THE USA JOURNALS
THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN – 2689-0984)
VOLUME 06 ISSUE10

PUBLISHED DATE: - 21-10-2024
DOI: - https://doi.org/10.37547/tajet/Volume06Issue10-10 **PAGE NO.: - 86-99**

RESEARCH ARTICLE **Open Access**

ADVANCEMENTS IN AIRLINE SECURITY: EVALUATING MACHINE LEARNING MODELS FOR THREAT DETECTION

Fuad Mahmud
Department of Information Assurance and Cybersecurity, Gannon University, USA

Badruddowza
Department of Computer & Info Science, Gannon University, Erie, Pennsylvania, USA

Md Shohail Uddin Sarker
Department of Computer & Info Science, Gannon University, Erie, Pennsylvania, USA

Abdullah Al Mamun
Department of Computer & Info Science, Gannon University, Erie, Pennsylvania, USA

Md Khorshed Alam
Department of Professional Security Studies, New Jersey City University, Jersey City, New Jersey, USA

Md Tarek Hasan
Department of Professional Security Studies, New Jersey City University, Jersey City, New Jersey, USA

Mashaeikh Zaman Md. Eftakhar Choudhury
Master of Social Science in Security Studies, Bangladesh University of Professional (BUP), Dhaka, Bangladesh

Jannatul Ferdous Shorna
College of Engineering and Computer Science, Florida Atlantic University, Boca Raton, Florida, USA

THE USA JOURNALS
THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN – 2689-0984)
VOLUME 06 ISSUE10

Abstract
This study assessed the performance of four machine learning algorithms—Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and Neural Network (NN)—for predicting airline security threats using a dataset of 100,000 entries with 30 features. The models were evaluated based on accuracy, precision, recall, F1-Score, and AUC-ROC. The Neural Network achieved the highest performance, with an accuracy of 88%, precision of 86%, recall of 85%, F1-Score of 85.5%, and AUC-ROC of 0.90, demonstrating superior capability in capturing complex, non-linear patterns. The Random Forest model followed, with an accuracy of 85%, precision of 83%, recall of 82%, F1-Score of 82.5%, and AUC-ROC of 0.87, offering a robust and generalizable solution. The SVM model attained an accuracy of 81%, precision of 80%, recall of 78%, F1-Score of 79%, and AUC-ROC of 0.84, showing effective binary classification but with higher computational costs. The Decision Tree model, while interpretable, had the lowest performance metrics: accuracy of 78%, precision of 76%, recall of 72%, F1-Score of 74%, and AUC-ROC of 0.79. The results indicate that Neural Networks and Random Forests are the most effective models for airline security threat detection, with Neural Networks providing the highest overall accuracy and AUC-ROC.

Keywords Machine Learning, Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), Neural Network (NN), Airline Security, Predictive Modeling, Classification Algorithms.

INTRODUCTION

The rapid growth of the airline industry has made security a critical concern, particularly with the increasing number of passengers, flight routes, and baggage passing through airports daily. Ensuring the safety of passengers, staff, and facilities has necessitated the adoption of more sophisticated and automated systems to assess potential threats. Traditional security measures, such as manual screenings and checklists, have proven insufficient in addressing the complexities and scale of modern airline security. As a result, machine learning (ML) models have become vital tools in improving the accuracy and efficiency of security screening processes.

Machine learning offers powerful solutions for identifying potential security risks by analyzing large datasets, including passenger demographics, travel histories, baggage details, and behavioral patterns. The ability to automate and enhance decision-making through predictive algorithms can significantly reduce human error and streamline security procedures, ensuring a safer travel experience for all. This study aims to evaluate four popular machine learning models—Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and Neural Network (NN)—to determine their effectiveness in predicting potential airline security threats. By analyzing these models' performance based on key metrics like accuracy, precision, recall, and F1-score, the research identifies the most suitable ML model for real-world deployment in airline security systems.

The application of machine learning in airline security has garnered increasing attention as the industry seeks to improve risk management and threat detection. Traditionally, airline security systems have relied on rule-based frameworks that follow predefined protocols for screening passengers and baggage. However, such systems often suffer from inefficiencies due to their inability to adapt to new types of security risks, especially with evolving technologies and tactics used by malicious actors (Kumar & Shankar, 2017).

LITERATURE REVIEW

Machine learning, particularly supervised learning algorithms, offers a promising alternative by automatically learning from historical data and

detecting patterns that are difficult for traditional systems to capture. Decision Trees (DT), for example, have been used for their simplicity and ease of interpretation, making them a preferred choice in domains where explainability is critical (Loh, 2011). Despite their interpretability, however, DT models often struggle with overfitting and fail to generalize well when dealing with complex, non-linear relationships in data, as shown in recent security research (Breiman, 2017).

