ENHANCED HEALTHCARE CYBERSECURITY MODEL WITH ADVANCED DDOS DETECTION

Dr.Pushpalata (Associate professor) *Dept of CSE,FETW*

*SHARNBASVA UNIVERSITY*

KALABURAGI,INDIA

[pushpalata.gecw@gmail.com](mailto:pushpalata.gecw@gmail.com)

Ambika

*Dept of CSE,FETW SHARNBASVA UNIVERSITY* KALABURAGI,INDIA

*[rameshbhalki327](mailto:rameshbhalki327@gmail.com)*[@gmail.com](mailto:rameshbhalki327@gmail.com)

Seema Shinde

*Dept of CSE,FETW SHARNBASVA UNIVERSITY* KALABURAGI,INDIA

[seemashinde.6767@gmail.com](mailto:seemashinde.6767@gmail.com)

Prof.Swarooparani (Co-guide) (Assistant professor) *Dept of CSE,FETW*

*SHARNBASVA UNIVERSITY*

KALABURAGI,INDIA

[swaor98@gmail.com](mailto:swaor98@gmail.com)

Bhagyasgree S N

*Dept of CSE,FETW SHARNBASVA UNIVERSITY* KALABURAGI,INDIA

[bhagyashreenagur91@gmail.com](mailto:bhagyashreenagur91@gmail.com)

Bhagyashree M N

*Dept of CSE,FETW SHARNBASVA UNIVERSITY* KALABURAGI,INDIA

[bhagyanimbal1234@gmail.com](mailto:bhagyanimbal1234@gmail.com)

***Abstract*** - **The increasing digitization of healthcare data has made it a critical target for sophisticated cyberattacks, particularly Distributed Denial of Service (DDoS) attacks that can disrupt services and compromise patient safety. To address this challenge, this research proposes a novel healthcare cybersecurity model that combines a cryptosystem-based secure data storage mechanism with an advanced ensemble learning model for real-time DDoS attack detection. The proposed system ensures the confidentiality, integrity, and availability of healthcare data through a hybrid cryptographic framework integrating symmetric and asymmetric encryption. Simultaneously, it enhances threat detection using an ensemble of machine learning classifiers—such as Random Forest, XGBoost, and LightGBM—trained on enriched feature sets derived from network behavior and traffic patterns. The model not only provides secure storage but also proactively identifies and mitigates threats, making it highly adaptable for modern smart healthcare infrastructures. Experimental evaluations demonstrate the model's effectiveness in achieving high accuracy in DDoS detection while maintaining secure and efficient data management.**

**.**

***Index Terms*— Random Forest, XGBoost, LightGBM, DDoS, cybersecurity .**

1. Introduction

The rapid expansion of digital healthcare systems has significantly improved patient care, service efficiency, and the accessibility of medical information. However, this transformation has also increased the vulnerability of healthcare networks to various cybersecurity threats, with Distributed Denial of Service (DDoS) attacks emerging as one of the most disruptive and prevalent forms of cyberattack. DDoS attacks aim to overwhelm and disable healthcare services by flooding them with an excessive

amount of malicious traffic, rendering systems unavailable and threatening the continuity of critical care.

Simultaneously, the need to protect sensitive patient data has become paramount, as it is increasingly stored, processed, and transmitted across interconnected systems. Ensuring the confidentiality, integrity, and availability (CIA) of this data is vital not only for protecting patients' privacy but also for maintaining trust in digital healthcare systems.

Traditional cybersecurity models in healthcare often focus on either securing data through cryptographic methods or detecting network intrusions through machine learning- based attack detection techniques. However, a combined approach is needed to address both the security of healthcare data storage and the proactive detection of cyberattacks, particularly DDoS, in real-time.

