revista de EDUCACIÓN
2025 408(5)
ISSN: 0034-8082
DOI Link: https://doi.org/10.59671/KI3iR
Vol.408, Issue.5, Part 1., May 2025, PP. 95-129

Leveraging Generative Models, Deep Learning Architectures, and Machine Learning Classifiers for a Data-Driven Approach to Crime Detection and Prediction

Rami A. Alshahrani[1,*] **and Tariq J. S. Khanzada**[2]

[1] ORCID iD: 0009-0007-0602-3229, Department of Information System Faculty, King Abdulaziz University, Street, Jeddah, 100190, State, Saudi Arabia.
[2] ORCID iD: 0000-0003-1617-4403, Computer Systems Engineering Department, Mehran UET, Street, Jamshoro, 10587, State, Pakistan
* rmohammadalshahrani@stu.kau.edu.sa
* tkhanzada@kau.edu.sa

ABSTRACT

Crime poses a significant challenge to the prosperity and growth of nations. Various factors, including poverty, deficiencies in the legal system, unstable economic conditions, and insufficient technological capabilities for crime analysis and detection, contribute to its emergence. This work proposes a novel framework for crime identification and detection utilizing generative and deep learning models. Initially, we extract latent features from an available dataset using a combination of generative model, Deep Learning (DL) and Machine Learning (ML), techniques, including a Variational Auto-Encoder (VAE), transformers, Convolutional Neural Networks (CNN), and Principal Component Analysis (PCA), followed by K-means clustering. We then evaluate the effectiveness of this clustering approach using renowned classifiers, such as Random Forest (RF), Decision Tree (DT), Gradient Boosting (GB), and Naive Bayes (NB). As a result, the framework, which utilizes VAE for feature extraction and combines it with RF as the classifier, achieves the highest accuracy of 0.9993. The strength of the proposed framework lies in its unsupervised learning approach, which attains significant information from data without relying on labeled datasets. This data-driven methodology adeptly leverages generative and deep learning models for feature extraction, subsequently employing these features for crime detection. Furthermore, we analyze individual attributes in latent spaces and apply classifiers, with the VAE demonstrating exciting performance, achieving an accuracy of 0.999.

1 Introduction

Any unlawful and illegitimate act committed by a person that violates national or local regulations is considered a crime. Since the 1960s, crime has become a significant problem with a detrimental impact on nations' economies and social unity. It is caused by poverty, greed, and economic hardship. Crime has been a significant threat to a country, posing a challenge to its prosperity and national integrity. Crime has a significant impact on the economic growth of a country and the standard of living of its citizens. People sometimes use crime rates in cities as their primary consideration when relocating to avoid high-crime areas. In addition, the Institute for Economics and Peace Global Peace Index uses crime rates as a metric to assess nations around the world. However, globally,

security is a major concern and threat[1,2].

With advances in technology and the evolution of cities from simple to complex, there has been a significant increase in the availability of crime data, providing an opportunity to explore crime data in an automated manner and develop a state-of-the-art framework to detect and prevent crimes. However, it is challenging to analyze crime data correctly and effectively, as the data increase daily due to the rising crime rate. Hence, it requires more complex and dense patterns to be discovered from the crime data. To address these challenges, advanced machine learning (ML), deep learning (DL), and artificial intelligence (AI) frameworks can be utilized. These techniques can help identify complex patterns and hidden relationships, thus enhancing crime detection and prevention frameworks. The authors of the study[3] examined Brazil's crime rate, which has been rising sharply in recent years. In many predictive solutions, intelligent systems are used to determine when a criminal offense is likely to occur, allowing police to deploy to locations that are at risk. The authors investigated four machine-learning techniques for predicting the locations of criminal offenses in Fortaleza, Brazil, as part of their study. Their findings suggest that simple algorithms are effective in forecasting criminal activity. Additionally, they observed that the Bagging Regressor and Decision Tree approaches produced high-quality prediction results. The XGBoost algorithm is used in[4] to predict crime. The authors employed multi-class classification models such as OVR-XGBoost and OVO-XGBoost and created an optimized decomposition and fusion approach based on XGBoost, based on the theft incident records in H city. In[5], crime against women A method is presented that uses k-fold cross-validation machine learning for classifiers such as KNN, DT, and SVM. The use of DT and its variant, the evolutionary algorithm decision tree, for crime prediction is presented in[6]. The proposed work demonstrates the advantage of using machine learning for crime prediction. The work in[7] examines the prediction of crime using machine learning. In this study, two distinct data processing techniques are used to analyze crime statistics in Vancouver over the past 15 years. When using machine learning predictive models, such as boosted decision trees and K-nearest neighbor, to predict crime in Vancouver, an accuracy of 39 percent to 44 percent is achieved.Comparative evaluation of the accuracy of the prediction of crime and criminal activity in the Sleman Regency using k-NN, Naive Bayes, and Decision Tree algorithms is presented in[8]. Another important use of machine learning for crime prediction is predictive policing. Using data and analytics to guide law enforcement actions and reduce crime is known as predictive policing. To find crime hotspots and forecast upcoming criminal episodes, machine learning algorithms can be used to examine crime data from a particular geographic area, such as a city or a neighborhood. Therefore, the efficiency of law enforcement operations can be increased by using this information to focus police resources where they are most needed[9].

Deep learning has also gained attention in the fields of crime prediction and prevention, as it automatically extracts complex features and produces the best results. In[10],a deep learning technique that uses a Deep Reinforcement neural network (DRNN) is used to detect violence in videos. The VGGNet-19 pre-trained deep learning model is used; it can identify a knife and a gun in a person's hand that are aimed at another person. Furthermore, the paper examined how two distinct pre-trained models, such as GoogleNet InceptionV3, performed throughout training[11]. In order to analyze human behavior and identify suspicious activity, a ResNet-GRU model was trained in[12]. When there are indications of criminal activity, an alarm is sent out and the relevant authorities are informed. By accurately identifying offenders and items linked to crime, the suggested framework seeks to

make society safer. An LSTM-CNN-based model is implemented to forecast crime prediction is presented in[13]. Generative models have also begun to gain attention in the crime prediction and prediction field. In the paper, the authors use the XD-Violence dataset to develop a multimodal learning model that predicts crimes by incorporating both audio and text modalities into the same model. As an initial step, the data set is in audio using CNN (Convolutional Neural Network) and RNN (Recurrent Neural Network) before moving on to text using BERT (transformator bidirectional encoder representations)[14]. A generative adversarial network is used for the prediction of crime in[15]. The paper[16] presents the implementation of large language models for the identification of crimes. A deep autoencoder-based approach for the recognition of suspicious actions in surveillance videos is given in[17].

An autoencoder is also a powerful generative model that demonstrates the capability to handle high-dimensional data, compressing the information into a lower-dimensional latent space while effectively filtering out noise and retaining the underlying structures. Latent features are helpful in this analysis of crime data, revealing relationships that are not immediately visible in the raw data[18]. Autoencoders can encode complex relation among variables such as profiles of offenders, crimes committed, and geographic locations so that the derived data can be more informative for further analysis. Then, autoencoders transform the data in such a way that clustering algorithms may have a better chance of identifying patterns within it. Among unsupervised clustering algorithms, this one is particularly suitable for crime data. Instead, it relies on an intrinsic structure of the data that automatically discovers representative clusters or examples from the data points by passing messages between them[19]. Some advantages arising from the combination of deep learning with unsupervised clustering include the use of autoencoders for feature extraction, followed by k-means clustering. An additional benefit of using autoencoders in data processing is the creation of a more informative and condensed version of the data, which K-means then utilize to derive meaningful clusters. A clustering-based hotspot identification approach for crime prediction is presented and given in[20]. K-mean clustering and decision tree are used to predict the crime mentioned in[21]. The integration of K-Means clustering and support vector machine (SVM) has been presented in the prediction of the crime scene[22].

In this work, we present a framework that uses a generative model and deep learning together with clustering to predict the crime of a certain country. Consequently, VAE, transformer, CNN, and PCA models are used to extract features followed by clustering techniques. To validate the performance of clustering, the KNN, DT, NB and Gradient Boosting classifiers are used to perform classification. We also learned to use latent space via VAE for gender, location, and crime type, and applied classifiers. Fig. 1 illustrates the scenario being considered, in which the city is monitored using the latest technology to detect crime and take possible actions to reduce it.

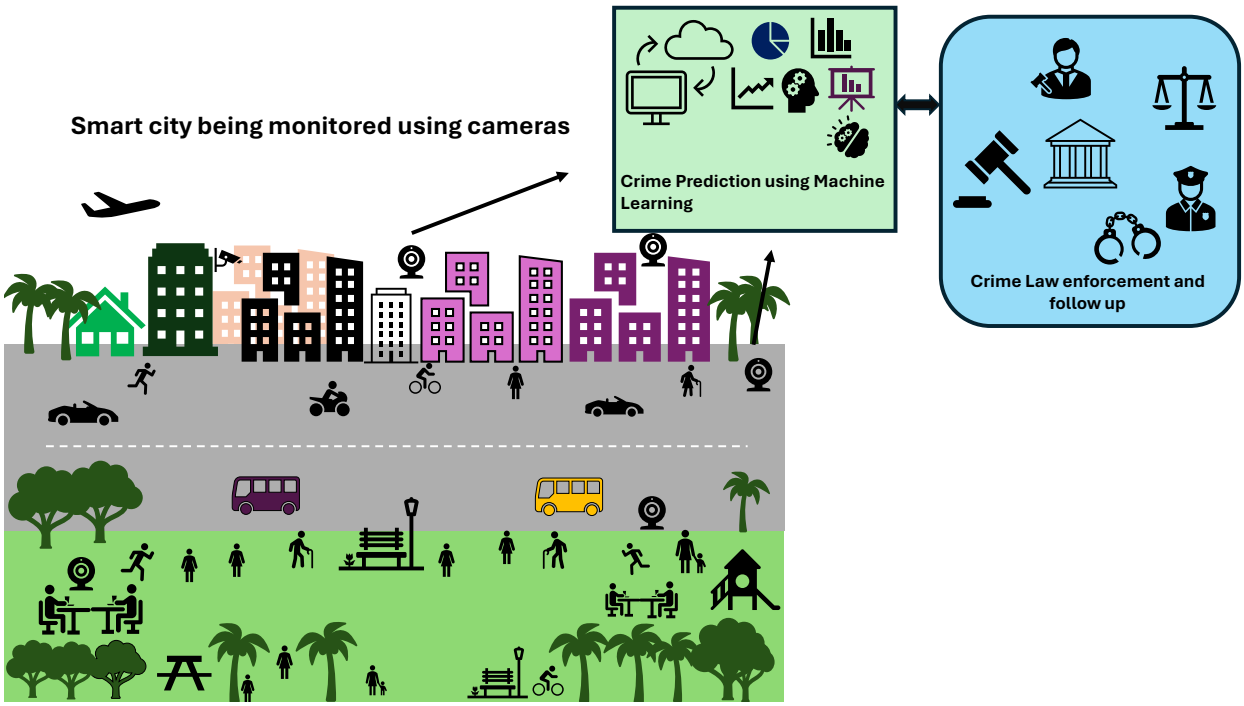

Figure 1. Smart city scenario using modern methods for crime prediction.

