Abstract: In today’s rapidly evolving society, as technology continues to advance, various new forms and methods of crime emerge incessantly. It becomes particularly crucial to accurately predict future criminal behaviors. This paper delves into the study of forecasting home burglary crimes in the realm of property-related offenses. Utilizing a dataset of criminal cases, relevant variables with high correlation to crime prediction are selected as features. Through employing diverse machine learning algorithms, the likelihood of the occurrence of home burglary crimes is forecasted. Consequently, a crime prediction model specifically tailored for home burglary cases is constructed, and the accuracy of the model is evaluated. By using the accuracy of the model as the benchmark, the optimal crime prediction model is chosen, and a system is implemented for building and evaluating the model. Experimental results demonstrate that the developed crime prediction model is capable of effectively foreseeing home burglary crimes, thereby providing valuable support and scientific evidence for the prevention and handling of such criminal cases.

Keywords: Crime Prediction, Machine Learning, Naive Bayes, Random Forest

I. INTRODUCTION

The traditional approach to criminal investigations follows a passive reactive mode, wherein investigations are always one step behind the occurrence of criminal activities. Public security organs can only swiftly respond and combat crimes after they have taken place, lacking the ability to effectively prevent them at their roots. Consequently, the traditional crime investigation model, based on previous empirical knowledge, has shown low efficiency and limited feasibility in terms of crime prevention measures. It fails to meet the needs of detecting various novel forms and methods of crime and can only serve as a limited guidance tool. In this context, crime prediction has emerged as a vital component of the theoretical foundation in the field of criminology and has now become an essential and indispensable task for law enforcement agencies.

In general criminal cases, property-related offenses hold a significant proportion, with theft crimes often constituting a substantial portion within this category. Therefore, it is crucial to pay close attention to theft crimes. Among theft crimes, home burglary cases are relatively common. Due to their propensity for forming patterns, as well as their covert methods and techniques, home burglary cases pose a severe threat to people’s lives and property, undermining social order and public security. Thus, this study focuses specifically on home burglary crimes, exploring methods for predicting their occurrence and implementing a system for building the model. The findings of this research can provide valuable insights for law enforcement agencies in terms of preventing home burglary crimes and facilitating further investigations into such cases.

II. RELATED WORK

Crime prediction refers to the process of forecasting the likelihood of individuals or groups engaging in criminal activities by analyzing and assessing their characteristics and behavioral patterns. Various crime prediction methods can have different impacts on the predicted outcomes. The following presents research focused on the theoretical aspects of crime prediction.

Wei et al. provided a comprehensive review and analysis of the application of data mining techniques in criminal cases. They concluded that utilizing data mining techniques for criminal case prediction can effectively identify future criminal cases and reduce the likelihood of their occurrence[1]. Dong et al. explored strategies based on different feature selection and optimization algorithms for crime prediction. They also conducted a brief
comparison and analysis of various algorithms[2]. Ke conducted research on the crime prediction mechanism using artificial intelligence technology[2]. Yunzhi conducted a study on home burglary cases, using the B City C District as an example, examining the spatiotemporal aspects of such cases[4].

A. Crime Prediction Method Based on Machine Learning

The crime prediction method based on machine learning involves the use of machine learning algorithms and techniques to analyze and forecast the likelihood of criminal behavior. This approach relies on training models on large-scale datasets, learning from known criminal cases’ data, and discovering patterns to predict potential future criminal events.