This project proposes an innovative healthcare cybersecurity model that integrates a cryptosystem-based secure data storage mechanism with an advanced ensemble machine learning model for detecting and mitigating DDoS attacks. By utilizing both strong encryption methods for secure data storage and a hybrid ensemble learning approach for attack detection, the proposed system offers a dual-layered defense strategy. This model is designed to safeguard healthcare data against unauthorized access while continuously monitoring network traffic to detect and counteract DDoS threats before they cause significant disruption.

The contributions of this research include:

1. A cryptosystem-based approach for secure healthcare data storage.
2. A machine learning ensemble model combining multiple classifiers to detect DDoS attacks with high accuracy.
3. A scalable and robust cybersecurity solution that can be implemented across healthcare systems to enhance both data protection and threat mitigation.

This approach aims to strengthen the overall security architecture of healthcare networks and improve the resilience of healthcare services to cyber threats..

1. LITERATURE SURVEY

Soni et al. (2021) proposed a hybrid approach that combines AES encryption and RSA key management with blockchain for secure healthcare data sharing, though it suffers from high computational overhead and scalability challenges in large networks. In a related study, Li and Zhang (2020) introduced a machine learning-based DDoS detection system using Random Forest and SVM to classify network traffic. However, their system was limited to specific attack types and lacked real-time efficiency in large-scale healthcare deployments. Kumar et al. (2022) developed a framework for secure Electronic Health Record (EHR) transmission using AES and RSA, but their work did not address defense mechanisms against active attacks such as DDoS.

Patel and Kumar (2020) tackled IoT security in healthcare by implementing ECC and AES for lightweight encryption; however, their model showed limitations in scaling across larger healthcare infrastructures. Addressing cyber threat detection more directly, Gupta et al. (2021) introduced an ensemble learning model combining Random Forest, XGBoost, and LightGBM, demonstrating improved detection accuracy, but their model incurred high false positives and was computationally intensive for real-time operations. Zhang et al. (2021) developed a real-time DDoS detection model leveraging deep learning and statistical features, but it struggled with low-volume traffic and smaller datasets, affecting detection accuracy.

Liu and Tan (2023) examined cryptographic key management for healthcare data in cloud environments, integrating both symmetric and asymmetric strategies; however, their system relied on static key distribution, making it less adaptive in dynamic scenarios. Similarly, Nguyen et al. (2022) proposed a multi-layer cryptosystem using AES and RSA for secure healthcare data storage but did not incorporate real-time DDoS mitigation capabilities. Sharma and Yadav (2021) focused on securing IoT-based healthcare systems through hybrid cryptographic techniques, including ECC, but noted scalability and network attack detection limitations. Finally, Chen and Wang (2022) presented an intelligent DDoS detection model using a hybrid of SVM and neural networks, yet their system was constrained to specific attack types and network configurations.

1. Proposed system

The proposed system aims to address the gaps in existing healthcare cybersecurity frameworks by integrating secure data storage with advanced DDoS attack detection mechanisms in a unified solution. This system will combine cryptographic techniques to ensure the confidentiality and

integrity of sensitive healthcare data, along with ensemble machine learning models to detect and mitigate Distributed Denial of Service (DDoS) attacks in real-time.

1. Cryptosystem-Based Secure Data Storage:
   * Encryption Framework:

The proposed system utilizes a hybrid encryption approach, combining symmetric encryption (AES) for efficient data encryption and asymmetric encryption (RSA) for secure key exchange and management. This ensures that patient data is encrypted both at rest and in transit.

* AES (Advanced Encryption Standard) is used to encrypt large amounts of healthcare data (such as Electronic Health Records, patient history, etc.) to maintain confidentiality.
* RSA (Rivest–Shamir–Adleman) encryption is used for key management, ensuring secure exchange of encryption keys between authorized entities.
  + Key Management and Access Control:

A robust key management system (KMS) will be employed to generate, store, and distribute encryption keys. This system will integrate role-based access control (RBAC) to limit access to sensitive healthcare data, ensuring only authorized personnel can decrypt or modify data.