1.1 Main Contribution

The following are the main contributions of this work:

1. Extension of crime detection and classification methodologies through the integration of advanced generative models and deep learning architectures, enhancing analytical capabilities in the field of criminology.

2. Comprehensive comparative analysis of various feature extraction techniques, including Variational Autoencoders (VAEs), 1D Convolutional Neural Networks (1D-CNNs), Principal Component Analysis (PCA), and Transformers. This analysis aims to evaluate their efficacy in capturing complex patterns within crime data, providing insights into optimal feature representation for crime analysis.

3. Systematic evaluation of various classifier models to determine their suitability and performance in crime classification tasks, contributing to the identification of optimal machine learning approaches for crime data analysis.

4. Development and validation of a robust and scalable model evaluation framework, addressing a critical challenge in crime prediction and prevention research by demonstrating applicability to large-scale datasets.

These contributions collectively advance the field of computational criminology, offering novel methodologies and insights for more effective crime analysis and prediction. The rest of the paper is

organized as follows: Section 2 describes the literature review, Section 3 presents the methodology and in Section 4, results and discussion are presented. Conclusions and future work are described in the last section.

2 Literature Review

Crime data analysis has long been a vital component in developing effective strategies to prevent crime and enhance public safety. As crime rates continue to shift globally, often influenced by regional socio-economic conditions, the complexity of understanding these patterns has grown. Nowadays, advanced techniques in crime forecasting and categorization are recommended because traditional methods are not reliable enough for today's vast and complex datasets. The authors in paper[23] propose a novel approach to crime prediction utilizing a stacked ensemble model that uses machine learning models such as J48, SVM, Random Forest, and Naïve Bayes.They integrated various classifiers to improve prediction accuracy, achieving a classification accuracy of 99.5% classification accuracy on violent crime datasets from 2001-2015. However, it has some limitations. The dataset used is relatively small, limiting the generalizability of the results to a broader spectrum or more complex crime datasets. Moreover, the paper does not effectively address real-world scenarios, such as integration with actual law enforcement systems. There is also a dependency on evaluation metrics such as accuracy, which might not fully show the potential of the model in actual crime scenarios. Lastly, the lack of detailed comparisons with other advanced ensemble techniques affects the validity of its claims. The paper[24], provides a machine learning (ML) and deep learning (DL) based solution for addressing crime detection and prevention. Using key models including convolutional neural networks (CNNs) and recurrent neural networks (RNNs) for classification, regression, and anomaly detection. However, it does not address data quality issues, as crime data usually suffer from biases, ambiguities, and inaccuracies, which could affect the reliability of the model. Additionally, ethical and privacy concerns related to data handling are only discussed briefly. The experiments performed were limited to specific scenarios; therefore, the model may not yield the same results under varying conditions. Furthermore, the paper does not sufficiently explore scalability challenges or real-world usage, which hinders its practicality for implementation. Furthermore, the paper does not sufficiently explore scalability challenges or real-world usage, which hinders its practicality for implementation. The approach used in[25] provides a detailed analysis of the integration of machine learning (ML) and computer vision (CV) techniques for crime prediction and prevention. They highlighted the shortcomings of traditional approaches; the authors propose machine learning algorithms such as decision trees, KNN, and DNN, combined with computer vision tools such as facial recognition and gait analysis, to enhance predictive accuracy and speed. The study also discusses the potential of creating a surveillance system by incorporating various other technologies, including cryptographic algorithms, neural networks, and heuristic engines, to monitor, predict, and prevent crimes in real time. The dependency of the proposed model on large datasets poses challenges in processing time, which may hinder its scalability and real-time applicability. Furthermore, the model assumes the availability of high-quality and diverse datasets, without considering biases and inaccuracies that may exist in incomplete or imbalanced datasets. Additionally, ethical concerns, such as privacy violations and potential misuse, are not adequately addressed, raising questions about the legal implications of such systems. Selvakumari and Peter

adopted an approach that was more localized by using data from Thoothukudi district to capture regional patterns of crimes better. This would make the reliance on widely used datasets negate localized crime dynamics, which can be said to differ from one area to another. Their work has also put a focus on more real-time data, especially in cases of crimes committed against vulnerable groups such as women and children. They concluded that autoencoders resulted in significant improvements in accuracy and performance in crime classification by applying techniques such as deep learning, including One-Dimensional Convolutional Neural Networks, Gated Recurrent Units, and autoencoders. This shows that deep learning techniques can unravel subtle patterns in crime data and therefore help to develop more strategic approaches to crime prevention[1]. Similarly, Gupta discussed the possibility of Convolutional Autoencoders, layered with ConvLSTM, for the purpose of crime prediction. After testing several optimizers, Gupta found that RMSProp yields the best achievable accuracy at 99.88%. Such results demonstrate the capabilities of deep learning models to achieve high precision under optimal conditions, particularly in cases involving real crime data, where precision is crucial. Such results ensure that deep learning, for example, autoencoders, can dramatically improve the quality of crime forecasting[26].

Traditional methods, such as decision trees and Naive Bayesian classifiers, have been widely applied to crime data analysis; however, they are not without limitations. Almanie et al. reviewed crime data in cities such as Denver and Los Angeles, examining the spatial and temporal patterns of criminal hotspots. Although these models identify risky areas, the intricacy of crime in urban regions has become increasingly complex, and therefore stronger models are needed. This also highlighted the need for methods that can handle large, complex datasets; thus, it lays a path open to the adoption of deep learning techniques that provide both scalability and accuracy [27].

Previous techniques that were applied include stochastic modeling and statistical equations. Wang highlights their theoretical strength, but their inefficiency in practice, especially when handling enormous volumes of data with extremely high dimensions and complicated correlations. Traditional statistical models cannot capture the intricacies of spatio-temporal crime data relationships, resulting in oversimplified or even inaccurate analysis. This gap has pushed forth the shift toward more data-driven, flexible models able to grasp the complexity of crime pattern[19]

The authors, Studiawan and Sohel, have applied autoencoders in anomaly detection for forensic timelines. They had successfully developed a baseline of everyday activities and detected anomalies solely through reconstruction errors. This method yields high precision, demonstrating the versatility of autoencoders in identifying unusual patterns in diverse datasets. This research falls under the umbrella of cybersecurity. However, its principles and methodologies can be applied directly to crime data to detect sudden shifts in rates, allowing for timely intervention in such matters [18].

The methodology applied for the systematic review involved a literature search at a broad level through databases such as IEEE and Science Direct. In this case, the interest was on machine learning and deep learning techniques that can be applied to the area of crime prediction (Chen et al., 2023)[24]. They performed an automatic filtering process along with the review of those studies manually, merely to include only those studies in which the criteria include the objectives, datasets, and algorithms used. The primary limitation of this review is that it depends on fewer databases which may be source restrictions for the scope of literature reviewed. Moreover, it could be difficult for any researcher that needs to replicate or expand the work done in neighborhood crime prediction, due to the scarcity of available public datasets. Zhang et al. (2023)[28] proposed a deep learning-based

LSTM model to predict energy consumption and detect theft in smart grids. This method compares the expected values of energy consumption with real-time readings from smart meters, highlighting anomalies that indicate potential tampering. Additionally, the authors presented an LSTM SVC technique for classifying loss as either technical or non-technical. However, the study has a number of limitations, such as the need to rely on historical data and the difficulty of selecting features that might affect the accuracy of the models. The performance of the proposed model depends on the quality and representativeness of the training data.

The anomaly detection model developed in the videos will use the UCF crime dataset, where the input videos are resolved into frames (Miller, 2024)[29]. The extraction of hidden patterns and features will be performed using a Convolutional Autoencoder neural network, and GANs will support the work by facilitating functions such as video generation and activity prediction. Different types of machine classifiers will be applied to the extracted data to identify anomalies. However, this approach has its limitations and depends on the quality and diversity of the training set; it may not consider including all types of possible anomalies which may affect model generalization in unseen scenarios. In addition, the methodology involves replacing video cameras with laser scanners that might not be as rich as videos, jeopardizing the effectiveness of the overall anomaly detection system. The methodology of the paper focuses on the use of a Compact Ensemble-based discriminator architecture trained on Deep Conditional Generative Adversarial Networks (DCGAN) to identify real-time deepfakes, particularly during video conferences, as noted by (Adams & Brown, 2024)[30]. It consists of splitting video frames, followed by compact ensemble-based classifier approaches to identify GAN images with appropriate fidelity and accuracy. Indeed, the paper acknowledges the limitations of requiring extensive and even highly diverse datasets for successful model training and recognizes that deepfakes are evolving. This necessitates the development of new methods to detect them, which must be constantly adapted and validated to ensure continued effective performance in various scenarios and datasets.

The approach, as Ashish Sharma and Neeraj Varshney have presented, is about the hierarchical methodology of the human activity detection system. Here, the input video frames go through processing, and human objects are segmented before getting features based on color, shape, and motion attributes[31]. The system, while classifying an activity as normal or abnormal, relies on deep learning techniques. The limitations of the paper are admitted regarding the definition of abnormal behavior, as it can vary significantly depending on the context, time, and actions of individuals. In addition, the challenge of gathering an extensive training dataset for abnormal events complicates the development of robust models for the real-time surveillance scenario of anomaly detection.

The research methodology introduced is a multi-step procedure that involves identifying suspicious activity in surveillance video using the concept of feature extraction through a 3D Convolutional Neural Network (C3D) proposed by Wang et al.(2023).[32]. This process begins by converting the datasets into frames and resizing them to meet the requirements of the C3D. It highlights the need for creating a semi-supervised model, as annotating video datasets can be tiring and time-consuming, requiring both frame-level and pixel-level information. A GAN aids in action classification, which typically receives labels only in the final stage. However, the study acknowledges limitations, particularly the focus on binary classification in existing architectures and the lack of comprehensive multi-class annotations, which hampers the effectiveness of action recognition in diverse environments. Furthermore, reliance on high-quality video data poses challenges in real-world applications,

where video quality may vary significantly. The article reviewed the different methodologies for video anomaly detection, focusing mainly on deep learning approaches, such as generative models, temporal regularity models, and hybrid models, as suggested by (Jones,2024),[33]. Such methods rely on more advanced techniques, such as CNNs and LSTM networks, to analyze video data to detect anomalies. Several limitations define the current state of these approaches, including the need for better datasets, challenges in reducing computational complexity, and the inability to capture the abstract and complex nature of human actions. Their effectiveness is further compromised by factors such as crowd density and occlusion, which directly impact the performance of object detection and tracking.

