ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

Performance Evaluation of a Hyperparameter Tuned Random Forest Algorithm Based on Artificial Bee Colony for Improving Accuracy and Precision of Crime Prediction Model

Hauwa Abubakar[1]; Souley Boukari[2]; Abdulsalam Ya'u Gital[3]; Fatima Umar Zambuk[4]

[1,2,3,4] Computer Science Department, Faculty of Computing Abubakar Tafawa Balewa University Bauchi, (ATBU) Bauchi, Nigeria

Publication Date: 2025/07/10

Abstract: Crime prediction is a crucial application of machine learning, enabling law enforcement to make proactive decisions. This research presents a novel crime prediction model that leverages a hybrid approach by tuning the hyperparameters of Random Forest (RF) classifier using the Artificial Bee Colony (ABC) optimization algorithm. The model was developed to improve the prediction accuracy and reliability of crime prediction systems by enhancing the performance of traditional machine learning classifiers. To validate the effectiveness of the proposed RF-ABC model, a comparative analysis against Decision Trees (DT), k-Nearest Neighbors (KNN), and the existing untuned Random Forest model was conducted. Experimental results demonstrate that the proposed RF-ABC model significantly outperforms the baseline models across multiple performance metrics. Specifically, the RF-ABC achieved an accuracy of 95%, precision of 90%, recall of 93%, and an F1-score of 90%. In comparison, the existing RF model yielded an accuracy of 81%, precision of 87%, recall of 84%, and an F1-score of 83%, while DT and KNN models recorded notably lower scores. DT obtained a PEI of 0.6900, PAI of 0.669 and RRI of 0.5200, while KNN has a PEI of 0.9647, PAI of 0.8670 and RRI of 0.5267, RF-ABC had the best result. PEI of 0.9800, PAI of 0.9000 and RRI of 0.7200. Crime prediction metrics show that These findings confirm that the integration of ABC with RF not only fine-tunes the hyperparameters efficiently but also enhances the model's predictive capabilities. The proposed hybrid approach shows promising potential for real-world crime analytic and decision support systems in law enforcement.

Keywords: *Crime Prediction, Hyperparameter, Artificial Bee Colony (ABC), Random Forest*.

How to Cite: Hauwa Abubakar; Souley Boukari; Abdulsalam Ya'u Gital; Fatima Umar Zambuk (2025). Performance Evaluation of a Hyperparameter Tuned Random Forest Algorithm Based on Artificial Bee Colony for Improving Accuracy and Precision of Crime Prediction Model. *International Journal of Innovative Science and Research Technology*, 10(6), 2952-2965. https://doi.org/10.38124/ijisrt/25jun1821

I. INTRODUCTION

Crime prediction leverages criminology, data science and machine learning, to forecast criminal activities using historical data. While advancements in big data and Artificial Intelligence (AI) have enhanced predictive accuracy, challenges persist with dynamic crime data, including issues of over-fitting, under-fitting, and the lack of transparency in "black-box" models like deep learning [1]. This concept has been significantly bolstered by advancements in technology, particularly in the realms of big data and AI. [2]. In addition to preventing crime, accurate predictions can significantly improve the allocation of law enforcement resources [3]. Moreover, accurate crime prediction can aid in solving crimes more efficiently by identifying patterns and correlations that may not be immediately apparent to human [4]. By uncovering these insights, law enforcement agencies can more quickly narrow down suspects, identify potential witnesses, and gather crucial evidence. This leads to faster resolutions of cases, increased clearance rates, and a greater sense of justice for victims.

Despite its potential benefits, crime prediction is not without its challenges and criticisms. One major concern is the risk of reinforcing existing biases in the data. If historical data reflects biased policing practices, predictive models may perpetuate these biases, leading to disproportionate targeting of certain communities.

Crime prediction process typically begins with data collection, where extensive datasets from various sources such as police reports, social media, economic indicators, and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

environmental sensors are gathered. This data is then cleaned, processed, and analyzed using sophisticated algorithms and statistical models. [5] By utilizing advanced data analytics and machine learning algorithms, such as Random Forests, law enforcement agencies can transition from reactive to proactive policing. [6]. However, achieving accuracy in crime prediction necessitates careful attention to data quality, algorithmic transparency, interpretability, and ethical considerations to ensure responsible and equitable use of these technologies.

The rapid evolution of technology and the increasing availability of data have catalyzed the development of predictive models across various domains, including crime prediction. However, despite numerous advancements, existing crime prediction algorithms often fail to meet the stringent requirements of accuracy, precision, and interpretability [7]. This inadequacy hampers their practical deployment and effectiveness in real-world scenarios where proactive crime prevention measures are crucial. Traditional crime prediction models frequently struggle with achieving high accuracy and precision [8]. This limitation is exacerbated by the dynamic and diverse nature of crime data, which can lead to either over-fitting or under-fitting. Consequently, these models may produce unreliable predictions, thereby reducing their utility for law enforcement agencies. While advanced machine learning techniques, such as deep learning, can achieve remarkable accuracy, they often function as "black boxes" [9]. The lack of transparency in their decision-making processes poses significant challenges for law enforcement agencies that require clear and interpretable insights to build trust, make informed decisions, and devise effective intervention strategies. Crime data is inherently complex and unpredictable, necessitating robust and adaptive modeling techniques. Current models often fall short in addressing this variability, resulting in sub-optimal predictions that hinder the development of proactive crime prevention strategies [10].

The aim of the work is to develop an Improved Random Forest algorithm that will enhance accuracy and precision of crime prediction model based on Artificial Bee Colony (ABC) hyper- parameter tuning and Recursive Feature Elimination with Cross Validation.

II. RELATED WORKS

The study provides an overview of **machine learning methods** relevant to crime prediction. It reviews **state-of-the-art techniques** that analyze crime data to identify patterns and develop predictive models, enhancing the accuracy and efficiency of crime forecasting. These techniques primarily analyze crime data to uncover patterns and generate predictive models. [11] investigates the influence of optimal hyper-parameters on machine learning algorithms for predicting heart disease, employing classifiers like Logistic Regression (LR), K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Decision Trees (DT), Random Forest (RF), and Extreme Gradient Boosting (XGBoost). The highest accuracy recorded was 87.9% with SVM, but the study faced challenges related to scalability and flexibility. [12] proposed hyper-parameter optimization for ensemble models in spam email detection using Grid-search for RF and XGBoost models. The results indicated high accuracy and sensitivity (97.78% and 98.09%, sensitivity of 98.44% and 98.84%, respectively), but it faced limitations in scalability and flexibility. [13] introduced a novel hyper-tuned ensemble Random Forest algorithm for detecting false basic safety messages in the Internet of Vehicles. The Random Forest (Ensemble RF) achieved better performance compared to KNN, DT, and other related works, but was constrained by computational costs due to exhaustive search methods. [14], focused on crime analysis and prediction using machine learning approaches within the context of the Hossana Police Commission. The study employed RF, DT, and KNN. They indicated that RF outperformed the others but was prone to overfitting, data quality issues, and high computational demands. [15], This research mapped crime risk terrains using machine learning, finding that RF outperformed KNN and kernel density estimation models at micro places but faced challenges related to interpretability and data quality. [7], discussed how advancements in technology and data availability have impacted predictive modeling for crime prediction, emphasizing that many algorithms struggle to meet accuracy and interpretability standards. [8], examined the challenges faced by traditional models leading to overfitting or under fitting issues. [5] compared KNN, DT and RF for crime prediction. The study analyzed various factors and patterns which the model identify areas or individuals that are at higher risk of being involved in criminal activities, The work make conclusion that a boosted decision tree classifier performed better than DT, KNN and RF. [16]), proposed a method for improving the model robustness of flood hazard mapping based on hyper-parameter optimization of Random Forest using Grid Search, Bayesian Optimization, Random Search and Gauss process, the Bayesian Optimization was found to be more efficient than Grid and Random search, especially for high-dimensional hyper-parameter spaces. Table1 Summarizes some of the relevant and related works.

