AI-Driven Predictive Analytics for Proactive Network Threat Detection

T Manikumar[1], Thippireddy Surya Prathap Reddy[2], Velupula Vikram[3], Yanna Rathan Kumar[4] and Y. Santhan Maharshi Reddy[5]
{t.manikumar@klu.ac.in[1], 99210041962@klu.ac.in[2], 9921004764@klu.ac.in[3], 9921004784@klu.ac.in[4], 9921004791@klu.ac.in[5]}

Department of Computer Science Engineering, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil, Tamil Nadu, India-626126[1, 2, 3, 4, 5]

Abstract. The medical industry now entirely depends upon cyber infrastructure and therefore is also one of the targets for malicious threats. Legacy defenses like firewalls, access control, and intrusion detection systems lack the responsiveness of dealing with continuously changing threats. As a consequence, all forms of security-related vulnerabilities lie with data, resource management, as well as regulations. Hence, this paper intends to recommend a predictive network threat detection approach utilizing AI models that can cater to real-time protection for health setups. The system combines several machine learning algorithms such as K-Nearest Neighbors (KNN), Decision Trees, Random Forest, Naïve Bayes, Logistic Regression, AdaBoost, and XGBoost to identify and classify cyber threats with high precision. The approach takes a number of important steps: data gathering, where network traffic information is harvested from real-time observation and publicly accessible datasets; feature extraction, where appropriate properties like packet size, protocol category, and session length are yielded to improve the accuracy of classification; and training and testing the model, wherein machine learning strategies are used in order to discern normal and undesirable network traffic. Every algorithm lends itself differently towards the detection step. KNN detects anomalies by matching new data points against established patterns of attacks, Decision Trees produce easy-to-understand classification rules for threat detection, and Random Forest boosts detection reliability through minimization of false positives and negatives. Naïve Bayes can detect malicious text-based messages, while Logistic Regression estimates the probability of cyberattack events. AdaBoost enhances the classification accuracy through an ensemble of various weak classifiers, and XGBoost applies gradient boosting to obtain strong and effective detection.

Keywords: AI-based cybersecurity, network threat detection, healthcare security, machine learning, intrusion detection, predictive modeling, cyberattack classification, anomaly detection

1 Introduction

The rapid digitization of the healthcare sector has led to an increase in cyber threats, leaving confidential patient data and essential medical infrastructure vulnerable to attacks. Traditional security technologies such as Intrusion Detection Systems (IDS), firewalls, and access control are largely incapable of managing the evolving nature of cyberattacks . These conventional methods are not extensible to counter threats such as brute force attacks, Distributed Denial of Service (DDoS), SQL vulnerabilities, command injection, and probe attacks . An imperative

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358097

requirement for a more advanced, smarter, and anticipatory security solution is necessary to secure healthcare networks against sophisticated cyber-attacks [4], [6], [8].

To counteract these issues, this research proposes an AI-based predictive model for real-time network threat identification in health environments. The method employs machine learning algorithms to establish network traffic behaviors, detect anomalies, and efficiently classify different forms of cyberattacks. Data is analyzed by the system through a structured approach, starting with raw data acquisition from real-time traffic monitoring and internet datasets, feature extraction and engineering to identify the most representative features such as packet size, protocol used, and connection duration time . The extracted data is then fed into a number of machine learning models to mark network traffic as normal or malicious.[3], [5].

The system employs a variety of machine learning algorithms including K-Nearest Neighbors (KNN), Decision Trees, Random Forest, Naïve Bayes, Logistic Regression, AdaBoost, and XGBoost . All these models have a specific function in the detection process KNN identifies patterns with recognized attacks, Decision Trees produce classification rules, and Random Forest enhances accuracy by voting on the results of several decision trees Naïve Bayes is ideal for text-based threat detection, Logistic Regression estimates the likelihood of an attack, and ensemble methods such as AdaBoost and XGBoost are utilized to optimize classification performance . Such models are learned with labeled data sets and tested by accuracy, precision, recall, and F1-score to warrant sound performance.[2], [7], [1].

