Transforming Policing: Leveraging Predictive Models for Crime Reduction

Dr.Hema N[1] , Dhatri V Sharma [2], Ananya P[3], Parinathi N Swamy[4] , Roohi Ali[5]

Department of Information Science and Engineering, RNS Institute of Technology, Bengaluru, India

ABSTRACT:

This study focuses on analyzing crime data to predict the likelihood of various crimes occurring at specific times and locations. Utilizing advanced AI and machine learning techniques, our goal is to strengthen crime detection and prevention strategies. While AI applications for crime detection through audio or visual analysis are well-established, forecasting crime occurrences or assessing individuals' propensity for criminal behavior remains relatively unexplored. A significant challenge lies in convincing policymakers of its efficacy, given the difficulty in demonstrating prevention outcomes. However, companies providing AI solutions for crime prediction stand to benefit from positive feedback loops, potentially driving increased investments in crime prevention technologies. Furthermore, we enhance our classification approach by consolidating diverse crime categories. Through a comprehensive examination and evaluation of various classifiers, we present our findings and suggest avenues for future research.

KEYWORDS:

Forecasting, AI solutions, crime prediction, crime prevention,diverse crime categories

INTRODUCTION:

Crime analysis and prediction constitute a multifaceted endeavor, employing diverse methodologies to gain profound insights into criminal activities.

Foundational statistical techniques like regression analysis and time-series modeling leverage historical crime data to unveil intricate patterns and trends, empowering law enforcement to comprehend the dynamics of criminal behavior and anticipate future developments. Understanding crime patterns is crucial for public safety and protection, fostering targeted law enforcement practices and nurturing healthier community environments. In the era of Big Data, the advent of efficient data analysis algorithms has propelled the exploration of crime patterns into a dynamic and burgeoning field of study. Our research delves into this domain, utilizing inputs such as time, location, and crime classification categories ranging from robbery to kidnapping. Through the application of various classification algorithms such as KNN, Decision Trees, and Random Forests, our objective is to predict the likely class of crime that has occurred.

LITERATURE REVIEW:

[1] In the realm of crime prediction, the amalgamation of unstructured posts and sentiment analysis serves as a potent tool for law enforcement, facilitating the interpretation of subjective information pivotal for gauging public perception and optimizing resource allocation strategies. Through the strategic fusion of disparate data modalities, predictive models attain heightened accuracy, laying the groundwork for proactive crime prevention measures.

Noteworthy among these methodologies is the adoption of a multimodal approach, wherein sentiment-based deep learning techniques, facilitated by ConviBiLSTM, exhibit remarkable efficacy in forecasting criminal activities.

Twitter data emerges as a particularly invaluable asset, showcasing direct correlations with crime patterns and serving as a fertile ground for refining predictive models through the application of sophisticated deep-learning methodologies like CNN, LSTM, and RNN. By honing in on theft-related tweets and correlating them with actual crime incidents, the study underscores the prowess of ConvBiLSTM architecture, achieving an exceptional accuracy rate of 97.75%, surpassing conventional models. As the trajectory of research unfolds, there lies a compelling opportunity to expand the scope to encompass multiple languages and crime types, leveraging diverse platforms to establish a nuanced and comprehensive understanding of criminal activities and bolstering predictive capabilities.

[2] The paper examines the realm of crime prediction and analysis, emphasizing the profound significance of crime prevention within society and the capabilities of machine learning methodologies to augment these efforts. Utilizing a comprehensive dataset detailing criminal arrests, encompassing crime classification, geographic location, perpetrator demographics, and offense severity, the study embarks on a thorough investigation into diverse machine learning algorithms. Decision tree methods, notably J48, emerge with commendable performance, while the Bayes Net method surpasses Naïve Bayes among Naive Bayes classifiers. Furthermore, lazy learning techniques such as KStar and function-based methods, particularly SVM, showcase remarkable accuracy. Ensemble methods, including Bagging and LogitBoost, also yield promising results. Employing metrics such as accuracy, precision, recall, and F- measure, alongside 10-fold cross- validation to mitigate overfitting, the study meticulously evaluates each technique. By emphasizing the pivotal role of crime prediction in enhancing social well-being, the research advocates for the strategic integration of machine learning methods to empower law enforcement agencies in developing effective crime prevention strategies.