Table 1 Summary of Related Works

SN	Authors	Methods	Result obtained	Limitation
1	[14]	RF, DT and KNN algorithms were used.	RF outperform DT and KNN having 81% Accuracy	Over fitting, interpretability, data quality, high computational requirements, and performed only classification,
2	[15]	Random Forests, KNN and Kernel Density Estimation	RF greatly outperforms other crime prediction models at micro places.	Interpretability, data quality, computational requirements, and ethical considerations
3	[2]	XGBoost machine learning method and SHAP method	It explores the integration of environmental factors, such as crime opportunity theory, routine	The trade-off between Interpretability and Transparency

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

			activity theory, rational choice theory, and crime pattern theory, into crime prediction models.	
4	[17]	Random Forest, Elastic Net, SVM	The study highlight the potential of ML models in identifying individuals at risk and devising proactive strategies to prevent criminal behavior among the population.	Refinement of risk prediction models is needed and variables with missing data were excluded from the analysis.
5	[18]	Na¨ıve Bayes (NB), K-Nearest Neighbour (KNN), Support Vector Machine (SVM), and Random Forest (RF).	The study accurately predict risks assessment it leverage a spatial and temporal data, and adapt to new information, handle large datasets and provide decision support.	Limited model accuracy when patterns of crime change over time
6	[5]	KNN, Decision tree, and Random forest	The study analyzed various factors and patterns which the model identify areas or individuals that are at higher risk of being involved in criminal activities.	Methods not Optimal

➢ *Framework for Crie Prediction using Random Forest with Parameter Optimization via Artificial Bee Colony Algorithm*

This framework predicts crime occurrences by analyzing historical crime data, socioeconomic factors, and spatiotemporal trends using a data-driven approach. It involves preprocessing and cleaning data, clustering crime records with K-Means to improve feature relevance, and reducing dimensionality through auto-encoders to retain key patterns while lowering complexity. The data is split into training, testing, and validation sets, ensuring balanced crime categories. A Random Forest model is trained and optimized using the Artificial Bee Colony (ABC) algorithm to enhance prediction accuracy and efficiency. The optimized model is then compared with Decision Trees and k-Nearest Neighbors (kNN) based on accuracy, precision, recall, F1-score, and computational efficiency. Finally, the framework evaluates feature importance and the effectiveness of ABC optimization, providing insights for practical crime monitoring and prevention. This integrated approach combines advanced techniques to improve the accuracy and applicability of crime prediction models

➢ *Simulation Framework for Crime Prediction Model using Random Forest Parameters Optimized with Artificial Bee Colony Optimization*

This framework details a virtual implementation of the crime prediction model, using structured steps for testing, validation, and analysis in a controlled environment. The process includes:

- *Data Preprocessing and Cleaning:*

Crime datasets are loaded, missing values imputed, outliers removed, numerical features normalized (Min-Max/Z-score), and categorical variables encoded (one-hot/label encoding).

- *Data Clustering with K-Means:*

Crime data is grouped by similarity, with optimal clusters determined via elbow/silhouette analysis.

- *Dimensionality Reduction via Autoencoder:*

An autoencoder neural network compresses data into lower dimensions, preserving essential patterns through reconstruction verification.

- *Data Splitting:*

Partitioning into training (70%), testing (20%), and validation (10%) sets, ensuring balanced crime category distribution.

- *Crime Prediction with ABC-Optimized Random Forest:*

A Random Forest classifier is trained, with hyperparameters (tree count, depth, etc.) optimized using the Artificial Bee Colony algorithm. Performance is evaluated on test/validation sets.

- *Model Comparison:*

Benchmarking against Decision Tree and KNN models using accuracy, precision, recall, F1-score, and computational efficiency.

- *Evaluation and Interpretation:*

Analyzing feature importance, ABC optimization impact, and deriving actionable insights for crime patterns. This end-to-end workflow leverages virtual tools and methodologies for robust algorithm testing, model validation, and hyperparameter optimization.

➢ *Research Gap*

Existing crime prediction models including linear regression, decision trees (DT), and support vector machines (SVM) struggle with overfitting and poor interpretability, compromising their accuracy, reliability, and trustworthiness. These limitations hinder law enforcement and policymakers from making data-driven decisions. Although [14] improved accuracy by combining DT, Random Forest (RF), and K-Nearest Neighbors (KNN), critical issues persist:

- *Unoptimized RF Hyperparameters*

Exacerbate overfitting and interpretability challenges.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

* *The Opaque Nature of RF Models*

Obscures prediction logic, limiting practical deployment.

To address these gaps, this research proposes a novel approach that enhances RF's strengths while prioritizing accuracy and interpretability. The goal is to develop a trustworthy model for effective crime prevention and control.

III. MATERIALS AND METHODS

The proposed system improves upon existing models by utilizing historical crime data with features like crime type, location, time, demographics, and weather. Data preprocessing involved handling missing values, encoding categorical variables, and normalizing numerical features. An autoencoder reduced data dimensionality and extracted meaningful features, followed by K-means clustering to group similar crimes. The dataset was split into training (70%), testing (15%), and validation (15%) sets. Random Forest (RF) was trained using bootstrap sampling and feature randomness at each tree split to reduce overfitting. The Artificial Bee Colony (ABC) algorithm optimized RF hyperparameters. Fully grown decision trees captured complex patterns, with classification based on majority voting and regression using averaged predictions. The model was evaluated using the testing data. The performance criteria include accuracy, precision, recall and F1 score, PAI, PEI and RRI etc. Figure 1 shows the Architecture of the proposed RF- ABC model. Figure 2 shows the framework of the proposed RF – ABC Model.

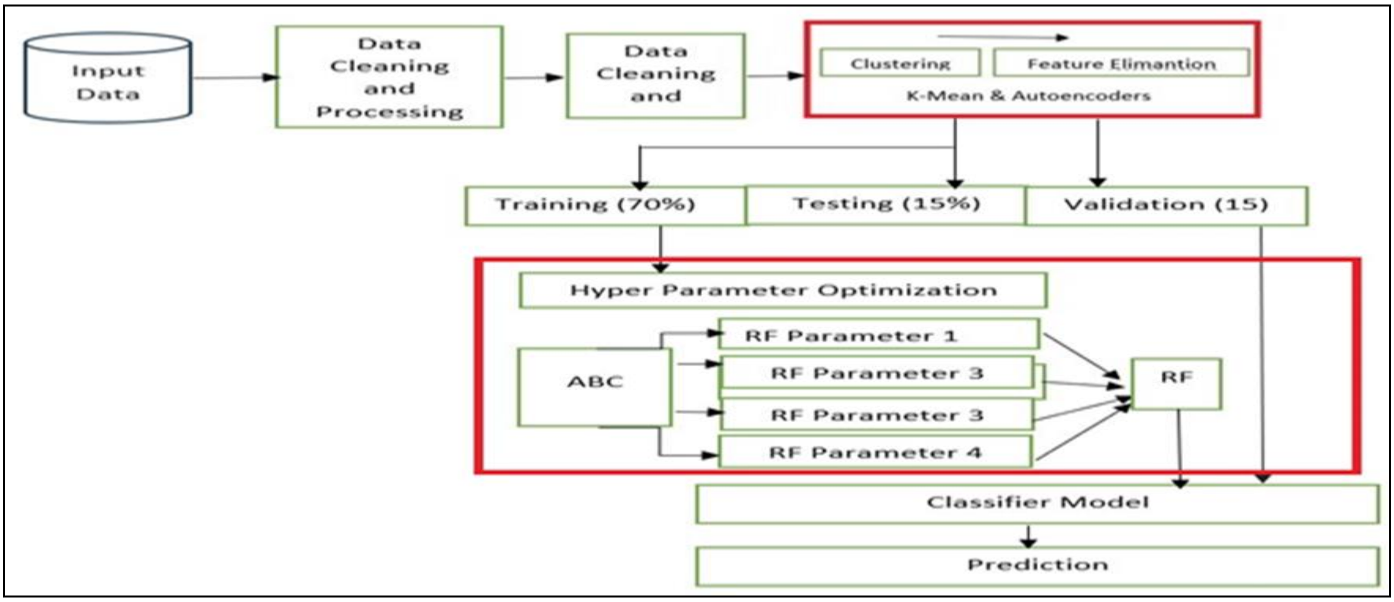

Fig 1 Architecture of the proposed RF- ABC
(Source: [19])

