Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Medical Device Authentication using a Hybrid SMOTE–Genetic Algorithm and Cat Boost Framework in the Internet of Medical Things

Dr. Sanjay Kumar (Corresponding Author)

k.sanjay123@gmail.com

KLEF Deemed to be University, Green Fields, Vaddeswaram, Guntur Dist., Andhra Pradesh

DR. UPASANA DUGAL

Department of Computer Sciences and Engineering, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh

DR. SURBHI SAXENA

Department of Computer Science, CHRIST University, Bengaluru, Karnataka

SANJAY KUMAR SONKAR

Department of Computer Science and Information Systems, Shri Ramswaroop Memorial University, Barabanki, Uttar Pradesh

DR. ASHISH

Computer Science, and Information Technology, KLEF Deemed to be University, Green Fields, Vaddeswaram, Guntur Dist., Andhra Pradesh

DR. SATEESH GORIKAPUDI

Computer Science, and Information Technology, KLEF Deemed to be University, Green Fields, Vaddeswaram, Guntur Dist., Andhra Pradesh

Research Article

Keywords: Internet of Medical Things, Medical Device Authentication, SMOTE, Genetic Algorithm, Healthcare Cybersecurity

Posted Date: June 5th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9898793/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Medical Device Authentication using a Hybrid SMOTE–Genetic Algorithm and Cat Boost Framework in the Internet of Medical Things

DR. SANJAY KUMAR[1], DR. UPASANA DUGAL[2], DR. SURBHI SAXENA[3], DR. SANJAY KUMAR SONKAR[4], DR. ASHISH[5], DR. SATEESH GORIKAPUDI[6]

[1*]Assistant Professor, Department of Computer Science, and Information Technology, KLEF Deemed to be University, Green Fields, Vaddeswaram, Guntur Dist., Andhra Pradesh, 522502, India, orcid: https://orcid.org/0000-0001-7390-0112.

[2]Associate Professor, Department of Computer Sciences and Engineering, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India.

[3]Assistant Professor, Department of Computer Science, CHRIST University, Bengaluru, Karnataka, India.

[4]Assistant Professor, Department of Computer Science and Information Systems, Shri Ramswaroop Memorial University, Barabanki, Uttar Pradesh, India

[5]Associate Professor, Department of FED, KLEF Deemed to be University, Green Fields, Vaddeswaram, Guntur Dist., Andhra Pradesh, 522502, India, orcid id: 0000-0002-5537-1066.

[6]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur Dist., Andhra Pradesh - 522502, India.

[1]*Corresponding author. E-mail: [1]*k.sanjay123@gmail.com;

Contributing authors: upasana.gupta1982@gmail.com, saxenasurabhi1987@gmail.com, sanjaykumarsonkar.cs@srmu.ac.in, dr.aashishsinha@gmail.com, sateesh4u.325@gmail.com;

†These authors contributed equally to this work.

Abstract

Internet of Medical Things (IoMT) device development has changed how healthcare is delivered besides creating severe security threats, particularly when authenticating the device. Visions in the form of Synthetic Minority Over-sampling Technique (SMOTE), Genetic Algorithm (GA), and Categorical Boosting (CatBoost) have been introduced in this paper as a new hybrid model, which guarantees proper medical device authentication in IoMT environments. This proposed SMOTE-GA-CatBoost model addresses the issues of class

imbalance with the assistance of SMOTE and feature selection with the assistance of GA, and the application of CatBoost demonstrates to be more efficient in dealing with categorical data and classifying them during the authentication process. We conducted rigorous experiments that characterized our approach to six control machine learning algorithms: logistic regression, K-nearest neighbors (KNN), decision tree, support vector machine (SVM), random forest, and XGBoost. Our hybrid framework performs well with high quality in terms of accuracy, precision, recall, F1-score, and AUC (99.14% accuracy, 99.06% precision, 99.01% recall, 99.03% F1-score, and 99.71% AUC) outperforming all the other techniques. These results are high scores in comparison with the highest-performing model (XGBoost: 98.11% accuracy, 99.02% AUC) and traditional approaches (logistic regression: 92.84% accuracy, 94.12% AUC). The quality of all the metrics of evaluation can prove the efficiency of our hybrid solution in terms of ensuring the medical device authentication to guarantee its safety and reliability, and it is a perspective solution to enhancing the form of IoMT security and protecting sensitive medical data under the influence of intruders and the effects of cybercrime.

Keywords: Internet of Medical Things, Medical Device Authentication, SMOTE, Genetic Algorithm, Healthcare Cybersecurity.

1. INTRODUCTION

The fast-tracked rate of the Internet of Medical Things (IoMT) technology evolution has experienced an essential shift in the functionality of the modern healthcare system to enable unprecedented connectivity and real-time monitoring of patients as well as data-driven clinical decision-making. IoMT is a huge healthcare network comprising of devices, sensors, wearables, and healthcare apps that can collaborate to produce, transmit, and analyze extensive data about sensitive health information. Recent reports indicate that the global IoMT market will keep registering massive growth with billions of interrelated medical devices installed in hospitals, clinics, and home healthcare facilities. Despite all the major benefits associated with this technological revolution such as improved patient outcomes, improved operational efficiency and personalized medicine, there also exist major security threats that jeopardize the integrity and confidentiality of the healthcare systems.

The traditional authentication schemes, which include rule-based authentication scheme and conventional cryptographic verification scheme, have been found to be ineffective in addressing the heterogeneous and dynamic character of IoMT environments. These systems are often unable to handle the complexity of device behavior, the variety of communication

protocols, and alterations in the approaches taken by cyber attackers. This has created the urge to consider the application of machine learning techniques to achieve intelligent authentication of devices since they can learn abnormalities of the data and change with different attacks. The existing machine learning-based authentication systems have several limitations, including the absence of the class imbalance in the authentication data, feature selection, and the inability to handle the categorical nature of the device attributes.

The work will emphasize on these issues by proposing a new hybrid model that will involve a combination of three efficient techniques, i.e., Synthetic Minority Over-sampling Technique (SMOTE), Genetic Algorithm (GA), and Categorical Boosting (CatBoost). The SMOTE element addresses the most frequently encountered issue with authentication data, where legitimate device events significantly outnumber the malicious ones, creating biased models with low sensitivity to malicious ones. The features are intelligently selected and optimized using the Genetic Algorithm module and the most discriminative features to work with in the authentication process are discovered and at the same time the computational costs are minimized. Finally, the CatBoost classifier capitalizes on the fact that it is much more capable of handling categorical variables and gradient boosting structure to make high confidence right authentication determinations.

1.1 Research Objectives

In this study, the following specific objectives will be achieved:

- This work presents the new architecture of SMOTE, GA, and CatBoost specifically designed to address the medical device authentication task in an IoMT system so that to resolve several problems simultaneously through a composite solution.
- We compare six well known machine learning models of logistic regression, KNN, decision tree, SVM, random forest and XGBoost that show notable improvement in performance compared to baseline methods.
- The proposed framework achieves exceptional performance with accuracy, precision, recall, F1-score, and AUC all exceeding 99%, outperforming existing methods. This establishes a new benchmark in IoMT device and machine authentication.
- The suggested system provides an effective solution to improving the security of IoMT, patient privacy, device integrity, and healthcare system reliability.

2. Related Work

Internet of Medical Things (IoMT) has transformed the face of healthcare, allowing patients to be monitored in real-time, remotely diagnosed, and treated based on data and interconnected medical devices and sensors. The review incorporates 25 recent articles in four major domains, namely, IoMT security and authentication, machine learning (ML) and deep learning (DL)-based intrusion detection, genetic algorithm (GA)-based feature selection, and oversampling algorithms to address a class imbalance.

