

# Machine Learning Enhanced Healthcare Cybersecurity Framework for Secure Medical Information Management

Dr. Neha Upadhyay

Assistant Professor, MANIT Bhopal

[nupadhyay@manit.ac.in](mailto:nupadhyay@manit.ac.in)

Corresponding Author: \*Dr Neha Upadhyay ([nupadhyay@manit.ac.in](mailto:nupadhyay@manit.ac.in))

Received: 18 July 2026 | Revised: 20 August, 2026 | Accepted: 3 September, 2026 |

**Abstract**—The increasing digitalization of healthcare, protecting sensitive patient information and healthcare systems has become a critical challenge. The confidential nature of medical data and the growing number of cyber threats highlight the need for advanced cybersecurity solutions. This research proposes a Healthcare Cybersecurity Framework using machine learning and deep learning methods to handle Medical Information securely and detect cyber-attacks effectively. The proposed framework makes use of the WUSTL-EHMS-2020 dataset and preprocessing techniques such as data cleaning, normalization, label encoding, and SMOTE-based sampling. The accuracy, precision, recall and F1-score are employed for the model development and evaluation in DNN and XGBoost. In terms of accuracy, precision, recall, and F1-score, the experimental findings show that the suggested DNN model reached 99.98%, while the XGBoost model reached 99.96%, PRE 99.91%, REC 99.95%, and F1-score 99.97%. The findings show that the suggested architecture successfully increases the ACC of threat detection and safeguards the medical data management process in terms of security.

**Keywords**—Healthcare cybersecurity, Internet-of-Medical-Things, Ransomware detection, Intrusion detection systems, Machine learning, Anomaly detection.

## I. INTRODUCTION

The healthcare industry has been greatly impacted by the fast development of digital technologies, which have improved the accessibility, efficiency, and quality of medical services. Digital health infrastructure, such as EHRs, HIX platforms, mobile apps, cloud services, and wearable medical devices, is becoming more and more important to contemporary healthcare systems [1][2][3]. These technologies provide for live patient monitoring, streamlined data management and better clinical decisions. The widespread adoption of interdependent digital systems has, however, raised concerns about the security, privacy, and integrity of sensitive healthcare data [4]. The protection of patient information and the provision of reliable healthcare services have emerged as critical issues for healthcare organizations across the globe [5][6].

The use of Internet of Things (IoT) and Internet of Medical Things (IoMT) has also added another dimension to healthcare capabilities, allowing for continuous monitoring [7]. Remote diagnosis, and intelligent medical assistance. The internet of things devices, like wearables, remote patient monitoring, and sophisticated diagnostic equipment, generate significant amounts of healthcare data that enable personalized and timely care for patients [8][9][10]. The growing connectivity among healthcare devices and networks has broadened the attack surface, making healthcare systems vulnerable to cyber threats like unauthorized access, data breaches, ransomware attacks, and information manipulation.

Failure to provide security can result in identity theft, loss of funds, privacy breaches and patient safety risks [11][12].

Healthcare organizations are at a high risk of cybersecurity threats because of the complexity of digital infrastructures, the continuous advancement of cyber threats, and the continuous expansion of medical data [13]. Digital infrastructures, continuous advancement of cyber threats, and continuous expansion of medical data pose significant cybersecurity challenges in the healthcare industry. Basic security measures like encryption, firewalls, authentication and access control methods are essential security, but are not sufficient to cope with the sophisticated and ongoing cyber-attacks [14][15]. Healthcare environments are dynamic and unpredictable, and demand intelligent and adaptive security solutions that can detect unknown attacks, suspicious activity and offer real-time protection. Thus, creating efficient cybersecurity system for secure use of medical information in management has become a very vital line of research [16].

ML and DL have attracted attention for the last few years as potential solutions to enhance healthcare cybersecurity, as it is possible to use intelligent analysis of large-scale and complex healthcare data[17]. ML and DL have gained traction in recent years for their potential to bolster healthcare cybersecurity by leveraging intelligent analysis of vast and intricate healthcare datasets [18]. When using ML and DL models, the dependence on attack signatures is not the only way to find hidden patterns, detect anomalies, classify cyber threats, predict potential security breaches, and automate

response mechanisms. These strategies enable adaptive and real-time threat detection, as well as strengthened security of electronic health records, IoMT networks, and healthcare information systems [19][20][21]. Hence, this study proposes ML and DL models that have the potential to improve cyber threat detection, reduce security risks, and protect sensitive healthcare information.

#### A. Motivation and Contribution

As digital healthcare systems grow more intricate, the safeguarding of sensitive medical data from evolving cyber threats has become a major challenge. Conventional security methods are not enough to identify complex and unknown attacks in dynamic healthcare environment. This encourages the development of an intelligent cybersecurity framework with ML and DL as techniques for accurate threat detection. The proposed method is designed to improve the security, privacy and reliability of data in modern healthcare information systems. The research has made several important contributions as mentioned below:

- A healthcare cybersecurity framework is suggested based on ML and DL models to safeguard the sensitive health data and to identify cyber threats.
- The dataset WUSTL-EHMS-2020 is utilized, effective preprocessing techniques are applied including data cleaning, encoding of data label, data normalization and data balancing by SMOTE to enhance model reliability.
- A models-based approach uses DNN and XGBoost models to improve cyber-attack detection in healthcare environments.
- ACC, PRE, REC, F1, and ROC curve metrics are used to perform a detailed performance evaluation.
- The proposed models prove to be more effective in terms of classification performance than the current methods, making them suitable for secure management of medical data and applications in healthcare cybersecurity.