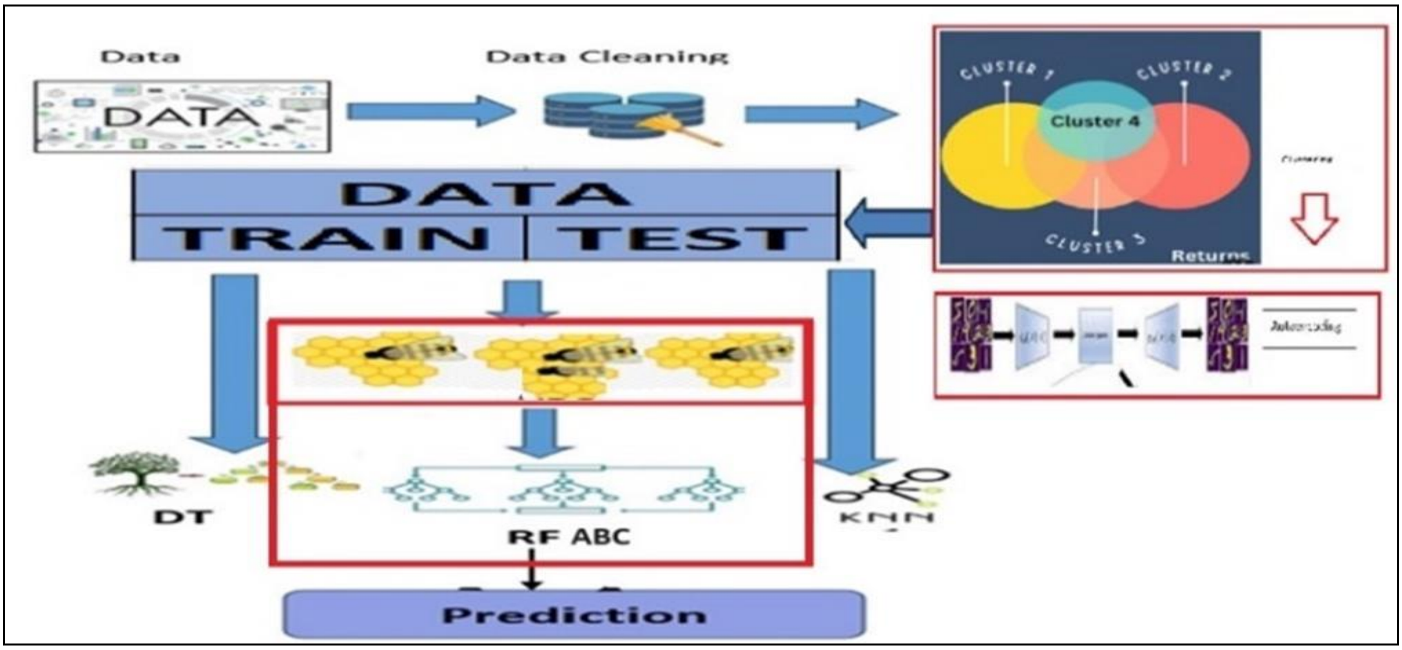

Fig 2 Framework of the proposed RF- ABC
(Source: [19])

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

➢ *Model selection and Training*

Random Forest is an ensemble learning method used for classification and regression. It builds multiple decision trees from bootstrapped samples of the data and combines their results to improve accuracy and reduce overfitting. Randomness is introduced by selecting a random subset of features at each split, which decreases correlation among trees. For classification (e.g., crime type prediction), the final decision is made by majority voting, while for regression (e.g., crime rate prediction), it averages the outputs of all trees. Model performance depends on hyperparameters like the number of trees, tree depth, and features considered for splits. The Artificial Bee Colony (ABC) algorithm is used to tune these hyperparameters effectively. The steps Random Forest and ABC algorithms are presented below:

Algorithm 1 RF

1. Initialize Random Forest Parameters (*T, L, S, G)*

2. *For* each *tree* draw a bootstrap sample with replacement from original *dataset* D_t

(Some data points may be repeated, and some may be left out: out-of-bag samples).

3. Build and Train Decision *Trees* h_t

At each node select random subset of m features based on *chosen criterion*

Split nodes using best feature

Continue splitting until *stopping criteria is met*

4. Aggregate *Prediction from all trees*

$P = mode\ (h_t, h_t, h_t, h_t, h_t, h_t \ldots\ldots\ldots)$

5. Output the final class or regression *(Y)*

Algorithm 2 ABC

1. Initialization: Initialize a population of potential solutions (bee colony). $X_i = (1=1,2, 3, n)$ and initialize ABC parameters Where each bee $X_i = X_0 + rand\ (0,1) * (X_{max} - X_{min})$

2. Determined the fitness of each search agent (Employed Bees Phase).

3. Each employed bee explores a new solution in its neighborhood *V*

$V = X_i + \alpha * (X_i - X_k)$ *where* X_k is a random solution and α is between [-1.1]

4. Onlooker Bees Phase perform *step 3. Using a probability based on fitness.*

5. Scout Bees *perform step 2&3 if* solution is not improved

6. *While number o*f explorations are repeated *(Iteration t < max_ iterations):*

7. *For* each search agent;

8. *Modify* the current search agent's position.

9. *Evaluate* the fitness of all search agents

10. Modify X_o, X_b, *and* X_c

11. $++t$

12. *End while*

Algorithm 3 RF-ABC

The algorithm for the hybrid Random Forest Algorithm with hyperparameters optimized using artificial bee colony is shown in the steps below. The flow chart of the proposed model is shown in figure 5.

Steps:

1. Initialization: Initialize ABC parameters and generate potential solutions (bee colony). $X_i = (1=1,2, 3, n)$ consisting of RF parameter (n_estimators max_depth, *min_samples_split, min_samples_leaf) Where each bee* $X_i = X_0 + rand\ (0,1) * (X_{max} - X_{min})$

2. Determined the fitness of each search agent *(Employed Bees Phase)*

1. Initialize Random Forest Parameters *(T, L, S, G)*

2. *For* each tree draw a bootstrap sample with replacement from original dataset D_t (Some data points may be repeated, and some may be left out: out-of-bag samples).

3. Build and Train Decision *Trees* h_t

4. At each node *select* random subset of m features based on chosen criterion

5. *Split* nodes using best feature

6. Continue splitting until stopping *criteria is met*

7. Aggregate Prediction from all tress $P = mode\ (h_t, h_t, h_t, h_t, h_t, h_t \ldots)$

8. Output the final class or regression *(Y)*

3. Each employed bee explores a new solution in its *neighborhood V*

4. $V = X_i + \alpha * (X_i - X_k)$ where X_k is a random solution *and α is between [-1.1]*

5. *Onlooker Bees P*hase perform step 3. Using a probability based on fitness.

