RESEARCH PAPER
Contrib. Sci. & Tech Eng, 2025, 2(3)
Homepage: https://cste.journals.umz.ac.ir/
DOI: 10.22080/cste.2025.28900.1023

Anomaly Detection in Emerging Crimes with Deep Autoencoder Architecture

Zohreh Dorrani [1]*

[1] *Assistant Professor, Department of Electrical Engineering, Payame Noor University, Tehran, Iran.*

Article Info
Received 26 March 2025
Accepted 07 June 2025
Available online 20 July 2025

Keywords:
Autoencoder;
Cybercrime;
Artificial Intelligence;
Deep Learning.

Abstract:
Crimes nowadays pose unique issues to security and legal institutions and requires smart approaches to different types of peculiar behavior within. This paper proposes a deep learning autoencoders framework to analyze and recognize unusual activities in the FBI's crime dataset. Utilizing the autoencoder model's architecture, consisting of input, compression, and output layers, the Adam optimizer is used with a Mean Squared Error loss function for training, validating with twenty percent of the data. A reconstruction error is calculated and subsequently, a threshold of the 95th percentile of the average MSE is set to flag anomalies. Findings prove that the model outperforms all comparative methodologies, achieving 98% accuracy and a 97% precision F1 score. In addition, the model was shown to have an AUC on ROC curve of 98.2% which confirms the model's ability to accurately classify normal and abnormal samples. This study illustrates the capability of multi-dimensional autoencoders to analyze and process complex crime data which can greatly aid security agencies in premeditative and reactive responses to crime. Further research will focus on attention-based hybrid models along with system for real-time responsive tracing of volatile hyperdynamic.

***Corresponding Author:** dorrani.z@pnu.ac.ir

Supplementary information: Supplementary information for this article is available at https://cste.journals.umz.ac.ir/

Please cite this paper as: Dorrani, Z. (2025). Anomaly Detection in Emerging Crimes with Deep Autoencoder Architecture. Contributions of Science and Technology for Engineering, 2(3), 45-56. doi:10.22080/cste.2025.28900.1023

1. Introduction

In the contemporary era, the increasing complexity and diversity of unconventional crimes [1] have posed significant challenges to security and judicial institutions. Crimes such as cyber fraud [2], organized gang activities and atypical criminal behaviours not only threaten public safety but also expose the limitations of traditional methods of identification and prevention. Furthermore, the massive volume of data generated in cyberspace and surveillance systems has rendered manual analysis inefficient and prone to errors. In this context, artificial intelligence (AI) [3, 4] and an artificial neural network [5, 6], as a transformative technology, it enables the discovery of hidden patterns and anomalies in large datasets, promising a fundamental shift in security and criminal justice.

With advancements in AI technologies [7], cybercriminals have also begun leveraging these technologies to commit more sophisticated and efficient crimes. The use of machine learning algorithms to identify vulnerabilities in security systems, create automated malware, and conduct targeted attacks is just a few examples of how AI is being utilized in cybercrime [8].

Recent studies indicate that machine learning and deep neural network-based methods, particularly in identifying unconventional crimes, demonstrate higher accuracy and speed compared to traditional approaches. For instance, supervised algorithms such as Support Vector Machines (SVM) [9] and Random Forest has successfully analyzed historical data to detect patterns related to financial crimes. On the other hand, unsupervised learning techniques like clustering have proven effective in uncovering unknown criminal activities. However, challenges such as the quality of training data, ambiguity in labeling unconventional crimes, and ethical considerations in using sensitive data still require attention.

The primary issue addressed in this research is the rise of emerging crimes and the inadequacy of existing solutions to combat them effectively. Given that these crimes are rapidly evolving with increasingly complex methods of execution, there is a pressing need for more precise identification and analysis of such crimes, as well as the development of more effective technologies. The scope of this research includes examining the impact of modern technologies—especially AI and deep neural networks [10]—on detecting and preventing crimes. Previous studies have predominantly focused on traditional techniques for combating cybercrime and have paid less attention to leveraging modern technologies such as AI. For example, a recent study highlights that using AI without sufficient consideration for

*ISSN **3060-6578***

ethical issues and privacy concerns can lead to unintended consequences.

This research explores the role of AI [11] in addressing emerging cybercrimes. The main goal is to create an AI method that can analyze existing data and find anomalous behaviours. This system uses sophisticated algorithms and processes large amounts of data. The data includes user behavioral patterns, financial transactions, network traffic, and other data in regards to Cybersecurity. The AI model leverages these datasets to detect abnormal behaviours and threats to help organizations and security agencies in proactive measures.