#### B. Justification and Novelty

The study's justification lies in the growing cyber threats that healthcare systems face, necessitating robust solutions to safeguard valuable medical data and manage it securely. The proposed framework adopts a novel combination of preprocessing techniques and DNN and XGBoost models to enhance the ACC of cyber-attack detection. The approach effectively handles data imbalance and extracts valuable patterns from healthcare and network features. The experimental results demonstrate the novelty and effectiveness of the proposed framework for enhancing healthcare cybersecurity.

#### C. Organization of the Paper

The paper is organized as follows: Section II reviews related work, Section III introduces the dataset, the preprocessing and the model implementation, Section IV discusses the results of the experiments and the comparisons, and Section V concludes the study, drawing out the findings and suggesting future research directions.

## II. LITERATURE REVIEW

A detailed review of existing studies on the Secure Healthcare Cybersecurity Framework was performed to

support the development and enhancement of the proposed research framework.

Reddy Palavali et al. (2026) AI-based Claims Adjudication System using Transformer-based NLP, Ensemble ML and a Two-step Fraud Detection Pipeline. Structured claim attributes, provider behaviour, utilization, and clinical-text embeddings are used in the system to ensure adjudication that is accurate and transparent. The claim classification is done using a weighted XGBoost, Random Forest, and neural network ensemble, and the fraud detection is performed using hybrid unsupervised and supervised learning. Experimental results indicate that 94.7% of the classification ACC, 67% faster processing time, 37% better fraud detection rate has been achieved when compared with the rule-based systems [22].

Thapar et al. (2026) proposes a medical chatbot using ML and generative reasoning. The LLM independently makes a diagnosis, compares it with the ML predictions and asks medical questions for further diagnosis until it has reached a confident conclusion. The prototype obtains 96% ACC and 0.94 F1, which is better than single-source methods. The chatbot's reliability and responsible use are further strengthened by privacy protection frameworks and safety triggers [23].

Zhumabekova et al. (2025) reviews the application of ML and DL Models in Healthcare Cyber Security such as RF, XGBoost, CatBoost, AdaBoost, DNN, and Hybrid Model GRU-LSTM. Data cleaning, normalization, feature selection, class balancing, and model classification (ACC, PRE, REC and F1) are included in the methodology. RF achieved the highest ACC of 0.989, followed by XGBoost (0.982), CatBoost (0.974), GRU-LSTM (0.966), DNN (0.960), and AdaBoost (0.953), demonstrating the robustness and effectiveness of Random Forest [24].

Rao et al. (2025) suggests a novel method for predicting blood types from fingerprint patterns by utilizing cutting-edge ML systems. The pipeline unifies CNN, RF, and SVM for image preprocessing, feature extraction, and classification. An ACC of above 90% indicates that the CNN-based model outperforms conventional classifiers in experiments. The fields of emergency medicine, forensics, and blood donor matching might all benefit from this fast and non-invasive method. Its value is demonstrated by its incorporation into a user-friendly online application.[25].

Thinakaran (2025) aims to develop a secure healthcare IoT platform using DL and ML. The proposed two-layer security system provides mutual authentication between sink and source nodes and employs a lightweight game-theoretic intrusion detection system (G-IDS) for detecting RPL and conventional network threats. Compared with CNN, LSTM, and hybrid DNN models, G-IDS achieves 92.4% ACC, 96.8% detection ACC, 94.3% PRE, 95.6% REC, and an F1 of 0.95. It also reduces energy consumption by 21% and false positives by 3.2%, while detecting RPL-specific attacks, demonstrating robust and efficient protection for resource-constrained healthcare IoT environments [26].

ElSayed, Elsayed and Bay (2024) An ML-based architecture designed to address security vulnerabilities in healthcare IoT devices. Using an advanced convolutional ML architecture, the system proactively monitors and detects threats while protecting sensitive healthcare information, reducing cost, and improving portability for healthcare and

emergency environments. Experimental results achieve up to 93.6% attack prediction ACC, demonstrate zero-day detection using the CICIOT2023 dataset, and reduce costs by 10×, highlighting its effectiveness in strengthening secure healthcare IoT systems [27].

Daher (2023) investigate the most common dangers that endanger the private health information gathered by IoMT devices. Following an overview of the literature on medical IoT systems and reinforcement learning, they study a healthcare dataset and construct models that combine classical

ML techniques with deep reinforcement learning models trained using Q-learning to form various intrusion detection systems. With an ACC level of 92%, they ran comprehensive simulations utilizing the built models and compared the outcomes using various performance indicators [28].

Table I presents an overview of recent studies related to the Secure Healthcare Cybersecurity Framework, highlighting the proposed approaches, employed datasets, key outcomes, and identified challenges.