The proposed video anomaly detection method integrates the U-Net architecture on multiple scales, Shortcut Inception Modules, and asymmetric convolution layers, thus increasing feature extraction while reducing the number of training parameters (Garcia & Patel, 2023)[34].The generator network is trained to minimize reconstruction errors in normal data; error signals indicate anomalies during the testing phase. Despite its effectiveness, this framework is specifically designed for a particular set of benchmark datasets; therefore, its generalizability to diverse real-world scenarios may be limited. Although architecture improves detection accuracy, the computational capacity of the network may be a concern in resource-constrained environments. In essence, a brief overview of the broad literature reveals that the traditional approach to crime analysis is only valid in specific contexts and lacks the richness necessary to capture the complexity and high volume of modern crime datasets. Deep learning models, specifically autoencoders with their unique ability to extract and interpret high-dimensional data, combined with flexible clustering techniques, can provide a more accurate, dynamic, and robust approach to crime data analysis. The combination not only improves the accuracy, but also deepens knowledge about the hidden patterns in crime data. Therefore, it is one of the most advanced methods currently available for crime prediction and prevention. In Table1, we present a literature review and in Table.2, literature review is presented with the proposed work. Fig.2 describes and gives an aerial view of the literature review.

Figure 2. Major literature breakdown regarding crime prediction.

Table 1. Systematic Literature Review (SLR)

Paper	Year	Machine Learning	Deep Learning	Generative Models	Technique Summary
[23]	2021	✔	×	×	Utilized a stacked ensemble model that uses machine learning models like J48, SVM, Random Forest, and Naïve Bayes. They integrated various classifiers for enhanced prediction accuracy yielding 99.5% classification accuracy on violent crime datasets from 2001-2015.
[24]	2023	✔	✔	×	Proposed a machine learning (ML) and deep learning (DL) based solution for addressing crime detection and prevention. By utilizing key models including convolutional neural networks (CNNs) and recurrent neural networks (RNNs) for classification, regression, and anomaly detection.
[25]	2021	✔	×	×	The paper highlighted the shortcomings of the traditional approaches, the authors propose a machine learning algorithms like decision trees, KNN, and DNN, combined with computer vision techniques such as facial recognition and gait analysis, to enhance predictive accuracy and speed.
[26]	2021	×	✔	×	Discussed the possibility of Convolutional Autoencoders, layered with ConvLSTM, for the purpose of crime prediction. After testing several optimizers, authors found that RMSProp yields the best achievable accuracy at 99.88%.
[1]	2024	✔	✔	×	They concluded that autoencoders resulted in significant improvements in accuracy and performance in crime classification by applying techniques such as deep learning, including One-Dimensional Convolutional Neural Networks, Gated Recurrent Units, and autoencoders.
[26]	2021	✔	×	×	It uses traditional methods like Decision Trees and Naive Bayesian classifiers and even though these models detect risky areas, the intricacy of crime in urban regions has become more complex, and therefore, stronger models are needed.

Table 2. Literature review with proposed solution (SLR)

Paper	Year	Machine Learning	Deep Learning	Generative Models	Technique Summary
18	2021	×	✔	✔	The authors have utilized autoencoders for anomaly detection in forensic timelines. The proposed approach results in high precision and, thus, marks the versatility of autoencoders for determining unusual patterns in diversified datasets.
32	2024	×	✔	×	The research methodology introduced is a multi-step procedure through identification of suspicious activity in surveillance video using the concept of feature extraction through a 3D Convolutional Neural Network (C3D) proposed by Wang.
28	2022	×	✔	×	They suggested a deep learning-based LSTM model for the prediction of energy consumption and identification of theft in smart grids. In addition to that, the authors also presented an LSTM SVC technique for the classification of loss as technical or non-technical.
30	2024	×	×	✔	The paper methodology centers on the utilization of a Compact Ensemble-based discriminator architecture trained on Deep Conditional Generative Adversarial Networks (CED-DCGAN) to identify real-time deepfakes, especially during video conferences.
31	2020	×	✔	×	It follows a hierarchical methodology of the human activity detection system. Here, the input video frames go through processing, and human objects are segmented before getting features based on color, shape, and motion attributes. The system, while classifying an activity as normal or abnormal, relies on deep learning techniques.
34	2021	×	✔	×	The proposed video anomaly detection method integrates the U-Net architecture at multi-scale, Shortcut Inception Modules, and asymmetric convolution layers, increasing feature extraction with reduced numbers of training parameters.

Continued on next page

Paper	Year	Machine Learning	Deep Learning	Generative Models	Technique Summary
[35]	2023	✔	×	×	The paper examines how machine learning enhances forensic DNA analysis by improving upon time-consuming and error-prone methods that are currently carried out manually. The text highlights why the forensic and computer science areas must learn about the potential of ML through a detailed literature review.
[36]	2025	×	✔	✔	This paper discusses AI's involvement in handling cyber threats by considering Deep Learning, Natural Language Processing, Gen-AI, and Explainable AI. This research examines the differences between ML and DL, investigates the field of XAI for anomaly detection, and explores NLP as applied to threat intelligence and simulation.
Proposed Solution	2024	✔	✔	✔	The proposed framework leverages generative and deep learning models including VAEs, Transformers, CNN, and PCA for feature extraction. Furthermore, machine learning clustering algorithms such as random forest (RF), decision tree (DT), gradient boosting, and naive bayes have been utilized for the classification. The results illustrate that combining VAEs with the Random Forest yields the best performance, achieving an accuracy of 99.87%.

3 Methodology

In this section, we describe the dataset and then outline the implementation of the model. Fig. 3 depicts the proposed methodology for this work. We present two independent frameworks for detecting crime. One approach involves F.E. from well-known techniques, followed by the clustering algorithm. After clustering, the classifiers employed are used to assess the performance of the clustering and feature extractors. In the second approach, the latent space is learned from the features extracted from individual attributes, such as crime location, gender, and nationality. And then we directly applied classifiers to analyze the performance.

3.1 Dataset

This section describes the analysis methodologies used, including the features of extraction approaches, machine learning models, and assessment metrics used to assess model performance. Each stage was meticulously examined to enhance the responsiveness, dependability, and integration of

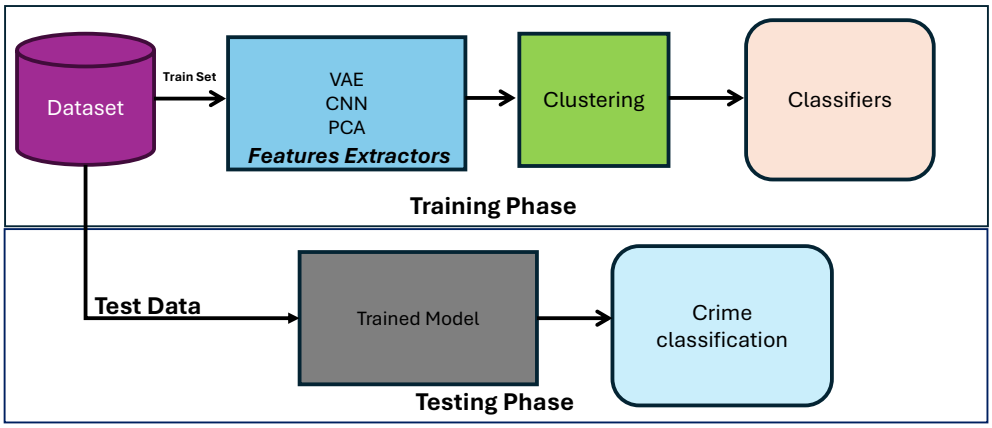

Figure 3. Proposed methodology that involves training and testing phases.

features using both processing methodologies. The preliminary analysis of the dataset involved determining its dimensionality and evaluating the variability of the data points between key features, which informed the selection of optimal feature extraction and classification methods. The data set contains information on the type, location, date, and nationality of the crime and can be represented as.

$$D = \{d_1^{1-12}, d_2^{1-12} \ldots . d_{43682}^{1-12}\} \tag{1}$$

Here, the superscript shows the dimension of the data that contain the prisoner's name, gender, location, crime type, age, etc. In the following Fig. 4 and Fig. 5, we plot some information about the dataset.

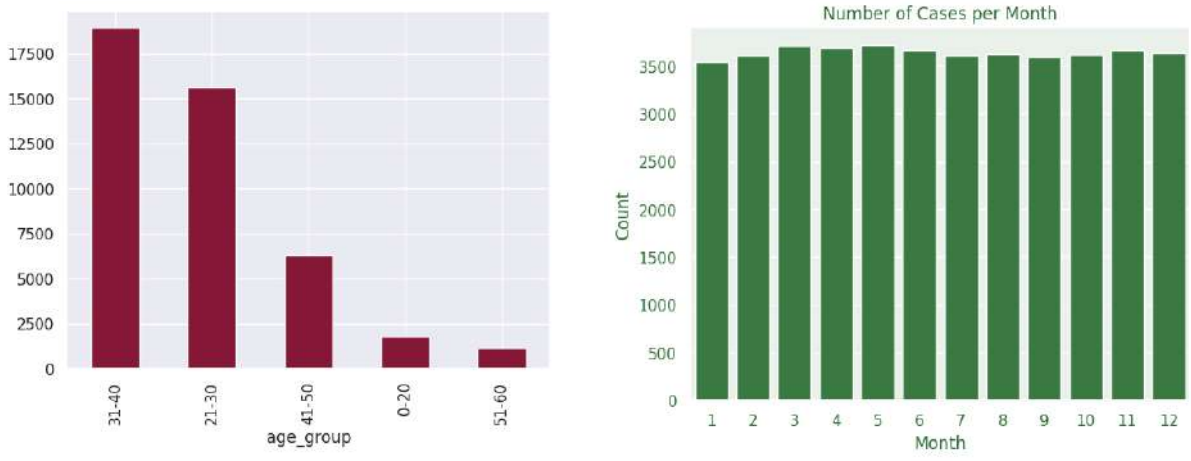

Figure 4. Number of cases per month (on right side) and cases age group (on left side) phases.