6. Scout Bees perform step 2&3 if solution is not improved

7. While number of explorations are repeated *(Iteration t < max_iterations):*

8. *For* each search agent;

9. Modify the current search agent's position.

10. *Evaluate* the fitness of all search agents

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

11.	Modify X_o, X_b, *and* X_c
12.	*+ + t*
13.	*End while*

Fig 3 Flow Chart of the Proposed Model
(Source: [19])

➢ *Dataset*

The Chicago Crime Dataset is a publicly available dataset that contains detailed records of crimes reported in the city of Chicago, Illinois, USA. It is maintained by the Chicago Police Department and is part of the city's open data initiative. The dataset is widely used for research, analysis, and predictive modelling in criminology, urban planning, and data science (19). The original dataset comprised 228004 records and 22 attributes. These attributes include the offender's name, ID number, sex, age, education status, job, and marital status, as well as the victim's sex, age, and the place and type of crime. The dataset includes incidents from 2010 through May 2023. The system collects relevant data sources, such as crime incident reports, socio-demographic data, and environmental factors. The collected data was then prepossessed, cleaned, normalized, and integrated to create a comprehensive dataset for analysis. Data was then divided in to training data and testing data. Table 2 shows the overview of the database and Table 3 presents the description of each feature in the dataset. The table has 12 categorical features and 10 numerical features.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

Table 2 Overview of Database.

Item	Description
Name	Chicago crime
Data Source	Chicago crime dataset
Total Records	239,559
Total Columns	24
Total Features	23
Class	5
Categorical Values	5
Numerical Values	19
Class Distribution	6
Missing Values	6,222
Year	16-94 years
Period	12 Months

Table 3 Description of Features from Database.

S/n	Feature	Type	Full Name	Units
1	ID	Number	Identification Number	Number
2	Case Num	Categorical	Number of Case	Number
3	Date	Categorical	Date crime was committed	Date
4	Block	Categorical	Block crime was committed	Block
5	fUCR	Number	classification system	Classification
6	Prim Type	Categorical	Primary Type of crime	Type
7	Description	Categorical	Description of Crime	Description
8	Location	Categorical	Location crime was committed	Location
9	Gender	Categorical	Sex offender	Male/Female
10	Arrest	Categorical	Arrest was made	True/False
11	Domestic	Categorical	Domestic crime or not	True/False
12	Beat	Number	Geographic area	Location
13	District	Number	District crime was committed	District
14	Ward	Number	Ward crime was committed	Ward
15	Community	Number	community	Community
16	Crime Code	Categorical	code of crime	code
17	X Cord	Number	x coordinates	Degrees
18	Y Cord	Number	y coordinates	Degrees
19	Year	Categorical	Year of crime	2022-2022
20	Updated	Categorical	updated on database	Yes/No
21	Latitude	Number	Longitude	Degrees
22	Longitude	Number	Latitude	Degrees

➢ *Data Preprocessing*

The data used for model development was thoroughly cleaned and processed to ensure high quality, including handling missing values, removing noise and outliers, and converting file formats for compatibility. After cleaning, 228,004 records with 10 attributes were retained for the model development.

➢ *Feature Selection*

To improve crime prediction accuracy, the system used Recursive Feature Elimination (RFE). Recursive feature elimination is a popular feature selection algorithm that is often used [20]. This process allows feature elimination to identify the most important features in the dataset and rank them in order of importance. Another advantage is that it is less sensitive to the choice of tuning parameter, which can lead to more stable and reliable results [21].

➢ *Performance Evaluation Techniques*

The proposed model integrates Artificial Bee Colony (ABC) optimization with Random Forest (RF) to improve crime prediction accuracy and precision. Its performance is evaluated using several key techniques.

➢ *Evaluation Metrics*

The developed ensemble learning model's performance was evaluated using accuracy, precision, recall, and F1-score, assessing its effectiveness in predicting crime rates and types. Compared to baseline and existing methods, integrating the Artificial Bee Colony (ABC) algorithm for hyperparameter tuning strengthened the Random Forest model, resulting in improved performance and prediction quality.

- *Accuracy Rate*

Accuracy is a metric that measures how often a machine learning model correctly predicts the outcome. Accuracy is obtained by dividing the number of correct predictions by the total number of predictions

$$\text{Accuracy Rate} = \frac{TP+TN}{TP+FP+TN+FN} \tag{1}$$

- *Precision*

Precision measures the accuracy of a model's positive predictions by calculating the ratio of true positives to all predicted positives. It is especially useful for imbalanced datasets, reflecting how well the model identifies the target class. It is given as;

$$\text{Precision} = \frac{TP}{TP+FP} \tag{2}$$

- *Recall*

Recall is a metric that measures how often a machine learning model correctly identifies positive instances (true positives) from all the actual positive samples in the dataset. It is calculated by dividing the number of true positives by the number of positive instances. The latter includes true positives (successfully identified cases) and false negative results (missed cases).

$$\text{Recall} = \frac{TP}{TP+FN} \tag{3}$$

- *Predictive accuracy index (PAI)*

The Prediction Accuracy Index (PAI) measures how accurately a model predicts crime hotspots by comparing the variance of estimated responses during review and development phases. Unlike other metrics, PAI accounts for the size of study areas. The PAI is calculated as follows:

$$PAI = \left(\frac{TP+TN}{TP+TN+FP+FN}\right) \tag{4}$$

Where:

- ✓ TP: True Positives (correctly predicted crime hotspots)
- ✓ TN: True Negatives (correctly predicted non-crime hotspots)
- ✓ FP: False Positives (incorrectly predicted crime hotspots)
- ✓ FN: False Negatives (incorrectly predicted non-crime hotspots)

- *Interpretation of PAI:*

- ✓ *PAI > 0.5:*

Indicates good prediction accuracy, suggesting the model effectively identified both actual crime hot-spots and non-hotpots.

- ✓ *PAI = 0.5:*

Represents chance performance, suggesting the model does not significantly improve upon random guessing.

- ✓ *PAI < 0.5:*

Indicates poor prediction accuracy, suggesting the model frequently misidentified crime hot-spots.

- *Predictive Efficiency Index (PEI)*

The PEI measures how well a forecasting algorithm does compare to how well it could have done in forecasting the number of crimes [10]. The PEI can be expressed as a proportion (varies from 0 to 1) or a percentage (varies from 0 to 100).

The Predictive Efficiency Index (PEI) evaluates crime forecasting models by measuring both the accuracy of predictions and the resources needed to produce them.

The PEI is calculated as follows:

$$PEI = \left(\frac{TP+TN}{TP+TN+FP+FN}\right) * \left(\frac{T}{C}\right) \tag{5}$$

Where:

- ✓ TP is the number of true positives (correctly predicted crimes)
- ✓ TN is the number of true negatives (correctly predicted non-crimes)
- ✓ FP is the number of false positives (incorrectly predicted crimes)
- ✓ FN is the number of false negatives (incorrectly predicted non-crimes)
- ✓ T is the total number of predicted crimes
- ✓ C is the total number of actual crimes

The PEI ranges from 0 to 1, with a higher score indicating a better-performing model. PEI is a good measure because it considers both accuracy and resource efficiency. It is relatively easy to calculate and can be used to compare different models. On the contrast, PEI is sensitive to the distribution of crimes and PEI may not be suitable for all types of crime forecasting models. PEI also does not consider the severity of crimes.

- *Recapture Rate Index (RRI)*

The Recapture Rate Index (RRI) is a metric used to assess the precision of crime forecasting models, focusing specifically on their ability to recapture crime hotspots in a future period. It considers changes in crime density over time, making it a valuable tool for evaluating long-term forecasting performance. RRI is a measure of the percentage of actual crimes that are correctly predicted. The RRI is calculated as follows:

$$RRI = \left(\frac{HRR*HD}{HRR+HNR}\right) \tag{6}$$

Where:

- ✓ *HRR:*

Hotspots Recaptured Ratio = Number of predicted crime hotspots that were actual hotspots

in the future period / Total number of predicted crime hotspots.

- ✓ *HD:*

Historical Density = Average crime density across the entire study area in the historical period.

- ✓ *HNR:*

Hotspots Not Recaptured Ratio = Number of predicted crime hotspots that were not actual hotspots in the future period / Total number of predicted crime hotspots.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

- *Interpretation of RRI:*

✓ *RRI > 1:*
Indicates an increase in crime density in predicted hotspots, suggesting the model accurately identified potential hotspots.