TABLE I. SUMMERY OF RECENT STUDIES ON SECURE HEALTHCARE INFORMATION MANAGEMENT IN CYBERSECURITY

| Author                        | Proposed Work                                                                    | Dataset                          | Results                                                              | Limitations & Future Work                                                                 |
|-------------------------------|----------------------------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Reddy Palavali et al. (2026)  | AI-based claims adjudication using NLP, ensemble ML, and fraud detection.        | Healthcare claims data           | 94.7% accuracy; 67% faster processing; 37% improved fraud detection. | Limited real-world validation; future work should improve scalability and explainability. |
| Thapar et al. (2026)          | ML and LLM-based medical chatbot with iterative diagnosis and safety mechanisms. | Medical/clinical data            | 96% accuracy; 0.94 F1-score.                                         | Requires broader clinical validation and stronger safety evaluation.                      |
| Zhumabekova et al. (2025)     | ML/DL-based healthcare cybersecurity threat classification.                      | Healthcare cybersecurity dataset | RF achieved 98.9% accuracy; XGBoost 98.2%.                           | Model generalization and real-time deployment require further investigation.              |
| Rao et al. (2025)             | CNN, RF, and SVM for fingerprint-based blood-type prediction.                    | Fingerprint images               | CNN achieved >90% accuracy.                                          | Limited application scope; requires larger and more diverse datasets.                     |
| Thinakaran (2025)             | Secure healthcare IoT using authentication and game-theoretic IDS.               | Healthcare IoT/RPL data          | 92.4% accuracy; 95.6% recall; F1-score 0.95.                         | Computational efficiency and deployment in large IoT networks need further study.         |
| ElSayed, Elsayed & Bay (2024) | ML-based architecture for healthcare IoT attack detection.                       | CICIOT2023                       | 93.6% attack prediction accuracy; 10× cost reduction.                | Further testing against evolving and complex zero-day attacks is required.                |
| Daher (2023)                  | ML and deep reinforcement learning for IoMT intrusion detection.                 | Healthcare dataset               | Accuracy exceeded 92%.                                               | Requires real-time validation and evaluation against diverse IoMT attacks.                |

**Research Gaps:** Previous research has explored the use of ML and DL for healthcare security, fraud detection, and intrusion detection, but many of the approaches struggle with issues of class imbalance, generalization, and accurate real-time threat detection. Current frameworks often focus on specific healthcare applications rather than providing a comprehensive solution for secure medical information

management. Hence, an integrated cybersecurity framework is required that integrates effective data preprocessing, balancing techniques, and advanced ML/DL models. This study aims to fill these gaps by creating a comprehensive framework for precise cyber-attack detection and improved healthcare data security.

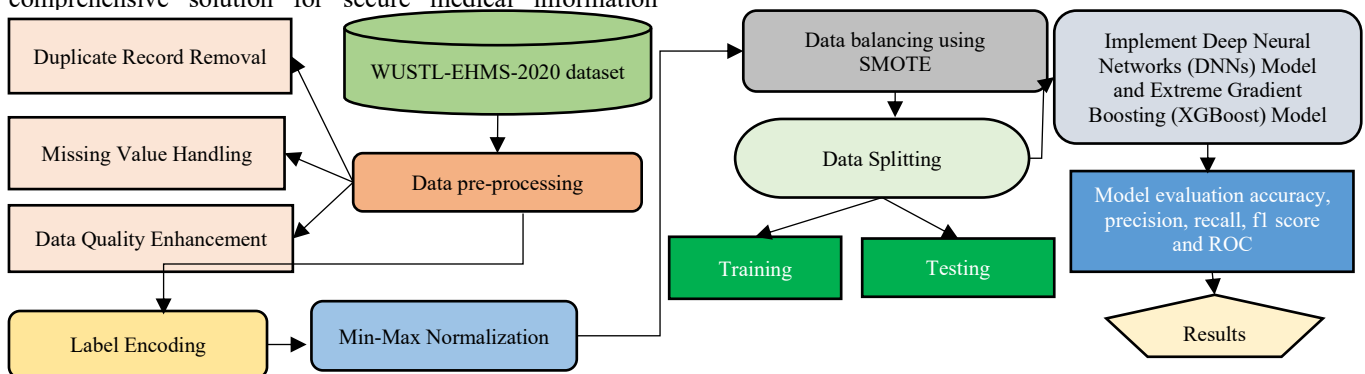


Fig. 1. Proposed Architecture of Healthcare Cybersecurity Framework for Medical Data Security

### III. RESEARCH METHODOLOGY

The proposed Healthcare Cybersecurity Framework leverages the WUSTL-EHMS-2020 dataset, using preprocessing methods such as data cleaning, label encoding, normalization and SMOTE balancing to improve data quality and model performance. Processed data is split into train and test sets, and DNN and XGBoost models are developed for managing medical information securely and detecting cyber-attack. The evaluation is done by ACC, PRE, REC, F1 and ROC curve analysis and the proposed framework is presented

in Fig. 1, which is a proposed Secure Healthcare Cybersecurity Framework based on ML and DL models.

The subsequent section outlines each of the proposed stages in detail:

#### A. Data Gathering and Analysis

The data for this study is from WUSTL-EHMS-2020. The dataset contains 44 features, 35 of which are network flow features, 8 are patient's biometric features and 1 is a label feature. The dataset containing 14,272 normal samples (87.5%) and 2,046 attack data samples (12.5%), with 16,318

data points. The distribution of attacks and correlations of the features are shown below using visualizations like bar plots and heatmaps:

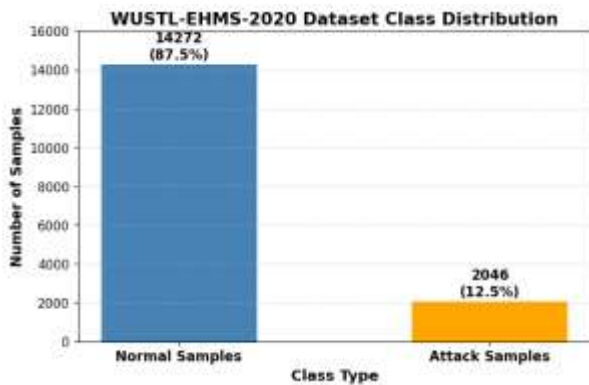


Fig. 2. Bar Graph of Class Distribution Analysis

The Class Distribution Analysis (CDA) in Fig. 2 shows the distribution of the data between normal and attack samples. The visualization demonstrates the unbalanced nature of the two classes, with the majority of data being normal and a smaller number of samples belonging to the attack class, which assists in comprehending the data properties prior to the model's development.