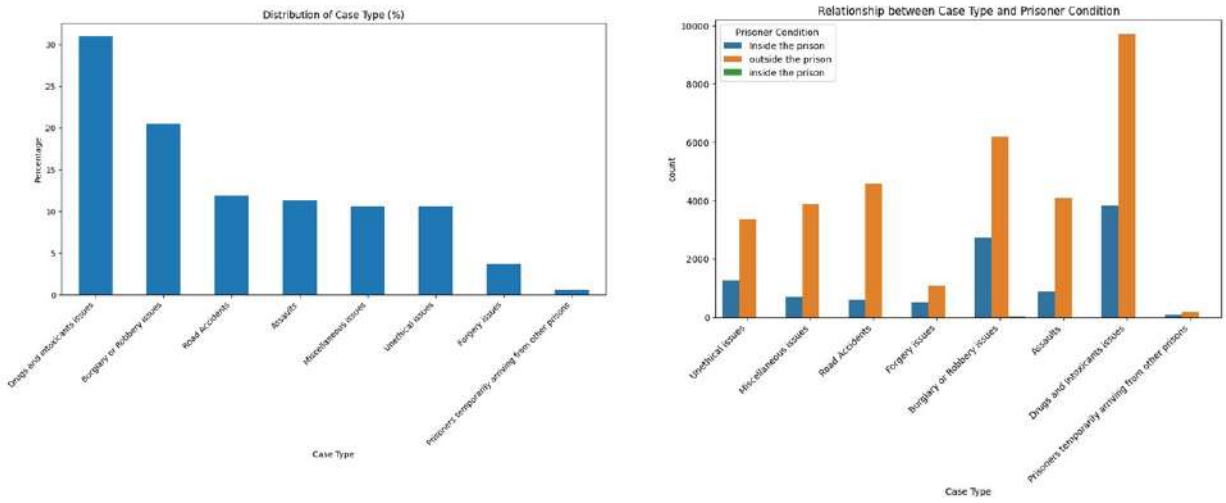

Figure 5. Case type and prisoner (on right side) and distribution of case type (on left side) phases.

3.2 Learning Compact Representation

Feature extraction is an important and essential step in the extraction of features from complex data and then in the learning of AI models based on those features. In this work, we use state-of-the-art AI models together with a conventional approach for feature extraction on some latent spaces. The details of the feature extractors are as follows:

3.2.1 Variational Autoencoder (VAE)

A deep learning-based approach to reduce the dimensionality of the dataset and retain essential structures. VAE learns probabilistic latent variables that encode the data in a lower-dimensional space with a compressed representation, while attempting to maintain as much variance as possible from the original distribution. Several classical classification models were used, with the VAE as input. In VAE, the encoder maps D to a latent representation z that encodes the distinguishing patterns in the data D. Hence it can be written as[37],

$$q_{\Theta}\left(\frac{z}{d}\right) \sim N\left(z, \mu_{\theta}\left(d\right), \xi_{\theta}\left(d\right)\right) \tag{2}$$

Where, θ is the parameter that represents neural network, $\mu_{\theta}\left(d\right)$ mean of the data sample predicted by the encoder network and $\xi_{\theta}\left(d\right)$ shows covariance of the data samples.

3.2.2 Transformers

The Transformer architecture was extended to feature extraction within the dataset, utilizing attention mechanisms. Since they are strong in capturing dependencies between data points, transformers lend themselves to discovering complex patterns. It works by using attention mechanisms to effectively weight the relationship between each data point and its features, which is particularly useful when dealing with high-dimensional data. Transformers work on the principle of attention mechanism, which is given as[38],

$$attention(q,k,v) = Activation function(qk^T/sqrt\,(d_k)) \tag{3}$$

Where q is query, k is key, v is value, are the parameters obtained from data sample D, and dk is the dimensionality of the key vectors which are used to scale dot products to obtain numerical stability.

3.2.3 Convolutional Neual Network (CNN)

These were used to capture the spatial hierarchies in the data by using convolutional filters. CNNs are typically used in image data, but can also be implemented in structured datasets with multiple layers of convolution and pooling, resulting in a smaller subset of features that efficiently convey the underlying understanding. For our data sample D, the filter output is[39]

$$y = \sum_{c=1}^{C} \sum_{i=1}^{I} WD + b \tag{4}$$

Where w is $w_(i,c,k)$ i show position, c represents depth of the channel and k denotes filters and input is shown as $d_((i+j-k),k)$ and b shows bias for the filter.

3.2.4 Principal Component Analysis (PCA)

PCA is a classical linear technique used for dimensionality reduction, preserving the most critical variance in this case. PCA identifies orthogonal components, known as principal components, that explain the variance in the data and therefore effectively reduce the feature space for models to process. This approach was opted for for the case of using a lightweight framework for computational efficiency while not sacrificing too much on performance as well. The following equation describes equations related to PCA[40],

Let the dataset D be an n x p matrix, where n is the number of observations (samples), and p is the number of features (variables).

$$Z = \frac{d-\mu}{\sigma}, C = \frac{1}{n-1} ZZ^T \tag{5}$$

After extracting key representations from the dataset, the altered features were grouped to reveal underlying patterns, which were then used for classification. This study used k-means clustering [22] to categorize the set of characteristics into separate groups. K-means were used because of their efficacy in managing large datasets and their ability to group similar data points into distinct regions based on feature similarity. The clustering procedure enabled a more systematic method for classification, improving the overall effectiveness of the models by providing clearly delineated data groups for the classification phase. In this work, we select the cluster number equal to 8 corresponding to the crime type. Model selection was performed to find out which feature extraction technique was most effective. Various machine learning models were trained on the extracted features to manage high-dimensional data and evaluate the performance of the feature extraction methods. Subsequently, we apply ML models to perform classification tasks. We use the following classifiers in our work:

- **Random Forest**[41]: Random Forest is an ensemble learning technique based on ensembles of decision trees. ince Random Forests do well with complex, non-linear feature interactions — it consistently performed the best across all extracted features.
- **K-Nearest Neighbors (KNN)**[42]: This non-parametric model classifies instances based on the majority vote of their neighbors. Although simplistic, it was shown that KNN could be a competitive approach if the extracted features are well represented, as shown in the study. It is the most beneficial in the cases involving VAE and PCA, as their reduction of dimensionality improved its performance.
- **Naive Bayes**[43]: It's a probabilistic classifier based on Bayes' theorem with the assumption of independence between features. However, contrary to this assumption, Naive Bayes works well on high-dimensional datasets. Primarily, in this study, it is used as a simple benchmark model and taken for comparison with more sophisticated models, especially those employing the PCA features.
- **Decision Tree**[44]: The naives model with the potential to be very powerful. We used Decision Trees because of their high variance and non-linear nature of making decisions by splitting the feature space. The Decision Trees performed well with the VAE + CNN features (second to Random Forest in that sense but a fair bit better than this model), though it was not as strong as the Random Forest.
- **Gradient Boosting**[45]: Gradient Boosting is another ensemble machine-learning algorithm that constructs new models that can correct the errors of previously built ones. This is due to its ease of achieving high accuracy, especially given the features of VAE or PCA, which motivated us to use it in the ablation study discussed above.

4 Model Training and Evaluation

The implementation phase consists of two stages: training and testing, as shown in Figure 3. Firstly, after a data cleaning process, the features are extracted using VAEs, transformers, CNNs, and Principal Component Analysis (PCA). The configuration parameters of the AI models are presented in Table.3,5,6 and 4. The input to the feature extractors is D, a dataset containing 43682 samples. After learning latent spaces, clustering is applied with k = 8 to organize the data into the respective samples. Subsequently, classifiers are used to enhance the performance of both the feature extractor and the clustering algorithm. The details of the training and testing process are given in Algorithm 1. After model training, we evaluate the learned model using the same data. We use the following parameters to analyze the performance of the AI models.

Table 3. Parameters and configurations used in the VAE model.

Parameter	Value	Description
`input_dim`	`scaled_data.shape[1]`	Dimensionality of the input features (determined by the number of columns in `scaled_data`).
`latent_dim`	`20`	Size of the latent space where input data is encoded.
`encoder layer sizes`	`128, 64, latent_dim`	Layer sizes in the encoder: 128 → 64 → `latent_dim` (20).
`decoder layer sizes`	`64, 128, input_dim`	Layer sizes in the decoder: `latent_dim` (20) → 64 → 128 → `input_dim`.
`Dropout rate`	`0.3`	Dropout probability applied to the first encoder layer for regularization.
`activation function`	`ReLU, Sigmoid`	ReLU for hidden layers, Sigmoid for the output layer in the decoder.
`KL weight (annealing)`	`min(1.0, epoch / 50)`	KL divergence weight gradually increases to 1 over the epochs.
`epochs`	`50`	Number of training epochs for the VAE model.
`batch_size`	`64`	Batch size used for training.
`learning_rate`	`0.001`	Learning rate for the Adam optimizer.
`optimizer`	`Adam`	Optimizer used for training the VAE.
`reconstruction loss`	`MSE`	Mean Squared Error used as the reconstruction loss function.
`KL divergence loss`	`-0.5 * sum(...)`	KL divergence component of the VAE loss.

Table 4. Parameters and configurations for Principal Component Analysis (PCA).

Parameter	Value	Description
Algorithm	`PCA`	Principal Component Analysis for dimensionality reduction.
`n_components`	`50`	Number of principal components to retain, reducing the dimensionality of the feature space. Adjusted based on data and desired variance retention.
Input Data	`features`	Feature matrix (output from a previous model, such as the 1D CNN or BERT).
Output Reduced Features	`reduced_features`	Transformed features with reduced dimensionality, maintaining key variance across 50 principal components.

Table 5. Parameters and configurations used in this BERT-Transformers.

Parameter	Value	Description
`model_name`	`"bert-base-uncased"`	Pretrained BERT model variant used for feature extraction.
`tokenizer`	`AutoTokenizer`	Tokenizer loaded from the `bert-base-uncased` model.
`text_data length`	`len(data['text'])`	Total number of records in the dataset converted to text.
`max_length`	`128`	Maximum token length for BERT input; truncates sequences longer than this.
`batch_size`	`64`	Number of records processed in each batch for efficient memory usage and GPU processing.
`padding`	`True`	Pads sequences to the same length within each batch for compatibility with BERT input requirements.
`truncation`	`True`	Truncates sequences longer than `max_length` to avoid overflow.
`feature extraction layer`	`last_hidden_state`	Uses the last hidden state layer from BERT; the first token representation is used as a sentence feature.
`output feature dimension`	`768`	Dimensionality of the BERT embeddings for each record (BERT base model has 768 dimensions).

ISSN: 0034-8082

Table 6. Key parameters and configurations for the 1D CNN feature extraction setup.