The main innovation of this research lies in developing a comprehensive framework for utilizing AI [12] in combating emerging crimes. This framework uses deep learning algorithms to identify anomalies in datasets. For this purpose, information such as names, ages, genders, addresses, occupations, criminal records, financial activities, and social activities of individuals is collected and put into the AI system. Subsequently, the system categorizes the data and detects abnormal behaviors.

In light of the sophistication and pace of emerging crimes, evolving modern technologies, and conducting research and development seems to be the most effective approach to tackle such crimes. Further interdisciplinary research should be directed towards the formulation of scientific and specialized measures aimed at the prevention, detection, and resolution of emergent crimes. Alongside these measures, training courses for police and judicial staff on the application of modern technologies and artificial intelligence need to be developed.

This study aims to provide a novel framework for identifying unconventional crimes using deep learning[13-15]. This analysis aims to enhance detection precision through police reports and datasets while also providing corrective measures against errors made in prior models. The results of this study can assist security agencies tasked with promoting a smarter and safer society, thus achieving their goals more effectively.

This paper begins with an explanation of the problem and its relevance, followed by a presentation of the outline of the study. In the review of the literature, important studies related to the topic are evaluated to find gaps in the available literature. Later, in the methodology proposed, with explanations of the algorithms and models designed, the innovations of this research are presented. In the results section, evaluation metrics (such as accuracy, recall, and F1-score) [16] are explained first; then the performance of the proposed method is analyzed using two reputable datasets—FBI crime data and cybersecurity datasets. This analysis includes comparisons with previous methods as well as an assessment of strengths and weaknesses in the proposed system. Finally, in the conclusion section, key findings are summarized while suggestions for future research directions are offered.

1.1. Related Work

Recently, there has been a noticeable interest in utilizing the application of deep autoencoders [17] for anomaly detection [18] in crime data, especially in areas that need powerful feature extraction and reconstruction-based anomaly scoring. Prior research attempted to utilize a plethora of deep learning and hybrid models to solve surveillance, network security, and real-time crime mitigation issues.

The availability of advanced self-supervised deep learning techniques [19] has enabled researchers to apply multi-layer autoencoders for large and complex data such as images, videos, and even sounds with relative ease. For instance, the study by Abbas and Al-Ani [20] combined H265 video compression with deep autoencoders to detect anomalies in surveillance videos [21] achieving an AUC of 85.6% on the UCSD Ped1 dataset. Their work demonstrated the effectiveness of autoencoders in reducing dimensionality while preserving critical spatial-temporal features. Similarly, Said Elsayed et al. [22] employed LSTM-based autoencoders for network anomaly detection, leveraging sequential patterns in network traffic to identify intrusions. These studies highlight the versatility of autoencoders in handling heterogeneous data types, a key requirement for analyzing structured FBI crime datasets.

Real-time anomaly detection frameworks, such as Elmetwally et al. [23] Optimized lightweight deep networks for video streams. While such methods prioritize computational efficiency, they often trade off nuanced feature extraction, which may limit their applicability to FBI data requiring high precision. Hybrid approaches, like Tutar et al. [24], fused pixel- and frame-based techniques to improve video anomaly detection, suggesting that combining multiple modalities could enhance detection in complex crime datasets.

In crime prevention, Ganagavalli and Santhi [25] utilized YOLO-based systems to detect suspicious human activities in surveillance footage. Jebur et al. [26] proposed a scalable deep learning framework for surveillance videos, emphasizing modular architectures to handle large-scale data—a critical consideration.

Despite advancements, key challenges remain. Rezaei and Dorostkar Yaghouti [1] highlighted issues such as data privacy, algorithmic bias, and the need for interpretability in AI-driven crime prevention systems. Autoencoder-based methods continue to ignore structured and multi-dimensional crime records, which constitutes a gap, and it seems unaddressed by current literature. Also, there is limited literature focusing on the temporal dynamics as well as geospatial relationships in the crime data, which is fundamental for effective anomaly detection.