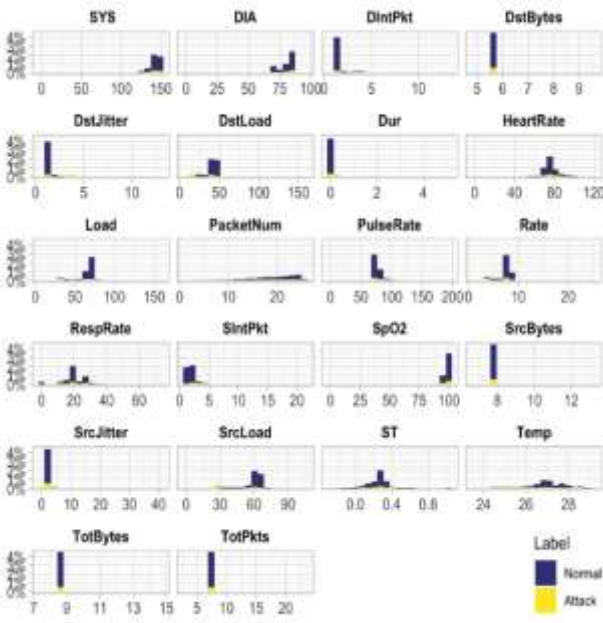


Fig. 3. Histograms of Feature Distribution for Normal and Attack Classes

The distribution of the different features of the traffic in the healthcare and attack classes is shown in Fig. 3, which allows to clearly compare their value patterns. The visualization can help highlight the discriminative features and data variability, aiding in feature analysis and the development of ML models.

Fig. 4 shows the distribution of the features for the healthcare and network traffic classes, where it is possible to clearly compare the values of the features in the normal and attack classes. The visualization aids in data variability comprehension and identification of discriminative features, assisting in the effective analysis of features and construction of ML models.

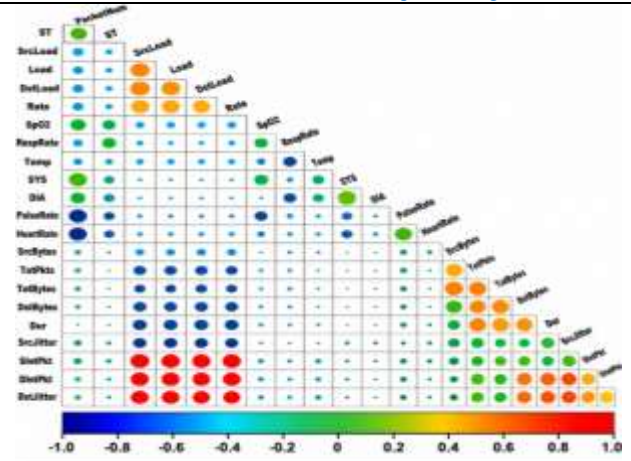


Fig. 4. Correlation Matrix of Healthcare and Network Features

### B. Data Pre-Processing

The WUSTL-EHMS-2020 dataset was used as the main data for data preparation including data integration, data cleaning, and feature engineering. In the pre-processing phase, missing data were filled, redundant data and duplicated data were eliminated, and noisy data were filtered to enhance data quality. Then data labeling and normalization were carried out to make the data consistent, and ready for training the ML model to be used. The key preprocessing steps are summarized below.

### C. Data Cleaning

Data cleaning is a crucial pre-processing phase that enhances data quality, consistency, and reliability for analysis and model construction. Duplicate records were detected and eliminated to avoid redundancy and possible bias. The missing values were investigated for all features, and handled with suitable statistical imputation methods including mean and median replacement. These operations enhanced data quality and ensured that the data was suitable for analysis and accurate model training.

### D. Label Encoding

Categorical attributes were encoded into numeric values so that the ML algorithms can efficiently process non-numeric data. This transformation helped to maintain the uniqueness of each category while also enhancing computation efficiency when training the model.

### E. Min-Max Normalization

Normalization is crucial to ensure that numerical data features are comparable in scale, enabling fair comparisons and enhancing the ACC of ML models. In this study, min-max scaling method was used to normalize the numerical characteristics of data. This process rescales each feature between 0 and 1, keeping the relative relationships between data points and reducing the effect of differing scales. Normalization was performed based on the following mathematical Equation (1):

$$X_{normalized} = \frac{X - \min(X)}{\max(X) - \min(X)} \quad (1)$$

$X_{normalized}$  is the scaled value,  $X$  is the data point,  $\min(X)$  represents the minimum value of the feature in the dataset, and  $\max(X)$  represents the maximum value of the feature in the dataset.

### F. Data Balancing Using SMOTE

Data balancing is a critical pre-processing technique for the class imbalance problem in which the number of attack samples is much less than the number of normal samples. The SMOTE was used to create artificial samples of the minority class in this study, which enhanced class distribution without compromising key data properties. The balanced dataset improves the ML model's ability to learn more and minimize the bias it has toward the majority class, thereby increasing the ACC of detection of cyber-attacks.



Fig. 5. Bar Graph of Class Distribution After SMOTE

The dataset is balanced in the sense that there are an equal number of samples in both classes, and it is illustrated in Fig. 5. The SMOTE algorithm effectively addresses the class imbalance present in the original dataset by creating synthetic minority samples, thereby distributing them among the majority samples for better training and classification ACC.

### G. Data Splitting

The developed model was then tested with a 20% of data that was reserved for testing, with the 80% data used for training, thus avoiding overfitting which is widely recommended. The model was trained on the training set, and its performance on unseen data was tested on the testing set.