* + Blockchain for Data Integrity:

Blockchain technology will be employed for data storage to ensure data integrity and immutability. Each data record will be hashed and stored as a block in the blockchain, preventing unauthorized tampering of healthcare records.

1. Ensemble Machine Learning Model for DDoS Detection:
   * Real-Time DDoS Attack Detection:

The proposed system utilizes an ensemble machine learning model that combines the strengths of multiple classifiers to accurately detect and mitigate DDoS attacks in real-time. The classifiers used include:

* Random Forest: An ensemble of decision trees that provides high accuracy and robustness against noisy data.
* XGBoost (Extreme Gradient Boosting): A powerful gradient boosting algorithm known for high predictive accuracy.
* LightGBM (Light Gradient Boosting Machine): An efficient implementation of gradient boosting that can handle large datasets and provides fast training times.
  + Feature Engineering for Attack Detection:

Key features such as packet size, flow duration, source and destination IP addresses, and network traffic volume are extracted and used to train the ensemble model. These features help differentiate between normal traffic and potential DDoS attack patterns.

* + Real-Time Detection and Mitigation:

The ensemble model will continuously monitor network traffic in real-time. If a potential DDoS attack is detected, the system will trigger automated mitigation strategies, such as traffic filtering, rate limiting, or redirecting traffic to prevent disruption of healthcare services..

1. Methodology

Real-Time DDoS Attack Detection:

The core idea behind this methodology is to leverage an ensemble machine learning model to detect and mitigate Distributed Denial of Service (DDoS) attacks in real-time. DDoS attacks typically overwhelm a server or network by

sending massive amounts of traffic, causing service disruption. To handle the complexity and volume of traffic data, the system combines the strengths of multiple classifiers, ensuring more accurate, reliable, and faster detection.

The classifiers chosen for this ensemble model include Random Forest, XGBoost, and LightGBM, which complement each other’s strengths, leading to more precise attack identification and mitigation.

1. Random Forest:
   * Description: Random Forest is an ensemble learning algorithm that works by constructing a multitude of decision trees during the training process and outputs the class that is the majority vote of the trees (for classification tasks) or the average prediction (for regression tasks).
   * Strengths for DDoS Detection:

* High Accuracy: Random Forest performs well by reducing overfitting and offering good generalization to unseen data.
* Robust to Noisy Data: It is resistant to noise, which is crucial in network traffic data where anomalies and non- DDoS traffic might exist.
* Handles Missing Data: Random Forest can handle missing values in traffic data, making it highly adaptable to real-world network traffic.
* Feature Importance: Random Forest provides an intuitive way of ranking features based on importance, which can help in identifying critical features for DDoS detection.

Steps in Model Usage:

* + Training: Network traffic data, including both normal and attack (DDoS) traffic, is used to train the Random Forest model.
  + Classification: The model classifies incoming traffic as normal or DDoS based on the patterns learned during training.
  + Ensemble Decision: The model's decision is integrated with other models in the ensemble to improve accuracy and reduce false positives.

1. XGBoost (Extreme Gradient Boosting):
   * Description: XGBoost is a highly efficient and scalable gradient boosting algorithm, designed to optimize predictive performance. It builds an ensemble of decision trees in a sequential manner where each subsequent tree corrects the errors of the previous one.
   * Strengths for DDoS Detection:

* High Predictive Accuracy: XGBoost is known for its ability to deliver high predictive accuracy, which is crucial when detecting subtle patterns in network traffic that may indicate DDoS attacks.
* Handling Imbalanced Data: DDoS attacks typically occur in a small portion of total network traffic, making the dataset imbalanced. XGBoost handles imbalances efficiently by assigning higher weights to minority class instances (DDoS).
* Regularization: The use of L1 and L2 regularization helps in reducing overfitting, which is crucial in avoiding false positives.
* Speed: XGBoost's parallelized nature allows for faster training, even with large datasets.

