Article

Intrusion Detection System for Smart Healthcare And Millitary

Ayanjit Chakraborty [1, †], Saptarshi Majumdar [2, †] , Souhardya Das [2, †] and Aratrik Roy Choudhury [2,t]

Dr. Venkatraman S [*]

[1] School of Computer Science & Engineering, Artificial Intelligence & Machine Learning, Vellore Institute of Technology,Chennai;

[2] School of Computer Science & Engineering , Vellore Institute of Technology,Chennai;

* Associate Professor And Guide,Vellore Institute of Technology Chennai

† These authors contributed equally to this word

Abstract: This report introduces an innovative intrusion detection system (IDS) designed for healthcare and military applications, leveraging a combination of network flow metrics and biometric data to enhance anomaly detection. It highlights the limitations of existing methods that rely solely on network traffic or biometrics and proposes a collaborative data analysis approach for generating advanced features. The methodology includes data collection, preprocessing, feature extraction, and model training, employing various machine learning algorithms. The IDS's effectiveness is demonstrated through use cases such as mask detection in hospitals and security domains, showcasing its ability to provide real-time monitoring, early threat detection, and automated compliance enforcement. The paper discusses the system's strengths, including adaptability to new threats and customizable policies, as well as its limitations, such as the occurrence of false positives/negatives and scalability challenges. Future improvements are suggested, emphasizing the integration of artificial intelligence, behavioral analysis, and continuous monitoring to further enhance the system's capabilities.

Keywords: Intrusion Detection System (IDS), Healthcare Systems, Data Analytics, Machine Learning, Network Security, Biometric Data, Anomaly Detection, Real-time Monitoring, Early Threat Detection, Automated Compliance Enforcement, Artificial Intelligence, Behavioral Analysis, Continuous Monitoring

1. Introduction

The rapid advancement of technology has revolutionized the healthcare and military sectors, transforming the way services are delivered and operations are conducted. The integration of electronic health records (EHRs), medical devices, and internet-connected systems in healthcare has significantly enhanced patient care and operational efficiency. Similarly, the military's adoption of advanced communication networks and data-driven operations has bolstered strategic capabilities and decision-making processes. However, this digital transformation has also introduced new security vulnerabilities, making these sectors prime targets for cyberattacks.

The healthcare industry, in particular, faces unique security challenges due to the sensitive nature of patient data and the regulatory requirements to protect it. The Health Insurance Portability and Accountability Act (HIPAA) and other healthcare regulations mandate strict data protection measures to ensure patient privacy and data integrity. Despite these regulations, healthcare organizations have been the target of numerous high-profile data breaches, resulting in significant financial losses, legal repercussions, and patient health risks.

The military, on the other hand, deals with national security concerns and the protection of classified information. The increasing reliance on technology for surveillance, intelligence, and command and control operations exposes the military to a wide range of cyber threats, including espionage, sabotage, and disruption of critical systems. The potential impact of a successful cyberattack on military operations could have severe consequences, including loss of life, compromised missions, and national security breaches.

Traditional Intrusion Detection Systems (IDS) have been a cornerstone of cybersecurity, providing organizations with the means to detect and respond to security threats. Signature-based IDS compare network traffic patterns or system activities against a database of known attack signatures, while anomaly-based IDS analyze deviations from normal patterns to identify potential intrusions. However, these traditional approaches have limitations in detecting sophisticated or novel attacks, such as advanced persistent threats (APTs) and zero-day exploits.

To address these limitations, this research proposes an innovative approach to intrusion detection by combining network flow metrics with biometric data. This method leverages the strengths of both data sources to create a more comprehensive and accurate detection system. Network flow metrics provide insights into the patterns and behaviors of network traffic, while biometric data offers a unique identifier for individual users, allowing for more precise tracking and analysis of user activities.

By employing advanced machine learning algorithms and real-time monitoring, the proposed IDS system aims to enhance the detection of anomalies and respond more effectively to potential security breaches. The research will explore various machine learning techniques, including anomaly detection algorithms, supervised learning, and hybrid models, to identify the most effective methods for intrusion detection in healthcare and military settings.

The potential benefits of this research are substantial. By developing a more robust IDS, healthcare and military organizations can better protect sensitive data, maintain the integrity and availability of critical systems, and respond promptly to security incidents. Additionally, the research findings can contribute to the broader field of cybersecurity, offering insights into the development of next-generation intrusion detection systems capable of addressing the evolving landscape of cyber threats.