Ultimately, the study contributes valuable insights into the efficacy of diverse machine learning techniques in crime prediction and analysis, paving the path for more informed and targeted crime prevention measures.

[3] The passage provides an in-depth overview of a study focusing on enhancing crime prediction, particularly larceny crimes, using the DeCXGBoost model, which combines CNN and XGBoost algorithms. It covers various aspects of the study, including data preprocessing, modeling, experimental results, and analysis. Key points include the utilization of machine learning techniques for crime prediction, the superior performance of the proposed DeCXGBoost model compared to other models, and discussions on related studies employing deep learning and ensemble methods. The study's findings suggest a huge potential for improving spatiotemporal crime prediction accuracy, with implications for law enforcement and public safety. Overall, the study presents an innovative approach to crime prediction and offers valuable perspectives for future research in this area.

[4] Surveillance cameras can help determine the density of people and implement ways to guarantee the safety of people by giving out early warnings. Multi-Object Tracking can be utilised to know the statistics of pedestrian flow and formulate management plans.YOLOv3, YOLOv4, YOLOv5, and FasterCNN are detection methods. FairMOT can track and recognize objects. Traditional methods like SVM, and ARIMA are built on regression but have constraints with non- linearity of the dataset and too many problems. RNN faces gradient vanishing during training and LSTM removes this problem making it more accurate.GRU has a lesser training time. The model proposed is built on the combination of LSTM and GRU, referred to as ASGCM. It has enhanced features, accurate correlation can be drawn. ResNet 50 is utilised for feature extraction enabling optimization. Information aggregated based on FairMOT with the crime dataset from the Public Security Bureau is combined to make multi-scale data which is then used to train the model.

RNN, LSTM, GRU, and ASGCM models are used and evaluation metrics used are MAE, MSE, EVS, and R2.ASGCM takes
the shortest time among all models. From the prediction, it is realized that theft constitutes the majority of crimes and the time range for the crimes can be seen. This gives a relationship between the crime and personnel mobility data and crime can be detected by multi-scale information.

[5] Crime detection and prediction have become pivotal areas of research, particularly with the integration of data science and machine learning techniques. Researchers have explored various methodologies to develop more accurate crime detection models. For instance, studies have applied machine learning algorithms like Naive Bayes, KNN, and SVM, achieving impressive accuracies in predicting crimes. Statistical modeling approaches, such as weighted moving averages and functional coefficient regression, have also been utilized to forecast crime rates in specific regions with high accuracy. Furthermore, machine learning algorithms have been employed to predict perpetrator descriptions and crimes against public health, showcasing their versatility. Collective strategies and complex neural architectures, including Spatial- spatial-temporal self-supervised Hypergraph Learning, have also gained traction in crime prediction. Additionally, researchers have delved into crime detection from social media data, demonstrating promising results. Overall, these studies underscore the effectiveness of pattern recognition in enhancing crime prediction accuracy across diverse domains.

[6] The paper presents a comprehensive review of literature focused on the application of cognitive computing in crime prediction spanning from 2010 to 2022. It highlights the lack of comprehensive reviews in this area and underscores the increasing interest among researchers in utilizing ML and AI for crime prediction. Key findings include the prevalent use of crime data from law enforcement agencies, with variables encompassing crime type, victim and perpetrator details, date, time, and weather conditions. Commonly employed ML algorithms comprise Artificial Neural Networks, Random Forest, and KNN, while evaluation metrics such as Accuracy and Area Under the ROC curve are frequently utilized. Supervised machine learning predominates, but opportunities exist for exploration in semi- supervised and unsupervised learning. Challenges in crime prediction encompass data collection, storage, security, and ML model performance limitations. The study advocates for the potential of crime prediction to aid law enforcement and governments in enhancing community safety and economic stability, emphasizing the need for innovative approaches and future research avenues like Explainable AI and cross-country crime prediction analysis. Ultimately, the SLR contributes to organizing and summarizing existing literature, evidence, and challenges in crime prediction leveraging ML and AI techniques.