Saraiva et al., using official police data from Porto, Portugal, between 2016 and 2018, studied the characteristics of crime in that area by employing machine learning algorithms such as random forest Error! Reference source not found.. Zhang et al. utilized the XGBoost algorithm to train a model and investigated the importance of each variable in predicting crime occurrences through the Shapley Additive Explanation (SHAP) method[5]. Khan et al. analyzed crime patterns and trends in San Francisco using multiple machine learning predictive classification algorithms on crime data[6]. Lingfeng proposed a machine learning-based method for predicting social public safety incidents Error! Reference source not found.. Zhongying et al. developed a crime quantity forecasting model based on the LSTM algorithm to predict regional crime rates Error! Reference source not found.. Zihan et al. presented a machine learning-based method for predicting typical financial crime occurrences [9]. Qi et al. trained theft crime data using various machine learning algorithms and tested the classification performance of each algorithm[11]. Xu conducted in-depth research on the spatiotemporal distribution patterns of public theft cases from different perspectives[12]. Zhao designed and developed a crime analysis and prediction system based on Spark, utilizing machine learning algorithms[13].

B. Crime Prediction Method Based on Deep Learning

The crime prediction method based on deep learning utilizes deep neural network models to analyze and forecast criminal behavior. Deep learning is a subfield of machine learning that uses multi-layered neural networks to learn and extract features, enabling the processing of complex nonlinear relationships.

Dong et al. proposed an improved ST-3DNet framework for fine-grained spatiotemporal crime prediction based on deep spatiotemporal 3D convolutional neural networks (ST-3DNet) Error! Reference source not found.. Zhou et al. introduced a crime prediction method based on recurrent neural networks, utilizing crime records, Point of Interest (POI), and other features[14]. Hou et al. presented an integrated graph model for urban crime spatiotemporal prediction within city police districts, incorporating an attention mechanism [16]. Vimala et al. used Sacramento city crime data as an example and proposed an adaptive deep reinforcement learning network (DRQN) based on deep learning to predict crime trends Error! Reference source not found.. WeiHong et al. employed a BP neural network-based method to automatically learn and train the nonlinear correlations between factors and theft crimes, constructing a prediction model for theft crimes[17]. Shengchang proposed a deep learning-based model for crime prediction[19]. Meilin developed a crime prediction model based on an improved ST-ResNet using fine-grained crime data grids[19]. Hanlei et al. utilized Long Short-Term Memory (LSTM) models to predict and study home burglary crimes [19].

Machine learning or deep learning methods have been applied to predict and analyze various types of crimes, employing different models and algorithms. However, these studies often focus on analyzing and researching crime within broad crime categories, lacking specificity in targeting individual crimes. In contrast, this paper proposes a machine learning-based predictive method specifically for home burglary crimes. This method accurately detects the characteristics of this particular crime, thereby reducing the occurrence of home burglary cases at the source.

III. APPROACH

The subject of this study is home burglary crimes, which fall under the category of property-related crimes. Taking into account the characteristics and challenges faced by grassroots public security agencies, this study aims to predict and analyze the likelihood of home burglary crimes. By providing accurate data references, this study assists public security agencies in preventing the occurrence of home burglary crimes.

The research approach in this study involves using machine learning techniques to establish a model that predicts the likelihood of home burglary crimes. Firstly, the raw dataset is subjected to data preprocessing, where valuable features relevant to predicting home burglary crimes are selected. Next, a machine learning model is constructed using the selected features, and the model’s performance is evaluated using cross-validation. Finally,
the machine learning model is utilized to predict the likelihood of home burglary crimes, and the accuracy of the model is assessed.

A. Data Preprocessing

Due to the presence of missing values, duplicates, and irrelevant data in some columns of the raw dataset, these factors can impact the predictions of home burglary crimes made by the machine learning model. Missing values result in data incompleteness, rendering the model unable to analyze the missing information and thus affecting the accuracy and reliability of the predictions. Duplicates and irrelevant data introduce redundancy in the dataset, which can undermine the model’s generalization capability. Data preprocessing encompasses several fundamental steps, as illustrated in Figure 1:

B. Feature Engineering

Feature engineering is the process of extracting useful features from raw data, with the aim of creating features that enable machine learning algorithms to achieve optimal performance. It is a crucial step in machine learning, as the quality of feature selection directly impacts the results of subsequent model training. By extracting more useful and representative features from the raw data, removing redundant and irrelevant features, we can assist the model in better capturing patterns and characteristics of the data. This, in turn, improves the accuracy and generalization ability of the model, reduces model complexity, and decreases training time and computational costs. Ultimately, it enhances the accuracy in predicting instances of residential home burglary crimes.