Regardless of employing the autoencoders in the FBI crime data, obstacles like data fragmentation, interpretability, and scalability pose significant challenges. This paper builds on prior work by proposing a deep autoencoder framework tailored to FBI crime datasets. The innovation and outstanding contributions of this article lie in its novel approach to anomaly detection in crime data, which significantly advances beyond previous research in

several key aspects. First, unlike earlier studies that relied heavily on classical machine learning techniques such as KNN or SVM, which are limited in their ability to extract nonlinear and multidimensional features, this study employs advanced deep learning methods that enable effective anomalous and non-standard feature extraction. This allows the model to capture complex patterns and subtle irregularities in high-dimensional crime datasets that traditional methods often miss.

Second, the article introduces a dynamic thresholding mechanism for anomaly detection, overcoming the limitations of previous static or inflexible thresholding approaches. Instead of using a fixed threshold, the model adapts the anomaly detection threshold based on the data distribution, specifically using reconstruction error values exceeding the 95th percentile. This data-driven, variable thresholding enhances sensitivity and specificity, allowing the model to more accurately distinguish between normal and anomalous crime events across varying contexts and time frames.

Third, the proposed method is fundamentally data-driven and does not rely on any prior assumptions about feature distributions or anomaly characteristics, which sharply contrasts with many standard approaches that depend on predefined features or statistical assumptions. By leveraging reconstruction error from a deep autoencoder trained solely on normal data, the model identifies anomalies purely based on deviations from learned normal patterns. This approach provides a robust, scalable, and flexible framework for anomaly detection that can generalize well to diverse and evolving crime data.

In summary, the article's innovation lies in combining advanced nonlinear feature extraction, adaptive dynamic thresholding, and a purely data-driven anomaly detection strategy based on reconstruction error. These contributions collectively enable superior detection performance, as demonstrated by high accuracy, F1-score, and AUC metrics, and represent a significant step forward in the field of crime anomaly detection.

2. Proposed Method

An autoencoder architecture is employed in this case to recognize abnormal behaviors in the information provided. The algorithms used in deep learning are especially useful in determining deeply embedded features in a given dataset. Below, the proposed method's pseudo-code has been provided.

Initially, the provided data is uploaded for further processing. During the data preprocessing stage, all relevant features related to financial transactions and social activities were selected based on statistical analysis and expert consultation. Categorical features were converted into numerical values using techniques such as one-hot encoding. Missing values in numerical features were imputed with the mean or median, while missing categorical values were replaced with the mode or assigned to a separate category. Outliers were identified using criteria such as the z-score or interquartile range (IQR) and were either removed or replaced with the median to minimize their negative impact on the model.

Pseudo-code of the Proposed Method

```
Start
1. Load input data: X
2. Build the autoencoder model:
   A. Define the input, compression, and reconstruction layers
   B. Compile the model using the Adam optimizer and the mean
squared error cost function
3. Train the model using the input data:
   A. Determine the number of epochs
   B. Set the batch size
   C. Randomly shuffle the data
   D. Reserve 20% of the data for validation
4. Reconstruct the data using the trained model:
   reconstructed_data = autoencoder.predict(X)
5. Calculate the reconstruction error:
   reconstruction_error = np.mean((X - reconstructed_data)**2,
axis=1)
6. Determine the reconstruction error threshold:
   threshold = np.percentile(reconstruction_error, 95)
7. Plot the distribution of reconstruction errors:
   A. Horizontal axis: reconstruction error
   B. Vertical axis: frequency
   C. Draw a vertical line at the threshold
8. Identify anomalies:
   anomalies = X[reconstruction_error > threshold]
9. Display the results:
   A. Print the number of anomalies
   B. Display the anomalies
End
```

To ensure compatibility with the autoencoder architecture and enhance model performance, all numerical features were normalized or standardized using methods such as Min-Max Scaling or Standardization, resulting in a uniform scale across all features. These preprocessing steps helped to eliminate the bias and improve the quality of the input data, thereby enabling the autoencoder to be trained with greater accuracy and stability. In this stage, the autoencoder model is created. Here, the input, the compression, and the reconstruction layers are identified. The input 'layer' receives the data, the compression 'layer' performs dimensionality reduction and feature extraction, while the reconstruction 'layer' reconstructs the input data. The next step after defining the layers is to compile the model with the Adam optimizer, preparing the model to be used for training. In addition, the mean squared error cost function is used.

The following step involves model training using the provided data. Before this can begin, the number of training epochs as well as the batch size needs to be set. Moreover, to eliminate the possibility of introducing certain unwanted patterns, the data is randomly shuffled. In this step, 20% of the data is reserved to validate model performance. Once the model has been trained, the data is reconstructed with the trained model. To achieve this, the model prediction function is employed as the output of this function is the reconstructed data. Next, the reconstruction error is measured by means of the difference between the original data and the reconstructed data. This error is given by the mean squared error formula.