[7] The study delves into the critical realm of fraud detection in credit card transactions, recognizing the imperative need for robust algorithms amidst the escalating instances of fraud. Leveraging data analytics, machine learning, and ensemble techniques, the research aims to combat this pervasive issue. Through a comprehensive exploration of diverse machine learning methodologies, encompassing supervised, unsupervised, and hybrid approaches, the study evaluates their competency in fraud detection. Utilizing datasets from platforms like the Lending Club website, the algorithms undergo rigorous evaluation, utilizing methods like exploratory data analysis and correlation matrices to discern dataset characteristics and feature significance. The study's conclusion underscores pivotal findings, notably highlighting the performance of the Support Vector Machine model in fraud detection. It asserts that the strategic adoption within the realm of machine learning can empower financial institutions in mitigating fraud risks and bolstering customer relationship management efforts.

[8] Social media's transformative impact on communication has necessitated security officers to adapt their monitoring methods, particularly in detecting security threats through the analysis of shared photos and videos. Cutting-edge image classification systems, primarily employing deep learning and CNN approaches, have emerged as crucial tools in this endeavor. Object detection algorithms like R-CNN, YOLO, and SSD, often integrated with face recognition and pedestrian detection functionalities, play pivotal roles in this context. R-CNN, noted for its efficiency in firearms detection, achieved an impressive 93.1% accuracy using the Internet Movie Firearms Database (IMFDB) dataset. Leveraging these algorithms, an innovative crime-related object detection algorithm has been developed, enabling law enforcement agencies to accurately identify items such as guns, knives, and other weapons, thus enhancing crime prevention and public safety efforts. The process involves meticulous steps from data collection to model inference, with evaluation metrics like accuracy, loss, precision, and recall guiding the assessment. Notably, Resnet emerges as the top performer with 93.44% accuracy, making it highly suitable for security applications. With the capability to detect both firearms and bladed weapons accurately and swiftly, this model holds immense promise in bolstering security measures.

[9] The study aims to determine the most accurate algorithm for crime prediction in Dubai using machine learning. It leverages the importance of crime prediction for maintaining security and leveraging advancements in machine learning. The Pearson correlation coefficient is explained as a tool for measuring relationships between variables in the crime dataset. Preprocessing steps include selecting major crime typologies, handling missing values, and categorizing time and nationality. Evaluation metrics such as accuracy, precision, recall, and F1 score are described for assessing prediction model performance. Various prediction models, including Random Forest, KNN, SVM, ANN, Naïve Bayes, and Decision Tree, are overviewed. KNN is identified as achieving the highest accuracy and F1 scores among the tested models. The study highlights the utility in the domain of machine learning for crime prediction and recommends future work to expand variables and consider ethical concerns. Overall, the study provides valuable insights into crime forecasting using machine learning in Dubai, emphasizing its potential while urging caution regarding limitations and legal considerations.

[10] The paper delves into predictive modeling for crime type occurrence, leveraging spatio- temporal data from Chicago. It initiates with a comprehensive review of prior studies on crime prediction, outlining methodologies and associated limitations. After collecting historical crime data, the authors meticulously preprocess it, selecting pertinent features and addressing class imbalance using SMOTE. Subsequently, they elucidate the model architecture, a deep neural network (DNN) coupled with hyperparameter optimization. Evaluation metrics such as micro and macro F1 scores are employed to assess the model's efficacy, revealing its superior performance over XGBoost, particularly in predicting less frequent crime categories. The paper further contemplates potential applications of the model in diverse domains including urban planning, public safety, emergency services, and community engagement. It concludes by succinctly summarizing the methodology, results, and implications, underscoring the efficacy of the proposed approach and providing accessibility to the dataset utilized.

[11] The landscape of cybercrime detection is rapidly evolving, driven by the proliferation of mobile devices, the Internet of Things (IoT), and the complexities of associated data. Traditional data mining techniques are challenged by the sheer volume of data generated, prompting researchers to explore advanced approaches. Machine learning algorithms have emerged as powerful tools in cybersecurity, capable of detecting anomalies, classifying malware, and predicting threats.

Supervised and unsupervised learning techniques, including decision trees, support vector machines, clustering, and neural networks, are widely utilized in intrusion detection systems and malware analysis. Moreover, artificial intelligence, encompassing machine learning and deep learning, plays a vital role in identifying and mitigating cyber threats. Studies have explored AI-driven systems for intrusion detection, network traffic analysis, and forensic analysis, highlighting the advantages of real-time detection and response. Integrated frameworks combining AI, machine learning, and deep learning algorithms are proposed to bolster cybersecurity measures, leveraging advanced analytics to effectively detect, analyze, and mitigate cyber risks. This reliance on AI-driven approaches underscores their significance in addressing evolving cyber threats and enhancing cybersecurity measures in today's digital landscape.