C. Model Establishment

Model establishment refers to the process of learning patterns and structures from known data and applying them to predict outcomes for new data. Model establishment involves several fundamental steps, as illustrated in Figure 2:

First, the dataset is divided into training and testing sets. Then, the training sets are used to train the models, including the Naive Bayes model and the Random Forest model. The Naive Bayes algorithm is a classification algorithm that calculates the posterior probability of each element with other elements in each class. It determines the likelihood of each element appearing in each class and uses the posterior probability to decide which class attribute to use for describing the element. The Random Forest algorithm is an ensemble learning algorithm based on decision trees. It constructs multiple decision trees by randomly selecting samples and features and combines them for classification or regression tasks. The construction of the Random Forest algorithm can be divided into five steps: (1) selecting N samples from the training set, where N is a parameter specified by the user; (2) selecting
M features from the training set, where M is also a parameter specified by the user; (3) constructing a decision tree based on the selected samples and features; (4) repeating step 3 until a sufficient number of decision trees are constructed; (5) finally, selecting the optimal decision result from the results of these decision trees.

After model training, model prediction and evaluation are carried out to ensure the usability of the model.

IV. IMPLEMENTATION AND EXPERIMENT

A system is implemented for building and evaluating the model. The experimental environment for this study is presented in Table 1:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Windows 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development Language</td>
<td>Python 3.8</td>
</tr>
<tr>
<td>Machine Learning Library</td>
<td>Scikit-Learn 1.1.2</td>
</tr>
<tr>
<td>Model</td>
<td>Naive Bayes, RandomForest</td>
</tr>
</tbody>
</table>

A. Data Introduction

The dataset used in this study is a collection of crime cases in Montreal, Canada, from 2015 to 2021. It consists of over 130,000 records, including information such as crime types, crime dates, crime cities, and latitude-longitude coordinates. The specific field descriptions of the dataset are shown in Table 2, and the first 5 rows of data are presented in Table 3:

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unnamed: 0</td>
<td>Numerical</td>
<td>Criminal record number</td>
</tr>
<tr>
<td>category</td>
<td>Character</td>
<td>Type of crime</td>
</tr>
<tr>
<td>date</td>
<td>Character</td>
<td>Date of crime</td>
</tr>
<tr>
<td>postal_code</td>
<td>Character</td>
<td>Criminal location number</td>
</tr>
<tr>
<td>city</td>
<td>Character</td>
<td>Crime City</td>
</tr>
<tr>
<td>neighbourhood</td>
<td>Character</td>
<td>Year of crime</td>
</tr>
<tr>
<td>year</td>
<td>Numerical</td>
<td>Area of crime</td>
</tr>
<tr>
<td>count</td>
<td>Numerical</td>
<td>Number of crimes</td>
</tr>
<tr>
<td>longitude</td>
<td>Numerical</td>
<td>Longitude of crime</td>
</tr>
<tr>
<td>latitude</td>
<td>Numerical</td>
<td>Latitude of crime</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unnamed: 0</th>
<th>category</th>
<th>date</th>
<th>postal_code</th>
<th>city</th>
<th>neighbourhood</th>
<th>year</th>
<th>count</th>
<th>longitude</th>
<th>latitude</th>
<th>Home_Invasion</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Motor vehicle theft</td>
<td>2018/9/13</td>
<td>H1Z 189</td>
<td>MONTREAL</td>
<td>Saint-Michel</td>
<td>2018</td>
<td>1</td>
<td>-73.626</td>
<td>45.567</td>
<td>Motor vehicle theft</td>
</tr>
<tr>
<td>1</td>
<td>Motor vehicle theft</td>
<td>2018/4/30</td>
<td>H1Z 189</td>
<td>MONTREAL</td>
<td>Saint-Michel</td>
<td>2018</td>
<td>1</td>
<td>-73.626</td>
<td>45.567</td>
<td>Motor vehicle theft</td>
</tr>
<tr>
<td>2</td>
<td>Home Invasion</td>
<td>2018/1/10</td>
<td>H1Z 2V6</td>
<td>MONTREAL</td>
<td>Saint-Michel</td>
<td>2018</td>
<td>1</td>
<td>-73.629</td>
<td>45.569</td>
<td>Home Invasion</td>
</tr>
<tr>
<td>3</td>
<td>Mischief</td>
<td>2018/11/12</td>
<td>H1Z 2V6</td>
<td>MONTREAL</td>
<td>Saint-Michel</td>
<td>2018</td>
<td>1</td>
<td>-73.629</td>
<td>45.569</td>
<td>Mischief</td>
</tr>
<tr>
<td>4</td>
<td>Mischief</td>
<td>2018/12/15</td>
<td>H1Z 2V6</td>
<td>MONTREAL</td>
<td>Saint-Michel</td>
<td>2018</td>
<td>1</td>
<td>-73.629</td>
<td>45.569</td>
<td>Mischief</td>
</tr>
<tr>
<td>5</td>
<td>Home Invasion</td>
<td>2018/1/11</td>
<td>H1Z 2V6</td>
<td>MONTREAL</td>
<td>Saint-Michel</td>
<td>2018</td>
<td>1</td>
<td>-73.629</td>
<td>45.569</td>
<td>Home Invasion</td>
</tr>
</tbody>
</table>

