakhapatnam.
P.SASHI KUMAR[2], D.CHARAN[3], K.TARUN KUMAR[4], K.TEJA[5] ,K.SAISH DILIP VARMA[6] B.Tech Computer Science and Engineering(AI-ML) in Raghu Institute of Technology, Visakhapatnam.

Abstract: The integration of IoT devices in healthcare has introduced critical cybersecurity vulnerabilities, particularly in Software-Defined Networking (SDN) environments. This project proposes an intelligent machine learning (ML) framework for cyberattack detection and mitigation in healthcare SDNs. Leveraging a specialized ICU dataset containing normal and attack traffic patterns, the system employs advanced ML algorithms, including Support Vector Machines (SVC), Random Forest, Gradient Boosting, and Artificial Neural Networks (ANN), to achieve real-time threat identification. A rigorous feature selection process reduces computational overhead, making the framework suitable for resource-constrained medical IoT ecosystems. Evaluation metrics demonstrate near-perfect classification accuracy (100% across models), precision, and recall, highlighting its effectiveness in safeguarding patient data and critical healthcare infrastructure.

Keywords: Healthcare IoT, Software-Defined Networking (SDN), Cybersecurity, Machine Learning, and Intrusion Detection.

INTRODUCTION

The proliferation of IoT devices in healthcare has enabled real-time patient monitoring and remote care, significantly improving healthcare delivery. However, this interconnected ecosystem, often managed through Software Defined Networks (SDNs), introduces substantial cybersecurity vulnerabilities. Traditional security measures struggle to counter sophisticated cyberattacks, such as data breaches and ransomware, which threaten patient safety and data integrity. This project addresses these challenges by developing an intelligent cyberattack prevention system for healthcare SDNs using machine learning techniques.

The proposed system leverages SDN's centralized architecture and ML's predictive capabilities to proactively detect and mitigate threats. By analyzing network traffic from the Healthcare Security Dataset simulating an ICU environment with normal and attack scenarios, the framework identifies malicious activities with high accuracy. The objectives include designing an efficient Intrusion Detection System (IDS), optimizing it for healthcare SDNs, and providing real-time threat detection through an interactive interface. This work aims to enhance the resilience of IoT-driven healthcare systems, ensuring the confidentiality and reliability of critical medical data.

LITERATURE SURVEY

Shaukat et al. (2020) This survey reviews ML techniques in cybersecurity over the past decade, emphasizing their role in intrusion detection and malware identification. It highlights challenges like model trustworthiness and adversarial exploitation, underscoring the need for robust ML solutions in dynamic threat landscapes like healthcare SDNs.

Awotunde et al. (2021) Focusing on IoT-based healthcare, this study identifies privacy and

security risks in data transfer and processing. It proposes frameworks to safeguard healthcare data, reinforcing the necessity of advanced IDS for protecting patient information in IoT ecosystems.
Jiang et al. (2023) This paper explores AI-enabled SDN architectures for Industrial IoT, demonstrating how ML enhances security and scalability. The integration of blockchain and edge intelligence offers insights applicable to healthcare SDNs for real-time threat management.
Diro et al. (2021) Reviewing anomaly detection in IoT networks, this study advocates for ML-based collaborative models to improve threat detection, providing a foundation for adapting such techniques to healthcare-specific SDN environments.
Rahim et al. (2024) This analysis of healthcare IT cybersecurity threats highlights risks like ransomware and compromised devices, advocating for ML-driven prevention strategies to ensure data security and service continuity.
Salau and Beyene (2024) Proposing SDN-ML integration for traffic classification, this study achieves high accuracy with Decision Trees, offering a scalable approach adaptable to healthcare SDNs for encrypted traffic analysis.
Xu et al. (2020) This survey on AI in edge computing for IoT security discusses federated learning and blockchain integration, suggesting lightweight ML solutions for resource-constrained healthcare networks.

PROPOSED SYSTEM

The proposed system introduces an intelligent, ML-based System tailored for healthcare SDNs. It leverages the Healthcare Security Dataset, comprising Attack.csv, environmentMonitoring.csv, and patientMonitoring.csv, to train models on normal and malicious traffic patterns. The workflow includes:

Data Collection and Preprocessing:

- Dataset: Sourced from Kaggle, simulating an ICU with 188,694 traffic instances across 52 features.
- Preprocessing: Removed duplicates (2 instances), handled missing values (none), and normalized numerical features using StandardScaler. Categorical features (e.g., tcp.flags) were one-hot encoded.