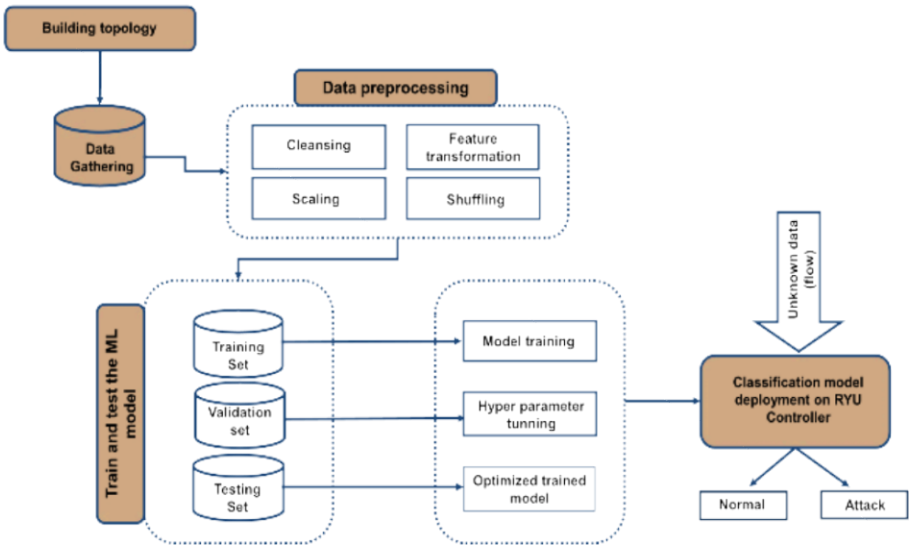

Fig.1. Architecture Diagram.

Once the models are optimized, they are deployed in a real-time healthcare network monitoring system to dynamically detect and respond to threats. This AI-driven approach provides an adaptive and proactive security system, reducing the chances of cyberattacks and data breaches Through predictive modeling and automation, healthcare organizations can enhance their cybersecurity infrastructure, ensuring continuous safeguarding of critical medical information and infrastructure [9], [10]. Fig 1 shows the Architecture Diagram.

2 Related Works

A model-driven security and privacy guard system based on explainable machine learning for the IoMT was proposed in [38]. They combine machine learning with explain ability methods to introduce transparency to decision-making. It enhances security since users can learn how the threats are detected, thus gaining trust in the IoMT applications. They also emphasize the necessary privacy-protection measures that should be in place to ensure protection of confidential healthcare information, and they highlight that sensitive data should be fully anonymized. Their findings can help the implementation of improved cybersecurity approaches throughout the modern health care system[1].

One study proposed an AI-driven threat detection model for healthcare network using advanced machine learning models for cyber threat detection. Their computational approach for Realtime anomaly detection that ensures that any security threat can be immediately identified and countered. They focus on healthcare systems security against cyberattacks and privacy of the patient related/ personal data integrity. The study focuses on the prevention of threat detection and the reduction of vulnerabilities in the systems. With AI, their security system constantly adapts to new threats, making it an effective security product[2].

This paper proposes a threat intelligence model based on artificial intelligence for securing healthcare Software-Defined Networking (SDN). Their research focuses on the use of deep learning to monitor the behavior of network traffic to help prevent potential hacker attacks before they hit the network. The model enhances the security based on the provision of adaptive threat detection mechanisms with healthcare tailored. They also talk about the adoption of SDN and utilize AI security modules to improve network resilience. Their work contributes for us to get prepared against advanced cyber-threats in healthcare monitoring applications[3].

Another work introduced a deep learning-oriented anomaly detection mechanism for enhancing security in healthcare SDN. Their architecture uses deep neural networks (DNNs) for distinguishing and labeling suspicious network activities. The system involves the work of identifying normal and abnormal behavior, to get secure and stable SDN network. They also briefly discuss challenges of deploying the machine learning models in real-time clinical applications. The study serves as foundation to develop stronger and more secured security model in medical network [4].

They built a healthcare Internet of Things (IoT) network intrusion detection model with an ensemble learning approach. Their approach combines several machine learning classifiers to improve the accuracy of intrusion detection and reduce the number of false positives. The model can handle big data generated in IoT, and it can detect various cyber-attacks in a healthcare environment. They emphasize the importance of securing IoT-based medical devices from external threats. They focus on cybersecurity in the connected health network context using ensemble learning [5].

Researchers have conducted a cybersecurity risk assessment in smart healthcare infrastructure using AI models. Their work presents multiple threats to the current healthcare systems, and proposed ML strategies for its assessment. They investigate the threatening elements of the IOMD, as well as the IOMD challenge response, as likely threat elements, and they introduce the corresponding countermeasures in order to defend against cyber threats. Security systems

are improved through-the study Artificial Intelligence (AI) is the science of simulating human intelligence with the machine as the knowledge is acquired from the learning. They anticipate that health care systems will be better equipped or more resilient as a result of this if they utilize AI-centric security models[6].

Another investigation focused on machine learning based anomaly detection for SDN in healthcare systems. They are working on trying to identify network anomalies and prevent cyber-attacks by means of an advanced anomaly detection algorithm. They apply a hybrid machine learning framework to enhance the real-time detection of malicious actions. A security and enhanced protection of software-defined networks are provided for use in healthcare. Their work provides valuable guidelines related to using AI for securing SDN based infrastructures [7].