B. Data Preprocessing

Data Preprocessing involves handling missing data, removing duplicates, and eliminating irrelevant data from the original crime dataset to obtain a highly usable dataset.

Based on the imported raw dataset, the first step is to address missing data. In this study, the mean imputation method is used as an example, where the missing values in the respective columns are filled with the mean value. Next, duplicate records are removed to ensure the dataset’s uniqueness and integrity. Finally, irrelevant data is processed. From the specific content of the data and the subsequent feature engineering, it is determined that the columns “Unnamed: 0”, “postal_code”, and “count” are irrelevant to the training of the final model. Consequently, these columns are deleted. Once the data preprocessing is completed, the remaining data will consist of relevant information for prediction purposes. This processed dataset can be used for model training and evaluation.
C. Feature Engineering

Feature engineering is a crucial step in transforming the preprocessed data to improve model performance and enhance the accuracy of predicting home burglary crimes in the subsequent machine learning training process. It involves the extraction, transformation, splitting, and merging of features. The steps of feature engineering are illustrated in Figure 3:

![Figure 3: Steps of Feature Engineering]

As depicted in the diagram, the first step involves selecting representative features from the cleaned data to reduce the dimensionality of the dataset. Then, effective feature extraction is carried out on these selected features. For example, extracting useful values such as month, day, and day of the week. Next, feature transformation is applied to the extracted features. The month values are mapped to corresponding season values, such as mapping months 1, 2, and 3 to “Spring”. The day of the week values can be mapped to a binary indicator representing whether it is a weekend or not, where 0 indicates a non-weekend day and 1 indicates a weekend day. Additionally, the day values can be transformed into a binary indicator representing whether it is a holiday or not, where 0 indicates a non-holiday and 1 indicates a holiday. Moreover, within the crime type variable, values that do not correspond to home burglary crimes are set to 0, while values indicating home burglary crimes are set to 1. This step converts the continuous variables of month, day, day of the week, and crime type into discrete variables denoting season, weekend status, holiday status, and whether it is a home burglary crime.

Subsequently, the transformed features are further split into multiple binary features. Specifically, the year is split into multiple binary features, where each feature corresponds to a specific year. The month is split into multiple binary features, with each feature representing a specific month. The weekend status is split into multiple binary features, with each feature representing a specific weekend scenario. The season is split into multiple binary features, where each feature corresponds to a specific season. Lastly, the holiday status is split into multiple binary features, where each feature represents a specific holiday situation.