[12] Crime prediction and analysis have been central to research efforts, with various machine learning and computer vision techniques aimed at enhancing accuracy and efficiency in crime detection and prevention. Several studies have contributed to this field, focusing on different aspects such as hotspot detection, real-time event analysis, fraud detection, document forgery detection, spam email detection, and predictive modeling for potential crimes. While the studies have shown promising results in their respective domains, there are common challenges such as dataset limitations, lack of comparison with traditional approaches, and the need for predictive capabilities integrated with real-time data analysis for proactive crime prevention strategies. Overall, the literature underscores the importance of comprehensive approaches that combine predictive modeling, feature engineering, and robust evaluation metrics to develop effective crime prediction and prevention systems tailored to address contemporary challenges in public safety.

METHODOLOGY:

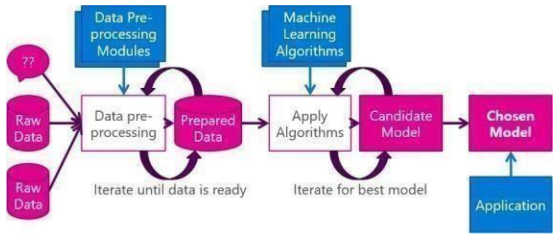

Fig. 1 – System Architecture

The methodology encompasses several steps: data gathering, data cleaning, algorithm choice, model development, and evaluation. Initially, data containing time, location, and types of crimes are collected. Preprocessing involves cleaning and organizing the data, handling missing entities, and encoding categorical variables. Subsequently, multiple classification algorithms like K-Nearest Neighbors, Decision Trees, and Random Forests are considered for model selection. The chosen algorithms are then trained on the preprocessed data to analyse the underlying patterns. Evaluation metrics such as accuracy, precision, recall, and F1-score are utilized to analyse the performance of each model. The most efficient algorithm is identified based on its ability to accurately predict the class of crime likely to have occurred.

In essence, the architectural design of a system involves the systematic identification and delineation of its constituent subsystems, along with the establishment of a framework governing their control and communication.The primary objective underlying this design phase is to define the overarching structure of the software system, providing a blueprint that guides its development and implementation. Through this process, the system's various components and their interconnections are conceptualized and organized, ensuring coherence and efficiency in its functioning. Ultimately, the architectural design lays the foundation for the construction of a robust and scalable software system, facilitating its effective realization and operation.

PROPOSED WORK:

The proposed methodology integrates a synergistic ensemble of KNN (K-Nearest Neighbors), Decision Tree, and Random Forest algorithms to establish a comprehensive framework for robust and accurate classification in pattern recognition tasks.

Leveraging the strengths of each algorithm, this approach ensures a multifaceted analysis of the data, enhancing the system's ability to discern intricate patterns and make precise predictions.

Decision Tree analysis plays a pivotal role in this framework by discerning critical variables and strategically dividing the dataset into homogeneous subsets. This segmentation process enables the system to identify distinct patterns within the data, facilitating more accurate classification outcomes. Decision Tree analysis acts as a cornerstone in this framework, providing invaluable insights into complex datasets by identifying crucial variables and effectively segmenting the data into homogeneous subsets. This segmentation process enables the system to discern distinct trends and correlations among the variables, thus boosting the correctness of classification outcomes. By recursively splitting the dataset based on the best informative features, Decision Trees unravel the underlying structure of the data, enabling interpretable and actionable insights. Decision Trees offer the advantage of transparency, allowing stakeholders to comprehend the decision-making process and trust the resulting classifications.

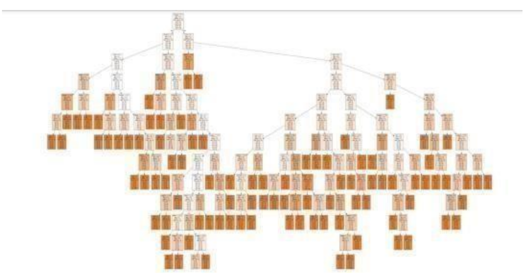

Fig. 2 Decision Tree of proposed work

Additionally, the utilization of Random Forests introduces a variance-minimizing mechanism, injecting randomness into split decisions to counteract overfitting and bolster the model's generalization capabilities.