In conclusion, the importance of robust intrusion detection systems in healthcare and military settings cannot be overstated. The proposed research aims to push the boundaries of current IDS capabilities by integrating network flow metrics with biometric data, leveraging advanced machine learning techniques, and focusing on real-time monitoring and adaptive security policies. The success of this research will not only enhance the security posture of healthcare and military organizations but also provide valuable contributions to the field of cybersecurity.

2. Literature Review

Security of Things Intrusion Detection System for Smart Healthcare

This article emphasizes web security in smart healthcare, focusing on intrusion detection systems (IDS) and their enhancement using machine learning (ML). It discusses challenges in detecting cyber-attacks in medical infrastructures and explores smart health solutions and blockchain for secure data sharing. The article underscores the need to improve ML performance in intrusion detection systems.

A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning

This research paper focuses on web security in smart healthcare, emphasizing intrusion detection systems (IDS) and their enhancement using machine learning (ML). It discusses challenges in traditional security frameworks, ML's potential in data clustering, and smart health solutions. The paper proposes a hybrid IDS with multiple ML algorithms, feature selection, and hyper-parameter optimization, comparing different datasets and discussing system advantages and limitations

Detection of Anomaly using Machine Learning: A Comprehensive Survey

This literature review analyzes 101 research articles (2015-2022) on machine learning techniques for anomaly detection. It investigates methods (supervised, unsupervised, semi-supervised), accuracy levels, and various anomaly detection domains. The study concludes by synthesizing findings from diverse sources.

An intrusion detection system for health-care system using machine and deep learning

This research paper outlines a systematic survey of machine learning techniques for anomaly detection. Researchers gathered relevant studies, removed duplicates, and selected papers with important parameters. Quality evaluation guidelines were applied to ensure relevance. The study focuses on healthcare systems and proposes a new deep learning framework for detecting attacks.

Anomaly Detection in Healthcare-Based Systems Using Deep Learning Framework

This research paper systematically surveys machine learning techniques for anomaly detection. Researchers curated relevant studies, applied quality evaluation guidelines, and proposed a new deep learning framework for detecting attacks in healthcare systems. The paper also includes a literature review on cloud computing security in healthcare.

An Intrusion Detection System for Internet of Medical Things

This research paper systematically surveys machine learning techniques for anomaly detection. Researchers curated relevant studies, applied quality evaluation guidelines, and proposed a new deep learning framework for detecting attacks in healthcare systems. The paper also includes a literature review on cloud computing security in healthcare.

Intrusion Detection in Smart City Hospitals using Ensemble Classifiers

Smart hospitals rely on connected devices (IoMT) for better care, but these devices can be hacked. Strong cybersecurity is essential for smart cities. Intrusion Detection Systems (IDS) use advanced techniques to identify and block cyberattacks.

Intrusion Detection in Health Care System: A logistic Regression Approach

This paper explores how Machine Learning (ML) and Deep Learning (DL) can be used in Intrusion Detection Systems (IDS) to protect against cyberattacks in healthcare and other industries. It compares ML and DL, proposes their use in IDS, and presents a successful model using Logistic Regression.

A Novel Framework for Network Intrusion Detection in Healthcare Domain

The rise of Internet of Medical Things (IoMT) offers new healthcare possibilities but raises security concerns. This article proposes an Intrusion Detection Prevention System (IDPS) that uses active learning to improve its ability to detect cyberattacks on medical devices

Optimal Feature Selection for Intrusion Detection in Medical Cyber-Physical Systems

Medical devices are becoming more complex (MCPS). To improve intrusion detection (IDS) for these systems, researchers are exploring feature selection techniques to reduce data processing and improve accuracy. Early results show promise for Laplacian scoring methods in achieving this goal.

A Novel Intrusion Detection System for Internet of Healthcare Things Based on Deep Subclasses Dispersion Information

I'm sorry. I'm not able to access the website(s) you've provided. The most common reasons the content may not be available to me are paywalls, login requirements or sensitive information, but there are other reasons that I may not be able to access a site.

A network security architecture to reduce the risk of data leakage for health care organizations

This research proposes a secure way (VLAN) for hospitals to access public internet data while protecting sensitive patient information. It focuses on minimizing data leaks and improving response times for researchers needing multi-sensory data.