Finally, based on the split features, the feature matrices of year, month, season, weekend status, holiday status, and home burglary crime type are merged together along the column direction (i.e., axis=1). This merging process creates a new training set feature matrix, transforming the original data into the desired format for building machine learning models.

D. Model Prediction

As shown in the diagram, the first step is to partition the dataset. The preprocessed feature “is_Home_Invasion” is selected as the dependent variable (Y), while the remaining features are considered independent variables (X). The dataset is divided into training and testing sets using a 7:3 ratio. The training set
consists of 95,649 data samples and 27 features, whereas the testing set contains 40,993 data samples and 27 features.

Next, the training set and testing set, which were previously partitioned, are used for model training. This involves training both the Naive Bayes model and the Random Forest model.

1) Bayes Model

In the context of the Bayes model, three common models are Gaussian Naive Bayes (GaussianNB), Bernoulli Naive Bayes (BernoulliNB), and Multinomial Naive Bayes (MultinomialNB). Since most of the features in the sample exhibit continuous value distributions, and Gaussian Naive Bayes (GaussianNB) can handle any continuous data, this paper will use Gaussian Naive Bayes as an example to train the sample data. The sample categories include year, month, season, weekend status, holiday status, and crime type. These correspond to the feature values \(x_1\) (year: 2015-2021), \(x_2\) (month: 1-12), \(x_3\) (season: spring, summer, autumn, winter), \(x_4\) (whether it is a weekend: weekend, non-weekend), \(x_5\) (whether it is a holiday: holiday, non-holiday), and \(y_1\) (crime type).

The steps for training the model are as follows:

1) Computing prior probabilities: Based on historical experience and analysis, for each sample \(Y=CK\) (where \(K\) is the number of sample categories, in this case, \(K\) equals 6), the prior probability \(P(y)\) for each category is calculated. This represents the probability of each category occurring in the entire dataset \(P(Y|CK)\).

2) Computing conditional probabilities: For each feature, the conditional probability \(P(x|y)\) is calculated given a specific category. This represents the probability of a specific value of a feature given a certain category. The calculation follows the formula shown in Equation (1).

\[ P(y_1|x_1,x_2,...,x_5) = \frac{P(x_1,x_2,...,x_5|y_1)}{P(x_1,x_2,...,x_5)} \]  

(1)

3) Computing posterior probabilities: The posterior probability for each category \(C_k\) is calculated based on a given feature. This represents the probability of a specific category given a particular feature. The calculation follows the formula shown in Equation (2).

\[ P(y_1|x_1,x_2,...,x_5) = \frac{P(x_1,x_2,...,x_5|y_1)P(y_1)}{P(x_1,x_2,...,x_5)} \]  

(2)

2) Random Forest Model

The random forest model utilizes randomly sampled data and feeds it into multiple weak learners (decision trees) for voting, ultimately resulting in the final output. In this paper, the features include year, month, season, weekend status, holiday status, and crime type, amounting to a total of 5 features. These features are used to divide the data into multiple samples \(S_1, S_2, S_3... S_n\), as shown in Figure 4. The following are the steps involved in training this model:
(1) Random sampling of samples: In order to create a training dataset, the bootstrap method is employed, which involves randomly sampling \( N \) training samples with replacement. This process is repeated \( k \) times to generate \( K \) datasets that are independent and identically distributed.

(2) Random sampling of features: From the five available features, a subset of \( m \) features is randomly selected \( (m << M) \).

(3) Voting for results: The decision trees obtained from the previous steps are combined, and the final result is determined through a democratic voting process. Each decision tree contributes to the classification and prediction, and the final output is based on the majority vote.

(4) Grid parameter tuning: Grid parameter tuning, including grid search and cross-validation, is performed to identify the optimal parameters for the random forest model.