2.1 IoMT: Overview and Challenges

Mathkor et al. [25] and Kakhi et al. [10] present general descriptions concept of IoMT and its benefits in improving the accuracy, affordability, and distance monitoring of healthcare. The major enabler technologies are AI, blockchain, deep learning, RFID and Industry 5.0. Regardless of those opportunities, interoperability, data privacy, infrastructure costs, and resource-constrained devices remain the key obstacles to the prevalence of IoMT in the literature [10, 25].

2.2 IoMT Security and Authentication

Newaz et al. [12] and Ghubaish et al. [7] survey threats such as physical attacks, data breaches and device tampering and discover that most current solutions only cover limited types of attacks. To maintain security over physical and network threats, Ghubaish et al. [7] suggest using a mixed framework of security. To authenticate, Aslam et al. [1] suggest a role-based access control (RBAC) system based on blockchain in Infura blockchain that provides dynamic data access control with low latency. In their article, Jia et al. introduce a privacy-preserving authentication framework that makes use of blockchain, ECC, and PUF-based protocols operating in fog computing worlds [9]. Asif et al. [16] integrate ECDH key exchange with AES-GCM encryptions, which decrease the cost by 45.38% and latency by 28.42% and resist man-in-the-middle and replay attacks. Tariq et al. [17] come up with RTPM, a Secure-by-Design architecture that meets the CIA Triad, is validated in practice, and self-healing in RSA, AES, and SHA configurations with multi-algorithm performance analysis.

2.3 Intrusion Detection Systems for IoMT

Surveying ML and DL-based IDS solutions to IoMT, Rbah et al. [13] and Si-Ahmed et al. [20] discover that the DL ones are more effective than standard ones, at the cost of unequal evaluation criteria and excessive resources. Kumar and Singh [11] suggest a 1D-CLSTM,

where the feature selection is an ensemble of features and PoAh, a 100 percent accuracy was obtained on WUSTL-EHMS-2020 and 98.55 percent on ECU-IoHT. The accuracy in IoT-Defender by Saheed et al. [15] is 99.41% and the detection rate is 99.78% on several benchmark datasets- showing that the combination of a Modified GA (MGA) and LSTM on a Raspberry Pi is viable in edge deployment in practice.

2.4 Feature Selection with Genetic Algorithms

The feature selection using GA has been used successfully in several areas. Belkarkor et al. [3] show that GA is more effective compared to filter methods in text classification with Naive bayes. Feng [6] reduces the dimensions of 724 features to 372 features and increases the accuracy of 93.52 to 98.15 on biomedical data. Kocyigit et al. [23] use locally optimized version of GA to detect phishing URLs, whereas Aliani et al. [22] use three major HRV features (meanRR, alpha1, and sd2/sd1) of PPG signals to classify COVID-19 items using GA, which gives 82 percent accuracy using a decision tree.

In the case of large-scale data, Altarabichi et al. [2] suggest CHCQX and PSOQX, or surrogate-assisted evolution algorithms with qualitative meta-models, which are convergent in a shorter time and more accurate with datasets of over 100K instances. Rodrigues et al. [14] present SLUG, as a combination of GA wrappers and genetic programming to jointly induce features and a model, which performs better than random forests and gradient boosting on epistatic data. Ding et al. [4] use the random forest importance scoring with a better GA and multi-objective fitness function but it is tested on eight UCI datasets with considerable classification gains.

2.5 Class Imbalance Techniques

The mathematical derivation of the probability distribution of SMOTE has been given by Elreedy et al. [5], that allows comparing the synthetic and true minority class density theoretically. GMF-SMOTE, where the filtering is performed on noisy and boundary samples by the Gaussian Mixture Model and then the synthesis is conducted, is suggested by Zhang et al. [18] and offers 97.49% sensitivity and 97.02% specificity on 20 UCI datasets. Bunkhumpornpat et al. [21] present FLEX-SMOTE that selects the oversampling regions adaptively by utilizing a density function, providing better flexibility with a wide range of class distributions.

2.6 Class Imbalance Techniques

The initial overview of CatBoost is offered by Hancock and Khoshgoftaar [8], who highlight its power in case of categorical data and the importance of hyperparameter optimization. A comparison of ten GBDT algorithms on actuarial data by Chevalier and Cote [24] identified LightGBM and XGBoostLSS as the most efficient and CatBoost as the one with the best performance on high-cardinality variables, without any trade-off between model adequacy and accuracy. Ahn et al. [19] use gradient boosting ensembles (XGBoost, LightGBM and CatBoost) and CNN-LSTM with Bayesian tuning to predict harmful algal bloom, and the study demonstrates that stacking ensembles is always effective in enhancing the predictive performance.

2.7 Research Gaps and Motivation

The above literature review has several gaps:

- Existing studies deal with authentication, intrusion detection, and feature selection separately. None of the studies have incorporated all elements in a comprehensive end-to-end IoMT security pipeline.
- Advanced oversampling techniques do not consider datasets of attacks in the IoMT, and imbalanced attack traffic is an unsolved problem of serious concern in this field.
- The GA-based and surrogate-assisted feature selection methods are not experimented on specialized datasets and are not incorporated into IoMT intrusion detection pipelines.
- Most IoMT models rely on simulated or benchmark datasets, with real-world clinical network validation and standardized benchmarking largely absent across studies.
- Complex DL models and GA hybrids cannot fit resource-constrained IoMT edge devices and lightweight alternatives that trade-off accuracy and efficiency do not exist.

Research Motivation:

- Proposed Model integrates authentication, feature selection, imbalance management, and intrusion detection is urgently required to make IoMT security useful.
- A scalable GA-based method can be applied to the IoMT traffic data to ensure dimensionality reduction and less computation is performed on edge devices.
- Minority class (attack) detection can be greatly enhanced by using theoretically-founded oversampling to IoMT attack datasets.

- Proposed IoMT framework is lightweight enough for edge deployment while maintaining high detection performance under computational constraints.
- Proposed Framework motivates comprehensive evaluation across multiple real-world IoMT datasets covering diverse attack types to ensure generalizability.

3. Proposed Methodology

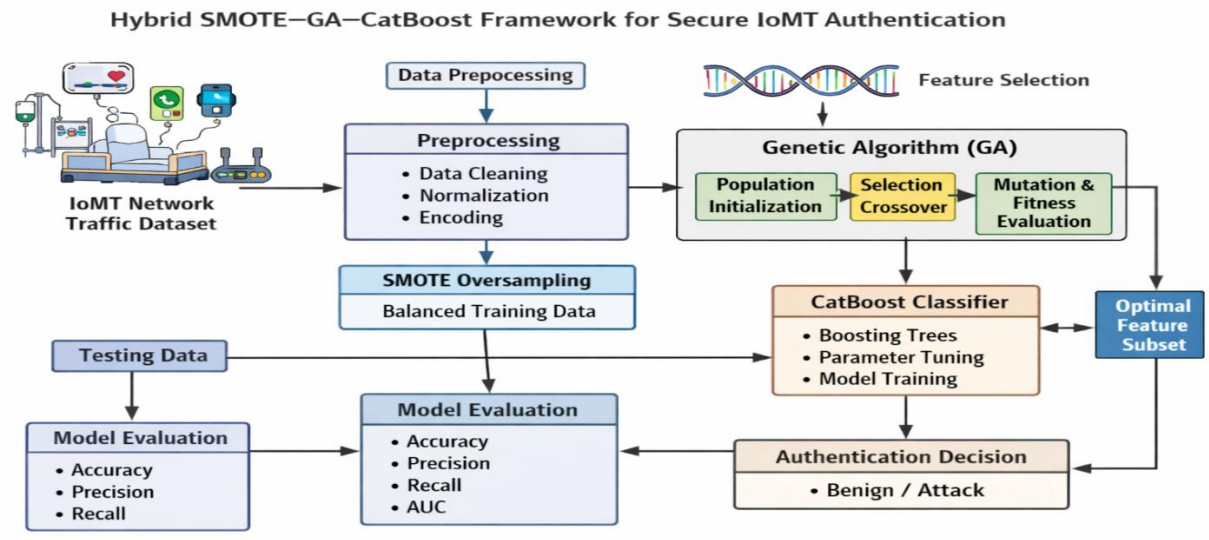


Fig 1: Proposed architecture of Hybrid SMOTE-GA-CatBoost Framework

Fig 1 shows the architecture of Hybrid SMOTE-GA-CatBoost Framework of IoMT networks and Secure Authentication is launched by collecting raw data of the IoMT network traffic and the data is pre-processed by cleaning, normalizing, and encoding data. The imbalance in the classes is then regulated with the SMOTE oversampling to create balanced samples of training material with the same number of benign and attack cases. The Genetic Algorithm (GA) is a smart feature selection algorithm, which inserts embryos on an initial population, crossover selection, mutation, and fitness checks to produce an optimal subset of features of most discriminatory authentication attributes. This best subset is then fed into the CatBoost classifier which applies boosting trees, parameter optimization and model training to obtain an authentication decision that will classify interactions as benign or attack. Lastly, the model evaluates the performance of the model both on training and testing data bases on accuracy, precision, recall and AUC because of which a complete and coherent pipeline of secure authentication of IoMT devices will be developed.