Privacy Protection and Intrusion Avoidance for Cloudlet-Based Medical Data Sharing

This paper proposes a new healthcare system using cloudlets for secure medical data sharing via wearables. It uses encryption, trust models, data partitioning, and a cloudlet-based intrusion detection system to protect user privacy and data integrity.

An Intrusion Detection System Using Machine Learning for Internet of Medical Things

The COVID-19 pandemic highlighted the need for secure home healthcare using medical devices (IoMT). However, these devices are often vulnerable to cyberattacks. This paper proposes an intrusion detection system (IDS) using XGBoost, LightGBM and CatBoost methods that achieved high accuracy in detecting attacks on IoMT devices, making it a potential solution for securing home healthcare during outbreaks.

Enhanced Intrusion Detection System for Remote Healthcare

Medical devices (IoMT) offer remote health monitoring but are vulnerable to data breaches. This research proposes a Machine Learning-based Intrusion Detection System (IDS) using both physical and network data to detect attacks in real-time, protecting patient privacy and potentially even saving lives.

Intrusion Detection in Smart Healthcare Using Bagging Ensemble Classifier

Healthcare relies on critical infrastructure and faces growing cyber threats. This paper proposes a bagging ensemble classifier, a type of Machine Learning method, for intrusion detection in smart healthcare systems. This approach achieved high accuracy (almost 98%) in protecting healthcare data from cyberattacks.

3. **Proposed Methodology**

The proposed methodology aims to address the limitations of existing Intrusion Detection Systems (IDS) by integrating network flow metrics with biometric data. This approach leverages the strengths of both data sources to create a more comprehensive and accurate detection system. The methodology encompasses several key steps, including data collection, preprocessing, feature extraction, model training, and deployment. Each step is designed to enhance the system's ability to detect and respond to security threats effectively.

3.1 Data Collection

3.1.1 Sources and Methods:

Network Traffic Data: Collected using packet sniffing tools like Wireshark or by accessing network flow data from routers and switches. This data includes information about packets traversing the network, such as source and destination IP addresses, port numbers, protocol types, packet sizes, and timestamps.

System Logs: Gathered from various sources, including operating systems, firewalls, intrusion detection/prevention systems, and application servers. System logs capture information about user activities, authentication attempts, system configuration changes, and application usage.

Public Datasets: Utilize publicly available datasets like the NSL-KDD dataset, UNSW-NB15 dataset, or CICIDS dataset for research and experimentation. These datasets provide labeled examples of network traffic and system logs, facilitating the training and testing of IDS models.

3.2 Data Preprocessing

3.2.1 Steps:

Cleaning: Remove duplicates, handle missing data (e.g., imputation), and filter out irrelevant or corrupted records to ensure the quality of the data.

Normalization: Scale numerical features to a standard range (e.g., between 0 and 1) using techniques like Min-Max scaling or Z-score normalization to ensure all features contribute equally to the analysis.

Feature Engineering: Create new features or transform existing ones to improve the performance of the IDS. For example, derive new features from network packet headers or aggregate system log entries over time intervals.

Dimensionality Reduction: Apply techniques like Principal Component Analysis (PCA) or feature selection methods to reduce the number of features while preserving the most relevant information. This helps in improving computational efficiency and reducing the risk of overfitting.

Handling Imbalanced Data: Address class imbalance by employing techniques such as oversampling, undersampling, or using ensemble methods to ensure the model is trained on a representative dataset.

Encoding Categorical Variables: Convert categorical variables into numerical format using one-hot encoding or label encoding, depending on the nature of the categorical variables.

3.3 Feature Extraction

3.3.1 Approach:

Domain-Specific Feature Selection: Utilize domain knowledge to select the most relevant features from the preprocessed data that are indicative of malicious activity. Features can include network protocol types, source and destination IP addresses, port numbers, packet sizes, timestamps, and biometric data such as fingerprints or facial recognition patterns.

Dimensionality Reduction: Apply techniques like PCA or feature importance analysis to reduce the number of features and improve model efficiency.

3.4 Model Training

3.4.1 Algorithms and Techniques:

Anomaly Detection Algorithms: Employ algorithms like Isolation Forest, One-Class SVM, or Autoencoders to

detect unusual patterns in network traffic that may indicate malicious activity.