E. 4.5 Model Evaluation

Model evaluation is the process of assessing the predictive performance of a model using various metrics to determine its ability to accurately predict home burglary crimes. Common evaluation metrics include accuracy, recall, F1 score, and logarithmic loss. In this study, accuracy and logarithmic loss are chosen as the evaluation metrics.

(1) Evaluating the Naive Bayes model

To evaluate the Naive Bayes model, the predicted results are compared with the true labels in the test set. The number of correctly predicted samples is counted, and then divided by the total number of samples in the test set. The resulting accuracy is approximately 0.738, indicating that the model accurately predicts home burglary incidents with an accuracy rate of 73.8%.

(2) Evaluating the random forest model

In Scikit-Learn, the parameters “n_estimators” and “random_state” are selected with values ranging from 1 to 10 as an integer sequence. The “n_estimators” parameter represents the number of decision trees in the random forest model. Its effect on the accuracy of the model is generally monotonically increasing—larger values of “n_estimators” often lead to better model performance. However, there may be a point at which increasing “n_estimators” no longer improves the accuracy or starts to fluctuate. The “random_state” parameter is used to control the randomness in bootstrapping and the selection of samples. To evaluate the model, the predicted results are compared with the true labels in the test set. The number of correctly predicted samples is counted and divided by the total number of samples in the test set. The accuracy before grid search is approximately 0.769. Next, a grid search object, “modeled”, is created. It takes the “model” and the parameter dictionary “param_dict” as input. The number of cross-validation folds is set to 3. By performing grid search, the best parameters for the trained model are found, which are n_estimators=4 and random_state=1. After training the model with the best parameters, the accuracy after grid search is approximately 0.770. This indicates that the model accurately predicts home burglary incidents with an accuracy rate of 77.0%. From the model evaluation, it is evident that the random forest model, after grid search, has a slightly higher accuracy than the Naive Bayes model. However, the difference is not significant. It is recommended to use both models separately when predicting with other data and choose the model that performs better in terms of adaptability for further predictions.

V. CONCLUSION

A machine learning-based method for predicting home burglary crimes was proposed in this study. Firstly, a substantial amount of historical data on home burglary crimes was collected. Next, the data was analyzed using machine learning techniques, resulting in the development of a predictive model for home burglary crimes. Then a system was implemented to build and evaluate the model. Through experimental results, the effectiveness of the model was demonstrated. However, there were still several limitations in this study. For example, there is room for improvement in the accuracy of the machine learning predictions. The available dataset fields are limited, and a comprehensive integration of data from various fields and industries for predicting and assessing home burglary crimes is not achieved. These research directions will be pursued in the future.

The machine learning-based technique for predicting home burglary crimes has significant potential for development and is expected to play a crucial role in providing accurate and scientific evidence for the prevention and combat of such crimes by public security agencies in the future.

ACKNOWLEDGMENTS
This paper is supported by The “New Generation Information Technology Innovation Project” of the China University Industry, University and Research Innovation Fund(No. 2022IT171), Youth scientific research project of Guangdong police college (No. 2022-QN04), Cooperative education project of industry university cooperation between Ministry of education and 360 enterprise security group -- Web Attack and Defense Technology (web security and operation) (No. 201802007006), 2023 Campus level Teaching Quality and Teaching Reform Project of Guangdong Police College (Research on the Practical Teaching Reform of Police Big Data Course Based on the Integration of “Teaching, Studying, Training, Combating and Competition”), 2022 Campus level Teaching Quality and Teaching Reform Project of Guangdong Police College (Teaching Reform and Research on Police Big Data Course for Practical Use), Special Funds for the Cultivation of Guangdong College Students' Scientific and Technological Innovation (“Climbing Program” Special Funds, No. pdjh2021b0356), Special Funds for the Cultivation of Guangdong College Students' Scientific and Technological Innovation (“Climbing Program” Special Funds, No. pdjh2022b0373).

REFERENCES

[9] Zhongying Pan Design and implementation of a crime warning system based on machine learning algorithms (Doctoral dissertation, University of Electronic Science and Technology).