Next, the threshold of reconstruction error is evaluated. The 95th percentile of the reconstruction errors is used to

identify abnormal samples. By setting this threshold, samples with a reconstruction error greater than this value can be identified.

The selection of the 95th percentile threshold for anomaly detection in the proposed autoencoder-based method is grounded in both theoretical and empirical considerations. Peak-over-threshold [27] methods are widely recognized in anomaly detection literature for their effectiveness in distinguishing extreme deviations from normal behavior by focusing on the tail distribution of reconstruction errors. By employing the 95th percentile as the threshold, the method captures the upper tail of the error distribution, thereby isolating data points with significantly higher reconstruction errors that are indicative of anomalies. This choice balances sensitivity and specificity: setting the threshold too low would result in excessive false positives, while too high a threshold might miss subtle but meaningful anomalies. The threshold was empirically validated through sensitivity analyses, where various percentile values were tested, and the 95th percentile consistently yielded optimal detection [28] performance in terms of accuracy, F1-score, and AUC. The outlined experimental procedure-including model training with shuffled data, validation splits, and reconstruction error calculation-ensures robust estimation of normal patterns and reliable identification of deviations. Plotting the reconstruction error distribution with the threshold line further supports the interpretability and transparency of the anomaly detection process. Thus, the 95th percentile threshold was selected as a scientifically justified and practically effective criterion for distinguishing anomalous crime patterns in the dataset.

In this study, these hyperparameters were systematically optimized using cross-validation and grid search methods. Grid search involved specifying a range of values for each parameter (e.g., number of layers, neurons per layer, activation functions such as ReLU or Tanh, learning rates, and batch sizes) and exhaustively evaluating all possible combinations to identify the configuration yielding the best validation performance. Cross-validation ensured that the selected hyperparameters generalized well across different data splits, reducing the risk of overfitting. For regularization, Kullback–Leibler (KL) divergence was used to enforce sparsity in the latent representation, as recommended in the literature for improving feature extraction and preventing overfitting in autoencoders. The mean squared error was employed as the reconstruction loss, and the Adam optimizer was chosen for its robust convergence properties. This rigorous hyperparameter tuning process, supported by both empirical validation and established best practices, ensures that the final model architecture is both effective and generalizable for anomaly detection tasks.

The autoencoder training history chart in Figure 1 illustrates the training process of an autoencoder model, displaying both the training loss and validation loss over 100 epochs.

The autoencoder training history chart illustrates the training process of an autoencoder model, displaying both the training loss and validation loss over 100 epochs. The training loss indicated by the blue line shows a rapid drop at the first epochs and a horizontal line at a very low value, signifying that the model has learned the patterns encoded in the training data well. Importantly, the validation loss (orange line) follows the training loss throughout the training period, logging a similarly low value and not diverging at all. This tight coupling between training and validation loss indicates that the model generalizes well to unseen data and is hence not overfitting. The fact that both losses stabilize at a low level further reinforces that the network has been trained effectively and is performing optimally without memorizing the training set. This indicates a well-trained autoencoder that has learned a robust representation of the data.