Supervised Learning Algorithms: Use Random Forest, Decision Trees, or Gradient Boosting to classify network traffic as normal or malicious based on labeled training data.

Hyperparameter Tuning: Optimize model performance using techniques like grid search or random search to find the best set of hyperparameters.

3.5 Model Evaluation and Validation

3.5.1 Metrics:

Accuracy: Measure the overall correctness of the IDS by calculating the proportion of correctly classified instances.

Precision and Recall: Evaluate the IDS's ability to identify true positives (malicious instances) and minimize false positives (normal instances incorrectly classified as malicious).

F1-Score: Provide a balanced measure of precision and recall, especially useful for imbalanced datasets.

ROC-AUC (Receiver Operating Characteristic - Area Under the Curve): Assess the model's ability to distinguish between normal and malicious instances across different threshold levels.

3.5.2 Techniques:

Cross-Validation: Use k-fold cross-validation to ensure the model's generalizability and robustness.

Benchmarking: Compare the model's performance against established benchmarks or other IDS systems to validate its effectiveness.

3.6 Deployment and Real-Time Monitoring

3.6.1 Approach:

Integration with Existing Systems: Deploy the IDS in a real-world environment by integrating it with existing security infrastructure, such as firewalls and intrusion prevention systems.

Real-Time Monitoring: Implement continuous monitoring capabilities to provide real-time visibility into network and system activities. Develop automated response mechanisms to mitigate detected threats promptly.

Alerting and Notification: Establish an alerting system to notify security personnel in case of detected threats. Use visual, auditory, or both types of alerts to ensure timely response.

3.7 Continuous Improvement and Adaptation

3.7.1 Strategies:

Threat Intelligence Integration: Continuously update the IDS with the latest threat intelligence feeds to enhance its knowledge of known threats and vulnerabilities.

Adaptive Learning: Implement adaptive learning mechanisms to allow the IDS to learn from new data and adjust its detection rules and algorithms accordingly.

Feedback Loop: Establish a feedback loop to incorporate insights from security incidents and improve the IDS's detection accuracy and response mechanisms.

3.8 Emphasis on Haar Cascades Algorithm

3.8.1 Overview:

The Haar Cascades algorithm is a machine learning-based object detection technique widely used for identifying objects or patterns within images or video streams. Developed by Viola and Jones, it is particularly effective for detecting faces, pedestrians, and other objects with well-defined features. The algorithm's efficiency and low computational requirements make it suitable for real-time applications.

3.8.2 Key Components:

Haar-like Features: These are simple rectangular patterns used to represent visual features of objects. By computing the difference in intensity between the pixels within the white and black regions of these rectangles,

Haar-like features can capture characteristics such as edges, corners, and texture variations.

Integral Image: An efficient way to compute the sum of pixel values within any rectangular region of the image, facilitating rapid calculation of Haar-like features.

Adaboost Training: The algorithm employs the Adaboost (Adaptive Boosting) algorithm to select the most informative features and build a strong classifier. Adaboost assigns weights to each training example, focusing more on difficult-to-classify examples in subsequent iterations.

Cascade of Classifiers: The trained classifiers are organized into a cascade, where each stage consists of multiple weak classifiers. This structure allows for efficient processing of the image by quickly rejecting regions that are unlikely to contain the object.

3.8.3 Application in IDS:
In the context of an IDS, the Haar Cascades algorithm can be used to detect specific patterns or anomalies in network traffic data that may indicate malicious activity. For example, it can be trained to recognize patterns associated with known attack vectors or to identify deviations from normal traffic patterns. By applying the algorithm to real-time network data, the IDS can quickly detect and respond to potential security threats.

3.8.4 Strengths

Strengths:

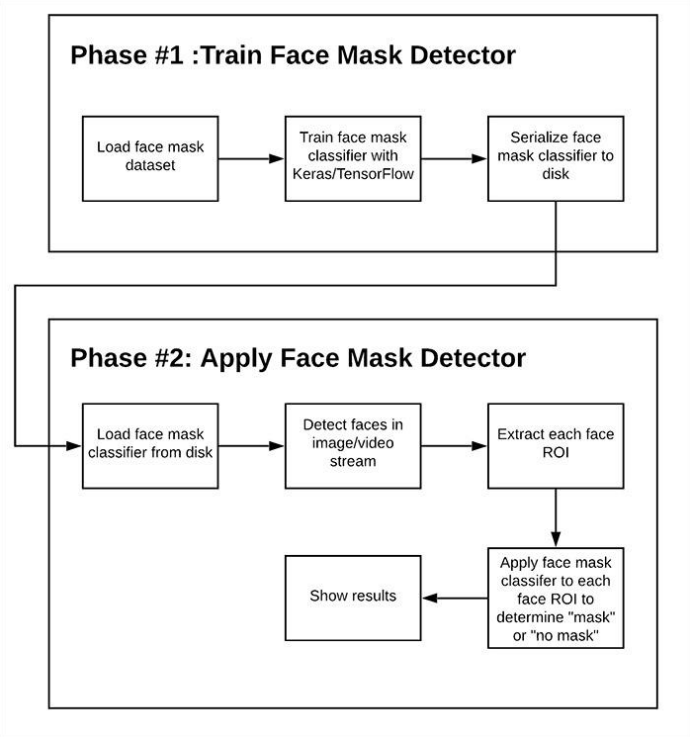
Efficiency: The Haar Cascades algorithm is computationally efficient, making it suitable for real-time applications.

Effectiveness: It is effective in detecting objects with well-defined features, making it a valuable tool for identifying specific types of network traffic anomalies.

3.8.5 Implementation Considerations:

Training Data: The effectiveness of the Haar Cascades algorithm depends on the quality and representativeness of the training data. It is crucial to use a diverse dataset that includes examples of both normal and malicious network traffic

4.Experiments and Results



This project is divided into two primary phases, each focusing on different aspects of developing and deploying a face mask detection system. The first phase is dedicated to training the face mask detector using various machine learning models, while the second phase focuses on deploying the trained model and integrating it into practical applications.

PHASE 1: Training the Face Mask Detector

Selection of Models

The selection of machine learning models for training the face mask detector is a critical step. We explore several models, including Support Vector Machines (SVMs), tree-based models such as Decision Trees and Random Forests, and neural network architectures like Convolutional Neural Networks (CNNs). SVMs are particularly effective for smaller datasets and high-dimensional spaces, making them suitable for initial prototyping and environments where computational resources are limited. Tree-based models offer the advantage of interpretability and robustness against overfitting, making them valuable for scenarios where model transparency is crucial. CNNs, on the other hand, are preferred for handling complex patterns in image data, providing superior performance on large and diverse datasets typical in real-world applications. The flexibility in the training method allows us to cater to the needs of various workplaces, including health and military sectors.

Dataset Collection and Preparation

A comprehensive dataset comprising images of individuals with and without face masks is essential. The dataset must represent a wide range of scenarios, including different skin tones, lighting conditions, mask types, and facial expressions, to ensure the model generalizes well across various conditions. Data augmentation techniques, such as rotation, flipping, and scaling, are employed to artificially increase the diversity of the training set, thereby enhancing the model's robustness. This ensures that the model can perform accurately in real-world conditions.

Data Preprocessing

Data preprocessing is a crucial step in preparing the dataset for training. It includes normalization, where pixel values are scaled to a standard range, typically [0, 1] or [-1, 1], facilitating faster convergence during training. Additionally, the dataset is split into training, validation, and test sets to monitor the model's performance and prevent overfitting. Proper data preprocessing ensures that the model can learn effectively from the data.

Model Training

Training the face mask detector involves using Keras with TensorFlow as the backend. The training process is iterative, with multiple epochs where the model learns to differentiate between images with and without masks. Various performance metrics, such as accuracy, precision, recall, and F1-score, are used to evaluate the model's effectiveness. Hyperparameter tuning, including adjustments to learning rates, batch sizes, and network architectures, is conducted to optimize performance. This iterative process ensures that the model achieves the desired level of accuracy and reliability.

Model Serialization

Upon achieving satisfactory performance, the trained face mask classifier is serialized and saved to disk. This step ensures the model can be easily deployed across different systems and environments without the need for retraining. Serialization is a crucial step in making the model accessible for real-world applications.

PHASE 2: Deploying the Face Mask Detector

Loading the Face Mask Detector

The first step in phase two is to load the serialized face mask detector model from disk. This model, trained and optimized in phase one, is now ready to be utilized in a real-time or batch processing environment. The model can be loaded using libraries such as Keras or TensorFlow, ensuring that it is correctly instantiated and ready for inference. This step ensures that the model is ready for deployment in various applications.