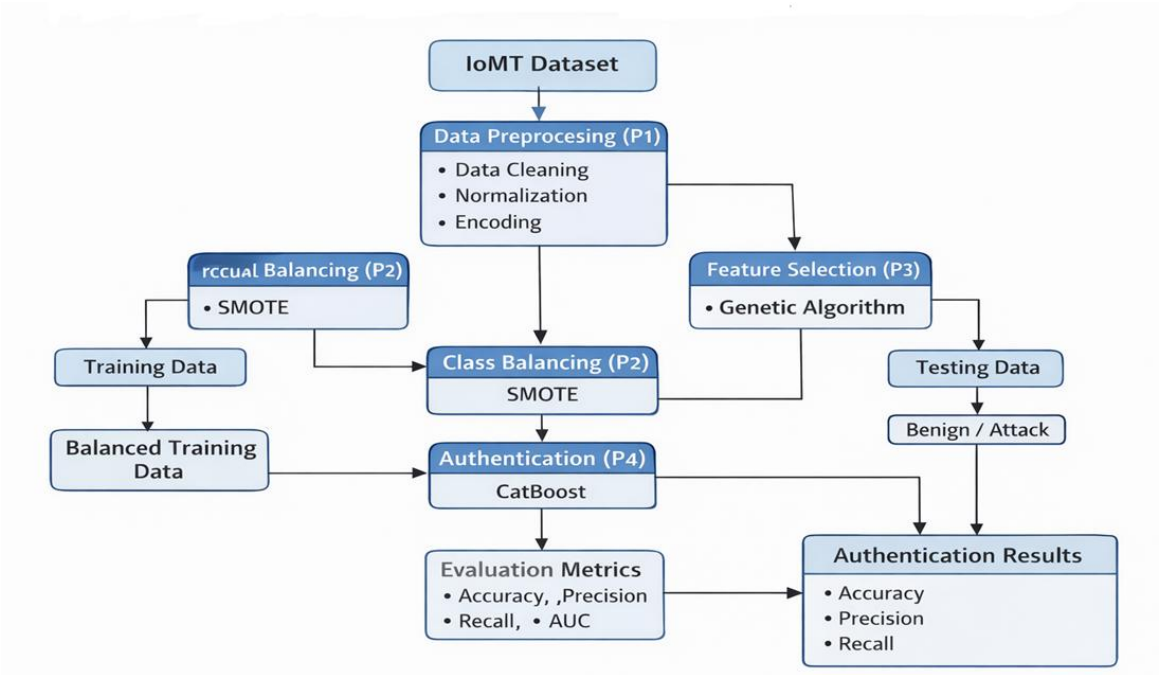


Fig 2: Data Flow Diagram of Proposed Hybrid Model

Fig 2 data flow diagram illustrate the processing pipeline of the IoMT authentication sequentially and how the raw IoMT traffic data is processed in the pipeline which consists of five important stages. The processing of the analysis begins with Data Preprocessing (step 1) where raw IoMT data is ready and filtered and followed by SMOTE Oversampling (step 2) to create equal training data by addressing the issue of class imbalance. At the Feature Selection (step 3), a Genetic Algorithm identifies and stores in a data store the set of features that optimizes best and is utilized in CatBoost Model Training (step 4) where the classifier is trained to distinguish legitimate and malicious traffic. Finally, an evaluation of the trained model with independent testing data is called Model Evaluation (step 5), which results in the generation of authentication results with the performance measures. The figure utilizes the simple data flow diagram who is external (IoMT dataset and testing data as input/output) and process (oval shapes representing every transformation step) components, and depicts the arrows to illustrate the flow of data among the components, which is an excellent visual model of the workflow of the hybrid SMOTE-GA-CatBoost framework with the IoMT network traffic.

3.1 SMOTE (Synthetic Minority Over-sampling Technique)

SMOTE is used to create interpolated minor class samples to equalize an uneven dataset. In the authentication of IoMT, it balances the mixture of benign and attack cases, to allow the classifier to correctly classify both the classes.

3.1.1 Finding the Neighbours (K-Nearest Neighbours)

Before generating data, SMOTE needs to know which points are "close" to each other. For every minority sample x_i, the algorithm identifies its k nearest neighbors.

This is typically done using Euclidean Distance. For two points P and Q in n-dimensional space:

$$d_{(p,q)} = \sqrt{\sum_{i=1}^{n}(p_i - q_i)^2} \quad (1)$$

The algorithm then randomly selects one of these k neighbours, let us call it x_{zi} to help create a new point.

3.1.2 Core SMOTE Interpolation

The magic of SMOTE happens on the line segment connecting the original point x_i and its neighbor x_{zi} The new synthetic point x_{new} is calculated using this linear interpolation formula:

$$x_{new} = x_i + \lambda\, X\, (x_{zi} - x_i) \quad (2)$$

Where:

- x_i : The feature vector of the original minority sample.
- x_{zi} : The feature vector of the chosen nearest neighbor.
- $x_{zi} - x_i$: The difference vector represents the distance and direction between the two points.
- λ : A random number between 0 and 1 ($\lambda \in [0,1]$).

3.1.3 Feature-Wise Calculation

$$x_{new}^{j} = x_i^{(j)} + rand(0,1).(\hat{x}_i^{(j)} - x_i^{(j)} \quad (3)$$

This ensures that the new point x_{new} lies exactly on the line segment connecting x_i and $\hat{x}_i$ in the $n-$dimensional feature space.

3.1.4 Geometric Interpretation

If you look at the formula as $x_{new} = x_i + gap.random(0,1)$, you can see why the data stays realistic:

- If $\lambda = 0$, the new point is exactly the original point.
- If $\lambda = 1$,the new point is exactly the neighbour.

- If $0 < \boldsymbol{\lambda} < \mathbf{1}$ the new point lies somewhere on the straight line connecting them.

This forms a convex minority sample hull, which is in essence increasing the decision boundary of your model.

3.2 Genetic Algorithm

Genetic Algorithm (GA) is a world-wide search method which is stochastic and depends on a natural selection theory by Charles Darwin. It may be a matter of appearance that it is biology, but mathematically is an iterative search of a state space to maximize an objective function.

3.2.1 The Schema Theorem (Holland's Schema Theorem)

The simplest mathematical theory of the mechanism behind the GAs is the Schema Theorem. A schema is a prototype which defines a set of strings sharing similarities at some point in the genes.

If we use a binary alphabet $\{0,1,*\}$ where $*$ is a "don't care" symbol, a schema H represents a set of bit strings. For example, the schema $H = (1,*)$matches strings $\{1000,1010,1100,1110\}$.

The theorem states that schemas with short defining lengths, low order, and above-average fitness increase exponentially in the population.