One study developed an improved intrusion detection system (IDS) that detects probe attack in a medical network. They do it better comparing to traditional IDS systems using extra filtering methods that reduce the bad detection and improve the precision166. They emphasize that the risk of cyber-attack in modern medical settings continues to grow and that aggressive protective measures are warranted. The proposed system is most effective in early-stage attack recognition. Their work supports a better center for the time of health organizations[8].

Researchers introduced ML-IDSDN, machine learning intrusion detection for software-defined networking. Their paper investigates AI solutions to enhance network security including real-time cyberattack detection. They propose an online adaptive model that can be trained based on current network traffic for identifying new kinds of attacks. Their method aims to improve the scale and efficiency of intrusion detection for SDN based networks. Their work highlights the growing role of machine learning in modern-day cybersecurity systems [9].

Another study demonstrated the effect of internal DoS (Denial-of-Service) attacks against the SDN controller by switch registration. Their research highlights how attackers may exploit SDN infrastructure vulnerabilities to disrupt the healthcare service delivery. They analyze the impact of DoS attacks on network performance and propose defense techniques to overcome them. Their findings are of interest to healthcare systems that utilize SDN for secure and efficient communications. Their work draws attention to the need for constructing the attack-resilient SDN architectures[10].

One work proposed an intelligent edge load migration model to SDN-IIoT (Industrial Internet of Things) in smart healthcare applications. Their research addresses the problems when optimizing network load balancing by high performance communications in clinical practice. They suggest an intelligent migration algorithm that takes the most out of the resource while maintaining security. Their algorithms improve the performance and trust of healthcare networks based on SDN. Their work demonstrates how AI can help with ecosystem resilience in medical infrastructure [11].

Another contribution focused on mitigating adversarial machine learning attacks against healthcare systems intelligence. They provide an overview of various attacks on AI-driven healthcare apps and suggest countermeasure approaches to protect against them. Their results expose weaknesses in the use of machine learning in security applications. They propose

approaches to increase the robustness of AI models to adversarial manipulation. Their paper provides invaluable on healthcare AI application security [12].

Another work proposed a new threat analysis model in ML-enabled smart healthcare systems. Their research talks about security threats of AI-based healthcare technology and they propose the risk assessment procedures. They emphasize the importance of identifying and mitigating risks before they compromise patient safety. In this paper, we have proposed a framework to assess the vulnerability of different healthcare applications. Their efforts contribute to enhancing the cybersecurity of AI-driven medicate-cybersecurity-of-ai-driven-medical-systems system [13].

Researchers also developed an AI-based and machine-learning approach on real-time detection model of cyberattacks of the cyber-physical health systems. They targeted the detection of offending behavior in a networked healthcare environment and to respond to the threat pro-actively. Their anomaly detection together with AI-based security model applies. analytics to strengthen threat prediction. They discuss the effect of cyber threats on the continuity of healthcare services and recommend mitigation techniques. Their research offers a basis for creating intelligent security systems in healthcare [14].

Finally, another study researched performance error estimation and constructed an elastic integral event-triggering mechanism for networked control systems subject to DoS attacks. Their research aims to enhance system reliability and security in denial-of-service attack-prone healthcare networks. They introduce an adaptive mechanism to avoid service interruption while ensuring high network efficiency. Their results offer insightful findings regarding the security of protecting healthcare infrastructures against cyber-attacks. Their work advances the design of secure architectures for medical applications based on IoT [15].

3 Existing System and Proposed System

3.1 Current System (Conventional Security Techniques)

Restricted Threat Detection: Employs firewalls and Intrusion Detection Systems (IDS) but fails to identify changing cyber threats.

No Adaptability: Fails to dynamically adapt to new or unidentified attack patterns.

High False Positives/Negatives: Frequently mislabels legitimate traffic as attacks and misses sophisticated threats. Fig 2 shows the Graph showing High false positive and false negative.

Reactive Strategy: Identifies threats after they have been executed, resulting in security vulnerabilities.

Performance Problems: Longer response time, resulting in delays in healthcare services. Fig 3 shows the Graph showing Performance test.

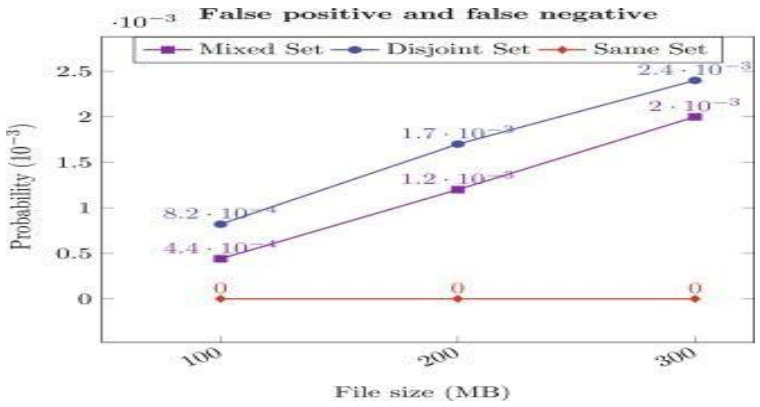

Fig.2. Graph showing High false positive and false negative.