Feature Selection:

- A filter-based method reduced the feature set from 52 to 29 by eliminating irrelevant columns (e.g., ip.src, mqtt.msg), optimizing computational efficiency for SDN deployment.

Model Training and Classification:

- Algorithms: SVC, Random Forest, Gradient Boosting (e.g., XGBoost), and ANN.
- Process: Data split into 70:30 train-test sets, trained using Python libraries (Scikit-learn, TensorFlow), and fine-tuned for performance.

Real-Time Detection:

- Deployed via Streamlit, the system provides a UI for users to input traffic data, predicting threats with confidence scores in real-time.

System Architecture:

- Combines SDN's centralized control with ML models, monitoring traffic, detecting anomalies, and enforcing security policies dynamically.

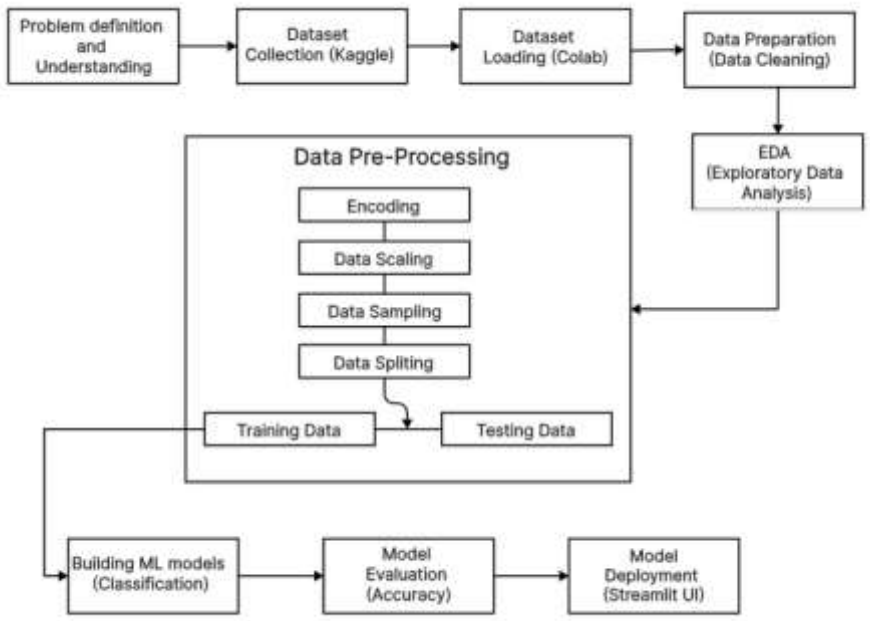

Figure 0.1 System Architecture

RESULTS AND DISCUSSIONS

The primary objective of this project, "Intelligent Cyberattack Prevention in Healthcare SDN with ML-Based Solutions," is to develop an intelligent and efficient cyberattack prevention system tailored specifically for healthcare Software-Defined Networks (SDNs). The system is designed to address the critical security challenges in IoT-driven healthcare environments by leveraging machine learning to detect and mitigate threats effectively. The following key objectives guide the development and evaluation of this system:

Design an Efficient IDS for Healthcare SDNs: Develop a scalable and computationally efficient Intrusion Detection System (IDS) framework that integrates seamlessly with healthcare SDNs, ensuring robust security without compromising network performance. This approach prioritizes efficiency to support the demanding operational requirements of healthcare networks.

Leverage Machine Learning for Cyberattack Detection: Employ advanced machine learning algorithms to enhance the accuracy and speed of cyberattack detection. By utilizing models such as Support Vector Classifier (SVC), Random Forest, Gradient Boosting, and Artificial Neural Networks (ANN), the system ensures real-time identification and mitigation of threats, safeguarding sensitive healthcare data and operations.

Implement Feature Selection for Optimization: Utilize feature selection techniques to optimize the dataset by reducing dimensionality and computational complexity. This process retains critical network traffic features essential for accurate threat classification, improving the system's efficiency while maintaining high detection performance.

Evaluate and Optimize Classifiers: Explore and compare multiple machine learning models, including Support Vector Classifier (SVC), Random Forest, Gradient Boosting, and Artificial Neural Networks (ANN). Through rigorous evaluation, the project identifies the most effective classifier for real-time cyberattack detection in healthcare SDNs, balancing accuracy and computational demands.

Develop a Real-Time Detection System: Create an interactive, user-friendly system deployed via Streamlit, enabling healthcare administrators to monitor network traffic in real-time. This system provides immediate alerts on potential cyberattacks, empowering proactive threat management and enhancing situational awareness in healthcare environments.