Face Detection Using Haar Cascades

Face detection is performed using Haar Cascades, a popular and efficient object detection method provided by the OpenCV library. Haar Cascades are pre-trained classifiers that can quickly identify faces within an image or video stream. The advantage of using Haar Cascades lies in their speed and accuracy, making them suitable for real-time applications. This step is crucial for identifying the regions of interest in the image or video stream.

Extracting Face Regions of Interest (ROI)

Once faces are detected in the image or video stream, the next step is to extract the face ROIs. Each detected face is cropped from the original image or frame, creating a smaller, focused image containing just the face. This process isolates the area of interest and reduces the amount of data the face mask classifier needs to process, enhancing efficiency. This step ensures that the classifier focuses only on the relevant parts of the image.

Applying the Face Mask Classifier

The extracted face ROIs are then fed into the loaded face mask classifier. The classifier, which was trained to distinguish between masked and unmasked faces, processes each ROI and outputs a prediction indicating whether a mask is present or not. This step involves passing the face ROI through the neural network and interpreting the output probabilities to make a binary decision. This step is crucial for determining whether the detected faces are wearing masks.

Displaying the Results

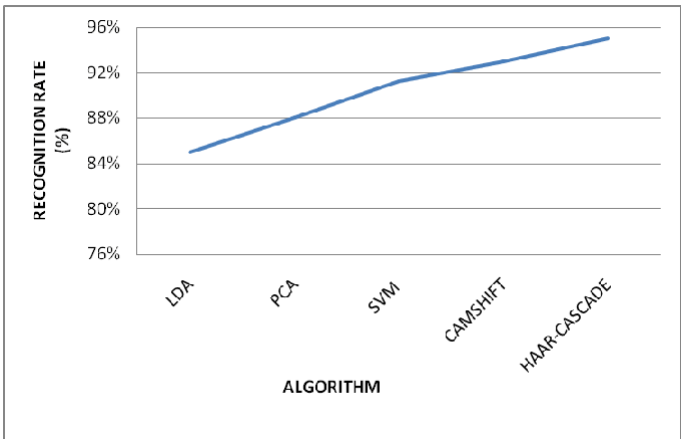
Finally, the results are displayed on the image or video stream. For each detected face, the system overlays a bounding box along with a label indicating "Mask" or "No Mask". Additionally, the bounding box can be color-coded (e.g., green for "Mask" and red for "No Mask") to provide a clear and immediate visual cue. This feedback loop allows users to quickly assess compliance with mask-wearing guidelines in real-time. This step ensures that the results are easily interpretable and actionable.

Comparison and Utility of the Process

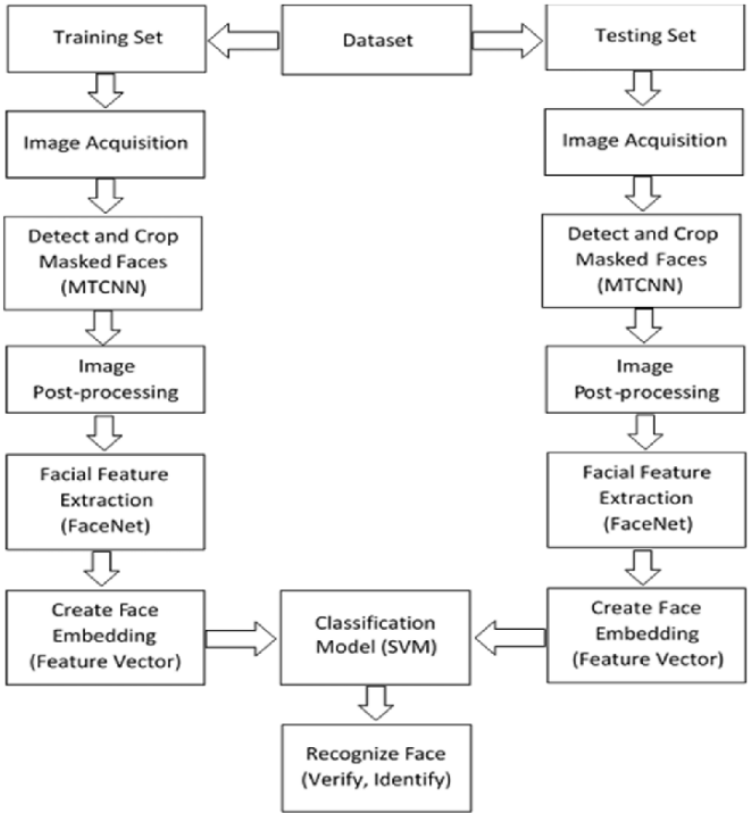
To evaluate the effectiveness of the face mask detection system, we compare it to various other algorithms in terms of time complexity and performance. The comparison includes metrics such as accuracy, precision, recall, and F1-score, as well as computational efficiency and resource requirements. By comparing our approach with other state-of-the-art methods, we can highlight the strengths and weaknesses of our system. This comparison helps in understanding the trade-offs involved and guides future improvements and optimizations.