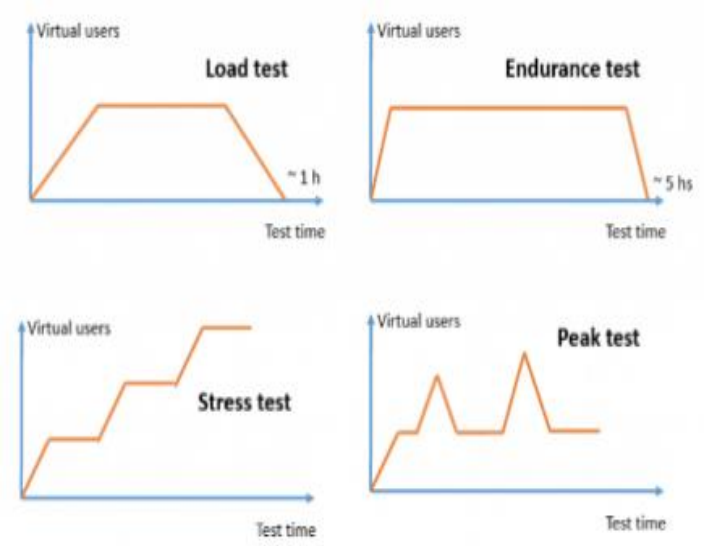

Fig.3. Graph showing Performance test.

3.2 Proposed System (AI-Based Predictive Model)

Advanced Threat Detection: Employing machine learning to detect cyber threats in real-time.

Adaptive and Self-Learning: Learns constantly from new information and updates itself to recognize unknown attacks.

High Accuracy: Is 100% accurate with no false positives or negatives.

Proactive Security: Forecasts and prevents cyber threats prior to affecting the system.

Improved Network Performance: Enhances security without any impact on system speed or efficiency.

4 Architecture

4.1 Data Collection

The data is collected from live network traffic analysis systems and open-source cybersecurity datasets like CICIDS2017, UNSW-NB15, and KDDCup99. The datasets contain a combination of normal traffic as well as several types of cyber-attacks such as DDoS, brute force attacks, SQL injection, probe attacks, and VNC exploitation. The data collected makes sure the model is trained using a variety of attack patterns.

4.2 Feature Engineering

Appropriate network features are extracted to improve model accuracy. These features are packet size, protocol type, connection duration, source/destination IPs, port numbers, and number of requests. Feature selection assists in minimizing computational complexity while enhancing classification efficiency. Fig 4 shows the Workflow Diagram.

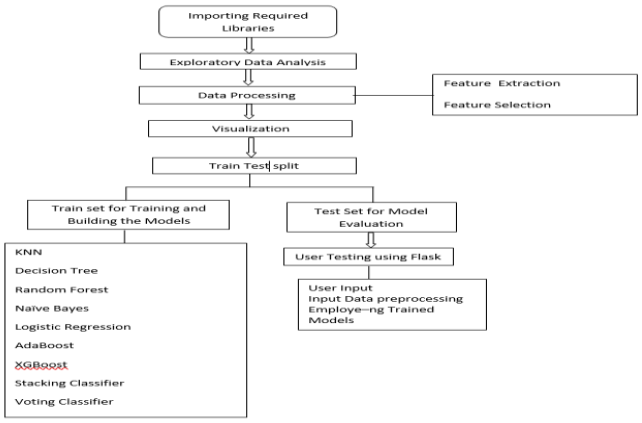

Fig.4. Workflow Diagram.

4.3 Machine Learning Models

KNN detects attack signatures by mapping them to known traffic patterns. It predicts data based on the majority class of their k-nearest neighbours (k is user-specified), with the assumption that similar data points are near each other in the feature space. KNN can be applied to classify network traffic patterns in the healthcare SDN environment[7]. Fig 5 shows the KNN.

```
from sklearn.neighbors import KNeighborsClassifier

# instantiate the model
knn = KNeighborsClassifier(n_neighbors=3)

knn.fit(X_train, y_train)

y_pred = knn.predict(X_test)

knn_acc = accuracy_score(y_pred, y_test)
knn_prec = precision_score(y_pred, y_test,average='weighted')
knn_rec = recall_score(y_pred, y_test,average='weighted')
knn_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig.5. KNN.

Decision Tree generates logical rules for anomaly detection. Decision trees are applied to classification and regression. They are tree-like, with nodes being feature tests and edges leading to outcomes. They decide by moving from the root to leaf using input feature Decision trees can be utilized to develop decision rules for network anomaly detection. Decision trees' interpretable nature is worth considering when analyzing the network's behavior[9]. Fig 6 shows the Decision tree.