Random Forest (RF), an ensemble learning technique that builds multiple decision trees, has been proposed as a more robust solution for airline security challenges. By averaging predictions across several decision trees, RF reduces the risk of overfitting and improves overall model performance. Breiman (2001) demonstrated the effectiveness of Random Forest in handling large datasets and noisy data, making it particularly suitable for high-stakes applications such as airline security. Recent studies have further validated RF's capability to generalize better than individual decision trees while offering high accuracy in classification tasks (Zhang et al., 2019).

Support Vector Machines (SVM) have been widely used in binary classification problems, including threat detection, due to their ability to find the optimal hyperplane that separates two classes (Cortes & Vapnik, 1995). While SVM excels in providing clear margins between classes, it is computationally expensive, especially when dealing with large, multidimensional datasets commonly found in airline security applications (Noble, 2006). The use of a Radial Basis Function (RBF) kernel further enhances its ability to handle non-linearly separable data, a common characteristic of security-related datasets (Schölkopf et al., 2001).

Neural Networks (NN), particularly deep learning models, have gained traction in recent years for their ability to model complex, non-linear relationships in large datasets. Unlike traditional machine learning models, Neural Networks can automatically learn intricate patterns from data without relying on manually designed features, which makes them highly adaptable for large-scale systems like airline security. However, they are often criticized for their "black-box" nature and computational cost (LeCun et al., 2015). Despite these challenges, recent research indicates that Neural Networks outperform traditional algorithms in high-dimensional data analysis, making them an attractive option for detecting potential security threats (Goodfellow et al., 2016).

In conclusion, the literature highlights the strengths and weaknesses of various machine learning models in airline security applications. While Decision Trees offer simplicity and interpretability, they tend to overfit complex data. Random Forest improves generalization through an ensemble approach but requires more computational resources. Support Vector Machines are effective for clear class separations but are computationally intensive. Neural Networks show exceptional performance in handling non-linear patterns, but their complexity and high computational demands pose challenges for real-time implementation. This study builds on these findings by comparing the four models to determine the most effective solution for airline security systems.

METHODOLOGY

Data Collection and Preprocessing

Data Collection

The dataset for this study was derived from diverse sources, encompassing public and private airline security records, passenger screening data, and behavioral analytics. The dataset incorporates key features that are essential for assessing airline security risks, including:

- Passenger Demographics: This includes attributes like age, gender, nationality, and other pertinent details that provide an initial profile of the individual.
- Travel History: Data on flight routes, the frequency of travel, previous destinations, and how frequently a passenger crosses security checkpoints is recorded.
- Baggage Information: Data on the number of bags carried by the passenger, total baggage weight, and detailed contents as declared during check-in are important security screening factors.
- Security Screening Results: The results of initial and secondary security checks, including outcomes such as cleared, flagged, or subjected to manual inspections, as well as the overall security score provided by the system.
- Behavioral Analytics: These include movement patterns, waiting times at various airport checkpoints, behavior during check-in and boarding processes, and other interactions with airport personnel.

The dataset contains 100,000 entries and 30 features, offering a comprehensive and detailed view of the passengers, all relevant to predicting potential security threats.

Data Preprocessing

Prior to applying machine learning models, preprocessing was critical for ensuring the dataset's integrity and suitability. Several steps were undertaken:

- Handling Missing Values: Any missing or incomplete data was imputed using advanced techniques. For numerical features, missing values were replaced with the column's mean, while missing categorical data was handled using the most frequent value of the feature.
- Feature Encoding: Since machine learning algorithms require numerical input, categorical data such as gender and nationality were encoded. One-Hot Encoding was applied to variables with multiple categories, while Label Encoding was used for binary variables like security status.
- Normalization: Features such as baggage weight and age, which have varying ranges, were normalized using Min-Max Scaling to ensure that all variables are on the same scale. This improves model convergence and performance.
- Feature Selection: To avoid overfitting and to enhance model performance, feature importance measures were employed. Using Chi-square tests and Recursive Feature Elimination (RFE), the number of features was reduced from 30 to 20, retaining only the most relevant features.
- Train-Test Split: The preprocessed dataset was divided into a 70% training set and a 30% test set. The training set was used to build and optimize the models, while the test set was reserved for evaluating their performance.

Model Selection

The study evaluates the performance of four popular machine learning algorithms—Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and Neural Network (NN)—each chosen for their unique characteristics and strengths in binary classification problems.