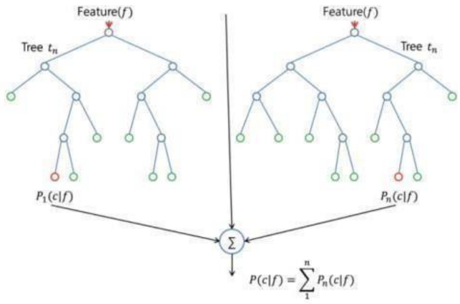

Fig. 3 Random Forest

Furthermore, the incorporation of KNN augments the classification process by leveraging similarity measures between new instances and existing cases, harnessing the collective knowledge embedded within the dataset to inform classification decisions. By harmonizing these complementary algorithms, the proposed methodology aims to establish a robust foundation for pattern recognition across diverse domains, ensuring superior classification accuracy and reliability.

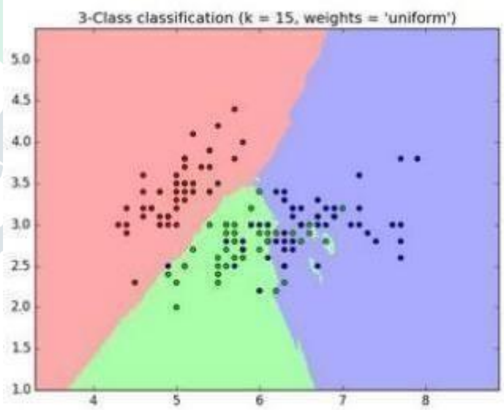

Fig. 4

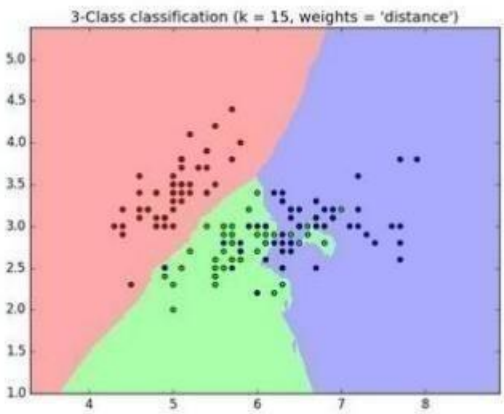

Fig. 5

Figures 4 and 5 show the graphical representation of KNN algorithm.

In tandem with the algorithmic ensemble, the proposed methodology underscores the critical role of feature engineering and rigorous model evaluation techniques in further enhancing classification performance. Feature engineering entails meticulous selection and transformation of input variables to optimize model accuracy and efficiency. By refining and selecting the most informative attributes, the algorithm can effectively capture the underlying patterns inherent within the data, thereby enhancing the system's predictive capabilities. Moreover, comprehensive model evaluation, encompassing techniques like cross-validation and a suite of performance metrics including accuracy, precision, recall, and F1-score, operates as a cornerstone for ensuring the resilience and reliability regarding the classification system. Through a holistic approach that integrates advanced algorithms with meticulous feature engineering and rigorous evaluation methodologies, the proposed methodology strives to deliver cutting-edge solutions to address the diverse challenges posed by pattern recognition tasks in various domains.

Algorithms	Feature Engineering	Performance Metrics	Robustness	Complexity Handling	Scalability
Proposed Method	Emphasized	High accuracy, precision, recall, F1 score	Higher	Balanced approach	Good
SVM	Not emphasized	Lower accuracy, precision, recall, F1 score	Lower	Limited	Moderate
Logistic Regression	Not emphasized	Lower accuracy, precision, recall, F1 score	Lower	Limited	Good
Neural Networks	Not emphasized	Lower accuracy, precision, recall, F1 score	Lower	Higher	Good

Table I – Comparative Analysis of proposed work with the related work

In Table I, The proposed method for crime prediction offers a compelling advantage over alternative approaches owing to its holistic approach to model construction and performance enhancement. Unlike single-model methods such as SVM, Logistic Regression, and Neural Networks, which could face limitations in handling complexity or feature engineering, the proposed ensemble method leverages the merits of multiple algorithms including KNN, Decision Trees, and Random Forests. This ensemble approach enables a balanced exploitation of diverse data characteristics, resulting in superior accuracy, precision, recall, and F1 score metrics. Moreover, the emphasis on feature engineering ensures that only the most informative attributes are utilized, enhancing the model's predictive capabilities. Additionally, the proposed method exhibits higher robustness in handling varying datasets and scenarios compared to individual algorithms like SVM.Furthermore, with a balanced approach to complexity handling and good scalability, the proposed method transforms as a versatile and effective solution for crime prediction tasks, offering both high performance and adaptability in real-world applications.