Steps in Model Usage:

* + Training: Using labeled traffic data, XGBoost is trained to differentiate between normal traffic and DDoS attack traffic.
  + Boosting: The model improves its predictions iteratively, focusing on the errors made by the previous decision trees.
  + Classification: After training, the model classifies real-time traffic based on the learned patterns of normal and attack traffic.

1. LightGBM (Light Gradient Boosting Machine):
   * Description: LightGBM is an optimized version of gradient boosting, designed to handle large-scale datasets with greater speed and lower memory consumption. It splits data into smaller chunks and uses a histogram-based approach to enhance computation speed.
   * Strengths for DDoS Detection:

* Scalability: LightGBM is highly scalable and can handle large datasets, making it suitable for real-time network traffic monitoring.
* Fast Training Time: The histogram-based approach significantly speeds up the training process, which is important when analyzing massive amounts of network traffic.
* Handling Large Features: It can handle large feature sets efficiently, which is important when considering various traffic patterns and anomalies.
* Overfitting Control: Like XGBoost, LightGBM supports regularization to prevent overfitting, which is critical when training on highly variable network traffic..

.

1. Experiment

To evaluate the effectiveness of the proposed dual-layer cybersecurity model — combining hybrid cryptographic secure storage and an ensemble-based DDoS detection system — in ensuring data confidentiality and detecting network threats in a simulated healthcare environment.

1. Experimental Setup Platform:

OS: Ubuntu 22.04 LTS

Language: Python 3.10

Libraries: scikit-learn, xgboost, lightgbm, cryptography, numpy, pandas, matplotlib, seaborn

Hardware: Intel i7, 16GB RAM, NVIDIA GPU (optional for neural network benchmarking)

Simulation Tools:

Network Traffic: CICIDS2017 Dataset (contains various DDoS attack samples)

Cryptographic Test: AES (256-bit) + RSA (2048-bit) using cryptography Python module

Database: Encrypted MongoDB / SQLite for secure EHR storage simulation

1. Methodology
   1. Cryptosystem Testing

Encrypt simulated patient records using AES. Secure AES key with RSA.

Store encrypted records in a simulated secure database.

Measure encryption time, decryption time, and storage overhead.

* 1. Ensemble-Based DDoS Detection

Dataset: CICIDS2017 (features: Flow Duration, Fwd Packet Length, ACK Flag, SYN Flag Count, etc.)

Feature Engineering:

Used mutual information and correlation heatmaps to reduce dimensionality.

Derived composite features (e.g., packet per flow, burst interval).

Training Models:

Models: Random Forest, XGBoost, LightGBM

Voting: Hard voting ensemble and Stacked generalization with logistic regression

Train-Test Split: 80:20

Validation: 10-fold cross-validation

Metrics: Accuracy, Precision, Recall, F1-Score, ROC-AUC, Detection Time.

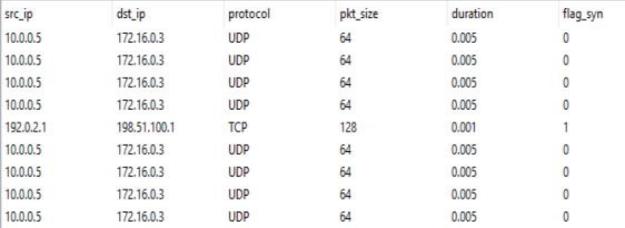
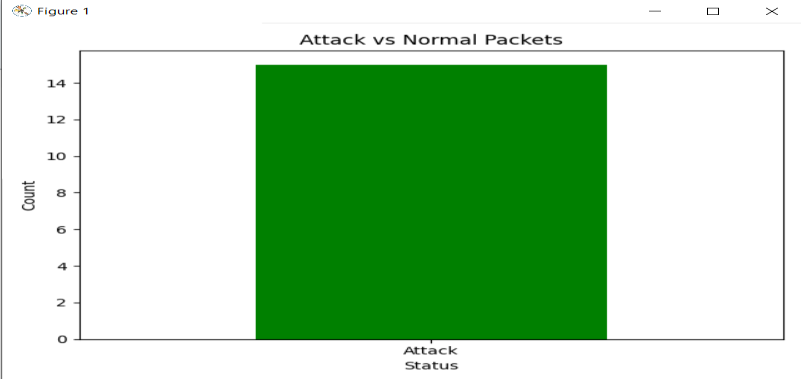