✓ *RRI =1:*
Indicates that no change in crime density in predicted hotspots, meaning the model did not predict future crime patterns effectively.

✓ *RRI < 1:*
Indicates a decrease in crime density in predicted hotspots, suggesting the model overestimated future crime activity.

The Recapture Rate Index (RRI) emphasizes precision, aiding resource allocation and long-term crime prevention by accounting for changes in crime density over time. It is simple to calculate and interpret but is sensitive to how crime hotspots and thresholds are defined. RRI is less suitable for short-term forecasts due to reporting delays and does not directly measure the accuracy of predicted crime counts. [22].

➢ *Experimental Setup*
The model was implemented in MATHLAB 2019 The model was then experimented using the dataset specified in the design. The system used is a laptop, laptop System Core (TM) i5-5200U, 2.20 GHz CPU, 8.00 GB RAM, 500GB hard drive. ABC was used to obtain the optimal parameters of a RF model as a result enhancing its performance in crime prediction tasks. The table 4 below shows the parameters for the RF (default) and the search range for ABC (minimum, and maximum values). Table 5 shows the ABC parameters. The default parameter settings for the Random Forest are NumTrees 50, MaxNumSplits 2, MinLeafSize 1 and MinParentSize 10. The ABC searched for the optimal parameters setting between the minimal and maximum range for the parameters.

Table 4 Default and Optimal Parameters of Proposed Model

RF Parameters	**Default**	**Minimum**	**Maximum**
NumTrees	50	10	100
MaxNumSplits	2	1	100
MinLeafSize	1	1	5
MinParentSize	10	5	20

Table 5 ABC Parameters

RF Parameters	**Default**
Maximum Iteration	100
Population of Bees	50
Onlooker Bees	50
Abandonment Limit	0.6
Acceleration Coefficient	1

IV. RESULTS AND DISCUSSIONS

The results are analyzed in two key phases: the performance of the standalone Random Forest model and the improvements achieved by incorporating the ABC optimization. The discussion includes a detailed evaluation of critical performance metrics such as accuracy, precision, recall, and F1-score.

Table 6 Shows the Default Random Forest Parameters and the Optimal Parameters Obtained after Optimizing with ABC.

	DT	**KNN**	**Existing (RF)**	**Proposed (RF-ABC)**
Accuracy	74	79	81	95
Precision	86	81	87	90
Recall	68	70	84	93
F1-Score	78	69	83	90

Table 7 Parameters Values for Existing and Proposed Models

RF Parameters	**Existing**	**Optimal (Proposed)**
NumTrees	50	70
MaxNumSplits	2	4
MinLeafSize	1	5
MinParentSize	10	10

➢ *Here is a Summary of the Optimized Random Forest Hyperparameters:*

- *NumTree (Number of Trees):*
Increasing the number of trees from the default 50 to 70 improves model stability and performance, though gains diminish beyond this point and computational costs increase.

- *MaxNumSplits (Maximum Number of Splits):*
Allowing more splits helps the model capture complex

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

patterns, but too many splits risk overfitting. The optimal value found is 2.

- *MinLeafSize (Minimum Leaf Size):*
  Smaller leaf sizes capture finer details but may cause overfitting, while larger leaf sizes simplify the model and can improve generalization.

- *MinParentSize (Minimum Parent Size):*
  It generally controls the minimum number of samples required to split a node, balancing model complexity and overfitting.

This minimum parent size controls the minimum number of observations required in a node for it to be split. Reducing this value leads to more complex trees; while increasing it can simplify the model. A value between 5 and 10 is generally effective. After fine tuning the ABC arrived at a value of 10. Figure 2 shows the architecture of the proposed system.

➤ *Optimized RF Parameters Using ABC*

The Artificial Bee Colony (ABC) algorithm optimizes Random Forest (RF) hyperparameters like the number of trees, tree depth, and features per split by mimicking honeybee foraging behavior to efficiently explore solutions. This fine-tuning improves model generalization, reduces overfitting, and enhances accuracy and precision, especially in complex tasks like crime prediction. ABC iteratively evaluates and refines candidate solutions resulting in a more robust RF model that outperforms default or manually tuned versions.

➤ *Model Performance*

Table 8 presents the performance of models developed, it compares the performance metrics of a standard DT, KNN and Random Forest (RF) models with RF model enhanced with the ABC optimization algorithm, the accuracy for the models DT, KNN, RF and RF-ABC are 74, 79, 81 and 95 respectively, while the precision for DT, KNN, RF and RF-ABC are 86, 81, 87 and 90 respectively. The recall obtained by the models Recall are 68, 70, 84 and 93 respectively. While the F1 score is 78, 69, 83 and 90 respectively. The table 8 shows the results obtained. Figure 4 presents a bar chart showing the performance comparison of the four metrics for the crime prediction Models developed and tested.

Table 8 Performance Comparison the Proposed Model with the Other State of the Art Models

	DT	KNN	Existing (RF)	Proposed (RF-ABC)
Accuracy	74	79	81	95
Precision	86	81	87	90
Recall	68	70	84	93
F1-Score	78	69	83	90

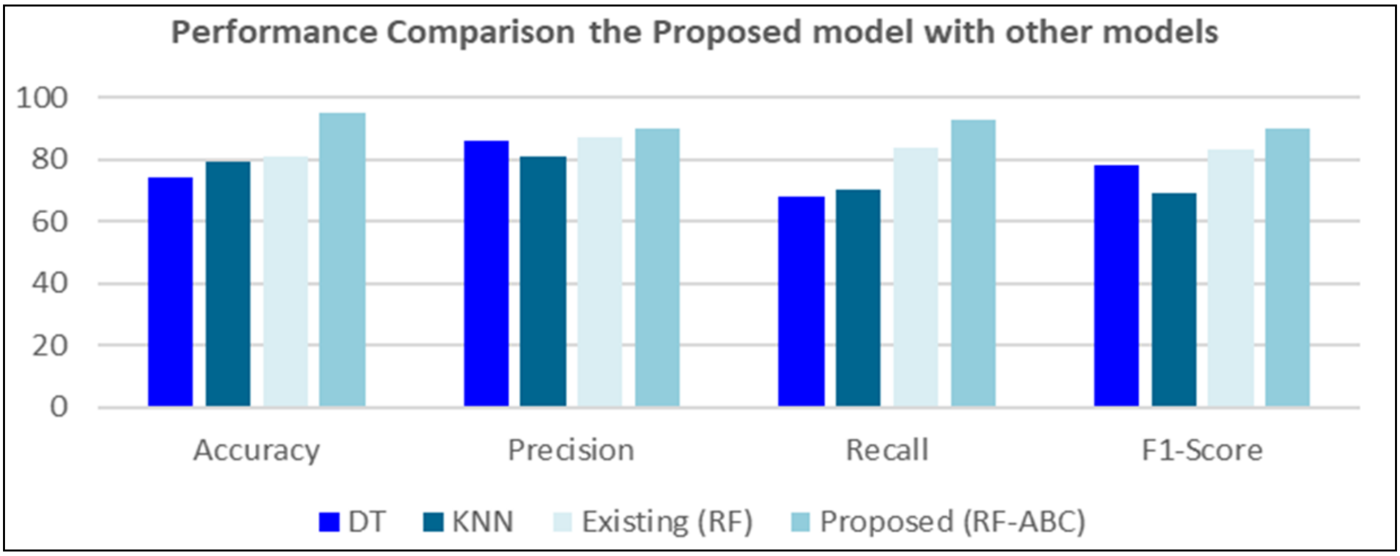

Fig 4 Performance Comparison the Proposed model with the other models

The RF-ABC model achieves an accuracy of 95%, which is significantly higher than the RF model's accuracy of 81%. This indicates that ABC optimization effectively improves the model's ability to make correct predictions across the dataset. The RF-ABC model performed better than RF, DT and KNN Models. Precision is slightly higher for the RF-ABC model (90%) compared to the standard RF (87%) and much better than DT (86%) and KNN (81%). This improvement reflects a reduced number of false positive predictions, suggesting that RF-ABC optimization helps in identifying the relevant features and reducing noise in the data. The RF-ABC model achieved the highest recall at 93%, outperforming the standard Random Forest (84%), Decision Tree (68%), and KNN (70%), indicating superior ability to identify true positives a crucial advantage in scenarios where missing actual cases has serious consequences. This strong recall is especially valuable for imbalanced datasets.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

In terms of F1-Score, which balances precision and recall, RF-ABC again led with 90%, followed by RF at 83%, DT at 78%, and KNN at 69%. KNN's low F1-Score suggests poor handling of noisy or complex data, while DT's moderate performance may be due to overfitting. The Random Forest model improved generalization and reduced overfitting, but the addition of ABC hyperparameter tuning further enhanced both accuracy and precision, making RF-ABC the best overall performer.