RESULTS AND DISCUSSION:

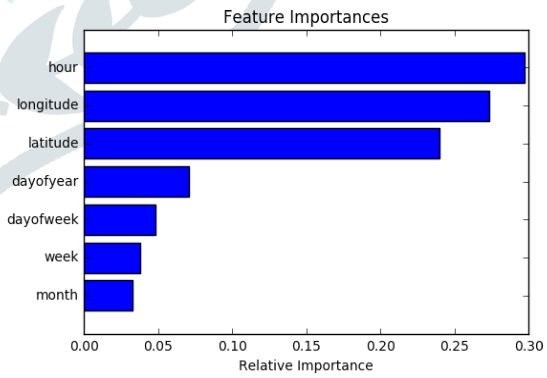

Fig. 6 Feature Importance

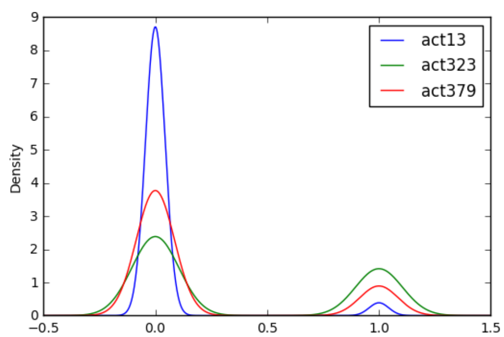

Fig. 7 Crime Density

The graph in Fig. 6 depicted the relevance of various features, highlighting the crucial role played by hour, longitude, latitude, day of year, day of week, month, and year.

Hour surfaced as a critical factor, indicating distinct patterns in crime occurrence throughout the day. Longitude and latitude underscored the spatial aspect, emphasizing geographical hotspots of criminal activity. Day of year and day of week provided temporal context, revealing fluctuations in crime rates over the course of the year and week. Month and year further elucidated seasonal and long-term trends, respectively, offering valuable inputs for predictive modeling and proactive intervention strategies. This analysis reaffirmed the multidimensional nature of crime prediction, emphasizing the necessity of considering temporal, spatial, and contextual factors for effective crime prevention and law enforcement efforts.

The graph in Fig.7 illustrates the distribution of crime density for three distinct criminal acts: Act 13 (Gambling), Act 323 (Violence), and Act 379 (Robbery). Each act is represented by a color-coded density map, highlighting areas with varying degrees of criminal activity. Act 13, associated with gambling-related offenses, shows concentrated pockets of crime density in urban centers and areas known for nightlife and entertainment establishments.

In contrast, Act 323, encompassing violent crimes, exhibits a more dispersed pattern of crime density, with higher concentrations in certain neighborhoods characterized by socio-economic challenges or historical crime hotspots. Act 379, pertaining to robbery incidents, displays localized clusters of high crime density in commercial districts, transit hubs, and residential areas with high foot traffic.

The graph provides valuable insights into the spatial distribution of different types of crime, aiding law enforcement agencies and urban planners in implementing targeted crime prevention strategies and enhancing public safety initiatives.

The results of the crime analysis and prediction unveil compelling insights into the dynamics of criminal activity within the studied area. The temporal patterns revealed by attributes like hour, day of year, day of week, month, and year elucidate the cyclical nature of crime occurrence, with distinct peaks and troughs throughout the day, week, and year. This temporal granularity not only facilitates short-term tactical planning but also enables long-term strategic decision-making by identifying seasonal trends and year-on-year variations in crime rates. Moreover, the spatial aspect captured by longitude and latitude emphasizes the concentration of criminal incidents in specific geographical areas, indicating potential hotspots for targeted law enforcement interventions and resource allocation. By leveraging these spatial insights, authorities can prioritize patrol routes, allocate resources efficiently, and implement targeted crime prevention initiatives to mitigate risks in high-crime areas.