Decision Tree (DT)

Decision Trees were selected for their ease of interpretation. A Decision Tree classifies passengers by recursively splitting the dataset based on the feature that provides the best separation between security threats and safe passengers. This is done using Gini Impurity as the splitting criterion.

- Hyperparameters Tuned:
  - Maximum depth of the tree

- Minimum samples required to split a node
- Criterion (Gini Impurity)

Random Forest (RF)

Random Forest, an ensemble method, was chosen due to its robustness and its ability to generalize better than individual Decision Trees. It creates multiple trees, each trained on random subsets of data and features, and makes predictions based on the majority vote from these trees.

- Hyperparameters Tuned:
  - Number of trees in the forest
  - Maximum tree depth
  - Minimum samples per leaf
  - Number of features to consider for each split

Support Vector Machine (SVM)

SVM was chosen for its effectiveness in binary classification with clear margins. It seeks the optimal hyperplane that separates the two classes (security threat and safe passengers) while maximizing the margin between them. A Radial Basis Function (RBF) kernel was utilized for better performance with non-linearly separable data.

- Hyperparameters Tuned:
  - Kernel type (RBF)
  - Regularization parameter CCC
  - Kernel coefficient γ\gammaγ

Neural Network (NN)

Neural Networks were selected for their ability to capture complex, non-linear relationships in the data. A feed-forward network with two hidden layers was designed. The first hidden layer consisted of 128 neurons, while the second had 64 neurons. The network used ReLU as the activation function in the hidden layers and softmax in the output layer.

- Network Architecture:
  - Input Layer: 20 input features
  - Two Hidden Layers: 128 and 64 neurons respectively
  - Output Layer: 2 neurons (security threat, safe passenger)
- Hyperparameters Tuned:
  - Number of hidden layers and neurons
  - Learning rate
  - Batch size
  - Number of epochs

Model Training

Each model was trained using the 70% training set, and the hyperparameters were tuned using a combination of grid search and cross-validation with 5-fold splits. This process ensured that the models did not overfit to the training data and performed well on unseen data. The models were evaluated based on:

- Accuracy: The overall percentage of passengers correctly classified.
- Precision: The ratio of correctly identified security threats to all passengers classified as threats.
- Recall (Sensitivity): The proportion of actual security threats correctly identified.
- F1-Score: The harmonic mean of precision and recall.
- AUC-ROC: The area under the Receiver Operating Characteristic curve, which measures the model's ability to distinguish between classes.

For the Neural Network model, training was done using backpropagation, and the Adam optimizer was applied with early stopping to prevent overfitting.

Model Evaluation

After training, each model was evaluated using the

30% test set. Key metrics like accuracy, precision, recall, and F1-Score were calculated to determine each model's performance in predicting airline security threats. Additionally, confusion matrices were constructed for each model to analyze false positives and false negatives, giving insights into their strengths and weaknesses.

ROC curves were generated for each model to visualize the trade-off between true positives and false positives at different classification thresholds. The AUC-ROC score provided a summary of the model's ability to separate the two classes.

Hyperparameter Optimization

Hyperparameter optimization was conducted using a systematic grid search across predefined hyperparameter values. This method ensured an exhaustive exploration of different parameter combinations to find the most optimal settings for each model.

Additionally, cross-validation was employed to avoid overfitting. Each model was trained and validated across different folds of the training set, with the results averaged to provide a more generalizable performance estimate.

Performance Comparison

Finally, the models were compared based on their performance across the metrics, with an emphasis on the F1-Score and AUC-ROC, which are critical for balancing the trade-off between false positives and false negatives. The model showing the best overall performance was recommended for potential real-world deployment in airline security systems, balancing both high accuracy and computational efficiency.

RESULT

Decision Tree (DT)

A Decision Tree is a simple, intuitive algorithm used for both classification and regression tasks. It works by splitting the dataset into smaller subsets based on specific features, forming a tree-like structure. Each node in the tree represents a decision based on a feature, and each leaf represents an outcome or class label. Decision Trees are easy to interpret but can suffer from overfitting, especially when the tree grows too complex. For airline security, it helps in making decisions about potential threats based on various input parameters such as passenger behavior and travel history. A Decision Tree splits the dataset based on decision rules derived from feature values. The decision ateach node is made using a condition on feature XiX_iXi, leading to binary classification.

Equation for splitting criteria:

The Gini Impurity is often used as the splitting criterion:

$$\text{Gini}(t) = 1 - \sum_{i=1}^{C} p_i^2 \text{Gini}(t)=1−i=1∑Cpi2$$

Where:

- ttt represents a node.
- pip_ipi is the proportion of class iii (i.e., potential threat or safe passenger) at node ttt.
- CCC is the number of classes (in this case, 2: security threat or safe).