Parameter	Value	Description
Input Data Dimension	`(batch_size, 1, n_features)`	Data reshaped to be compatible with 1D CNN. `n_features` represents the feature dimension of `scaled_data`.
Conv1 Layer	`Conv1d`	1D convolution with `in_channels=1`, `out_channels=16`, `kernel_size=3`, and `padding=1`.
Conv2 Layer	`Conv1d`	1D convolution with `in_channels=16`, `out_channels=32`, `kernel_size=3`, and `padding=1`.
Flattening Layer	`view`	Flattens the output after the last convolutional layer to feed into fully connected layers.
FC1 Layer	`Linear`	Fully connected layer with `input_dim=32*n_features` and `output_dim=128`.
FC2 Layer	`Linear`	Final fully connected layer with `input_dim=128` and `output_dim=64` (the final extracted feature dimension).
Loss Function	`MSELoss`	Mean Squared Error; loss type is less relevant here since the goal is feature extraction.
Optimizer	`Adam`	Optimization algorithm with a learning rate of 0.001.
Output Feature Dimension	`64`	Final output dimension after passing through the fully connected layers, representing extracted features for each input record.

ISSN: 0034-8082

Algorithm 1 Model Training and Testing Process

Step 1: Dataset (D)
Load the dataset (D).
Step 2: Preprocess Data
Clean, scale, and encode the data.
Step 3: Feature Extraction
Perform feature extraction using the following methods:

- Variational Autoencoders (VAEs)
- 1D-CNN
- BERT-Transformers
- Principal Component Analysis (PCA)

Step 4: Feature Clustering
Feature clustering using the following method:

- K-means

Step 5: Train Classifiers
Initialize multiple classifiers:

- k-Nearest Neighbors (KNN)
- Random Forest / Decision Tree
- Naive Bayes
- Gradient Boosting

Train each classifier on the reduced features.
Step 6: Testing
Use the trained classifiers to make predictions on the test set.
Step 7: Evaluation
Evaluate each classifier's performance:

- Calculate accuracy, precision, recall, and F1 score.
- Compute the confusion matrix.
- Display the evaluation metrics for each classifier.

Step 8: Model Selection
Select the best-performing model based on evaluation metrics (e.g., F1 score or accuracy).

Algorithm 2 Model Training and Testing Process

STEP 1: Data Preprocessing
a: Given Dataset: D.
b: Impute Missing Values: Replace missing values in feature x_j with mean $\bar{x}_j = \frac{1}{m}\sum_{i=1}^{m} x_{i,j}$.
c: Encode Categorical Variables: Map categories to integers using `LabelEncoder`.
d: Standardize Numerical Features:

$$x_{\text{Standardized}} = \frac{x_j - \mu_j}{\sigma_j}$$

STEP 2: Variational Autoencoder (VAE)
a: Encoder: Input X, output latent mean μ and log-variance $\log(\sigma^2)$.
b: Layers:

$$h_1 = \text{ReLU}(W_1 X + b_1), \quad h_2 = \text{Dropout}(h_1), \quad \mu = W_\mu h_2 + b_\mu$$

$$\log(\sigma^2) = W_{\log(\sigma^2)} h_2 + b_{\log(\sigma^2)}$$

c: Reparameterization Trick:

$$z = \mu + \sigma \cdot \varepsilon, \quad \varepsilon \sim N(0, I), \quad \sigma = \exp\left(\frac{1}{2}\log(\sigma^2)\right)$$

d: Decoder: Decodes z back to X' using layers:

$$h_3 = \text{ReLU}(W_3 z + b_3), \quad X' = \text{Sigmoid}(W_4 h_3 + b_4)$$

e: Loss Function:

- **i.** Reconstruction Loss (MSE):

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(x_i - x_i')^2$$

- **ii.** KL Divergence:

$$KL(q(z|X) \parallel p(z)) = \frac{1}{2}\sum_{j=1}^{d}\left(1 + \log(\sigma_j^2) - \mu_j^2 - \sigma_j^2\right)$$

- **iii.** Total Loss:

$$\text{Loss}_{\text{VAE}} = \text{MSE} + \beta \cdot KL$$

STEP 3: Training Process
1: Training: Minimize loss with gradient descent.
2: Extract Latent Features: Transform X to latent space Z using the encoder.
3: Train-Test Split: Split Z and target y into training and test sets:

$$(Z_{\text{train}}, Y_{\text{train}}) \quad \text{and} \quad (Z_{\text{test}}, Y_{\text{test}})$$

STEP 4: Testing Process
1: Classifier: Train on $(Z_{\text{train}}, Y_{\text{train}})$ and evaluate accuracy on the test set.
2: Metrics: Report precision, recall, F1-score, and plot confusion matrix.

$$\text{Accuracy}_{\text{test}} = \frac{\text{Correct Predictions in Test Set}}{\text{Total Test Set Samples}}$$

- **Accuracy:** It represents the number of correct predictions made from all the predictions made. This was used as the primary measure to evaluate how different feature extraction methods and classifiers were applied to a specific dataset.
- **AUC-ROC (Area Under the Curve - Receiver Operating Characteristic):** AUC-ROC is one of the most critical metrics for evaluating classification models, especially when working with imbalanced datasets. It quantifies the model's ability to distinguish between positive and negative points. A higher AUC value indicates good model performance.
- **Precision:** Precision is the ratio of true optimistic predictions to the total number of predicted positives. The performance of this metric is especially relevant in this study, as the number of false positives could significantly affect the type of model we will have.
- **Recall:** It is also called sensitivity. Recall calculates the proportion of actual activity that is correctly identified as activity, whether it is correctly or incorrectly identified. A high recall means that the model is identifying true positive cases at a high rate and does not necessarily imply that precision should be compromised.
- **F1 Score:** The F1 score is the harmonic mean of precision and recall. The combined performance of both metrics makes them helpful in measuring cases where an imbalanced class problem exists.

Fig. 6 and 7 demonstrate the model's performance in terms of ROC curves when the features are extracted from the Variational Autoencoder, Transformer, CNN, and PCA. Table7 presents the performance of the model in terms of precision, precision, recall, and F1 score, together with the corresponding metric scores. The results are excellent when VAE is used as a feature extractor. VAE demonstrates good performance because it learns the latent space in a probabilistic manner. In addition, the RF classifier demonstrates excellent performance with an accuracy of 0.9993% when VAEs are used as feature extractors.

To further extend the implementation, we learned features of individual attributes from the dataset using VAE. We selected VAE because it gives good performance in the first phase, which involves clustering. Algorithm 2 demonstrates the training and testing phases. In this perspective, Table.8 shows model's performance when we learned gender and region of the crime. We have selected three cities, A, B, and C. Table.9 describes classification report based on gender. where, 0 denotes male and 1 represents female. Table.10 and Table.11 show classification report based on the location of the crime and the type of crime, respectively. Figs. 8, 9, and 10 depict model performance in terms of confusion matrices when features are extracted from VAE and KNN, DT, RF, NB, and GB are used as classifiers. Since the VAE is performing very well as a feature extractor, therefore, all of the classifiers perform well in classifying crime based on crime type. Similarly, Figs. 11, 12, and 13 show model performance when CNN is used as a feature extractor and classifiers are applied to perform classification tasks. The performance of the transformer model and classifiers is given in Figs. 14 and 15. In Figs. 16, 17, and 18, the performance of the PCA model is given together with the classifiers.

We have also determined the time and memory consumption of feature extractors, along with the classifiers, as shown in Fig. 19. It is evident that a transformer utilizes more memory and takes longer to process. Nevertheless, the performance of VAE is good and acceptable in terms of memory and time consumption. Moreover, VAE outperforms other models as well.

Table 7. Proposed model performance in terms of accuracy, precision, recall, and F1.

Feature Extraction	Model	Accuracy	AUC ROC	Precision	Recall	F1 Score
VAE	KNN	0.9974	0.9999	0.9974	0.9974	0.9974
	Naive Bayes	0.9720	0.9995	0.9750	0.9720	0.9727
	Random Forest	0.9993	1.0000	0.9993	0.9993	0.9993
	Decision Tree	0.9982	0.9989	0.9982	0.9982	0.9982
	Gradient Boosting	0.9987	1.0000	0.9987	0.9987	0.9987
BERT-Transformer	KNN	0.9785	0.9973	0.9816	0.9809	0.9813
	Random Forest	0.9948	0.9999	0.9952	0.9948	0.9950
	Decision Tree	0.9835	0.9899	0.9858	0.9843	0.9850
1D-CNN	KNN	0.9898	0.9989	0.9922	0.9900	0.9911
	Naive Bayes	0.9496	0.9983	0.9514	0.9692	0.9594
	Random Forest	0.9972	0.9999	0.9977	0.9971	0.9974
	Decision Tree	0.9900	0.9927	0.9896	0.9869	0.9882
	Gradient Boosting	0.9944	0.9999	0.9954	0.9937	0.9946
PCA	KNN	0.9931	0.9994	0.9942	0.9935	0.9938
	Random Forest	0.9978	0.9999	0.9981	0.9977	0.9979
	Decision Tree	0.9950	0.9970	0.9954	0.9948	0.9951
	Naive Bayes	0.9183	0.9938	0.9264	0.9331	0.9281
	Gradient Boosting	0.9966	0.9999	0.9968	0.9967	0.9967

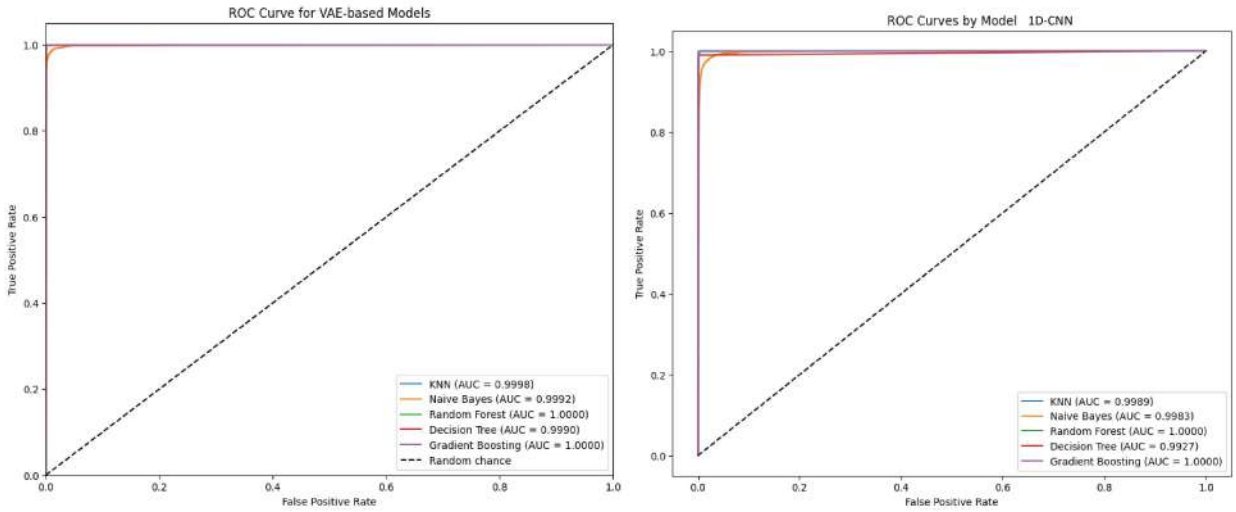

Figure 6. Model performance when features are extracted from VAE, and CNN and then fed into Clusters, and the Classifiers.