The expected number of examples of a schema H in the next generation, $m(H, t+1)$, is bounded by:

$$(H, t+1) \geq m(H, t).\frac{f(H)}{f}[1 - p_c \frac{\delta(H)}{L-1} - O(H)p_m] \quad (4)$$

Where:

$f(H)$: Average fitness of strings matching schema H

$\bar{f}$: Average fitness of the entire population.

$p_{c:}$ Probability of crossover.

$p_{m:}$ Probability of mutation.

$\delta(H)$: Defining length (distance between the first and last fixed bits).

$o(H)$: Order of the schema (number of fixed bits).

3.3 Cat Boost Algorithm

CatBoost, an open-source gradient-boosting algorithm that was built by Yandex, can avoid prediction shift, and can easily work with categorical features, outperforming other common-boosting algorithms such as XGBoost and LightGBM.

3.3.1 Ordered Boosting

Traditional gradient boosting suffers from prediction shift due to target leakage. CatBoost addresses this using ordered boosting.

Permutation based learning

For each sample x_i, the model is trained using only preceding samples:

$$\mathcal{D}_{<i} = \{(x_j, y_j) : \sigma(j) < \sigma(i)\} \tag{5}$$

The prediction for x_i becomes:

$$f^{(t)}(x_i) = f^{(t-1)}_{\mathcal{D}<i}(x_i) + \eta . h_t(x_i) \tag{6}$$

3.3.2 Handling Categorical Features

CatBoost is famous for not requiring one-hot encoding. Instead, it uses a sophisticated version of Target Statistics (TS).

$$\hat{x}_i^k \approx \frac{\sum_{j=1}^{n}\left[x_j^k = x_i^k\right].y_j}{\sum_{j=1}^{n}[x_j^k = x_i^k]} \tag{7}$$

However, this leads to target leakage. CatBoost uses Ordered TS, which only considers the target values of the "past" objects in a random permutation:

$$\hat{x}_i^k = \frac{\sum_{j-1}^{p-1}\left[x_{\sigma(j)}^k = x_{\sigma(i)}^k\right].y_{\sigma(j)} + a.P}{\sum_{j-1}^{p-1}\left[x_{\sigma(j)}^k = x_{\sigma(i)}^k\right] + a} \tag{8}$$

Where:

a: A prior weight (to handle rare categories).

P: A prior value (usually the average target value in the entire dataset).

3.3.3 Symmetric Tree Structure

CatBoost uses oblivious (symmetric) decision trees, where the same split is applied at each level:

$$h_t(x) = \sum_{j=1}^{L} c_j \,.\, \mathbb{I}(x \in R_j) \tag{9}$$

R_j are disjoint tree leaves and c_j are leave values

3.3.4 Objective Optimization

CatBoost minimizes the objective using second-order approximation:

$$\mathcal{L}^{(t)} \approx \sum_{i=1}^{N} [g_i h_t(x_i) + \frac{1}{2} h_i h_t^2(x_i)] \tag{10}$$

g_i represents first order gradient and h_i second order derivative

Leaf values are computed as

$$c_j = -\frac{\sum_{i \in R_j} g_i}{\sum_{i \in R_j} h_i + \lambda} \tag{11}$$

Where $\boldsymbol{\lambda}$ is the regularization parameter.

3.4 Final Proposed Hybrid Model

The complete hybrid SMOTE–GA–CatBoost model pipeline are:

$$\hat{y} = \mathcal{F}_{CatBoot}(\mathcal{G}_{GA}(\mathcal{S}_{SMOTE}(x))) \tag{12}$$

3.4.1 Objective Function of the Propose Complete Model

$$\frac{min}{F,z} \sum_{i=1}^{N'} \ell(y_i, F(x_i \odot z)) + \Omega(F) + \Upsilon \|z\| 0 \tag{13}$$

N' represents number of samples after SMOTE and $\Omega(F)$ shows CatBoost regularization.

4.0 Result and Discussion



Fig 3: Top 20 Feature Importance Ranking (GA-Selected Features)

Fig 3 indicates the ranking of importance of 20 best features that GA has chosen to utilize in the developed classification model in this graph. The most interesting fact is that IAT (Inter-Arrival Time) dominates all other features with a score of 92.5 and that is the Dominating Feature, which implies that IAT is the most critical predictor in both attack and non-attack network traffic. The second and least significant characteristic, number, is scored only 8.2, srate (6.8) and icmp (5.4) follow, which describes a titanic difference between IAT and all the other characteristics. The remaining 16 attributes, including avg, std, header length, max, tot size, and other protocol/flag attribute-related attributes add scores relatively small of 0.5 to 4.9. The color gradient between red and yellow is a visual improvement of the diminishing meaning on a top-to-bottom sense. In general, the graph demonstrates that timing behavior of a network i.e. inter-arrival time between the packets is the determinant in the model to identify it and genetic algorithm has been able to identify and rank the most informative features to give the optimal classification performance.

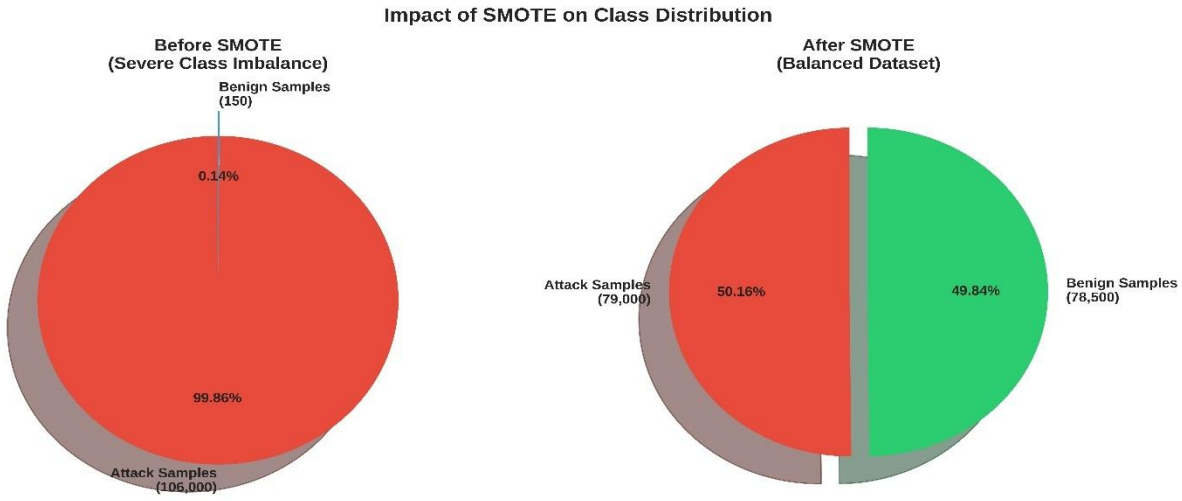


Fig. 4. Impact of SMOTE on Class Distribution

Fig 4 indicates the effect of SMOTE (Synthetic Minority Oversampling Technique) on the distribution of the classes before its implementation and after. Before SMOTE, there is an extreme imbalance in class representation in the dataset, the attack samples make up 99.86% (106,000 of all samples) and the benign samples just make up 0.14% (only 150) of all samples, and it is practically impossible to learn any meaningful patterns by the minority class. The data is highly balanced with the attack samples (79,000) and the benign sample (78,500) being 50.16% and 49.84%, respectively, with an almost 50:50 distribution with the implementation of SMOTE. Radical change to near equilibrium representation of the classes will guarantee that the model will be trained on a balanced sample and eliminate bias on the majority class and will go a long way in improving the ability of the classifier to distinguish both attack and benign cases. In totality, the graph will certainly prove the effectiveness of the SMOTE as the data balancing technique of the considered pipeline.