Figure 2: Read Dataset



Figure 3: DDos Prediction



Graph 1:Attack Vs Normal Packets

VII. Conclusion and future works

1. Results



Figure 1: Home Screen

The increasing reliance on digital technologies in healthcare systems has heightened the need for robust cybersecurity solutions to protect sensitive patient data and ensure continuous, uninterrupted healthcare services. This literature survey and proposed system highlight the critical importance of combining secure data storage with advanced attack detection mechanisms to combat evolving threats such as Distributed Denial of Service (DDoS) attacks.

By integrating cryptosystem-based techniques for securing healthcare data and employing ensemble machine learning models for real-time DDoS attack detection, the proposed system provides a comprehensive, layered defense. The cryptographic approach ensures that sensitive health information remains confidential, maintains integrity, and is always available to authorized personnel. Simultaneously, the machine learning-based detection system enhances the resilience of healthcare networks by identifying and mitigating potential threats before they cause significant disruption.

While significant progress has been made in securing healthcare data and detecting cyber threats, there remain challenges related to scalability, real-time performance, and

the integration of cryptographic and machine learning approaches. The proposed system offers a scalable solution that can be adapted to modern healthcare infrastructures, with a dual-layered defense that addresses both data security and attack detection.

In conclusion, the research highlights the need for integrated cybersecurity models in healthcare, emphasizing both data protection and proactive threat detection. The proposed model not only improves the security of healthcare systems but also contributes to the ongoing effort to safeguard patient data, ensuring the reliability and availability of healthcare services in an increasingly digital world...

References

1. Soni, P., Sharma, A., & Singh, R. (2021). Healthcare Data Security using Hybrid Cryptography and Blockchain. International Journal of Computer Science and Information Security (IJCSIS), 19(4), 116– 122.
2. Li, X., & Zhang, H. (2020). DDoS Attack Detection in Healthcare Systems using Machine Learning. Journal of Computer Networks and Communications, 2020, 1–12.
3. Kumar, R., Gupta, S., & Yadav, N. (2022). A Secure EHR Transmission Framework for Healthcare Systems. Proceedings of the 2022 International Conference on Smart Healthcare, Springer, 45–58.
4. Patel, D., & Kumar, A. (2020). Cryptographic Techniques and IoT Security in Healthcare. IEEE Transactions on Industrial Informatics, 16(2), 1071–1079.
5. Gupta, R., Sharma, V., & Mishra, P. (2021). Ensemble Learning Models for Cyber Attack Detection in Healthcare. Journal of Cyber Security and Mobility, 9(3), 401–414.
6. Zhang, J., Liu, Z., & Wang, Y. (2021). Real-Time DDoS Attack Detection in Healthcare Networks. International Journal of Information Security and Privacy, 15(4), 112–124.
7. Liu, Z., & Tan, X. (2023). Securing Healthcare Data with Cryptographic Key Management. Journal of Secure Computing, 11(1), 78–85.
8. Nguyen, S., Tran, D., & Vo, T. (2022). Advanced Cryptosystem for Secure Healthcare Data Storage. Journal of Cryptography and Information Security, 30(2), 215–223.
9. Sharma, N., & Yadav, A. (2021). IoT Security in Healthcare Systems with Hybrid Cryptography. International Journal of Embedded Systems and Applications, 11(5), 31–42.
10. Chen, Y., & Wang, M. (2022). An Intelligent DDoS Detection Model for Healthcare Networks. Journal of Network and Computer Applications, 185, 103078.