ISSN: 0034-8082

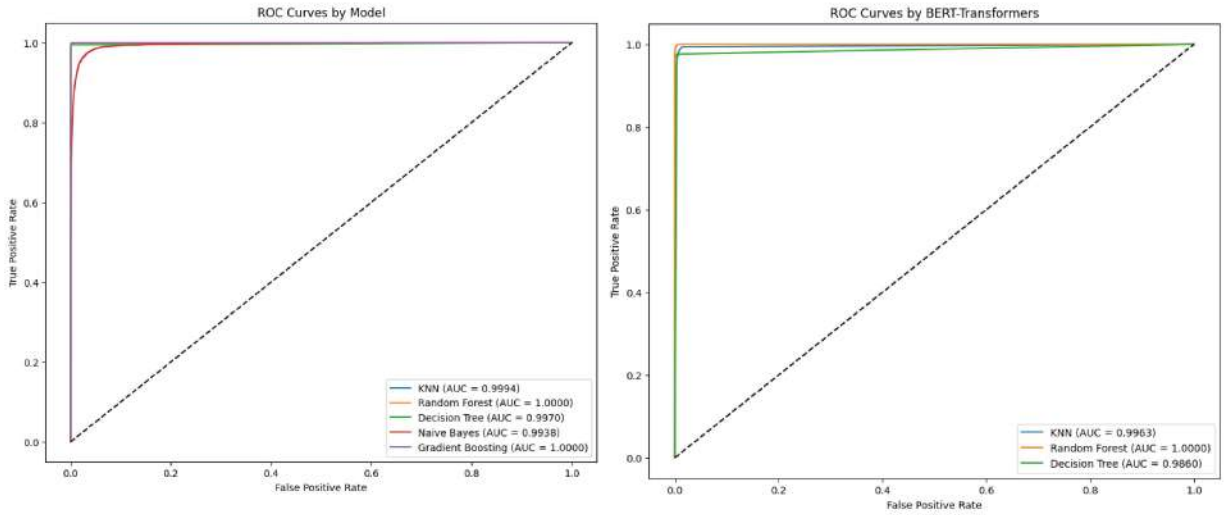

Figure 7. Model performance when features are extracted from PCA and Transformer and then fed into Clusters, and the Classifiers.

Table 8. Classification Report (Region & Gender)

Class	Precision	Recall	F1-Score
City A_Female	1.000000	0.125000	0.222222
City A_Male	0.982363	0.975482	0.978910
City B_Female	0.981818	0.977867	0.979839
City B_Male	0.996165	0.998786	0.997474
City C_Female	0.988636	0.887755	0.935484
City C_Male	0.995819	0.999618	0.997715
Accuracy	0.994277	0.994277	0.994277
Macro Avg	0.990800	0.827418	0.851941
Weighted Avg	0.994262	0.994277	0.993925

Table 9. Classification Report (Gender)

Class	Precision	Recall	F1-Score
0	0.984266	0.933665	0.958298
1	0.995101	0.998894	0.996994
Macro Avg	0.989683	0.966279	0.977646
Weighted Avg	0.994353	0.994392	0.994323

Table 10. Classification Report (Crime Location)

Class	Precision	Recall	F1-Score
0	0.991213	0.974093	0.982578
1	0.997247	0.999081	0.998163
2	1.000000	1.000000	1.000000
Macro Avg	0.996153	0.991058	0.993581
Weighted Avg	0.997704	0.997711	0.997702

Table 11. Classification Report (Nationality)

Class	Precision	Recall	F1-Score
0	1.000000	0.200000	0.333333
1	1.000000	0.500000	0.666667
2	0.000000	0.000000	0.000000
3	0.963680	0.971917	0.967781
4	0.969027	0.916318	0.941935
6	0.988630	0.998832	0.993705
7	0.000000	0.000000	0.000000
9	0.971347	0.967650	0.969495
10	0.982922	0.948718	0.965517
12	1.000000	0.333333	0.500000
13	0.983359	0.984848	0.984103
14	0.968750	0.911765	0.939394
15	0.000000	0.000000	0.000000
Macro Avg	0.755978	0.594875	0.635533
Weighted Avg	0.981981	0.982374	0.981868

Figure 8. Model performance when features are extracted from VAE without cluster.

Figure 9. Model performance when features are extracted from VAE without cluster Target Variable - *CaseType*).

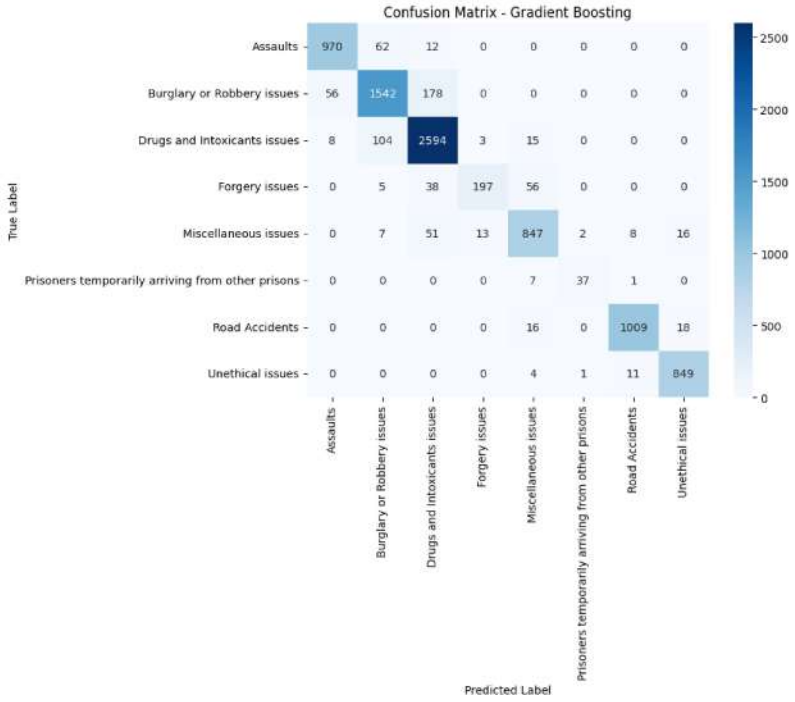

Figure 10. Model performance when features are extracted from VAE without cluster Target Variable - *CaseType*).

Figure 11. Model performance when features are extracted from 1D-CNN without Cluster Target Variable - *CaseType*).

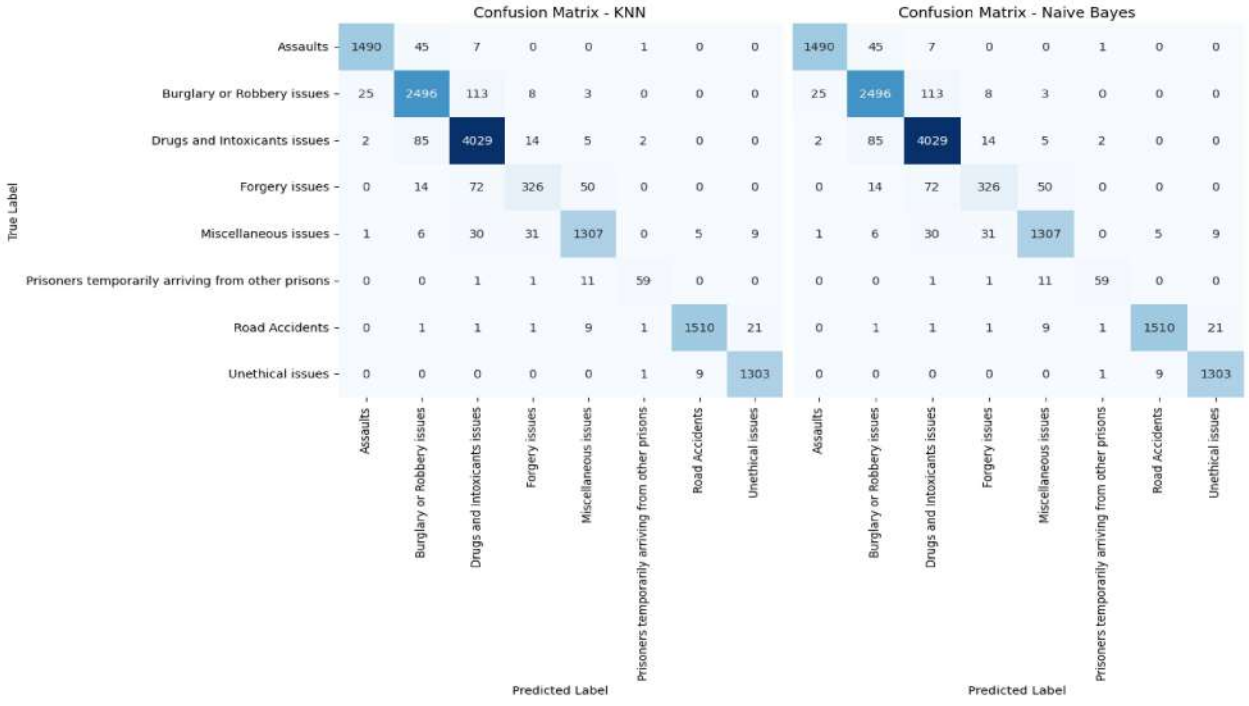

Figure 12. Model performance when features are extracted from 1D-CNN without Cluster Target Variable - *CaseType*).

Figure 13. Model performance when features are extracted from 1D-CNN without Cluster Target Variable - *CaseType*).

Figure 14. Model performance when features are extracted from BERT-Transformers without Cluster Target Variable - *CaseType*).