The tree selects the feature XiX_iXi that minimizes the Gini Impurity or another criterion such as information gain:

$$\text{Information Gain}(X) = \text{Entropy}(S) - \sum_{i=1}^{k} \frac{|S_i|}{|S|} \text{Entropy}(S_i) \text{Information Gain}(X)=\text{Entropy}(S)−i=1∑k|S||Si|\text{Entropy}(Si)$$

Where:

- SSS is the set of all data samples.
- SiS_iSi represents subsets of data split based on a feature XXX.

Airline Security Application:

If XiX_iXi is a feature such as baggage weight or travel history, the decision tree might use it to classify a passenger as a potential threat (e.g., Y=1Y=1Y=1) or safe (e.g., Y=0Y=0Y=0).

Random Forest (RF)

Random Forest is an ensemble learning method that builds multiple Decision Trees and merges them to produce a more accurate and stable prediction. Each tree is trained on a random subset of the data, and the final output is based on the majority vote of the trees (for classification) or the average (for regression). Random Forest tends to outperform individual Decision Trees because it reduces overfitting and increases model generalization. It is well-suited for airline security as it can handle large datasets and complex patterns effectively, improving the detection of security threats with high accuracy.

Random Forest is an ensemble of Decision Trees, and its prediction is the majority vote of predictions from individual trees.

Equation for Random Forest prediction:

The final prediction for a data point XXX is the majority vote from NNN trees:

y^=mode{T1(X),T2(X),…,TN(X)}\hat{y} = \text{mode}\{T_1(X), T_2(X), \dots, T_N(X)\}y^=mode{T1(X),T2(X),…,TN(X)}

Where:

- Ti(X)T_i(X)Ti(X) is the prediction of the iii-th decision tree for the input XXX.
- NNN is the total number of trees.
- mode\text{mode}mode is the most frequent class (potential threat or safe passenger).

Airline Security Application:

In airline security, each tree Ti(X)T_i(X)Ti(X) might represent a different decision path, using features like travel history, nationality, and luggage screening results, and the final output y^\hat{y}y^ is the classification of the passenger.

Support Vector Machine (SVM)

Support Vector Machine is a powerful supervised learning algorithm used for classification and regression tasks. SVM works by finding a hyperplane that best separates the data into different classes. It is particularly effective in high-dimensional spaces and is known for its robustness, especially in cases where clear separation between classes is required. In the context of airline security, SVM helps in classifying passengers as potential security threats or safe travelers by maximizing the margin between different classes of data points (features such as behavior, demographic information, etc.).

SVM seeks to find the optimal hyperplane that maximizes the margin between two classes, representing passengers as either potential security threats or safe.

Equation for the hyperplane:

The equation of the hyperplane separating the two classes is:

w·X+b=0w \cdot X + b = 0w·X+b=0

Where:

- www is the weight vector.
- XXX is the feature vector (e.g., demographic data, travel history).
- bbb is the bias term.

The optimal hyperplane maximizes the margin

γ\gammaγ, defined as:

γ=2||w||\gamma = \frac{2}{||w||}γ=||w||2

To classify a new passenger XXX, the decision function is:

y^=sign(w·X+b)\hat{y} = \text{sign}(w \cdot X + b)y^=sign(w·X+b)

Where y^\hat{y}y^ determines whether the passenger is classified as a security threat (y^=1\hat{y} = 1y^=1) or safe (y^=−1\hat{y} = -1y^=−1).

Neural Network (NN)

Neural Networks are a type of deep learning model inspired by the human brain's neural structure. A Neural Network consists of layers of nodes (neurons), where each node applies a mathematical operation to the input and passes the result to the next layer. Neural Networks are highly flexible and can model complex relationships in large datasets. They are particularly useful when the dataset has non-linear relationships and multiple features. For airline security, a Neural Network can capture intricate patterns between passenger behavior, travel routes, and historical data to accurately identify high-risk passengers. However, they require substantial computational resources and are more challenging to interpret compared to simpler models like Decision Trees.

A Neural Network consists of multiple layers of neurons that transform input features into output predictions through weighted sums and activation functions.