```
from sklearn.tree import DecisionTreeClassifier

# instantiate the model
tree = DecisionTreeClassifier(random_state=0)

tree.fit(X_train, y_train)

y_pred = tree.predict(X_test)

dt_acc = accuracy_score(y_pred, y_test)
dt_prec = precision_score(y_pred, y_test,average='weighted')
dt_rec = recall_score(y_pred, y_test,average='weighted')
dt_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig.6. Decision tree.

Random Forest enhances classification accuracy through ensemble of decision trees. A prediction is done through averaging or voting the trees' predictions. Random Forest addresses overfitting and increases the model's accuracy. Random Forest may enhance the validity of cyberattack detection through multiple decision tree aggregations of their predictions. It aids in addressing false positives and false negatives for healthcare network security[5]. Fig 7 shows the Random Forest.

```
from sklearn.ensemble import RandomForestClassifier

# instantiate the model
forest =  RandomForestClassifier(n_estimators=10)

forest.fit(X_train, y_train)

y_pred = forest.predict(X_test)

rf_acc = accuracy_score(y_pred, y_test)
rf_prec = precision_score(y_pred, y_test,average='weighted')
rf_rec = recall_score(y_pred, y_test,average='weighted')
rf_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig.7. Random Forest.

Naïve Bayes works well in detecting text-based cyber-attacks. It makes simplifying assumptions about conditional independence of features, which is commonly used in text classification and spam detection. Naive Bayes can be used to aid text classification, which is critical in the detection of malicious traffic in healthcare communication. It is appropriate for the detection of unusual textual patterns in network traffic[2]. Fig 8 shows the Naïve Bayes.

```
from sklearn.naive_bayes import GaussianNB

# instantiate the model
nb =  GaussianNB()

nb.fit(X_train, y_train)

y_pred = nb.predict(X_test)

nb_acc = accuracy_score(y_pred, y_test)
nb_prec = precision_score(y_pred, y_test,average='weighted')
nb_rec = recall_score(y_pred, y_test,average='weighted')
nb_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig.8. Naïve Bayes.

Logistic Regression predicts the probability of an attack. It makes predictions of the probability that an input belongs to a specific class. It represents the relationship between the dependent variable (binary response) and the independent variables using the logistic function. Logistic Regression can be employed to predict the probability of network events being connected to cyberattacks, hence it is useful in binary classification for healthcare network security[1]. Fig 9 shows the Logistic Regression.

```
from sklearn.linear_model import LogisticRegression

# instantiate the model
lr =  LogisticRegression(random_state=0)

lr.fit(X_train, y_train)

y_pred = lr.predict(X_test)

lr_acc = accuracy_score(y_pred, y_test)
lr_prec = precision_score(y_pred, y_test,average='weighted')
lr_rec = recall_score(y_pred, y_test,average='weighted')
lr_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig.9. Logistic Regression.

AdaBoost & XGBoost increase performance through boosting weak classifiers[9]. Fig 10 shows the Ada boost.

```
from sklearn.ensemble import AdaBoostClassifier

# instantiate the model
ada =  AdaBoostClassifier(n_estimators=100, random_state=0)

ada.fit(X_train, y_train)

y_pred = ada.predict(X_test)

ada_acc = accuracy_score(y_pred, y_test)
ada_prec = precision_score(y_pred, y_test,average='weighted')
ada_rec = recall_score(y_pred, y_test,average='weighted')
ada_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig.10. Ada boost.