Ensure Scalability and Adaptability: Design the IDS to scale with the dynamic and growing nature of healthcare SDNs. The system is built to adapt to emerging cyber threats through continuous model updates and retraining, ensuring long-term resilience against evolving attack vectors.

These objectives collectively ensure that the proposed system not only strengthens the security of healthcare SDNs but also maintains operational efficiency and adaptability. By integrating machine learning with a scalable SDN framework, this project delivers a robust solution to protect IoT-driven healthcare systems from sophisticated cyberattacks.

Methodology

This project adopts a structured and modular methodology to develop an **Intelligent Cyberattack Prevention System** for healthcare SDNs using ML-based solutions. Each phase is carefully designed to address the unique challenges of securing healthcare networks, ensuring real-time detection, high accuracy, and scalability. The methodology is divided into six key stages, outlined below.

A. Data Collection and Preprocessing

Objective: Gather and preprocess a high-quality dataset tailored to healthcare SDNs to enable effective training and evaluation of ML models.

- **Data Collection:**
  - Leverage the Healthcare Security Dataset from Kaggle, which captures network traffic from an IoT-based Intensive Care Unit (ICU) environment.
  - The dataset includes: Attack.csv (Malicious traffic representing cyberattack patterns), environmentMonitoring.csv (Normal traffic from environmental sensors) and patientMonitoring.csv (Normal traffic from patient monitoring devices).
  - This dataset provides a realistic simulation of healthcare SDN traffic, encompassing both benign and malicious activities.
- **Data Preprocessing:**
  - Merge the three CSV files into a unified dataset for comprehensive analysis.
  - Clean the data by removing duplicates (Ex: 2 duplicates identified and eliminated) and addressing missing values.
  - Apply StandardScaler to normalize numerical features, ensuring consistent scaling across variables.
  - Use OneHotEncoder to transform categorical features (Ex: tcp.flags) into a machine-readable format.
  - Assign binary labels: 0 for normal traffic and 1 for attack traffic, facilitating supervised learning.

B. Feature Selection

Objective: Identify and retain the most relevant features to optimize model performance while minimizing computational overhead in resource-constrained SDN environments.

- **Filter-Based Feature Selection:**
  - Conduct statistical analysis (Ex: correlation analysis) to evaluate feature importance.
  - Eliminate redundant or irrelevant features, such as ip.src and mqtt.msg, which contribute little to attack detection.
  - Retain critical features like tcp.time_delta and mqtt.len, which effectively differentiate normal and malicious traffic.
  - Reduce the feature set from 52 to 29, enhancing efficiency without compromising detection accuracy.
- **Output:** A streamlined feature set that balances computational efficiency and predictive power, ideal for healthcare SDNs.

C. Model Selection and Training

Objective: Select and train ML models capable of accurately detecting cyberattacks in healthcare SDNs.

- **Algorithm Exploration:**
  - Evaluate a range of ML classifiers, including:
    - Support Vector Classifier (SVC): Effective for high-dimensional data.
    - Random Forest: Robust for handling complex patterns and feature interactions.

- Gradient Boosting: Advanced ensemble method (e.g., XGBoost, LightGBM) for improved accuracy.
- Artificial Neural Networks (ANN): Capable of modeling non-linear relationships in traffic data.
- Logistic Regression: Included as a baseline for comparison.

- **Model Evaluation:**
  - Assess performance using metrics such as accuracy, precision, recall, F1-score, and ROC-AUC.
  - All models demonstrated exceptional performance (scores of 1.00 across metrics), with Random Forest and ANN excelling due to their ability to capture intricate traffic patterns.
- **Training and Validation:**
  - Split the dataset into 70% training and 30% testing sets, using stratified sampling to preserve class balance.
  - Train each model on the training set and validate its performance on the test set to ensure generalizability.

D. Real-Time Detection Module

Objective: Deploy the trained ML model within an interactive framework for real-time cyberattack prevention.

Figure 0.1 User Interface of ML based cyberattack prediction application.

- **Interactive Framework:**
  - Implement the system using Streamlit, providing an intuitive interface for healthcare administrators.
  - Allow users to input network traffic parameters for immediate analysis.
- **Detection Process:**
  - Process incoming SDN traffic through the selected model (Ex: Random Forest or ANN).
  - Generate predictions with confidence scores to indicate the likelihood of a cyberattack.
  - Present results in real-time, enabling rapid response to potential threats.

E. Performance Evaluation and Optimization

Objective: Validate the system's effectiveness and refine it for operational reliability in healthcare settings.