➢ *In Summary:*

- KNN (69%): Weakest, likely affected by noise or complexity.
- DT (78%): Better, but prone to overfitting.
- RF (83%): Stronger, with improved balance and generalization.
- RF-ABC (90%): Best performance due to optimized hyperparameters, achieving the highest accuracy and precision.

➢ *Crime Model performances*

The table 9 presents the performance of four crime analysis models DT, K-Nearest KNN, RF, and RF-ABC evaluated using three key crime-related indices: PEI, PAI, and RRI. Each index provides insight into how well these models predict, analyze, and assess crime trends.

Table 9 Performance Comparison Indices for the Crime Prediction Models

Parameter	DT	KNN	Existing (RF)	Proposed (RF -ABC)
PEI	0.6900	0.7117	0.9647	0.98
PAI	0.6617	0.6832	0.8670	0.90
RRI	0.5200	0.5023	0.5267	0.72

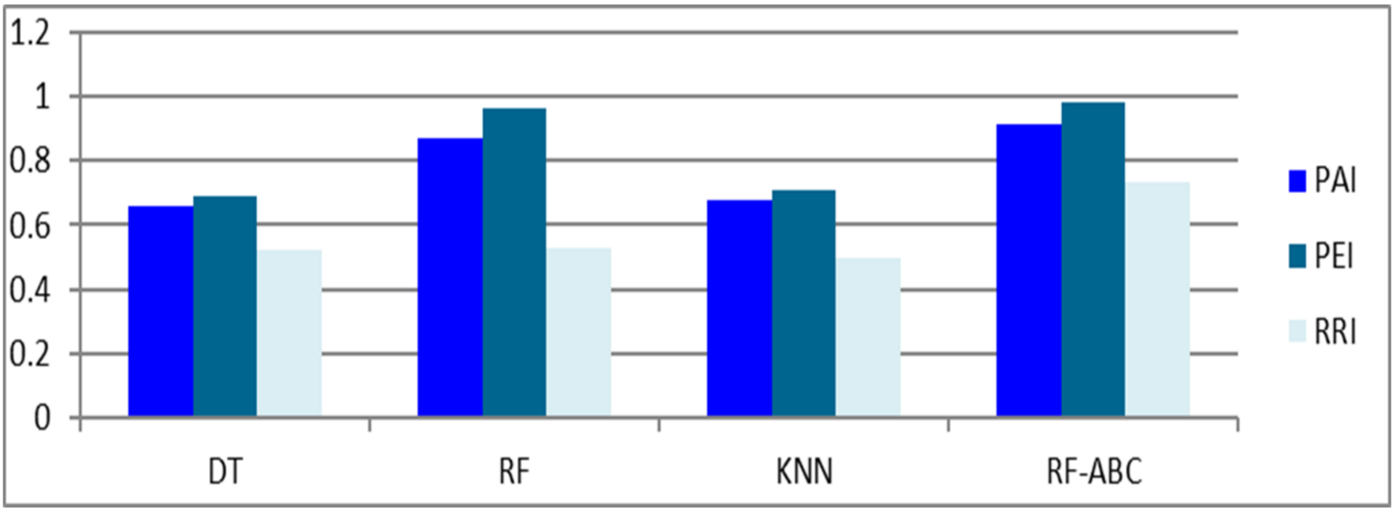

Fig 5 Performance comparison of the Crime indices of the prediction models

➢ *Predictive Efficiency Index (PEI)*

The Predictive Efficiency Index (PEI) evaluates how effectively a model distinguishes between crime and non-crime events. The RF-ABC model achieved the highest PEI (0.9811), demonstrating superior efficiency and accuracy in crime classification, thanks to ABC optimization fine-tuning Random Forest parameters. Standard Random Forest also performed well (PEI = 0.964) but was slightly less efficient without ABC optimization. KNN (0.7117) and Decision Tree (0.6900) had lower PEI scores, with KNN struggling on complex or overlapping data and DT being prone to overfitting, making both less reliable for accurate crime prediction. Overall, RF-ABC proved to be the most effective model for real-world crime prediction.

➢ *Predictive Accuracy Index (PAI)*

PAI measures how well models predict police actions based on crime trends. The RF-ABC model achieved the highest PAI (0.9006) due to enhanced feature selection and bias reduction from ABC optimization, making it highly effective for crime prevention and patrol planning. Standard Random Forest also performed well (0.8670) but was slightly less accurate without hyperparameter tuning. KNN (0.6832) and Decision Tree (0.6617) showed lower performance, struggling with dynamic crime patterns and nonlinear relationships, respectively. Overall, RF-ABC is the most accurate and reliable model for forecasting law enforcement activities.

➢ *Recapture Rate index (RRI)*

The Recapture Rate Index (RRI) evaluates how well a model identifies and distinguishes crime risks across locations, times, and demographic groups. The RF-ABC model achieved the highest RRI (0.7267), showing superior ability to detect subtle crime patterns and variations, making it valuable for targeted crime prevention and resource allocation. Standard Random Forest performed moderately (0.5267) but was less effective at differentiating crime risks. Decision Tree (0.5200) and KNN (0.5023) had the lowest RRI scores, struggling to accurately capture crime risk variations, which limits their usefulness for strategic crime prevention planning.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

➢ *Computational Resources*

- *Training Time:*

The training time for RF-ABC is 1291 seconds, compared to just 16 seconds for the standard RF model. This significant increase is due to the additional computational effort required by the ABC optimization algorithm, which searches for optimal hyperparameters or feature subsets. Table 10 shows the computational resources in terms of time and memory used by the developed models. The comparison of run time for various models is also presented in Figure 6.

Table 10 Comparison of Models Computational Resources.

	DT	KNN	Existing (RF)	Proposed (RF-ABC)
Time (s)	4	12	16	1291
Memory (kb)	1.3	1.6	2.81	2.85