### H. Implementation of the Proposed Model

The proposed Healthcare Cybersecurity Framework for Secure Medical Information Management is implemented using a DL-based DNN model and a ML-based XGBoost model to enhance medical data protection and threat detection.

#### 1) Proposed Deep Neural Networks (Dnns) Model

One DL technique that has gained widespread recognition among researchers is the DNNs. Fully connected input, hidden, and output layers make up a DNN's network architecture. Interlayer connections are nonexistent for each neuron; nonetheless, all neurons in the subsequent layer are linked. Enhance the impact of network learning by applying an activation function to the output after each network layer. Accordingly, DNN is also a lot like a big perceptron made of lots of smaller ones. For the forward propagation computation of the  $i$ th layer, for instance, the Equation (2):

$$x_{i+1} = \sigma(\sum w_i x_i + b) \quad (2)$$

when  $x$  stands for the input value,  $w$  for the weight coefficient matrices, and  $b$  for the bias vector. The activation function of a multi-class network often employs ReLU; the formula for this function is Equation (3)

$$\sigma(x) = \max(0, x) \quad (3)$$

The network's backpropagation is optimized using the loss function, which assesses the output loss of training samples and determines the network's structure. For classification tasks, the following formula is to be used when choosing a loss function: cross-entropy Equation (4):

$$C = -\frac{1}{N} \sum_x \sum_{i=1}^M (y_i \log p_i) \quad (4)$$

This is where  $N$  is the input data set count,  $M$  is the number of categories,  $y_i$  is the likelihood that the classification  $i$  matches to the actual category, and  $k_i$  is the chance of forecasting into category  $i$ . Using the following parameters: Adam optimizer, learning rate = 0.001, batch size = 32, epochs = 70, ReLU activation function, dropout rate = 0.5, and binary cross-entropy loss function, the suggested DNN model was set up.

#### 2) Proposed Extreme Gradient Boosting (Xgboost) Model

XGBoost is a DT based ensemble learning method. Reduce the disparity between the expected and actual values by using it to minimize a loss function; this may be used to regression situations. This is the mathematical paradigm that XGBoost regression follows: Equation (5):

$$y = f(x) \quad (5)$$

here,  $f(x)$  is the XGBoost model that uses  $x$  to forecast  $y$ ,  $y$  is the expected property price, and  $x$  is a vector of input characteristics like square footage and bedroom count. In order to calculate  $f(x)$ , XGBoost constructs a network of decision trees by training them to minimize the loss function known as MSE. A final prediction is reached by the model by combining the predictions of several DT. A general expression of the XGBoost regression model is Equation (6).

$$y = \sum (k = 1 \text{ to } K) f_k(x) \quad (6)$$

The forecast of the  $k$ th DTs is denoted as  $f_k(x)$ , and  $K$  is the total number of DTs in the ensemble. The training process teaches each tree its leaf values, and the prediction is just a weighted cumulative of those values. To get the XGBoost model's prediction for an input  $x$ , add up the forecasts of all the DTs in the ensemble. To get decent classification results, the suggested XGBoost model employed the following parameters:  $n\_estimators = 100$ , learning rate = 0.1, maximum depth = 6, subsample = 0.8, colsample\_bytree = 0.8, and goal = binary: logistic.

#### I. Evaluation Metrics

The performance of the proposed system is analyzed on the basis of recent studies and limitations based on ACC, REC, PRE and F1. The first step in classification of instances in the test dataset is the computation of a confusion matrix before calculating these metrics. True Positive (TP) refers to the correct classification of attack instances and True Negative (TN) refers to the correct classification of normal instances. The result that is labeled as attack when it is not is called False Positive (FP); the result that is labeled as normal when it is not is called False Negative (FN). Evaluation parameters Equation 7-10 are described as follows:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (7)$$

$$Precision = \frac{TP}{TP+FP} \quad (8)$$

$$Recall = \frac{TP}{TP+FN} \quad (9)$$

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (10)$$

The metrics used for evaluating the performance of the proposed model include ACC, PRE, REC, F1 and ROC curve. The ACC indicates the percentage of samples categorized correctly, whereas the PRE and the REC indicate the ability of the model to correctly identify positive classes as well as the number of actual positive samples, respectively. The F1 is balanced since it computes the harmonic mean of PRE and REC. ROC curve is a plot of TPR versus FPR across various decision thresholds.

#### IV. RESULTS AND DISCUSSION

This section outlines the experimental setup and evaluates the performance of the proposed ML and DL models, focusing on the results of the evaluation and the efficiency of computation.

##### A. Experimental Environment and Settings

The experiments were performed on a powerful computing platform with an Intel Core i5-13500 processor, 32 GB of DDR5 RAM, 1 TB NVMe M.2 storage, and an NVIDIA GTX 3060 graphics card for rapid data processing and accurate model execution. It was running on Windows 11 and used to provide computational speedup support to ML pipelines. The models were developed with Python programming language and the necessary ML libraries to achieve an effective training and evaluation of the models as well as its performance analysis.

##### B. Performance Evaluation Results

The proposed models were trained on the WUSTL-EHMS-2020 dataset and assessed using the following key performance indicators: ACC, PRE, REC and F1 (shown in Table II). The proposed DNN model showed excellent performance with ACC of 99.98%, PRE of 99.92%, REC of 99.99%, and an F1 of 99.98%. Likewise, the proposed XGBoost model achieved highly competitive results with 99.96% ACC, 99.91% PRE, 99.95% REC, and 99.97% F1, which shows the effectiveness of both models for healthcare cybersecurity classification.