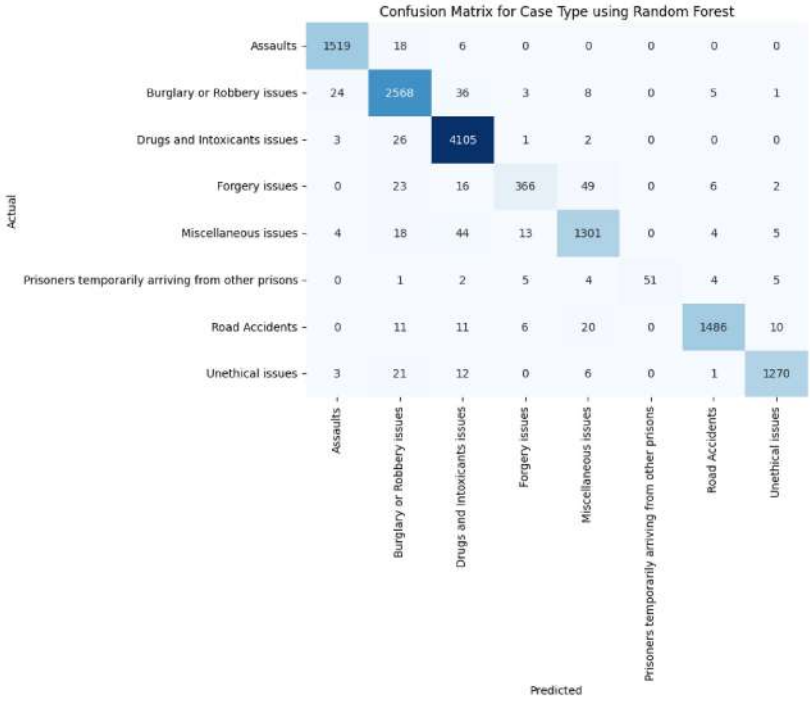

Figure 15. Model performance when features are extracted from BERT-Transformers without Cluster Target Variable - *CaseType*).

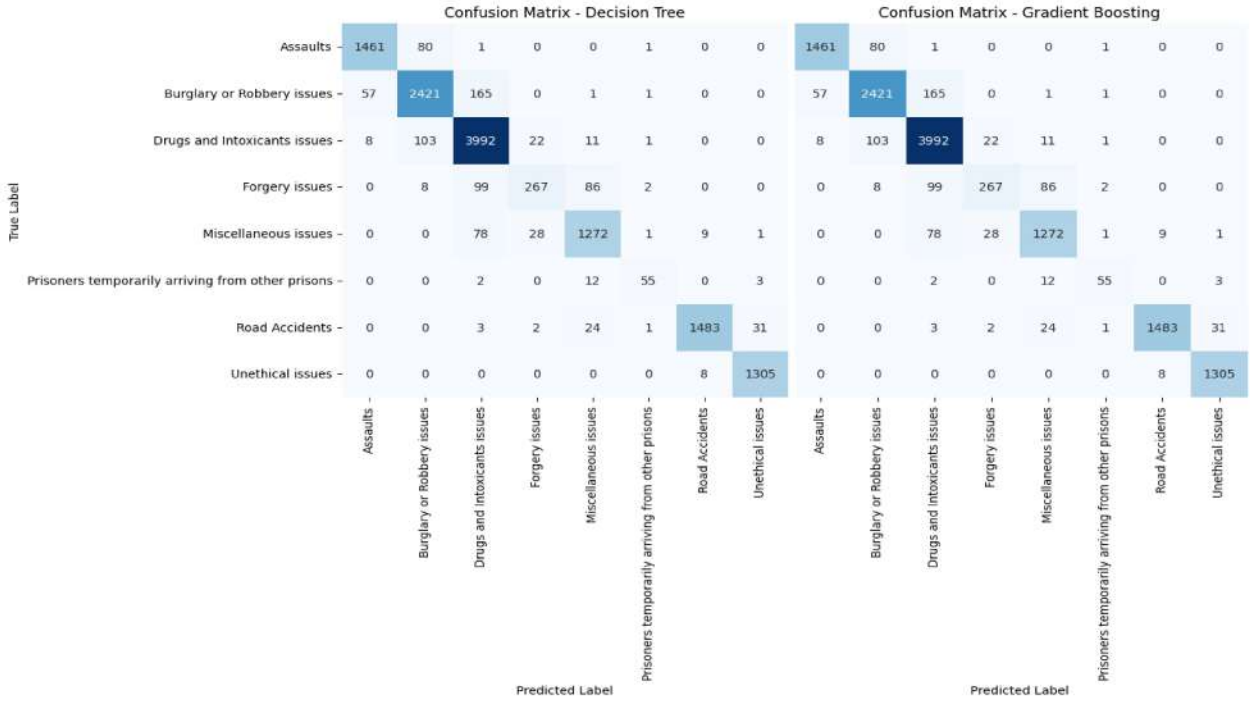

Figure 16. Model performance when features are extracted from PCA without Cluster Target Variable - *CaseType*).

Figure 17. Model performance when features are extracted from PCA without Cluster Target Variable - *CaseType*).

Figure 18. Model performance when features are extracted from PCA without Cluster Target Variable - *CaseType*).

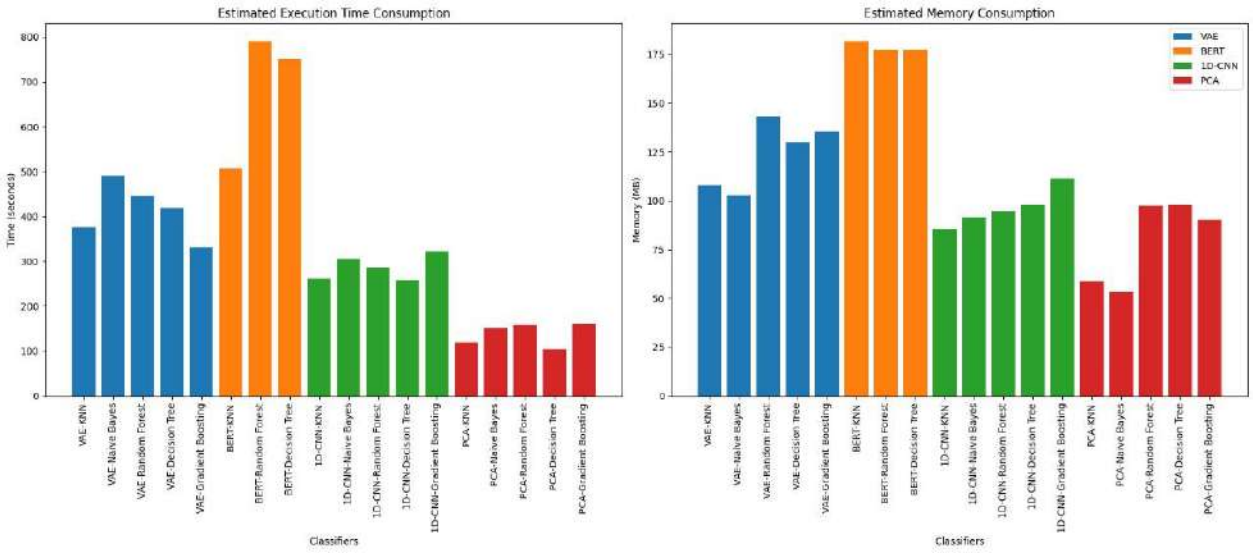

Figure 19. Time and Memory consumption of the implemented models.

5 Discussion

This research adds several original ideas to the field of criminology by using advanced models and deep learning techniques to enhance the methods of detecting and classifying crimes. Its main innovation lies in the use of modern technologies, such as generative models and deep neural networks, to surpass traditional techniques when working with crime data. These approaches have enabled the study to identify more detailed patterns in crime data, resulting in trustworthy and accurate crime detection tools. It is vital for criminology because the nature of crime patterns can change in many unexpected ways.

In addition, the study adds to the body of knowledge by comparing several feature extraction methods in detail. Looking at Variational Autoencoders (VAEs), 1D Convolutional Neural Networks (1D-CNNs), Principal Component Analysis (PCA) and Transformers, the study sheds light on which strategies best represent features in the analysis of crime data. Highlights both the advantages and disadvantages of each technique and provides guidance on selecting the most suitable methods for studying crime statistics. It opens up new avenues for research to optimize feature extraction and create more accurate and better-performing crime models.

Researchers systematically examine various machine learning tools to identify the models that best suit crime classification tasks. Using several classifiers, the study explains the various ways in which they interact with crime data and suggests which are most effective for crime prediction and prevention. Furthermore, developing a robust evaluation process for models facilitates the management of large amounts of crime data, making this a significant contribution to criminological studies. Its effectiveness and ability to scale enable it to be used in real-world cases, helping to advance crime prediction and prevention by introducing advanced and scalable solutions.

6 Conclusion and Future work

Specifically, the experimental results consistently indicate that Random Forest is the most stable and robust model for managing complex and high-dimensional crime data, particularly when combined with sophisticated feature extraction techniques such as CNN, VAE, and PCA. Random Forest, with VAE features, was the clear winner among the various models evaluated, achieving near-perfect accuracy and AUC-ROC scores. Although Gradient Boosting was also competitive, it was slightly behind Random Forest in terms of computational efficiency and speed, rendering Random Forest the more practical option.

Similarly to previous experiments, and one after the other, when features from transformers were blended with features from CNN, random forests performed outstandingly and applied well towards different feature extraction methodologies. Again, PCA performance improved on Random Forest, which reduced the computation load while keeping accuracy high and precision high, thus making it stronger as a dimensionality reduction tool.

The experiments demonstrate that, for this dataset, the best algorithm, particularly when combined with VAE features, is Random Forest, as it consistently exhibits outstanding performance across all metrics used, making it the most effective model for complex, high-dimensional data. Of course, gradient boosting remains a valid alternative. However, it is potentially suitable for use when higher computational costs are tolerable, and it provides a better-balanced solution in terms of efficiency and accuracy, as seen in random forests.

Almost the perfect solution for environments where computational efficiency is a consideration is Random Forest with Principal Component Analysis (PCA). Although both the Decision Tree and KNN models performed similarly, they fell short in terms of consistency and robustness compared to the Random Forest model in this experiment.

This technique, based on the combination of sophisticated feature extraction methods and ensemble models, represents an all-inclusive approach to the analysis of crime datasets. As such, it can be adapted for numerous scenarios and offers an accurate, scalable, reliable, and fast framework.

The results of the study indicate that Random Forest performs exceptionally well in crime datasets when combined with advanced feature extraction techniques, such as CNN, VAE, and PCA. Methodology could hold immense opportunities in terms of future research, which could further improve and enhance its applicability in many other fields.

These works rely on an existing technique, which includes VAE, transformers, CNN, and PCA. New advancements in feature extraction techniques by GNNs or self-supervised learning may be explored further ahead, especially with datasets having a social network, geographical data, or time-series crime patterns.