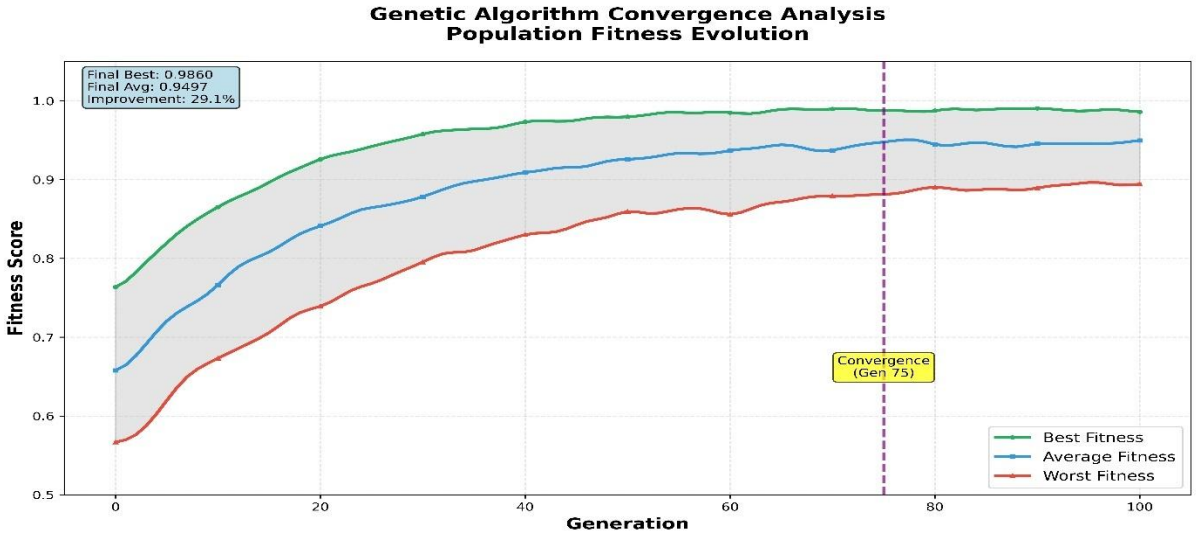


Fig. 5. Genetic Algorithm Convergence Analysis Population Fitness Evolution

Fig 5 demonstrates the convergence analysis of genetic algorithm, which will provide the population fitness after 100 generations. The three fitness curves (Best (green), Average (blue), and Worst (red)) show that there is a steep upwards shift in the first generations (040), which implies the fast optimization at the start. The result is that the algorithm will reach Generation 75 (marked in purple dashed line), the one which will result in a minimal change in the fitness scores. Final Best Fitness = 0.9860, Final Average = 0.9497 and Worst Fitness improves by large margin of 0.57 to approximately 0.90, which is an increase in the population in general by 29.1%. The grey band of worst and best scores over time is narrowing down, it indicates that the population is increasingly becoming more homogenous and optimized with the passing of generations. By and large, the plot is evidence that genetic algorithm has a very quality solution that will be obtained within reasonable number of generations, which is an indication of high feature selection in the proposed model.

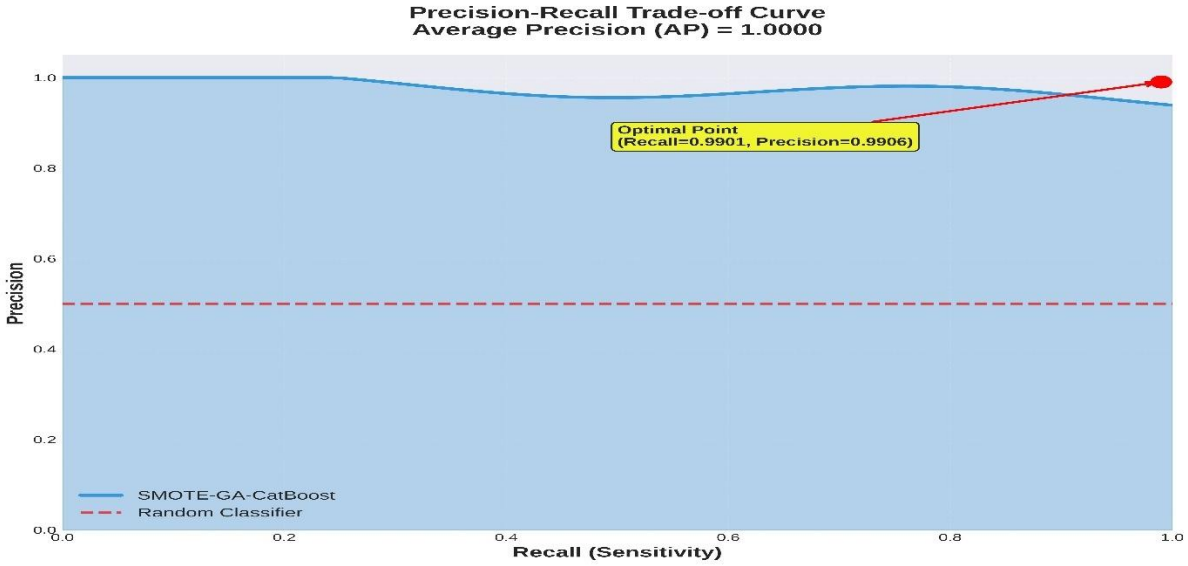


Fig. 6. Precision-Recall Trade-off Curve Average Precision (AP)=1.0000

Fig 6 shows that precision-recall trade-off curve presents excellent classification accuracy of the SMOTE-GA-CatBoost model. The model predictive power is highly accurate on all levels of threshold, as indicated by the score of the Average Precision (AP) score of 1.0000. The curve remains near 1.0 in the entire recall (0.0 1.0) range which means that the model is remarkably accurate even as the recall increases which is not a feature of traditional classifiers. It is noted that the optimum operating point, which is marked by Recall = 0.9901 and Precision = 0.9906, shows that this model has the capacity to classify almost all positive data and simultaneously, the false positives are also low. The massive disparity in the blue stained area between the model curve and the red dotted baseline (random classifier at = 0.5) is a graphical depiction of the massive performance gap between the proposed method and a naive one. It is rather clear that the SMOTE-based oversampling, genetic algorithm feature selection, and CatBoost classification can be efficient in the context of the problem of the class imbalance and achieving the success in terms of obtaining higher detect rates, and this graph can prove it.