TABLE II. PERFORMANCE EVALUATION OF PROPOSED MODELS FOR HEALTHCARE CYBERSECURITY FRAMEWORK

| Matrix    | Proposed DNN Model | Proposed XGBoost Model |
|-----------|--------------------|------------------------|
| Accuracy  | 99.98              | 99.96                  |
| Precision | 99.92              | 99.91                  |
| Recall    | 99.99              | 99.95                  |
| F1-score  | 99.98              | 99.97                  |

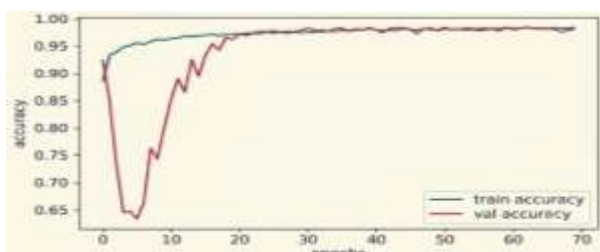


Fig. 6. Training and Validation Accuracy Curve for DNN Model

The ACC of the model has improved after 70 epochs with training and validation curve as shown in Fig. 6. The training ACC steadily rises, showing consistent learning and optimization. Validation ACC tends to converge with training

ACC after initial variations, with good generalization capability.

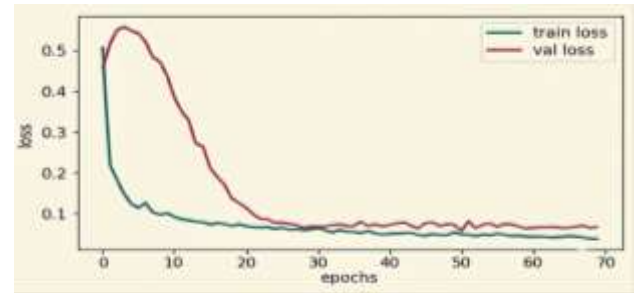


Fig. 7. Training and Validation Loss Curve for DNN Model

The training loss and validation loss of the model during training epochs are shown in Fig.7, where the loss decreases sharply during the 70 epochs of training. The training loss drops quickly and levels off, indicating efficient optimization and error minimization. The loss for the validation set stays nearly equal to the loss for the training set, which signifies stable generalization and good model learning.

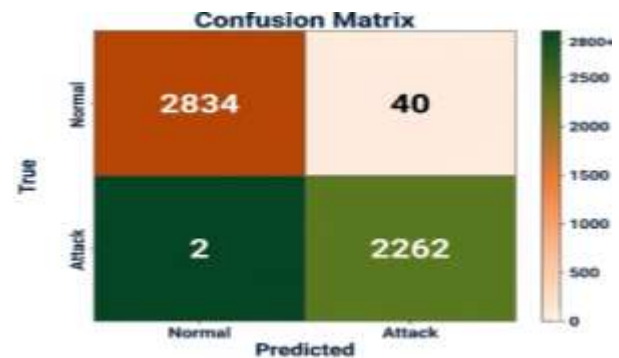


Fig. 8. Confusion Matrix for the XGBoost Model

The confusion matrix shown in Fig. 8 assesses the binary classification model that classifies the data as either Normal or Attack. These results indicate 2,834 TN, 40 FP, 2 FN and 2,262 TP, indicating high classification ACC. The model performs very well in detecting attack instances with a high PRE and REC and with relatively low misclassifications of normal network traffic.

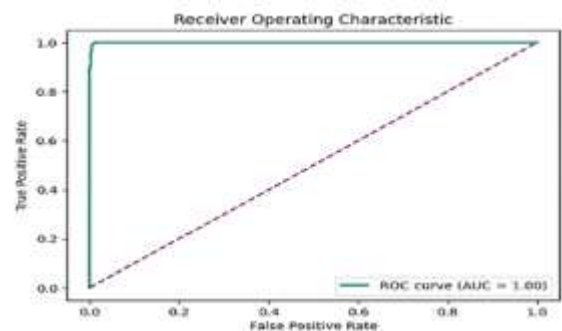


Fig. 9. ROC Curve for Xgboost Model

The XGBoost model's ROC curve is displayed in Fig. 9, which shows the TPR performance at various classification thresholds as the FPR increases. The model has an AUC of 1.00, which means that the classification power is very high, and almost perfect separation between the classes Normal and Attack is obtained. The curve stays near the top left corner, indicating high predictive performance.

### C. Comparative Analysis

A comparative performance evaluation of the proposed ML and DL models with existing models is provided in Table III to demonstrate the effectiveness of the proposed models. The results show that the proposed DNN model achieves better performance by obtaining 99.98% ACC, 99.92% PRE, 99.99% REC, and 99.98% F1 than conventional models like SVM, KNN, RF and GBM. The proposed XGBoost model also showcases its effectiveness with an ACC of 99.96%, PRE of 99.91%, REC of 99.95%, and F1 of 99.97% for secure medical information management and healthcare cybersecurity applications.