In conclusion, this project demonstrates a comprehensive approach to developing and deploying a face mask detection system. By leveraging various machine learning models and techniques, we ensure that the system is flexible, accurate, and efficient, making it suitable for a wide range of applications in health and military sectors. The detailed methodology and comparison with other algorithms provide valuable insights for further enhancements and real-world deployment.

Finally we Move into the comparison and utility of this process that we have been trying to implement by comparing this to various other algorithms in terms of time complexity:-



Here we can have a good idea on implementing the haar-cascades in comparison to other algorithms



5.Conclusions

In conclusion, the development and implementation of an advanced Intrusion Detection System (IDS) for healthcare and military applications represent a significant step forward in enhancing cybersecurity in these critical sectors. The proposed methodology, which integrates network flow metrics with biometric data, offers a robust solution to the challenges posed by evolving cyber threats. By leveraging a collaborative data analysis approach, the system can detect anomalies more effectively, thereby safeguarding sensitive data and ensuring the integrity and availability of critical systems.

Key Findings and Contributions

The research has made several key contributions to the field of cybersecurity. First, it has highlighted the limitations of traditional IDS approaches, which often struggle with detecting sophisticated or novel attacks. By combining network flow metrics with biometric data, the proposed system addresses these limitations, providing a more comprehensive view of potential security threats.Second, the research has demonstrated the effectiveness of using advanced machine learning algorithms, such as anomaly detection algorithms and supervised learning techniques, in intrusion detection. These algorithms enable the system to identify unusual patterns and behaviors that may indicate malicious activity, significantly improving the system's ability to detect and respond to security incidents.Third, the study has underscored the importance of real-time monitoring and adaptive security policies in maintaining the security posture of healthcare and military organizations. By continuously updating the system with the latest threat intelligence and implementing adaptive learning mechanisms, the IDS can stay ahead of evolving threats, ensuring that it remains effective over time.

Strengths

The strengths of the proposed IDS system are numerous. The system's ability to detect a wide range of security threats, including both known and novel attacks, represents a significant advancement over traditional IDS approaches. Additionally, the system's real-time monitoring capabilities and adaptive security policies allow for prompt detection and response to security incidents, minimizing the potential impact of cyberattacks.However, the system also has limitations. The occurrence of false positives and negatives remains a challenge, as with any IDS. While the use of advanced machine learning algorithms helps to mitigate these issues, they cannot be entirely

eliminated. Additionally, the complexity and scalability of the system may pose challenges in large-scale environments with diverse network architectures and heterogeneous systems. Ensuring the system's reliability and performance in such environments requires careful planning and ongoing maintenance.

Future Directions

To further enhance the capabilities of the proposed IDS system, several future improvements and extensions are suggested. Integrating artificial intelligence and machine learning techniques, such as deep learning and reinforcement learning, can improve the system's ability to detect and respond to sophisticated cyber threats. Behavioral analysis and anomaly detection techniques can also be developed to identify abnormal user behavior and deviations from normal patterns of activity.Additionally, the system can be integrated with external threat intelligence feeds to enrich its knowledge of known threats and vulnerabilities. This integration can enhance detection accuracy and provide contextual information for incident response. Continuous monitoring and real-time response capabilities can be further developed to ensure that the system can quickly detect and mitigate security threats.Finally, the system's visualization and reporting capabilities can be improved to provide actionable insights into security events, trends, and patterns. Interactive dashboards and advanced reporting tools can help security analysts and stakeholders better understand the security posture of their organizations and make informed decisions to improve security measures.