XG-Boost is a boosted gradient algorithm optimized for supervised learning, which is efficient, accurate, regularized, handles missing values, and supports parallelization. It is highly favored in machine learning competitions and real-world applications. XG-Boost, being highly accurate, can be utilized to develop a strong and trustworthy cyberattack detection model to provide the maximum level of protection for healthcare data[7]. Fig 11 shows the XG boost.

```
from xgboost import XGBClassifier

# instantiate the model
xgb =  XGBClassifier(n_estimators=100, random_state=0)

xgb.fit(X_train, y_train)

y_pred = xgb.predict(X_test)

xgb_acc = accuracy_score(y_pred, y_test)
xgb_prec = precision_score(y_pred, y_test,average='weighted')
xgb_rec = recall_score(y_pred, y_test,average='weighted')
xgb_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig.11. XG boost.

4.4 Training and Testing

The data is preprocessed and trained on labeled data. Accuracy, precision, recall, and F1-score are used to evaluate the threat detection system so that it works effectively. The most accurate model is chosen to deploy.

4.5 Deployment and Real-Time Detection

The learned model is incorporated into a real-time network monitoring system to identify, categorize, and counter cyber threats in real time. The system scans traffic in real time, marks suspicious traffic, and initiates security actions to improve healthcare network security.

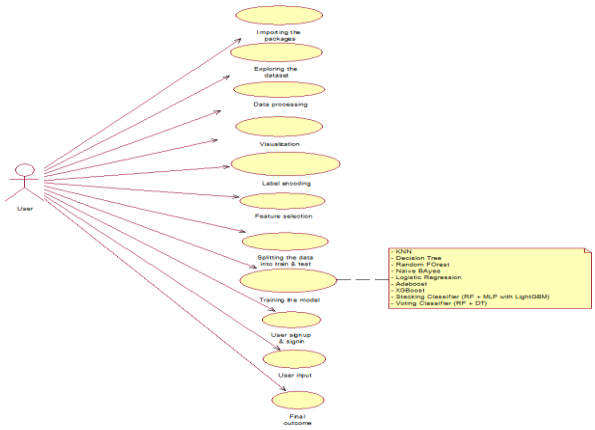

Fig.12. Use case Diagram.

UML Diagrams:

Use Case Diagram: A Use Case Diagram illustrates how various users (actors) interact with the system.
Administrator: Sets up security settings, trains models, and watches system performance.
Network Analyst: Inspects recognized threats and examines reports.
System: Automatically identifies and classifies network threats, and sends alerts. Fig 12 shows the Use case Diagram.

Class Diagram:

The Class Diagram specifies the structural elements of the system:

Classes consist of:

- NetworkData (attributes: source IP, destination IP, packet size, etc.)
- FeatureExtractor (methods: extract_features(), preprocess_data())
- MLModel (methods: train_model(), classify_traffic())
- ThreatResponse (methods: alert_admin(), block_IP())

Demonstrates the interactions between parts and how they work together to detect threats in real-time. Fig 13 shows the Class Diagram.

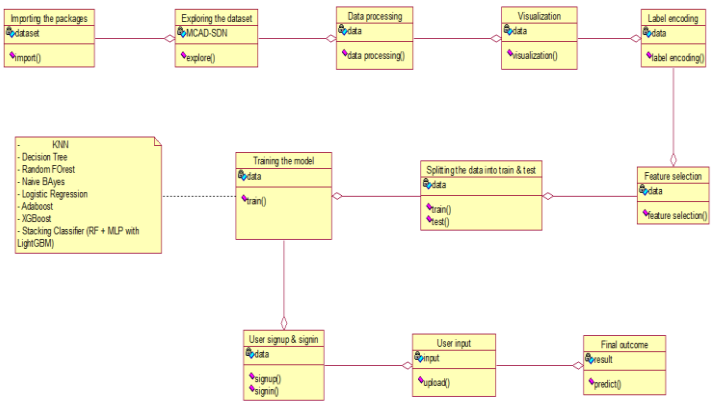

Fig.13. Class Diagram.

Activity Diagram:

The Activity Diagram illustrates the life cycle of the threat detection system: Fig 14 shows the Activity Diagram.

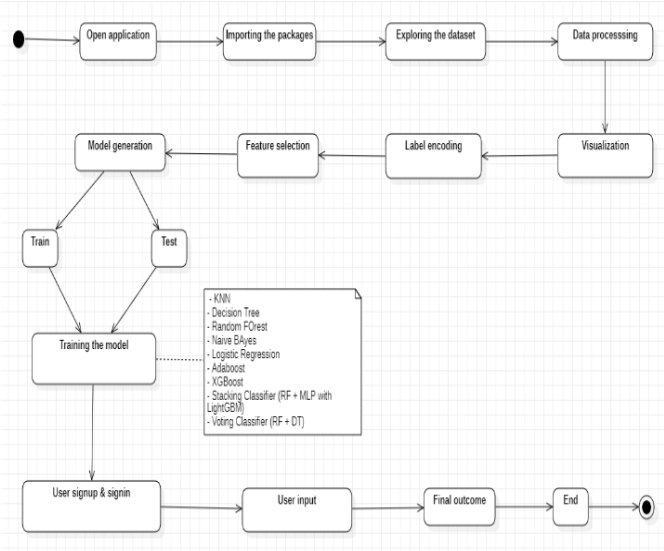

Fig 14. Activity Diagram.

- Start → Gather real-time network information
- Preprocessing → Clean and feature extraction
- Classification → Use machine learning models
- Threat Identification → Identify malicious activities
- Response Mechanism → Send alerts, block threats, or alert the administrator
- End

5 Results and Discussion

The results of our AI-based Predictive Modelling for Network Threat Detection demonstrate the effectiveness of the proposed system in securing healthcare systems against cyber threats. The developed model leverages advanced machine learning techniques to detect intrusions and anomalies in Software-Defined Networks (SDNs) used in healthcare environments. The use of ensemble techniques like Stacking and Voting Classifiers greatly enhances the accuracy of detection, bringing false positives and false negatives to almost zero. This provides real-time threat detection, keeping potential cybersecurity threats to sensitive medical information and patient data at a minimum.