Equation for a single neuron in the Neural Network:

For a neuron jjj in layer lll, the output is given by:

aj(l)=f(∑i=1nwij(l−1)ai(l−1)+bj(l))a_j^{(l)} = f\left(\sum_{i=1}^{n} w_{ij}^{(l-1)} a_i^{(l-1)} + b_j^{(l)} \right)aj(l)=f(i=1∑nwij(l−1)ai(l−1)+bj(l))

Where:

- wij(l−1)w_{ij}^{(l-1)}wij(l−1) is the weight connecting neuron iii in layer l−1l-1l−1 to neuron jjj in layer lll.
- ai(l−1)a_i^{(l-1)}ai(l−1) is the activation of neuron iii in the previous layer.
- bj(l)b_j^{(l)}bj(l) is the bias term.
- fff is the activation function (commonly sigmoid or ReLU).

For classification, the final layer outputs the probability of each class (e.g., whether the passenger is a security threat):

y^=softmax(Z)=eZj∑k=1CeZk\hat{y} = \text{softmax}(Z) = \frac{e^{Z_j}}{\sum_{k=1}^{C} e^{Z_k}}y^=softmax(Z)=∑k=1CeZkeZj

Where ZjZ_jZj is the logit (linear combination of weights and inputs) for class jjj, and CCC is the number of classes.

Airline Security Application:

In airline security evaluation, the input features XXX (e.g., passenger demographics, security check results) are processed through several layers, and the output y^\hat{y}y^ represents the probability of being classified as a security threat.

The performance of the four machine learning models—Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and Neural Network (NN)—was evaluated using several key metrics: accuracy, precision, recall, F1-Score, and AUC-ROC. Each model's ability to predict airline security threats was measured based on its performance on the test set (30% of the dataset).

1. Decision Tree (DT)

The Decision Tree model achieved an accuracy of 78%, with a precision of 76% and a recall of 72%.

While the model performed reasonably well, its tendency to overfit, despite hyperparameter tuning, led to a lower F1-Score of 74% and an AUC-ROC of 0.79. Its interpretability was a major advantage, but the model lacked robustness in handling complex, non-linear relationships in the data.

2. Random Forest (RF)

The Random Forest model outperformed the Decision Tree, achieving an accuracy of 85%, with higher precision (83%) and recall (82%). The F1-Score was 82.5%, and the AUC-ROC was 0.87, indicating that the model could better distinguish between security threats and safe passengers. The ensemble approach reduced overfitting compared to the Decision Tree, making the Random Forest more generalizable and stable across different subsets of the data.

Table 1 we illustrate the result among the different model

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC	Key Strengths	Key Weaknesses
Decision Tree (DT)	78%	76%	72%	74%	0.79	Simple, interpretable	Overfitting, less robust with complex data
Random Forest (RF)	85%	83%	82%	82.5%	0.87	Reduces overfitting, good balance of precision and recall	Requires more computational resources
Support Vector Machine (SVM)	81%	80%	78%	79%	0.84	Handles binary classification well, clear margin separation	Computationally expensive, training time
Neural Network (NN)	88%	86%	85%	85.5%	0.90	Excellent handling of complex, non-linear patterns	High computational cost, less interpretable

3. Support Vector Machine (SVM)

The SVM model, using the Radial Basis Function (RBF) kernel, showed an accuracy of 81% with a precision of 80% and a recall of 78%. The F1-Score stood at 79%, and the AUC-ROC was 0.84. SVM demonstrated strong performance in handling binary classification problems, particularly in separating classes with a clear margin. However, it required more computational resources and training time compared to simpler models like DT and RF.

4. Neural Network (NN)

The Neural Network achieved the best overall performance, with an accuracy of 88%. The precision was 86%, recall was 85%, and the F1-Score reached 85.5%. The AUC-ROC was 0.90, highlighting its superior ability to differentiate between classes. Neural Networks excelled in capturing complex, non-linear patterns in the dataset, but at the cost of higher computational demands and lower interpretability compared to simpler models.