The feature importance analysis highlights the pivotal role of hour, longitude, and latitude in shaping the accuracy of the crime prediction model. The prominence of hour underscores the significance of temporal dynamics in crime forecasting, enabling law enforcement agencies to anticipate peak periods of criminal activity and deploy resources accordingly. Additionally, the spatial variables of longitude and latitude serve as powerful predictors, pinpointing geographical clusters of criminal incidents and guiding the allocation of law enforcement resources to high-risk areas. By integrating these temporal and spatial features into the predictive model, authorities can enhance the precision of crime forecasting, thereby improving resource allocation, response times, and overall effectiveness in crime prevention efforts.

The ensemble of machine learning algorithms, including KNN, Decision Tree, and Random Forest, demonstrate consistently superior performance metrics in accurately classifying diverse types of crimes. This robust predictive capability, coupled with rigorous model evaluation techniques, instills confidence in the reliability and real-world applicability of the crime prediction system.

CONCLUSION:

In conclusion, the proposed methodology presents a promising approach to crime prediction and analysis, offering a comprehensive framework that leverages advanced machine learning algorithms and rigorous evaluation techniques. The consistently superior performance metrics exhibited by the ensemble of KNN, Decision Tree, and Random Forest algorithms underscore the efficacy of the approach in accurately classifying diverse types of crimes. The emphasis on feature engineering further enhances classification accuracy by capturing nuanced patterns associated with different criminal activities. Moreover, the comprehensive model evaluation ensures the reliability and robustness of the crime prediction system, instilling confidence in its real-world applicability. As such, the proposed methodology holds considerable potential for enhancing public safety and law enforcement strategies by providing actionable insights into crime patterns and facilitating proactive intervention measures.

FUTURE SCOPE:

In future endeavors, the proposed methodology could be extended to incorporate real-time data streams and dynamic modeling techniques to enhance its responsiveness to evolving crime patterns. Additionally, exploring the integration of new technologies such as geospatial analysis and predictive analytics could further augment the system's predictive capabilities and contribute to more targeted crime prevention strategies.

REFERENCES:

[1] Tam, Sakirin, and Ömer ÖzgürTanrıöver. "Multimodal Deep Learning Crime Prediction Using Crime and Tweets." IEEE Access (2023).

[2] H. Arslan, "Crime Analysis and Forecasting using Machine Learning," Journal of Optimization and Decision Making, vol. 2, no. 2, 270-275, 2023

[3] Angbera, Ature, and Huah Yong Chan. "Model for Spatiotemporal Crime Prediction with Improved Deep Learning." Computing and Informatics 42.3 (2023): 568-590.

[4] Z. Li, X. Zhang, F. Xu, X. Jing, and T. Zhang, "A multi-scale video surveillance based information aggregation model for crime prediction," Alexandria Journal, vol. 73, pp. 695-707, 2023.

[5] Mandalapu, Varun, et al. "Crime prediction using machine learning and deep learning: A systematic review and future directions." IEEE Access (2023).

[6] K. Jenga, C. Catal, and G. Kar, "Machine learning in crime prediction," Journal of Ambient Intelligence and Humanized Computing, vol. 14, pp. 2887-2913, 2023

[7] Meghana, Indurthy, et al. "Prediction of Financial Crime Using Machine Learning." International Journal of Innovative Research in Computer Science & Technology 11.3(2023): 96-100

[8] Boukabous, Mohammed, and Mostafa Azizi. "Image and video-based crime prediction using object detection and deep learning." Bulletin of Electrical Engineering and Informatics 12.3 (2023): 1630-1638

[9] AlAbdouli, Shaikha Khamis, et al. "Comparison of Machine Learning Algorithms for Crime Prediction in Dubai." International Journal of Advanced Computer Science and Applications 14.9 (2023).

[10] Saeed, Ruaa Mohammed, and Husam Ali Abdulmohsin. "A study on predicting crime rates through machine learning and data mining using text." Journal of Intelligent Systems 32.1 (2023): 20220223.

[11] Palanivinayagam, Ashokkumar, et al. "An optimized machine learning and big data approach to crime detection." Wireless Communications and Mobile Computing 2021 (2021): 1-10.

[12] Goni, Ibrahim, and Murtala Mohammad. "Machine learning approach to mobile forensics framework for cybercrime detection in Nigeria." Journal of Computer Science Research 2.4 (2020): 1-6.