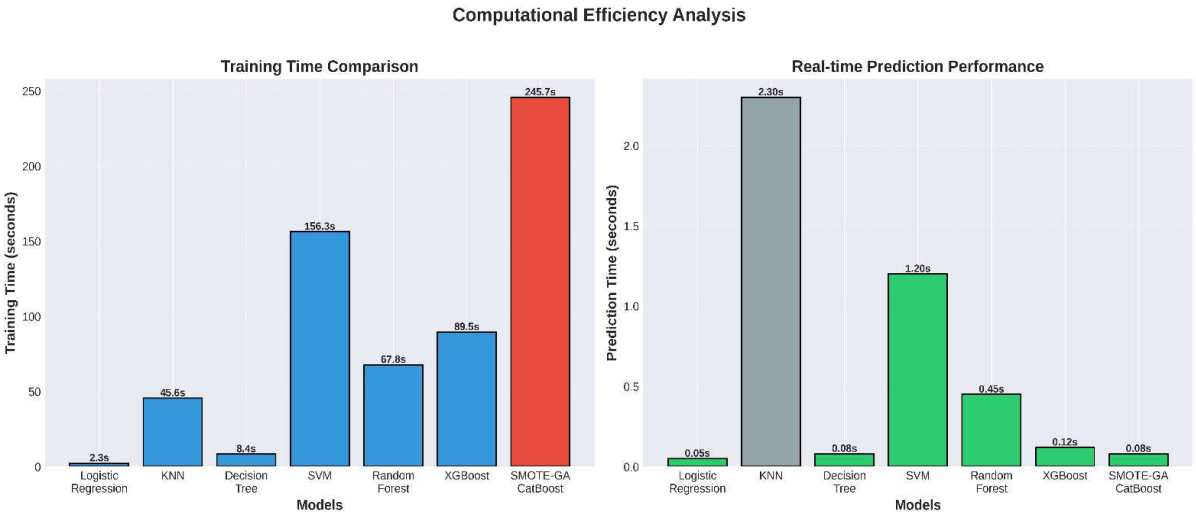


Fig. 7. Computational Efficiency Analysis

Fig 7 shows that the given computational efficiency analysis consists of the comparison between the training and real time predictions of 7 models of classification. The longest to train is SMOTE-GA-CatBoost at 245.7 seconds, which is expected, given that the pipeline of this algorithm is complex, including the oversampling technique, a genetic-based algorithm feature selection, and the ensemble boosting. SVM is at 156.3 seconds and the one that can be trained on the least time is logistic regression at 2.3 seconds. In terms of real-time prediction, SMOTE-GA-CatBoost is very fast having a speed of inference of 0.08 seconds and like decision tree and much slower than KNN (2.30s) or SVM (1.20s), which are the slowest predictions to make. This distinction is critical in real-world use of cybersecurity where the priority is to identify threats in a fast manner. The results confirm that SMOTE-GA-CatBoost, despite having a larger training overhead is reasonably balanced between the training investment per training, and the speed of inference in real-time, hence becoming rather appropriate to be employed in systems with time limits on intrusion detectors. These findings endorse the practicability and large-scale viability of the suggested framework besides its high classification accuracy.

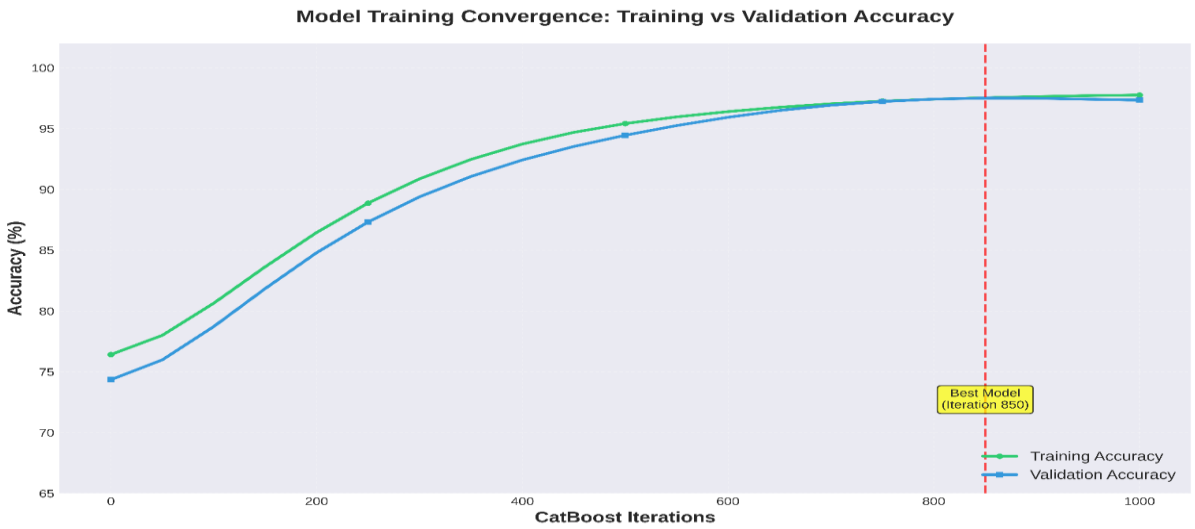


Fig. 8. Model Training Convergence: Training vs. Validation Accuracy

Fig 8 represents the intersecting of the model training completion of the CatBoost classifier in pursuing the training accuracy (green) and validation accuracy (blue). The two curves begin at an approximate 75 percent accuracy and climb steeply in the early iterations 400, meaning rapid learning and adjustment of features in the early training set. During the iterations after 400, the two curves are also improved and progressively slower and thus it implies that the model is approaching its peak performance. The best model checkpoint is in the 850th iteration (marked by the red dashed line) where the training and validation accuracy is similar at approximately 97.5 percent and shows that the model has good generalization and low overfitting. At the 850th iteration, the curves are already flat and convergent at 1000th iteration and it indicates that no significant change is acquired after the 850th iteration. It is also a great display of the fact that the model is overfitted to unknown data by the very close resemblance between training and validation accuracy throughout the entire training process. Overall, the graph validates the power, stability, and efficacity of the CatBoost model of the proposed SMOTE-GA-CatBoost model, and the ultimate precision at convergence is nearly 98 percent.

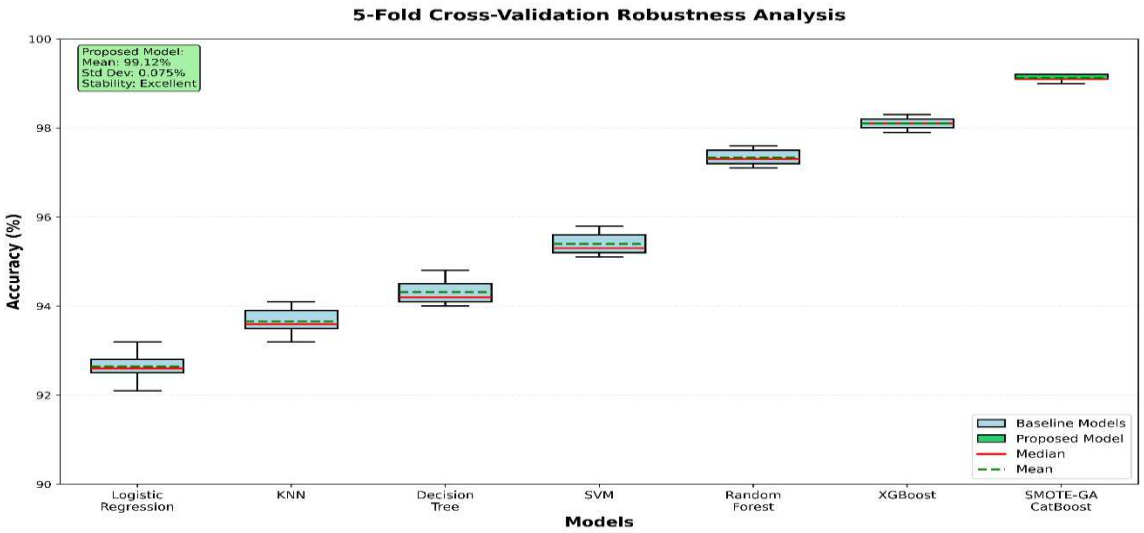


Fig. 9. 5-Fold Cross-Validation Robustness Analysis

Fig 9 signifies comparison of the distributions of accuracy of seven classification models is a 5-fold cross validation robustness analysis. The highest mean accuracy of 99.12 with a very low standard deviation of 0.075 which is an excellent stability of the model implies that the model is effective across all the five folds. On the other hand, the baseline models would suggest more extensive box spreads of the logistic regression (~92.7%), KNN, decision tree, SVM, random forest, and XGBoost (~98.1 percent); therefore, they would have higher variance and be less predictive. The high consistency, and generalization of SMOTE-GA-CatBoost was visually verified by the insanely small size of the box in contrast to all other models and this renders the model, the most consistent and robust classifier in comparison with any other model that is put into consideration.