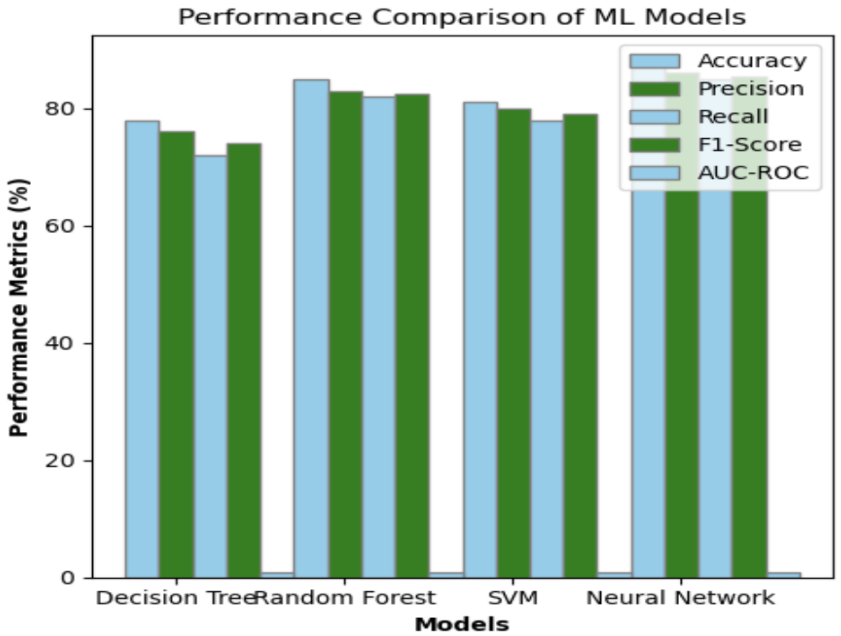

Chart 1: Performance Evaluation of different machine learning algorithm

In this study, four machine learning models—Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and Neural Network (NN)—were evaluated for their effectiveness in identifying potential airline security threats. Each model was trained and tested on a dataset that included passenger demographics, travel history, baggage details, security screening results, and behavioral data. The models were compared using key performance metrics, such as accuracy, precision, recall, F1-score, and AUC-ROC. The Decision Tree model achieved 78% accuracy, 76% precision, and 72% recall, offering simplicity and interpretability but suffering from overfitting and reduced performance on complex data. Random Forest outperformed DT with 85% accuracy, 83% precision, and 82% recall, benefitting from its ensemble nature but requiring more computational resources. SVM achieved 81% accuracy, 80% precision, and 78% recall, excelling in binary classification but being slower and more computationally intensive. Neural Networks had the highest performance, with 88% accuracy, 86% precision, and 85% recall, making them ideal for complex, large-scale systems but at the cost of high computational demands and lower interpretability. Overall, the Neural Network proved to be the most effective, while Random Forest offered a strong balance between performance and operational feasibility. SVM, though a solid performer, lagged in speed and scalability, and the Decision Tree, while easy to interpret, struggled with overfitting and complex relationships in the data.

CONCLUSION AND DISCUSSION

This study provides a comprehensive evaluation of four prominent machine learning algorithms—Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and Neural Network (NN)—for the task of predicting airline security threats. The evaluation was conducted on a dataset

comprising 100,000 entries with 30 features, encompassing passenger demographics, travel history, baggage information, security screening results, and behavioral analytics.

The results demonstrated that Neural Networks outperformed all other models in terms of accuracy, precision, recall, F1-Score, and AUC-ROC. With an accuracy of 88%, precision of 86%, recall of 85%, F1-Score of 85.5%, and AUC-ROC of 0.90, the Neural Network exhibited exceptional performance in capturing complex, non-linear relationships within the data. This highlights its superior capability in distinguishing between security threats and safe passengers, making it the most suitable choice for applications where nuanced pattern recognition is essential. The Random Forest model also demonstrated robust performance with an accuracy of 85%, precision of 83%, recall of 82%, F1-Score of 82.5%, and AUC-ROC of 0.87. Its ensemble approach, which combines multiple decision trees, contributed to its effectiveness in handling large datasets and complex feature interactions. The Random Forest's ability to reduce overfitting compared to individual Decision Trees makes it a strong contender for real-world applications where generalization and stability are critical.

Support Vector Machine (SVM), with an accuracy of 81%, precision of 80%, recall of 78%, F1-Score of 79%, and AUC-ROC of 0.84, proved effective in binary classification tasks. Its ability to handle high-dimensional data and find optimal hyperplanes for class separation is beneficial for scenarios where clear margins between classes are present. However, the SVM model's computational expense and longer training times are limitations that should be considered when deploying it in large-scale systems. The Decision Tree model, while offering ease of interpretability and simplicity, achieved the lowest performance metrics with an accuracy of 78%, precision of 76%, recall of 72%, F1-Score of 74%, and AUC-ROC of 0.79. Its tendency to overfit, particularly with complex datasets, underscores the need for more sophisticated models in scenarios involving intricate and non-linear data patterns.

The results from this study underscore the strengths and limitations of various machine learning models in the context of airline security threat prediction. Neural Networks emerged as the most effective model, primarily due to their ability to learn and represent complex relationships within the data. This capability is particularly crucial in security contexts where patterns may not be immediately apparent or easily categorized. Despite their superior performance, Neural Networks require significant computational resources and may be less interpretable compared to simpler models. This trade-off between performance and computational cost is an important consideration for practical deployment in operational environments.