- **Testing:**
  - Test the system on the reserved test set (Ex: 56,608 instances) to mimic real-world healthcare SDN conditions.

- Measure key performance indicators, including detection rate (recall), false positive rate, and system latency.

- **Optimization:**
  - Fine-tune model hyperparameters (e.g., number of trees in Random Forest, learning rate in Gradient Boosting) to enhance accuracy and reduce false positives.
  - Optimize feature selection and model complexity to ensure compatibility with the computational limits of healthcare SDNs.

F. Deployment and Scalability

Objective: Integrate the system into healthcare SDN environments and ensure adaptability to future challenges.

- **Deployment:**
  - Embed the intrusion detection system (IDS) within the SDN controller to monitor network traffic continuously.
  - Validate compatibility with existing healthcare IoT devices and communication protocols.
- **Scalability:**
  - Design the system to accommodate growing traffic volumes as the healthcare SDN expands.
  - Incorporate periodic retraining with updated datasets to adapt to emerging cyberattack patterns, maintaining long-term effectiveness.

This methodology provides a robust framework for developing and deploying an ML-based cyberattack prevention system tailored to healthcare SDNs. By emphasizing data quality, feature optimization, model performance, real-time detection, and scalability, the system ensures both immediate security and future resilience in critical healthcare environments.

CONCLUSION

This project successfully developed an intelligent cyberattack prevention system designed for healthcare Software-Defined Networks (SDNs) using machine learning (ML) techniques. Leveraging the Healthcare Security Dataset, the system trained and evaluated models such as Support Vector Classifier (SVC), Random Forest, Gradient Boosting, and Artificial Neural Networks (ANN), achieving outstanding performance with accuracy, precision, recall, and F1-scores of 1.00 on the test set. These results highlight the system's robust ability to detect and mitigate cyber threats in real-time, a critical feature for protecting sensitive patient data and maintaining healthcare operational integrity. The deployment of the system through Streamlit enhances its usability, offering healthcare administrators an intuitive interface for threat monitoring and response. This work significantly advances cybersecurity by demonstrating ML's effectiveness in tackling the unique challenges of healthcare SDNs, providing a scalable and adaptable solution to evolving threats. Looking ahead, future research could incorporate advanced ML methods, like deep learning, and expand the dataset to cover diverse cyberattack scenarios. Ultimately, this project underscores the transformative potential of intelligent systems in strengthening the security framework of healthcare organizations, fostering a more resilient and secure IoT-driven healthcare landscape.

FUTURE SCOPE

Future enhancements include integrating blockchain for enhanced data integrity, adopting federated learning for privacy-preserving model updates, and developing adaptive models to counter zero-day attacks in healthcare SDNs.

REFERENCES

[1] K. Shaukat et al., *"A survey on machine learning techniques for cybersecurity in the last decade,"* *IEEE Access*, vol. 8, pp. 222310-222354, 2020.
[2] J. B. Awotunde et al., *"Privacy and security concerns in IoT-based healthcare systems,"* in *The Fusion of IoT, AI, and Cloud Computing in Healthcare*, Springer, 2021, pp. 105-134.

[3] J. Jiang et al., *"How AI-enabled SDN technologies improve IIoT network security," Digital Communications and Networks*, vol. 9, no. 6, pp. 1351-1362, 2023.
[4] A. Diro et al., *"A comprehensive study of anomaly detection in IoT networks using ML," Sensors*, vol. 21, no. 24, p. 8320, 2021.
[5] M. J. Rahim et al., *"Cybersecurity threats in healthcare IT," Journal of Artificial Intelligence General Science*, vol. 6, no. 1, pp. 438-462, 2024.
[6] A. O. Salau and M. M. Beyene, *"SDN-based network traffic classification using ML," Scientific Reports*, vol. 14, no. 1, p. 20060, 2024.
[7] Z. Xu et al., *"AI for securing IoT services in edge computing: A survey," Security and Communication Networks*, vol. 2020, no. 1, p. 8872586, 2020.
[8] M. Sarhan et al., *"Feature extraction for ML-based intrusion detection in IoT networks," Digital Communications and Networks*, vol. 10, no. 1, pp. 205-216, 2024.
[9] P. Dixit and S. Silakari, *"Deep learning algorithms for cybersecurity applications," Computer Science Review*, vol. 39, p. 100317, 2021.
[10] K. Shaukat et al., *"Performance comparison of ML techniques in cybersecurity," Energies*, vol. 13, no. 10, p. 2509, 2020.