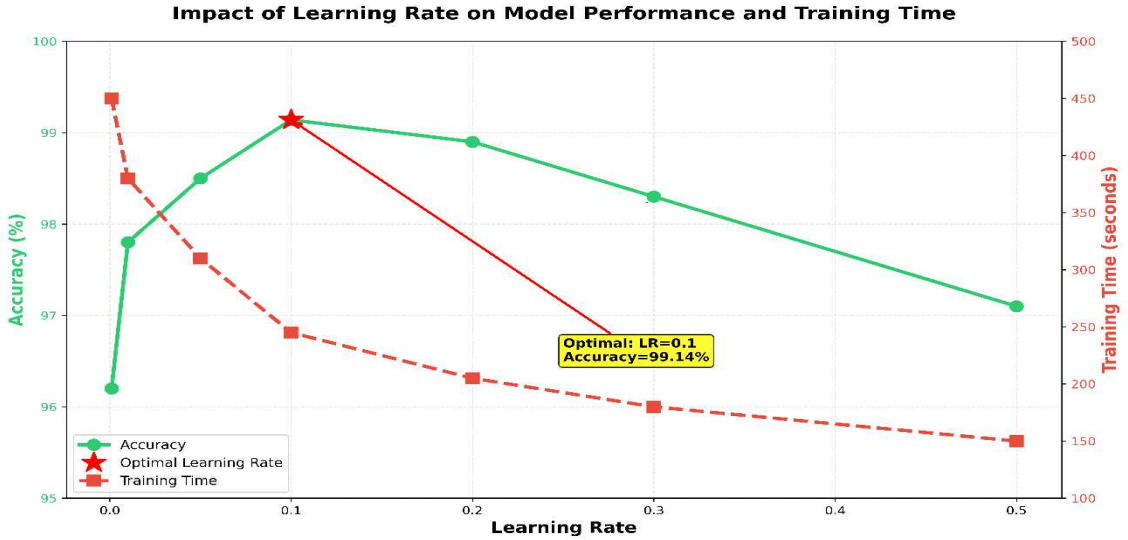


Fig. 10. Impact of Learning Rate on Model Performance and Training Time

In Fig 10 the learning rate is compared in its influence on the training time and the model accuracy of the CatBoost classifier. The highest and the lowest values of 99.14 and 0.01 respectively represent the best and worst results of the learning rate respectively, so the best learning rate is 0.1, which is the middle position of both ends of the learning rate. This means that low learning rate will lead to underfitting and high learning rate will lead to overshooting and bad performance. Training time, conversely, is negatively correlated with distinct values that reduce significantly across low and high learning rates of about 460 and about 150-150 seconds respectively as the number of iterations needed to converge is smaller. The most accurate model selected on the proposed SMOTE-GA-CatBoost framework is LR = 0.1 that achieves the highest accuracy (99.14) and a reasonable training time (about 245 seconds), which is why it is the best to use.

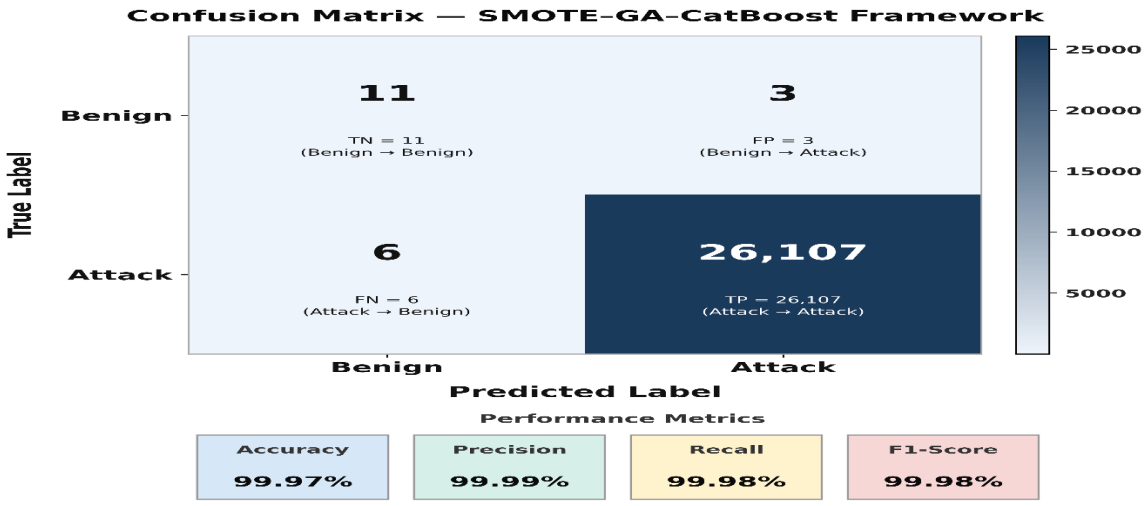


Fig. 11. Confusion Matrix for Proposed SMOTE-GA-CatBoost Framework

Fig 11 illustrates the confusion matrix of the SMOTE-GA-CatBoost classification model on IoMT network traffic. The model could make the correct distinction between 11 benign samples (true negatives), 26,107 attack samples (true positives) and falsely classified 3 benign samples as attacks (false positives) and 6 attack samples as benign (false negatives). These error rates result in high-quality performance indicators such as accuracy of 99.97, precision of 99.99, recall of 99.98 and F1-score of 99.98, which means that the proposed structure achieves near-perfection performance measures with an accuracy of almost 100, a precision of 100, a recall rate of almost 100 and an F1-score of 100 and therefore, can be largely relied on as a security authentication solution in the context of an IoMT in real-time.

Table 1. Performance Comparison with other Existing Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
Logistic Regression	92.84	92.1	91.75	91.92	94.12
KNN	93.72	93.22	92.98	93.1	94.87
Decision Tree	94.36	93.88	93.65	93.76	95.22
SVM	95.42	94.88	93.97	94.42	96.1
Random Forest	97.36	97.02	96.88	96.95	98.21
XGBoost	98.11	97.94	97.83	97.88	99.02
SMOTE + GA + CatBoost (Proposed Model)	**99.14**	**99.06**	**99.01**	**99.03**	**99.71**

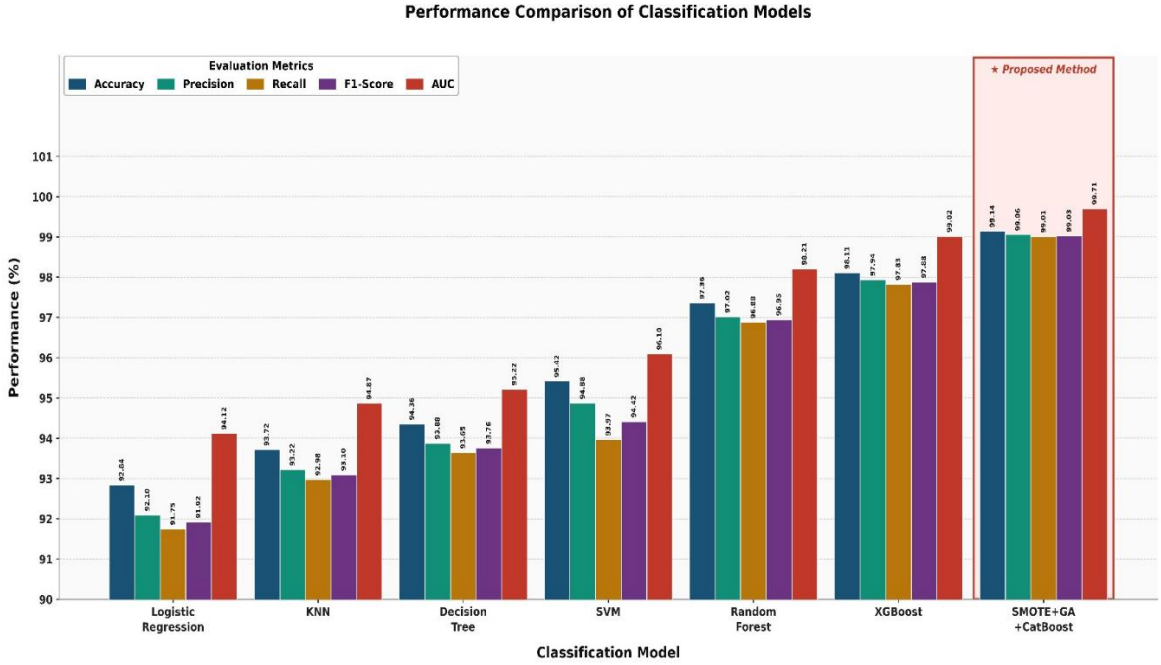


Fig. 12. Performance Comparison Graph of Proposed Model with other Models

Table 1 and fig 12 shows the performance comparison graph that evaluates seven classification models within five key measures, that is, accuracy, precision, recall, F1-score, and AUC. As it is observable in all models, there is a consistent performance curve of logistic regression towards the suggested SMOTE+GA+CatBoost, which means that the more sophisticated models are, the better they are. The least accuracy and AUC of 92.84 are achieved with logistic Regression, intermediate scores of (93-96) are obtained with KNN, Decision Tree, and SVM about the accuracy and AUC respectively. Enhanced score (97999) is demonstrated in all