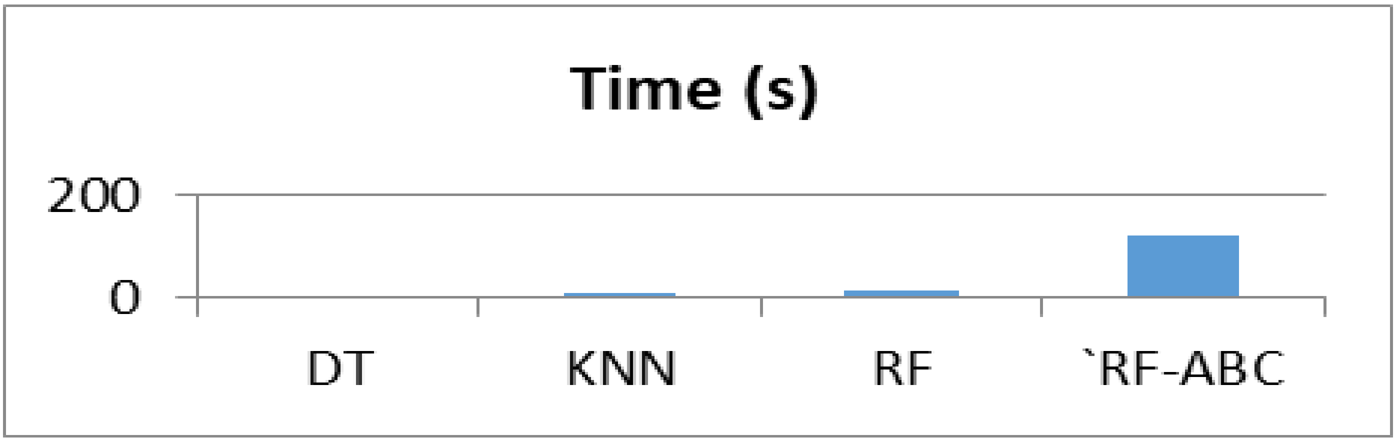

Fig 6 Graphical representation of Run Time of the crime prediction Models

➢ *Memory Usage*

From the table 10 and Figure 7, it can be seen that RF-ABC models use more memory due to the iterative nature of the ABC optimization process and the storage of intermediate results during hyperparameter tuning. The RF-ABC model shows clear advantages in terms of predictive performance (accuracy, precision, recall, and F1-Score). This makes it suitable for applications where accuracy is paramount and computational resources are not a constraint. However, the higher training time could be a drawback in real-time or resource-constrained environments. Additionally, the memory requirements (if higher) may limit the applicability in devices with limited hardware.

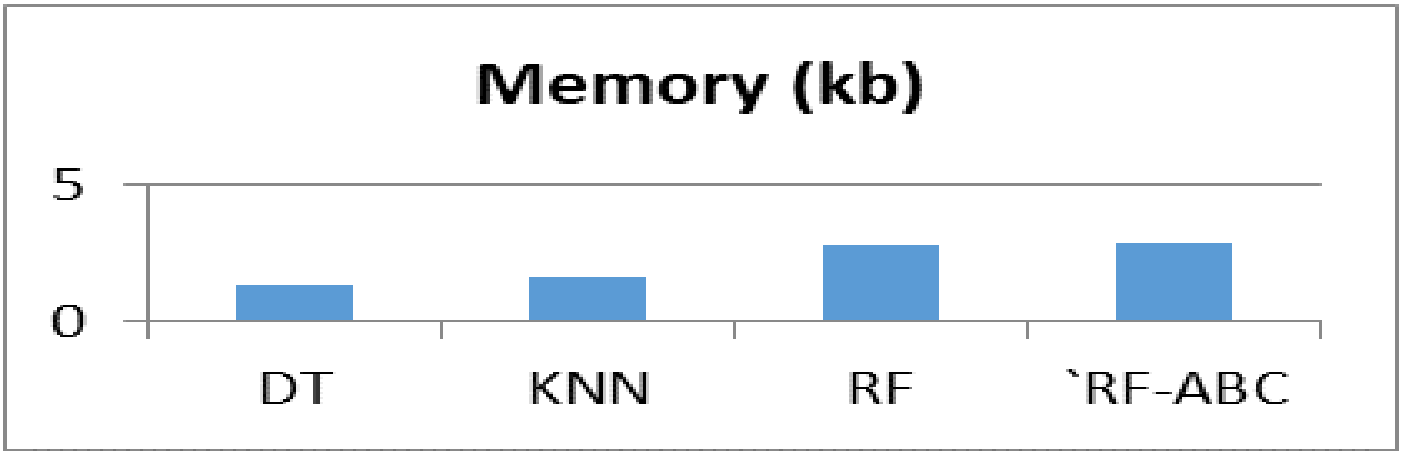

Fig 7 Graphical Representation of Memory Used for the Models

➢ *Confusion Matrix*

The confusion matrices for the Random Forest (RF) model and the RF model enhanced with ABC optimization (RF-ABC) show their crime prediction performance. The RF model predicted Burglary with 81.5% accuracy, Arson at 79%, and both Sex and Drug crimes at 80%, achieving an overall accuracy of 81.5%. In contrast, the RF-ABC model significantly improved predictions, achieving 95% accuracy for Burglary, 93.5% for Arson, 95.4% for Sex crimes, and 95.9% for Drug crimes, with an overall accuracy of 95.5%.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

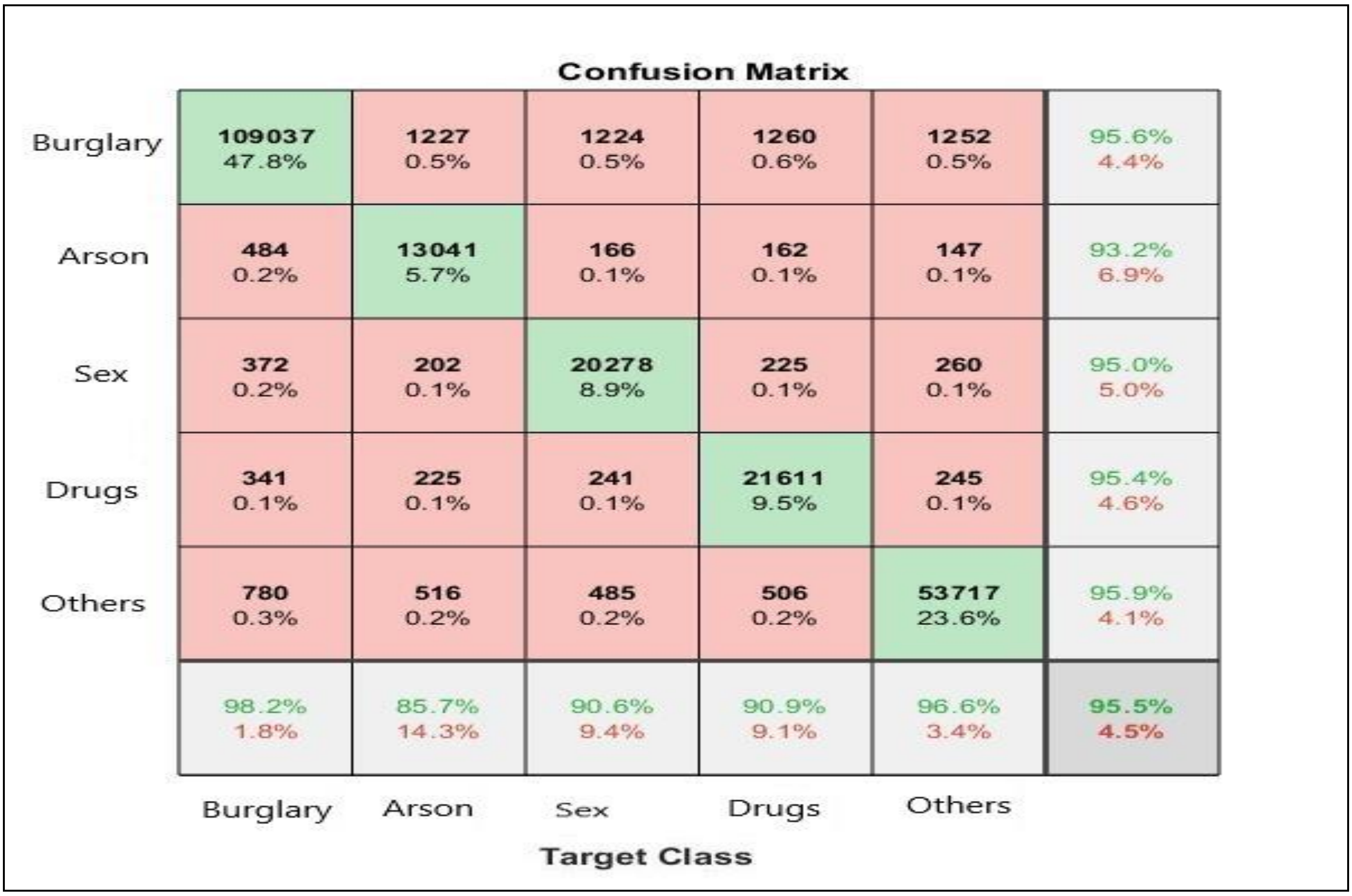

Fig 8 Confusion Matrix for Predicted Types using the RF-ABC Crime Prediction Model.