TABLE III. COMPARATIVE EVALUATION OF MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR SECURE MEDICAL INFORMATION MANAGEMENT

| Model            | Accuracy | Precision | Recall | F1-score |
|------------------|----------|-----------|--------|----------|
| SVM[29]          | 87.72    | 86.90     | 87.72  | 82.39    |
| KNN[30]          | 94       | 82        | 68     | 74       |
| RF[31]           | 94.07    | 84.91     | 98.35  | 73.03    |
| GBM[32]          | 96.5     | 96        | 96     | 95       |
| Proposed DNN     | 99.98    | 99.92     | 99.99  | 99.98    |
| Proposed XGBoost | 99.96    | 99.91     | 99.95  | 99.97    |

### D. Performance Discussion

The proposed DNN and XGBoost model achieves the ACC of 99.98% and 99.96%, respectively, with the classification performance. DNN model performs well to learn complex patterns within the Healthcare Cybersecurity dataset, thereby achieving the highest ACC, while XGBoost provides excellent and efficient classification performance. The results underscore the benefits of the proposed framework in enhancing threat detection ACC, minimizing misclassification, and ensuring secure medical information management. The high predictive performance confirms the suitability of both models for reliable healthcare cybersecurity applications.

### V. CONCLUSION AND FUTURE STUDY

In today's digital era, healthcare systems are heavily reliant on interconnected digital technologies for effective medical service, information sharing, and patient care, underscoring the critical nature of cybersecurity for safeguarding sensitive medical data. This study presented a ML enhanced Healthcare Cybersecurity Framework for secure medical information management and cyber-attack detection. The data in the WUSTL-EHMS-2020 set were cleaned, then encoded, normalized in the range [0, 1] and balanced using SMOTE. The primary implemented and evaluated models included DNN and XGBoost models with ACC, PRE, REC, F1, confusion matrix and ROC analysis. The DNN achieved 99.98% ACC, 99.92% PRE, 99.99% REC, and 99.98% F1, while XGBoost achieved 99.96% ACC and 99.97% F1. Both proposed models were compared with SVM, KNN, RF, and GBM, and the comparative results indicated that both models performed better than the three other models. The results highlight the potential of ML and DL methods to enhance healthcare cybersecurity and secure crucial patient data effectively.

The framework will be further validated with larger and more diverse datasets in healthcare cybersecurity and real-world environments in the future. Using advanced DL and ensemble techniques for improved detection of evolving and zero-day attacks can be investigated. Scalability,

explainability, adaptive threat detection, and privacy-preserving methods could be additional ways to further improve the scalability, transparency, and applicability of security.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.

**Conflicts of Interest:** The author declares no conflict of interest.

#### How to cite this article

N. Upadhyay, "Machine Learning Enhanced Healthcare Cybersecurity Framework for Secure Medical Information Management," *Journal of Artificial Intelligence in Governance and Public Policy*, vol. 1, no. 3, pp. 21–28, Jul.–Sep. 2026. Doi:XXX

### REFERENCES

- [1] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.
- [2] Y. Qiu, W. Ma, H. Wang, Y.-C. Tham, and T. Y. Wong, "The Landscape of Medical AI in China," *NEJM AI*, vol. 2, no. 7, Jun. 2025, doi: 10.1056/AI2401234.
- [3] D. P. Ramaraj and M. Mittal, "Deep Learning Models for Automated Medical Imaging: Accuracy, Ethics, And Deployment Challenges," *Int. J. Artif. Intell. Deep Learn.*, vol. 2, no. 1, pp. 11–31, June, 2025, doi: [https://doi.org/10.34218/IJAIDL\\_02\\_01\\_002](https://doi.org/10.34218/IJAIDL_02_01_002).
- [4] R. K. Kanneganti, "Impact of Custom Interface Widgets on User Efficiency in Content Navigation Platforms," *Eastasouth J. Inf. Syst. Comput. Sci.*, vol. 1, no. 01, pp. 179–186, Aug. 2023, doi: 10.58812/esiscs.v1i01.1121.
- [5] H. Lin, "Artificial Intelligence with Great Potential in Medical Informatics: A Brief Review," *Medinformatics*, vol. 1, no. 1, pp. 2–9, Feb. 2024, doi: 10.47852/bonviewMEDIN42022204.
- [6] G. Vukotich, "Healthcare and Cybersecurity: Taking a Zero Trust Approach," *Heal. Serv. Insights*, vol. 16, Jan. 2023, doi: 10.1177/11786329231187826.
- [7] J. Cabrero-Holgueras and S. Pastrana, "Towards realistic privacy-preserving deep learning over encrypted medical data," *Front. Cardiovasc. Med.*, vol. 10, Apr. 2023, doi: 10.3389/fcvm.2023.1117360.
- [8] K. Rajput, A. Darzi, and S. Ghafur, "Overlooked and under-reported: the impact of cyberattacks on primary care in the UK National Health Service," *Lancet Digit. Heal.*, vol. 7, no. 7, p. 100879, Jul. 2025, doi: 10.1016/j.landig.2025.100879.
- [9] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.
- [10] C. Tayal, S. Murumkar, and B. Mohan, "Semantic Web Healthcare Chatbot Using Ontology and Data Mining for Patient Information Assistance," in *2026 18th International Conference on Knowledge and Smart Technology (KST)*, Pattaya, Thailand, 2026, pp. 465–471, January. doi: 10.1109/KST67832.2026.11432402.
- [11] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The Emerging Threat of Ai-driven Cyber Attacks: A Review," *Appl. Artif. Intell.*, vol. 36, no. 1, p. 2037254, Dec. 2022, doi: 10.1080/08839514.2022.2037254.
- [12] R. Lingam, "Agentic AI and Federated Learning for Privacy-Preserving Dental Imaging," in *2026 Innovations in Machine, Engineering, and Digital Conference (IMED)*, Kota Kinabalu, Malaysia: IEEE, Mar. 2026, pp. 1–6. doi: 10.1109/IMED68921.2026.11484887.
- [13] A. Joon, "Smart Predictive Maintenance: AI-Driven Adaptation for Industrial Equipment," in *2025 IEEE North-East India International Energy Conversion Conference and Exhibition (NE-IECC)*, IEEE, Jul. 2025, pp. 1–6. doi: 10.1109/NE-