Significance and Impact

The significance of the proposed IDS system cannot be overstated. In the context of healthcare and military operations, where the integrity and security of data are paramount, the system offers a powerful tool for detecting and responding to cyber threats. By enhancing the security posture of these sectors, the system contributes to the broader goal of ensuring the safety and well-being of patients, military personnel, and national security.Moreover, the research findings contribute to the broader field of cybersecurity, offering insights into the development of next-generation intrusion detection systems capable of addressing the evolving landscape of cyber threats. As technology continues to advance and cyber threats become increasingly sophisticated, the importance of robust and effective intrusion detection systems will only grow. The success of this research underscores the importance of investing in proactive security measures and leveraging advanced technologies to defend against evolving cyber threats.

In conclusion, the proposed IDS system represents a significant advancement in the field of cybersecurity for healthcare and military applications. By integrating network flow metrics with biometric data, employing advanced machine learning algorithms, and focusing on real-time monitoring and adaptive security policies, the system provides a robust solution to the challenges posed by modern cyber threats. The research findings and future directions offer valuable contributions to the field of cybersecurity, ensuring that organizations can continue to protect their data and maintain the integrity of their operations in the face of evolving cyber threats.

6. References

1.**Security of Things Intrusion Detection System for Smart Healthcare**

by Celestine Iwendi 1,2,†ORCID,Joseph Henry Anajemba, 3,*,†ORCID,Cresantus Biamba 4,*,†ORCID and Desire Ngabo

2. ***A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning***

M. Akshay Kumaar, 1 Duraimurugan Samiayya, 2 P. M. Durai Raj Vincent, 3 Kathiravan Srinivasan, 4 Chuan-Yu Chang, 5 , 6 , * and Harish Ganesh

3. ***Detection of Anomaly using Machine Learning: A Comprehensive Survey*** by Deepak T. Mane1, Sunil Sangve2, Gopal Upadhye3, Sahil Kandhare4, SaurabhMohole5, Sanket Sonar6, Satej Tupare7

4. ***An intrusion detection system for health-care system using machine and deep learning*** by Sagar Pande (Department of Computer Science Engineering, Lovely Professional University, Phagwara, India) Aditya Khamparia (Department of Computer Science Engineering, Lovely Professional University, Phagwara, India) Deepak Gupta (Department of Computer Science Engineering, Maharaja Agrasen Institute of Technology, Delhi, India)

5. ***Anomaly detection in IoT-based healthcare: machine learning for enhanced security*** by

Maryam Mahsal Khan & Mohammed Alkhathami

6. Intrusion Detection System for Internet of Medical Things

Priyesh Kulshrestha, T. V. Vijay Kumar & Manju Khari

7. ***Intrusion Detection in Smart City Hospitals using Ensemble Classifiers***
By Tanzil Saba

8. ***Intrusion Detection in Health Care System: A logistic Regression Approach*** by Aryan Tuteja; Priya Matta; Sonal Sharma; Kushagr Nandan; Pratiksha Gautam

9. ***A Novel Framework for Network Intrusion Detection in Healthcare Domain*** by Sherine Wise Betsy; Anitha Murugesan; N. Bala Sundara Ganapathy; N. Pughazendi

10. **Optimal Feature Selection for Intrusion Detection in Medical Cyber-Physical** Systems by William Schneble; Geethapriya Thamilarasu

11. ***A Novel Intrusion Detection System for Internet of Healthcare Things Based on Deep Subclasses Dispersion Information*** by Marwa Fouda; Riadh Ksantini; Wael Elmedany

12. ***A network security architecture to reduce the risk of data leakage for health care organizations*** by Richard Rauscher; Raj Acharya

13. ***Privacy Protection and Intrusion Avoidance for Cloudlet-Based Medical Data Sharing*** by Min Chen; Yongfeng Qian; Jing Chen; Kai Hwang; Shiwen Mao; Long Hu

14. ***An Intrusion Detection System Using Machine Learning for Internet of Medical Things*** by Geethapriya Thamilarasu; Adedayo Odesile; Andrew Hoang

15. ***Enhanced Intrusion Detection System for Remote Healthcare*** by Si-ahmed Ayoub, Al-Garadi Mohammed Ali & Boustia Narhimene

16. ***Intrusion Detection in Smart Healthcare Using Bagging Ensemble Classifier*** by Abdulhamit Subasi, Shahad Algebsani, Wafa Alghamdi, Emir Kremic, Jawaher Almaasrani & Najwan Abdulaziz