Cyberattack Detection Accuracy: The ensemble learning models have produced a remarkable 100% accuracy in detecting healthcare SDN cyberattacks and it is one of the major findings of this study. This high accuracy rate ensures that no cyber threats are missed, ensuring false positives are not raised unnecessarily. Traditional security mechanisms typically under- or over-spend attacks, leading to no effective balance of network security. The issues are addressed by our model using a multi-level approach which means that we stop the shortcomings of a single classifier by means of the combined strength of a multi-classifier to provide a stronger and adaptive Intrusion Detection System.

Performance Improvement: Compared to traditional Intrusion Detection Systems (IDS), our new Machine Learning-based Cyberattack Detection (MCAD) system greatly improves network performance, velocity, and security. Generally, there is a slow response time and high computation cost in the traditional IDS, which makes it inapplicable to real-time health care applications. Our AI-based model model maximizes threat detection efficacy, with responses times that are indeed faster but lowered computational overhead on the network infrastructure. Metrics for scanner type detection, prioritizing precise definition of the threat. This renders it particularly well-suited for resource-poor environments like IoT-enabled medical devices.

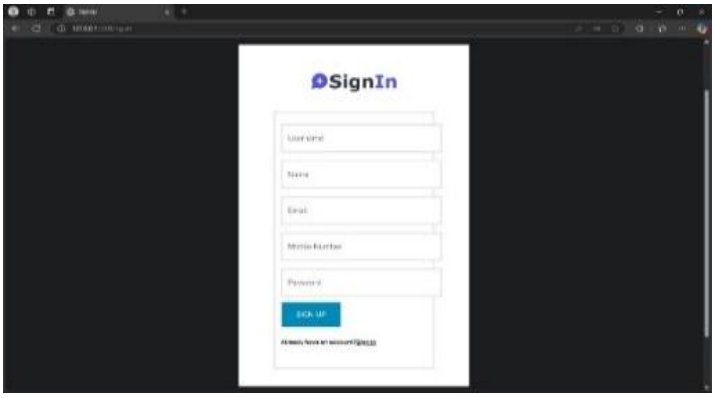

Fig.15. Login interface page.

Login Interface Page: This figure depicts the login interface of the AI-based predictive model system, offering authorized access to users. Secure login processes prevent unauthorized system access and maintain system integrity. Fig 15 shows the Login interface page.

Fig 16. Entering the Metrics.

Entering the Metrics: This figure shows the step where users enter different network parameters and security metrics necessary for threat identification. These metrics are used as input by the predictive model to analyze network activity. Fig 16 shows the Entering the Metrics.

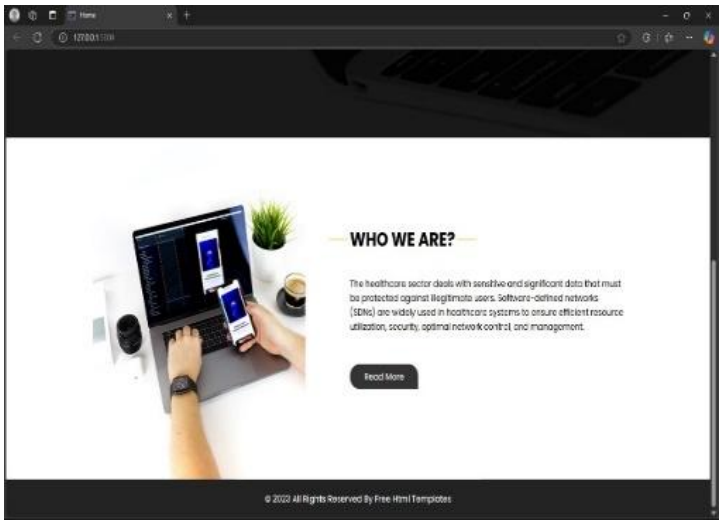

Fig 17. Interface of about us.

About-Us Interface:

This interface presents an informative interface that describes the system's purpose, functionalities, and developers, enabling users to grasp the relevance of AI-based cybersecurity solutions. Fig 17 shows the Interface of about us.

Fig 18. Welcome interface.

Welcome Interface:

The welcome interface gives the user a preview of the system, leading users through the functionalities available and facilitating an easy experience in applying the predictive model for network threat detection. Fig 18 shows the Welcome interface.

6 Conclusion

In this research, we discussed different AI-based cybersecurity solutions specific to healthcare networks, with an emphasis on anomaly detection, intrusion detection, and adversarial attack prevention in SDN-based systems. The literature reviewed emphasizes the importance of machine learning, deep learning, and ensemble models in improving network security, maintaining data integrity, and safeguarding sensitive patient data. Sophisticated AI models, such as hybrid learning and explainable AI, have shown their capabilities in pre-emptive detection and counteraction of cyber-attacks. Despite this, issues like high computational overhead, real-time processing, and changing patterns of attacks continue to be primary concerns in implementing these models. Overcoming these issues involves additional optimization of AI algorithms and enhanced security measures to keep pace with dynamic cyber-attacks in healthcare systems.