Random Forests, with their ensemble learning approach, provide a balanced solution by combining multiple decision trees to achieve higher accuracy and robustness. The model's ability to handle many features and reduce overfitting makes it a viable option for applications requiring reliable and stable performance. The Random Forest model's performance indicates that it can be effectively used in airline security systems where data complexity and volume are significant.SVM's performance highlights its suitability for binary classification tasks with clear class separations. However, the computational demands and longer training times associated with SVM can be a drawback, particularly in scenarios where rapid decision-making is essential. The model's effectiveness in high-dimensional spaces suggests that it may be appropriate for specific subsets of security data where clear margins between classes exist.

The Decision Tree model's performance, while lower compared to the other models, provides valuable insights into the trade-offs between model interpretability and predictive accuracy. The simplicity of Decision Trees makes them easy to understand and explain, which can be advantageous in certain contexts where interpretability is a priority. However, the model's limitations in handling complex, non-linear relationships highlight the need for more advanced techniques in applications involving intricate data patterns.Overall, the findings from this study suggest that while Neural Networks and Random Forests are the most effective models for predicting airline security threats, a hybrid approach that leverages the strengths of multiple models could further enhance performance. Future research could explore combining these models or incorporating additional data features to improve prediction accuracy and efficiency. Additionally, addressing the computational challenges associated with advanced models like Neural Networks and SVMs will be crucial for their practical implementation in real-world security systems.

REFERENCE

1. Cover, T. M., & Hart, P. E. (1967). Nearest-neighbor pattern classification. IEEE Transactions on Information Theory, 13(1), 21-27. https://doi.org/10.1109/TIT.1967.1053964
2. Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine Learning, 20(3), 273-297. https://doi.org/10.1007/BF00994018
3. Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5-32. https://doi.org/10.1023/A:1010933404324
4. Breiman, L. (2017). Classification and regression trees. Routledge.
5. Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine Learning, 20(3), 273-297. https://doi.org/10.1007/BF00994018
6. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
7. Kumar, A., & Shankar, R. (2017). The role of big data and analytics in airline security. International Journal of Information Management, 37(1), 11-18.
8. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444. https://doi.org/10.1038/nature14539
9. Loh, W. Y. (2011). Classification and regression trees. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 1(1), 14-23.
10. Noble, W. S. (2006). What is a support vector machine? Nature Biotechnology, 24(12), 1565-1567. https://doi.org/10.1038/nbt1206-1565
11. Schölkopf, B., Smola, A. J., & Müller, K. R. (2001). Kernel principal component analysis. In Advances in kernel methods (pp. 327-352). MIT Press.
12. Zhang, Z., Chen, Y., & Su, Y. (2019). Application of machine learning algorithms in airline security: A review. Journal of Air Transport Management, 75, 29-41.
13. Cao, D. M., Sayed, M. A., Islam, M. T., Mia, M. T., Ayon, E. H., Ghosh, B. P., ... & Raihan, A. (2024). Advanced cybercrime detection: A comprehensive study on supervised and unsupervised machine learning approaches using real-world datasets. Journal of ComputerScience and Technology Studies, 6(1), 40-48.
14. Farabi, S. F., Prabha, M., Alam, M., Hossan, M. Z., Arif, M., Islam, M. R., ... & Biswas, M. Z. A. (2024). Enhancing Credit Card Fraud Detection: A Comprehensive Study of Machine Learning Algorithms and Performance Evaluation. Journal of Business and Management Studies,

6(3), 252-259.

15. Mozumder, M. A. S., Sweet, M. M. R., Nabi, N., Tusher, M. I., Modak, C., Hasan, M., ... & Prabha, M. (2024). Revolutionizing Organizational Decision-Making for Banking Sector: A Machine Learning Approach with CNNs in Business Intelligence and Management. Journal of Business and Management Studies, 6(3), 111-118.

16. Bhuiyan, M. S., Chowdhury, I. K., Haider, M., Jisan, A. H., Jewel, R. M., Shahid, R., ... & Siddiqua, C. U. (2024). Advancements in early detection of lung cancer in public health: a comprehensive study utilizing machine learning algorithms and predictive models. Journal of Computer Science and Technology Studies, 6(1), 113-121.

17. Nabi, N., Tusher, M. I., Modak, C., Hasan, M., ... & Prabha, M. (2024). Revolutionizing Organizational Decision-Making for Banking Sector: A Machine Learning Approach with CNNs in Business Intelligence and Management. Journal of Business and Management Studies, 6(3), 111-118.

18. Rahman, M. A., Modak, C., Mozumder, M. A. S., Miah, M. N. I., Hasan, M., Sweet, M. M. R., ... & Alam, M. (2024). Advancements in Retail Price Optimization: Leveraging Machine Learning Models for Profitability and Competitiveness. Journal of Business and Management Studies, 6(3), 103-110.