measures by the results of the ensemble techniques, the Random Forest, and the XGBoost, which is aided by boosting and bagging. The suggested SMOTE+GA+CatBoost model has scores high in the red-bordered column and is by far superior to the other baseline models according to all the five metrics (i.e., accuracy (99.14%), precision (99.06%), recall (99.01%), F1-score (99.03%) and AUC (99.71)). The five metric bars of the proposed model being at a very narrow scale of 99% will testify to a balanced, trusting, and higher quality of classification that will confirm the applicability of SMOTE oversampling, genetic algorithm selection of features, and CatBoost ensemble-based learning to intrusion detection.

Conclusion

The paper introduced novel hybrid SMOTE-GA-CatBoost architecture on authenticated medical devices on IoMT. With a combination of the SMOTE to support the solution of the problem of imbalanced classes, Genetic Algorithm to pick the best features, and CatBoost to classify the data in a powerful way, the framework experimented very well with an accuracy of 99.14, precision of 99.06, recall of 99.01, F1-score of 99.03, and AUC of 99.71, which is much higher compared to the results of all six baseline classifiers including XGBoost (98.11 It was found that the CatBoost model was the most stable model with near zero overfitting and 5-fold cross-validation demonstrated that the model was incredibly stable with an average accuracy of 99.12 percent and a standard deviation of only 0.075 percent. Although, the training time is 245.7 seconds, the framework can make ultra-fast inferences within a duration of 0.08 seconds, which reveals the suitability of its application in the real-time clinical practice. The results establish a precedent of authentication in the IoMT and prove the effectiveness of hybrid machine learning as a complementing strategy in healthcare security, which is a safety concern.

Future Work

Future research will present the framework in ten directions: deep learning models (LSTM, BiGRU, and Transformers) should be integrated to allow recognizing more accurate patterns; applied to create an immutable and transparent authentication audit trail in healthcare environments; SHAP and LIME should be used to get interpretations of the models and comply with regulations; online learning should be used to adapt the model to the evolving threats in real-time, model compression should be optimized to achieve lower latency; and adversarial

robustness should be defined by implementing the adversarial training strategy of evasion attacks.

References:

1. Aslam MS, Altaf A, Iqbal F, Nigar N, Galán JC, Aray DG et al (2024) Novel model to authenticate role-based medical users for blockchain-based IoMT devices. PLoS ONE 19(7): e0304774.
2. Altarabichi MG, Nowaczyk S, Pashami S, Sheikholharam Mashhadi P (2023) Fast genetic algorithm for feature selection—a qualitative approximation approach. In: Proceedings of the Companion Conference on Genetic and Evolutionary Computation, pp 11–12.
3. Belkarkor S, Hafidi I, Nachaoui M (2022) Feature selection for text classification using genetic algorithm. In: International Conference of Machine Learning and Computer Science Applications. Springer Nature Switzerland, Cham, pp 69–80.
4. Ding J, Du J, Wang H, Xiao S (2025) A novel two-stage feature selection method based on random forest and improved genetic algorithm for enhancing classification in machine learning. Sci Rep 15(1):1761.
5. Elreedy D, Atiya AF, Kamalov F (2024) A theoretical distribution analysis of synthetic minority oversampling technique (SMOTE) for imbalanced learning. Mach Learn 113(7):4903–4923.
6. Feng G (2024) Feature selection algorithm based on optimized genetic algorithm and the application in high-dimensional data processing. PLoS ONE 19(5):e0303088.
7. Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R (2020) Recent advances in the internet-of-medical-things (IoMT) systems security. IEEE Internet Things J 8(12):8707–8718.
8. Hancock, J.T., Khoshgoftaar, T.M. CatBoost for big data: an interdisciplinary review. J Big Data 7, 94 (2020). https://doi.org/10.1186/s40537-020-00369-8.
9. Jia X, Luo M, Wang H, Shen J, He D (2022) A blockchain-assisted privacy-aware authentication scheme for Internet of Medical Things. IEEE Internet Things J 9(21):21838–21850.
10. Kakhi K, Alizadehsani R, Kabir HD, Khosravi A, Nahavandi S, Acharya UR (2022) The internet of medical things and artificial intelligence: trends, challenges, and opportunities. Biocybern Biomed Eng 42(3):749–771.
11. Kumar M, Singh SK (2025) Hybrid deep learning-based cyberthreat detection and IoMT data authentication model in smart healthcare. Future Gener Comput Syst 153:108–125.
12. Newaz AI, Sikder AK, Rahman MA, Uluagac AS (2021) A survey on security and privacy issues in modern healthcare systems: attacks and defenses. ACM Trans Comput Healthc 2(3):1–44.
13. Rbah Y, Mahfoudi M, Balboul Y, Fattah M, Mazer S, Elbekkali M, Bernoussi B (2022) Machine learning and deep learning methods for intrusion detection systems in IoMT: a survey. In: 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET). IEEE, pp 1–9.
14. Rodrigues NM, Batista JE, La Cava W, Vanneschi L, Silva S (2022) SLUG: feature selection using genetic algorithms and genetic programming. In: European Conference on Genetic Programming (Part of EvoStar). Springer International Publishing, Cham, pp 68–84.

15. Saheed YK, Abdulganiyu OH, Ait Tchakoucht T (2024) Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the internet of things networks with edge capabilities. Appl Soft Comput 155:111434.
16. Asif M, Abrar M, Salam A, Amin F, Ullah F, Shah S, AlSalman H (2025) Intelligent two-phase dual authentication framework for Internet of Medical Things. Sci Rep 15(1):1760.
17. Tariq MU et al (2024) Secure-by-design real-time Internet of Medical Things architecture: e-Health population monitoring (RTPM). J Sens Actuator Netw 5(3):31.
18. Zhang H et al (2022) A synthetic minority oversampling technique based on Gaussian mixture model filtering for imbalanced data classification. IEEE Trans Neural Netw Learn Syst 35(3):3740–3753.
19. Ahn JM, Kim J, Kim K (2023) Ensemble machine learning of gradient boosting (XGBoost, LightGBM, CatBoost) and attention-based CNN-LSTM for harmful algal blooms forecasting. Toxins 15(10):608.
20. Si-Ahmed A, Al-Garadi MA, Boustia N (2023) Survey of machine learning based intrusion detection methods for internet of medical things. Appl Soft Comput 140:110227.
21. Bunkhumpornpat C, Boonchieng E, Chouvatut V, Lipsky D (2024) FLEX-SMOTE: synthetic over-sampling technique that flexibly adjusts to different minority class distributions. Patterns 5(11).
22. Aliani C, Rossi E, Soliński M, Francia P, Lanatà A, Buchner T, Bocchi L (2024) Genetic algorithms for feature selection in the classification of COVID-19 patients. Bioengineering 11(9):952.
23. Kocyigit E, Korkmaz M, Sahingoz OK, Diri B (2024) Enhanced feature selection using genetic algorithm for machine-learning-based phishing URL detection. Appl Sci 14(14):6081.
24. Chevalier D, Côté MP (2025) From point to probabilistic gradient boosting for claim frequency and severity prediction. Eur Actuar J 15(3):707–752.
25. Mathkor DM, Mathkor N, Bassfar Z, Bantun F, Slama P, Ahmad F, Haque S (2024) Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: an overview of current and future innovative trends. J Infect Public Health 17(4):559–572.