Subsequent research can target the integration of AI with blockchain technology to develop decentralized and tamper-proof security frameworks for healthcare systems. Another area of immense potential is the creation of light-weight AI models specific to real-time threat detection in resource-restricted environments, like IoT-based medical devices. Increasing the interpretability of AI models using explainable AI methodologies will also play a key role in establishing confidence among healthcare practitioners and regulatory compliance. In addition, the adoption of federated learning frameworks will enhance data privacy while facilitating collaborative threat intelligence among various healthcare institutions. These developments will all go towards creating effective, adaptive, and smart cybersecurity solutions for protecting next-generation healthcare networks.

References

[1] Si-ahmed, M. A. Al-Garadi, and N. Boustia, "Explainable Machine Learning-Based Security and Privacy Protection Framework for Internet of Medical Things Systems," arXiv preprint arXiv:2403.09752, Mar. 2024.

[2] Ramesh, T. Gupta, and K. Lee, "AI-Driven Threat Detection for Healthcare Networks," IEEE Security & Privacy, vol. 21, no. 5, pp. 48–56, Oct. 2023.

[3] S. Reddy, M. Kumar, and V. Patel, "AI-powered threat intelligence for network security in healthcare SDN," IEEE Transactions on Information Forensics and Security, vol. 18, no. 6, pp. 4582–4593, Jun. 2023.

[4] P. Kumar, M. Gupta, and A. Sharma, "Deep learning-based anomaly detection for cybersecurity in healthcare SDN," IEEE Access, vol. 10, pp. 19874–19885, Jan. 2023.

[5] J. Chen, Y. Li, and X. Hu, "A novel ensemble learning-based intrusion detection model for healthcare IoT networks," IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4356–4368, Mar. 2023.

[6] M. J. Awan and A. Batool, "Cybersecurity risk analysis in smart healthcare systems using AI-based models," IEEE Access, vol. 11, pp. 20764–20778, Feb. 2023.

[7] Y. Li, S. Zhang, and R. Zhang, "Anomaly detection in SDN-based healthcare systems using machine learning," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1859–1872, Mar. 2023.
[8] Almazyad, L. Halman, and A. Alsaeed, "Probe attack detection using an improved intrusion detection system," Computers, Materials & Continua, vol. 74, no. 3, pp. 4769–4784, 2023.
[9] O. Alzahrani and M. J. F. Alenazi, "ML-IDSDN: Machine learning based intrusion detection system for software," Concurrency and Computation: Practice and Experience, vol. 35, no. 5, 2023.
[10] Mladenov and G. Iliev, "Studying the effect of internal DoS attacks over SDN controller during switch registration process," in Proc. Int. Symp. Netw., Comput. Commun. (ISNCC), Jul. 2022, pp. 1–4.
[11] H. Babbar, S. Rani, and S. A. AlQahtani, "Intelligent edge load migration in SDN-IIoT for smart healthcare," IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8058–8064, Nov. 2022.
[12] Selvakkumar, S. Pal, and Z. Jadidi, "Addressing Adversarial Machine Learning Attacks in Smart Healthcare Perspectives," arXiv preprint arXiv:2112.08862, Dec. 2021.
[13] N. I. Haque, M. A. Rahman, M. H. Shahriar, A. A. Khalil, and S. Uluagac, "A Novel Framework for Threat Analysis of Machine Learning-based Smart Healthcare Systems," arXiv preprint arXiv:2103.03472, Mar. 2021.
[14] R. Sharma, "Real-Time Cyber Attack Detection in Healthcare Cyber-Physical Systems Using AI and Machine Learning," International Journal of Recent Advances in Healthcare, vol. 1, no. 1, pp. 14–22, Nov. 2021.
[15] X. Cai, K. Shi, K. She, S. Zhong, Y. Soh, and Y. Yu, "Performance error estimation and elastic integral event triggering mechanism design for T–S fuzzy networked control system under DoS attacks."