- IECC64154.2025.11183108.
- [14] S. S. Gopalan, A. Raza, and W. Almobaideen, "IoT Security in Healthcare using AI: A Survey," in *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSIPA)*, IEEE, Mar. 2021, pp. 1–6. doi: 10.1109/ICCSIPA49915.2021.9385711.
- [15] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0."
- [16] I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature," *IEEE Access*, vol. 8, pp. 146598–146612, 2020, doi: 10.1109/ACCESS.2020.3013145.
- [17] S. Mukherjee, "Machine Learning-Enabled Classification of Diabetes Using Clinical via Lifestyle Health Data," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA: I, 2026, pp. 1–6, February. doi: 10.1109/ICAIC67076.2026.11395709.
- [18] G. Shukla, D. Sharma, V. Awasthi, D. Shekhawat, P. K. Shukla, and A. Saranya, "Survey on Asclepius: A User-Centric Chatbot Bridging the Gap in Healthcare Integrated with VPN Technology," in *2024 4th International Conference on Advancement in Electronics & Communication Engineering (AECE)*, IEEE, Nov. 2024, pp. 778–783. doi: 10.1109/AECE62803.2024.10911262.
- [19] K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," *IEEE Access*, vol. 12, pp. 173127–173136, 2024, doi: 10.1109/ACCESS.2024.3493957.
- [20] T. Öztürk, Z. Turgut, G. Akgün, and C. Köse, "Machine learning-based intrusion detection for SCADA systems in healthcare," *Netw. Model. Anal. Heal. Informatics Bioinforma.*, vol. 11, no. 1, p. 47, Dec. 2022, doi: 10.1007/s13721-022-00390-2.
- [21] W. Hurst, B. Tekinerdogan, T. Alskaif, A. Boddy, and N. Shone, "Securing electronic health records against insider-threats: A supervised machine learning approach," *Smart Heal.*, vol. 26, p. 100354, Dec. 2022, doi: 10.1016/j.smhl.2022.100354.
- [22] D. Reddy Palavali, S. Pothireddy, D. K. Elumalai, and M. Nagaraja, "AI-Driven Claims Adjudication: Optimizing Healthcare Systems with Machine Learning and Deep Neural Networks," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395689.
- [23] P. Thapar *et al.*, "Medicare-AI: A Secure LLM-Powered Conversational Healthcare System for Intelligent Symptom Analysis and Personalized Diagnosis," in *2026 International Conference on Intelligent Systems in Engineering, Secured Systems and Cybersecurity (ICISESSC)*, IEEE, Apr. 2026, pp. 266–269. doi: 10.1109/ICISESSC68634.2026.11542800.
- [24] A. Zhumabekova *et al.*, "The Application of Machine and Deep Learning Models for Detecting Malware Threats in Healthcare Organizations," in *2025 5th International Conference on Advanced Research in Computing (ICARC)*, IEEE, Feb. 2025, pp. 1–6. doi: 10.1109/ICARC64760.2025.10962965.
- [25] A. S. Rao, D. Amrutha, S. Prasanthi, K. Pavan, K. S. Rao, and J. Angireddy, "Machine Learning-Based Blood Group Detection Using Fingerprints," in *2025 IEEE 3rd International Symposium on Sustainable Energy, Signal Processing and Cybersecurity*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/iSSSC66652.2025.11388244.
- [26] K. Thinakaran, "Enhancing IoT Healthcare Security Through Machine Learning and Game-Theoretic Anomaly Detection," in *2025 5th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN)*, IEEE, Nov. 2025, pp. 1553–1560. doi: 10.1109/ICECMSN68058.2025.11382955.
- [27] Z. ElSayed, N. Elsayed, and S. Bay, "A Novel Zero-Trust Machine Learning Green Architecture for Healthcare IoT Cybersecurity: Review, Analysis, and Implementation," in *SoutheastCon 2024*, IEEE, Mar. 2024, pp. 686–692. doi: 10.1109/SoutheastCon52093.2024.10500139.
- [28] L. A. Daher, "Towards Secure IoMT: Attack Detection Using Deep Q-Learning in Healthcare Networks," in *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, IEEE, Dec. 2023, pp. 407–412. doi: 10.1109/DeSE60595.2023.10468942.
- [29] R. Sharma and N. Sharma, "Enhancing security of internet of medical things in fog-edge environment: a study on attack detection performance," *Sādhanā*, vol. 49, no. 4, p. 299, Nov. 2024, doi: 10.1007/s12046-024-02622-9.
- [30] I. H. Putro, "Cybersecurity In Smart Healthcare: A Machine Learning Approach," *J. Tek. Elektro*, Vol. 18, No. 1, Maret 2025 40-45 P-ISSN 1411-870X, E-ISSN 2656-3304, vol. 18, no. 1, pp. 245–260, 2025, doi: 10.1201/9781003630685-13.
- [31] W. Wu, H. Fouzi, S. Sidi-Mohammed, and S. Ying, "Improving cyber-attack detection in Internet of Medical Things using ensemble deep learning methods," *Cluster Comput.*, vol. 28, no. 14, p. 891, Nov. 2025, doi: 10.1007/s10586-025-05660-y.
- [32] H. Tauqeer, M. M. Iqbal, A. Ali, S. Zaman, and M. U. Chaudhry, "Cyberattacks Detection in IoMT using Machine Learning Techniques," *J. Comput. Biomed. Informatics*, vol. 4, no. 01, pp. 13–20, Dec. 2022, doi: 10.56979/401/2022/80.