Hybrid architecture and techniques from multiple models can be applied in unique ways, even though Random Forest consistently produces good performance results. For example, deep learning LSTMs or RNNs have demonstrated that incorporating random forests into them enhances their predictability, particularly for time-sensitive or sequential data, making them suitable for applications in crime analytics.

The further development of this model will be helpful in future work with real-time crime prediction systems. This will occur through the adaptation of models to function in streaming environments, where data streams into the system in real-time for immediate classification or

clustering.

For real-world data, crime datasets are often unbalanced, where a particular type of crime or a specific region may have significantly more data compared to other areas. Future research may enhance the generalizability of the models by incorporating synthetic data generation techniques, such as SMOTE (Synthetic Minority Over-Sampling Technique) or GANs (Generative Adversarial Networks), to create more balanced datasets. Additional steps can incorporate geospatial analysis and temporal feature engineering to further enhance the contextual information captured by models, as crime data often encompass both geographic and temporal dimensions. This may translate into being better able to predict the spatiotemporal distribution of crime, as well as gaining a deeper understanding of how the temporal dynamics of crime patterns evolve. One can envision further research into federated learning approaches, where models could be trained across numerous decentralized datasets, all without ever having access to sensitive data. This would thus enable a more privacy-aware approach to crime prediction while still leveraging the capabilities of thousands of data sources. These areas leave scope for future research to develop this paper further, enhance the model's performance, and increase the real-world applicability of machine learning models in crime prediction and beyond.

7 Data Availability

The datasets generated and/or analyzed during the current study are not publicly available due to privacy concerns, but are available from the corresponding author on reasonable request.

References

1. Selvakumari, S. J. & Peter, V. J. Crime classification using gru, cnn and autoencoder techniques. *Educ. Adm. Theory Pract.* **30**, 2950–2964 (2024).

2. Dayara, T., Thabtah, F., Abdel-Jaber, H. & Zeidan, S. Crime analyses using data analytics. *Int. J. Data Warehous. Min. (IJDWM)* **18**, 1–15 (2022).

3. da Silva, A. R. C., de Paula Júnior, I. C., da Silva, T. L. C., de Macêdo, J. A. F. & Silva, W. C. P. Prediction of crime location in a brazilian city using regression techniques. *2020 IEEE 32nd Int. Conf. on Tools with Artif. Intell. (ICTAI)* 331–336 (2020).

4. Yan, Z., Chen, H., Dong, X., Zhou, K. & Xu, Z. Research on prediction of multi-class theft crimes by an optimized decomposition and fusion method based on xgboost. *Expert. Syst. with Appl.* **207**, 117943, DOI: https://doi.org/10.1016/j.eswa.2022.117943 (2022).

5. Tamilarasi, P. & Rani, R. Diagnosis of crime rate against women using k-fold cross validation through machine learning. In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, 1034–1038, DOI: 10.1109/ICCMC48092.2020.ICCMC-000193 (2020).

6. Ma, Y., Nakamura, K., Lee, E.-J. & Bhattacharyya, S. S. Eadtc: An approach to interpretable and accurate crime prediction. *2022 IEEE Int. Conf. on Syst. Man, Cybern. (SMC)* 170–177 (2022).

7. Kim, S., Joshi, P., Kalsi, P. S. & Taheri, P. Crime analysis through machine learning. In *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 415–420, DOI: 10.1109/IEMCON.2018.8614828 (2018).

8. Wibowo, A. & Oesman, T. The comparative analysis on the accuracy of k-nn, naive bayes, and decision tree algorithms in predicting crimes and criminal actions in sleman regency. *J. Physics: Conf. Ser.* **1450**, 012076, DOI: 10.1088/1742-6596/1450/1/012076 (2020).

9. Meijer, A. & Wessels, M. Predictive policing: Review of benefits and drawbacks. *Int. J. Public Adm.* (2019).

10. Sahay, K. B. *et al.* A real time crime scene intelligent video surveillance systems in violence detection framework using deep learning techniques. *Comput. Electr. Eng.* **103**, 108319 (2022).

11. Navalgund, U. V. & K, P. Crime intention detection system using deep learning. *2018 Int. Conf. on Circuits Syst. Digit. Enterp. Technol. (ICCSDET)* 1–6 (2018).

12. Shenoy, R., Yadav, D., Lakhotiya, H. & Sisodia, J. An intelligent framework for crime prediction using behavioural tracking and motion analysis. 1–6, DOI: 10.1109/ESCI53509.2022.9758281 (2022).

13. Muthamizharasan, M. & R P, P. *Forecasting Crime Event Rate with a CNN-LSTM Model*, 461–470 (2022).

14. Boukabous, M. & Azizi, M. Multimodal sentiment analysis using audio and text for crime detection. 1–5, DOI: 10.1109/IRASET52964.2022.9738175 (2022).

15. Dulce, M., Gómez, Ó., Moreno, J. S., Urcuqui, C. & Villegas, Á. J. R. Interpreting a conditional generative adversarial network model for crime prediction. In Tavares, J. M. R. S., Papa, J. P. & González Hidalgo, M. (eds.) *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, 281–290 (Springer International Publishing, Cham, 2021).

16. Nikolakopoulos, A. *et al.* Large language models in modern forensic investigations: Harnessing the power of generative artificial intelligence in crime resolution and suspect identification. In *2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE)*, 1–5, DOI: 10.1109/EEITE61750.2024.10654427 (2024).

17. Ahmed, W. & Yousaf, M. H. A deep autoencoder-based approach for suspicious action recognition in surveillance videos. *Arab. J. for Sci. Eng.* **49**, DOI: 10.1007/s13369-023-08038-7 (2023).

18. Studiawan, H. & Sohel, F. Anomaly detection in a forensic timeline with deep autoencoders. *J. Inf. Secur. Appl.* **63**, 103002 (2021).

19. Wang, Q., Jin, G., Zhao, X., Feng, Y. & Huang, J. Csan: A neural network benchmark model for crime forecasting in spatio-temporal scale. *Knowledge-Based Syst.* **189**, 105120 (2020).

20. Hajela, G., Chawla, M. & Rasool, A. A clustering based hotspot identification approach for crime prediction. *Procedia Comput. Sci.* **167**, 1462–1470, DOI: https://doi.org/10.1016/j.procs.2020.03.357 (2020). International Conference on Computational Intelligence and Data Science.

21. Kumar, J., Sravani, M., Akhil, M., Sureshkumar, P. & Yasaswi, V. Crime rate prediction based on k-means clustering and decision tree algorithm. In Smys, S., Bestak, R., Palanisamy, R. & Kotuliak, I. (eds.) *Computer Networks and Inventive Communication Technologies*, 451–462 (Springer Nature Singapore, Singapore, 2022).

22. Aiman Awangku Bolkiah, A. H. *et al.* Crime scene prediction using the integration of k-means clustering and support vector machine. In *2022 IEEE 10th Conference on Systems, Process & Control (ICSPC)*, 242–246, DOI: 10.1109/ICSPC55597.2022.10001768 (2022).

23. Kshatri, S. S. *et al.* An empirical analysis of machine learning algorithms for crime prediction using stacked generalization: an ensemble approach. *Ieee Access* **9**, 67488–67500 (2021).

24. Mandalapu, V., Elluri, L., Vyas, P. & Roy, N. Crime prediction using machine learning and deep learning: A systematic review and future directions. *IEEE Access* **11**, 60153–60170 (2023).

25. Shah, N., Bhagat, N. & Shah, M. Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention. *Vis. Comput. for Ind. Biomed. Art* **4**, 9 (2021).

26. Tariq, H. *et al.* Employing deep learning and time series analysis to tackle the accuracy and robustness of the forecasting problem. *Secur. Commun. Networks* **2021**, 5587511 (2021).

27. Almanie, T., Mirza, R. & Lor, E. Crime prediction based on crime types and using spatial and temporal criminal hotspots. *arXiv preprint arXiv:1508.02050* (2015).

28. Tanwar, S. *et al.* Grab: a deep learning-based data-driven analytics scheme for energy theft detection. *Sensors* **22**, 4048 (2022).

29. Zaheer, M. Z. *et al.* Generative cooperative learning for unsupervised video anomaly detection. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 14744–14754 (2022).

30. Sharma, S. K., AlEnizi, A., Kumar, M., Alfarraj, O. & Alowaidi, M. Detection of real-time deep fakes and face forgery in video conferencing employing generative adversarial networks. *Heliyon* **10** (2024).

31. Sharma, A. & Varshney, N. Identification and detection of abnormal human activities using deep learning techniques. *Eur. J. Mol. & Clin. Medicine* **7**, 408–417 (2020).

32. Ahmed, W. & Yousaf, M. H. A deep autoencoder-based approach for suspicious action recognition in surveillance videos. *Arab. J. for Sci. Eng.* **49**, 3517–3532 (2024).

33. Nayak, R., Pati, U. C. & Das, S. K. A comprehensive review on deep learning-based methods for video anomaly detection. *Image Vis. Comput.* **106**, 104078 (2021).

34. Saypadith, S. & Onoye, T. An approach to detect anomaly in video using deep generative network. *IEEE Access* **9**, 150903–150910 (2021).

35. Barash, M., McNevin, D., Fedorenko, V. & Giverts, P. Machine learning applications in forensic dna profiling: A critical review. *Forensic Sci. Int. Genet.* **69**, 102994 (2024).

36. Ankalaki, S. *et al.* Cyber attack prediction: From traditional machine learning to generative artificial intelligence. *IEEE Access* (2025).

37. Kingma, D. P. Auto-encoding variational bayes. *arXiv preprint arXiv:1312.6114* (2013).

38. Vaswani, A. Attention is all you need. *Adv. Neural Inf. Process. Syst.* (2017).

39. Kiranyaz, S. *et al.* 1d convolutional neural networks and applications: A survey. *Mech. systems signal processing* **151**, 107398 (2021).

40. Wold, S., Esbensen, K. & Geladi, P. Principal component analysis. chimometrics and intelligent laboratory systems. In *IEEE Conference on Emerging Technologies & Factory Automation Efta*, 704–706 (1987).

41. Breiman, L. Random forests. *Mach. learning* **45**, 5–32 (2001).

42. Hart, P. The condensed nearest neighbor rule (corresp.). *IEEE transactions on information theory* **14**, 515–516 (1968).

43. Devroye, L., Györfi, L. & Lugosi, G. *A probabilistic theory of pattern recognition*, vol. 31 (Springer Science & Business Media, 2013).

44. Breiman, L., Friedman, J., Olshen, R. A. & Stone, C. J. *Classification and regression trees* (Routledge, 2017).

45. Friedman, J. H. Greedy function approximation: a gradient boosting machine. *Annals statistics* 1189–1232 (2001).