V. DISCUSSIONS

➢ *Ensemble Superiority:*

Both PEI and PAI metrics clearly show that ensemble methods (RF and RF-ABC) outperform the simpler DT and KNN approaches. The ensemble approach's ability to aggregate multiple decision trees provides a more robust and accurate prediction model for crime.

➢ *Impact of Optimization:*

The RF-ABC model consistently outperforms the standard RF across all three metrics, most notably in risk reduction (RRI). This demonstrates the potential benefits of applying an optimization algorithm, such as the Artificial Bee Colony algorithm, to fine-tune the model parameters or feature selection process. The improvements in PEI and PAI also suggest that the optimization not only enhances efficiency and accuracy but also contributes to more reliable predictions in risk-sensitive applications.

➢ *Risk Reduction Challenges:*

While the RF-ABC model significantly improves the RRI, the relatively lower values of RRI for DT, KNN, and even the standard RF indicate that risk reduction remains a challenging aspect of crime prediction. This might necessitate further research and development, possibly incorporating additional risk management strategies. or more sophisticated modeling techniques, to better address uncertainty and minimize prediction errors in high-stakes environments.

VI. CONCLUSIONS

The study demonstrates that for crime prediction tasks, the combination of ensemble learning with an optimization strategy RF-ABC enhances model performance across multiple evaluation metrics. These findings underscore the importance of not only selecting robust machine learning models but also optimizing them to better handle the complexities and risks associated with predicting criminal activities. The integration of ABC optimization significantly enhances the performance metrics of the Random Forest model, at the cost of increased computational time. For high-stakes applications where predictive accuracy is critical, the RF-ABC model is highly recommended. However, for less demanding tasks or real-time constraints, the standard RF model remains a viable option. Future work could explore additional optimization techniques or hybrid models to further refine these performance metrics, particularly the RRI, to support more effective and reliable crime prevention strategies.

ACKNOWLEDGEMENT

we will like to express our profound gratitude to Almighty Allah for making this work a successful one. We appreciate the collective efforts and support received from our department of Computer Science, Faculty of computing Abubakar Tafawa Baleawa University Bauchi (ATBU), Bauchi State, Nigeria

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun1821

REFERENCES

- [1]. Adeyemi, R. A., Mayaki, J., Zewotir, T. T., & Ramroop, S. (2021). Demography and Crime: A Spatial analysis of geographical patterns and risk factors of Crimes in Nigeria. *Spatial Statistics*, *41*, 100485.
- [2]. Zhang, H., GAO, Y., Yao, D., & Zhang, J. (2023). Interaction of Crime Risk across Crime Types in Hotspot Areas. ISPRS *International Journal of Geo-Information*, 12(4), 176.
- [3]. Bischl, B., Binder, M., Lang, M., Pielok, T., Richter, J., Coors, S., & Lindauer, M. (2023). Hyperparameter optimization: Foundations, algorithms, best practices, and open challenges. *Wiley Interdisciplinary Reviews:Data Mining and Knowledge Discovery*, *13*(2), e1484.
- [4]. Zhao, C., & Cao, H. (2022). Risk Evaluation of the Destination Port Logistics based on Self-Organizing Map Computing. In 2022 IEEE 22nd *International Conference on Software Quality, Reliability, and Security Companion* (QRS-C) (pp. 746-751). IEEE.
- [5]. Ganesh, M. S. S., Sujith, M. B. R. P., Aravindh, K. V., & Durgadevi, P. (2023). Crime Prediction Using Machine Learning Algorithms. Advances in Science and Technology, 124, 457-461.
- [6]. Plevris, V., Solorzano, G., Bakas, N. P., & Ben Seghier, M. E. A. (2022). Investigation of performance metrics in regression analysis and machine learning-based prediction models. In 8th *European Congress on Computational Methods in Applied Sciences and Engineering* (ECCOMAS Congress 2022). European Community on Computational Methods in Applied Sciences.
- [7]. Yin, J. (2023). Crime Prediction Methods Based on Machine Learning: A Survey. Computers, *Materials & Continua*, 74(2).
- [8]. Alsayadi, H. A., Khodadadi, N., & Kumar, S. (2022). Improving the regression of communities and crime using ensemble of machine learning models. *J. Artif. Intell. Metaheuristics*, 1(1), 27-34.
- [9]. Campedelli, G. M. (2022). Machine Learning for Criminology and Crime Research: at the crossroads. Routledge.
- [10]. Herzog, C. (2022). On the risk of confusing interpretability with explicability. *AI and Ethics*, *2*(1), 219-225.
- [11]. Ahamad, G. N., Shafiullah, Fatima, H., Imdadullah, Zakariya, S. M., Abbas, M., & Usman, M. (2023). Influence of optimal hyperparameters on the performance of machine learning algorithms for predicting heart disease. *Processes*, *11*(3), 734.
- [12]. Omotehinwa, T. O., & Oyewola, D. O. (2023). Hyperparameter optimization of ensemble models for spam email detection. *Applied Sciences*, *13*(3), 1971.
- [13]. Anyanwu, G. O., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2023). Novel hyper-tuned ensemble random forest algorithm for the detection of false basic safety messages in internet of vehicles. *ICT Express*, *9*(1), 122-129
- [14]. Wubineh, B. Z. (2024). Crime analysis and prediction using machine-learning approach in the case of Hossana Police Commission. *Security Journal*, 1-16.
- [15]. Wheeler, A. P., &Steenbeek, W. (2021). Mapping the risk terrain for crime using machine learning. *Journal of Quantitative Criminology*, *37*, 445-480.
- [16]. Liao, M., Wen, H., Yang, L., Wang, G., Xiang, X., & Liang, X. (2024). Improving the model robustness of flood hazard mapping based on hyperparameter optimization of random forest. *Expert Systems with Applications*, *241*, 122682.
- [17]. Watts, D., Moulden, H., Mamak, M., Upfold, C., Chaimowitz, G., & Kapczinski, F. (2021). Predicting offenses among individuals with psychiatric disorders-A machine learning approach. *Journal of Psychiatric Research*, *138*, 146-154.
- [18]. Rodrigues, A., González, J. A., & Mateu, J. (2023). A conditional machine learning classification approach for spatio-temporal risk assessment of crime data. *Stochastic Environmental Research and Risk Assessment*, *37*(7), 2815-2828.
- [19]. Abubakar, H., Boukari, S., Gital, A. Y., & Zambuk, F. U. (2024). A hyper-parameter tuned Random Forest algorithm-based on Artificial Bee Colony for improving accuracy, precision and interpretability of crime prediction. *Dutse Journal of Pure and Applied Sciences*, *10*(4a), 371-381
- [20]. Adorada, A., Permatasari, R., Wirawan, P. W., Wibowo, A., &Sujiwo, A. (2018, October). Support vector machine-recursive feature elimination (svm-rfe) for selection of Micro RNA expression features of breast cancer. In *2018 2nd international conference on informatics and computational sciences (ICICoS)* (pp. 1-4). IEEE.
- [21]. Awad, M., &Fraihat, S. (2023). Recursive feature elimination with cross-validation with decision tree: Feature selection method for machine learning-based intrusion detection systems. *Journal of Sensor and Actuator Networks*, *12*(5), 67.
- [22]. Van Patten, I. T., McKeldin-Coner, J., & Cox, D. (2009). A microspatial analysis of robbery: Prospective hot spotting in a small city. Crime Mapping: A journal of research and practice, 1(1), 7-32.