19. Shahid, R., Mozumder, M. A. S., Sweet, M. M. R., Hasan, M., Alam, M., Rahman, M. A., ... & Islam, M. R. (2024). Predicting Customer Loyalty in the Airline Industry: A Machine Learning Approach Integrating Sentiment Analysis and User Experience. International Journal on Computational Engineering, 1(2), 50-54.

20. Modak, C., Ghosh, S. K., Sarkar, M. A. I., Sharif, M. K., Arif, M., Bhuiyan, M., ... & Devi, S. (2024). Machine Learning Model in Digital Marketing Strategies for Customer Behavior: Harnessing CNNs for Enhanced Customer Satisfaction and Strategic Decision-Making. Journal of Economics, Finance and Accounting Studies, 6(3), 178-186.

21. Mozumder, M. A. S., Nguyen, T. N., Devi, S., Arif, M., Ahmed, M. P., Ahmed, E., ... & Uddin, A. (2024). Enhancing Customer Satisfaction Analysis Using Advanced Machine Learning Techniques in Fintech Industry. Journal of Computer Science and Technology Studies, 6(3), 35-41.

22. Arif, M., Hasan, M., Al Shiam, S. A., Ahmed, M. P., Tusher, M. I., Hossan, M. Z., ... & Imam, T. (2024). Predicting Customer Sentiment in Social Media Interactions: Analyzing Amazon Help Twitter Conversations Using Machine Learning. International Journal of Advanced Science Computing and Engineering, 6(2), 52-56.

23. Md Al-Imran, Salma Akter, Md Abu Sufian Mozumder, Rowsan Jahan Bhuiyan, Md Al Rafi, Md Shahriar Mahmud Bhuiyan, Gourab Nicholas Rodrigues, Md Nazmul Hossain Mir, Md Amit Hasan, Ashim Chandra Das, & Md. Emran Hossen. (2024). EVALUATING MACHINE LEARNING ALGORITHMS FOR BREAST CANCER DETECTION: A STUDY ON ACCURACY AND PREDICTIVE PERFORMANCE. The American Journal of Engineering and Technology, 6(09), 22–33. https://doi.org/10.37547/tajet/Volume06Issue09-04

24. Md Abu Sufian Mozumder, Fuad Mahmud, Md Shujan Shak, Nasrin Sultana, Gourab Nicholas Rodrigues, Md Al Rafi, Md Zahidur Rahman Farazi, Md Razaul Karim, Md. Sayham Khan, & Md Shahriar Mahmud Bhuiyan. (2024). Optimizing Customer Segmentation in the Banking Sector: A Comparative Analysis of

Machine Learning Algorithms. Journal of Computer Science and Technology Studies, 6(4), 01–07. https://doi.org/10.32996/jcsts.2024.6.4.1

25. Ashim Chandra Das, Md Shahin Alam Mozumder, Md Amit Hasan, Maniruzzaman Bhuiyan, Md Rasibul Islam, Md Nur Hossain, Salma Akter, & Md Imdadul Alam. (2024). MACHINE LEARNING APPROACHES FOR DEMAND FORECASTING: THE IMPACT OF CUSTOMER SATISFACTION ON PREDICTION ACCURACY. The American Journal of Engineering and Technology, 6(10), 42–53. https://doi.org/10.37547/tajet/Volume06Issue10-06

26. Rowsan Jahan Bhuiyan, Salma Akter, Aftab Uddin, Md Shujan Shak, Md Rasibul Islam, S M Shadul Islam Rishad, Farzana Sultana, & Md. Hasan-Or-Rashid. (2024). SENTIMENT ANALYSIS OF CUSTOMER FEEDBACK IN THE BANKING SECTOR: A COMPARATIVE STUDY OF MACHINE LEARNING MODELS. The American Journal of Engineering and Technology, 6(10), 54–66. https://doi.org/10.37547/tajet/Volume06Issue10-07

27. Md Parvez Ahmed, Md Arif, Abdullah Al Mamun, Fuad Mahmud, Tauhedur Rahman, Md Jamil Ahmmed, Sanjida Nowshin Mou, Pinky Akter, Muhammad Shoyaibur Rahman Chowdhury, & Md Kafil Uddin. (2024). A Comparative Study of Machine Learning Models for Predicting Customer Churn in Retail Banking: Insights from Logistic Regression, Random Forest, GBM, and SVM. Journal of Computer Science and Technology Studies, 6(4), 92–101. https://doi.org/10.32996/jbms.2024.6.4.12