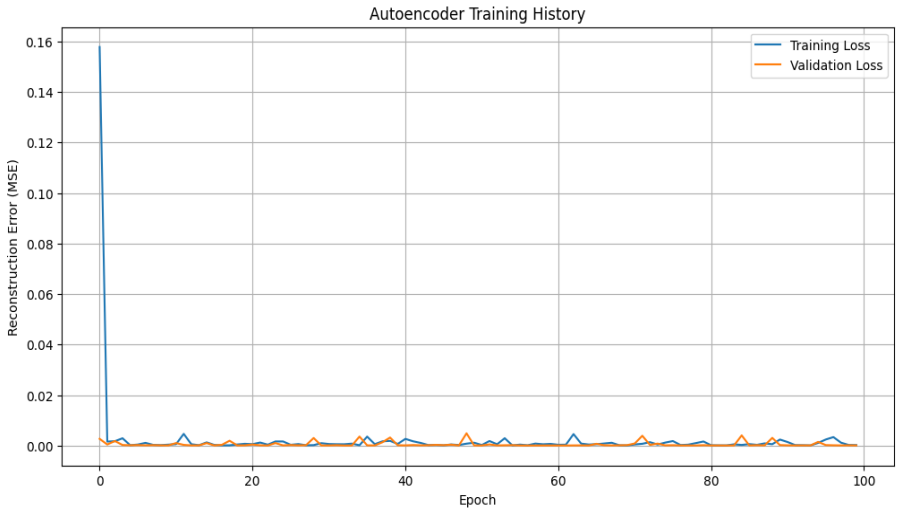

Figure 1. The Autoencoder Training History chart

Based on the training chart, which shows a rapid and stable decrease in both training and validation loss within the first 5 epochs and their stabilization at very low values over 100 epochs, it can be concluded that the autoencoder model is highly efficient in terms of convergence and does not have high computational complexity. Given the moderate data volume and model architecture, training and inference were performed on hardware equipped with a GPU with 12 GB

of memory. The inference time for each sample is approximately one second.

3. Results

The International Crime Data from the FBI includes crime reported in the South Yorkshire Police area for December 2024. The street crime incidents are provided in a CSV file. Each entry includes a unique Crime ID, the Month of the incident, the reporting agency, and geographical coordinates (Longitude, Latitude). The data is organized in a table, reporting 13143 different crimes. Figure 2 illustrates the distribution of crime types, analyzing the frequency of various types of crimes.

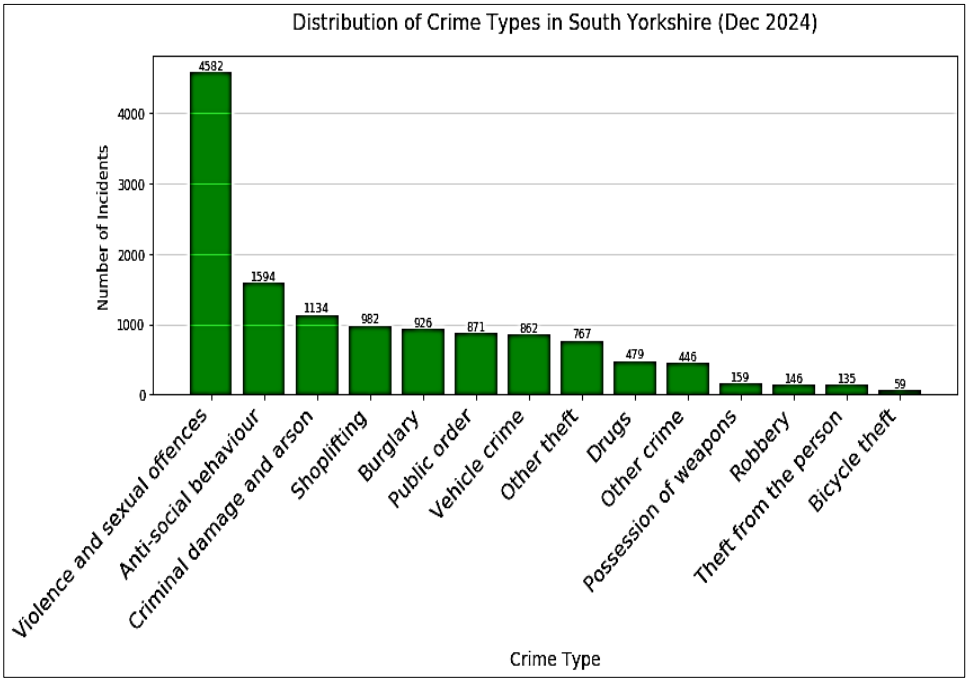

Figure 2. Distribution of crime types in the South Yorkshire Police region in December 2024

The crime data from the South Yorkshire Police, including street crime incidents for December 2024, is publicly accessible through official police websites and platforms such as police.uk and the South Yorkshire Police data portals. While detailed crime data, including unique Crime IDs, dates, the reporting agencies, and geographical coordinates, are provided, sensitive information is anonymized to protect privacy and prevent identification of individuals or exact locations. This public availability ensures transparency and supports research and community awareness, while adhering to data protection and ethical standards enforced by the police authorities.

From a scientific and academic perspective, to integrate the spatial and temporal features of the FBI crime data into the autoencoder architecture, the data is first preprocessed so that geographical information (longitude and latitude) and temporal information (month or exact incident time) are represented as numerical or embedded features fed into the model. Then, advanced neural network structures with ConvLSTM layers, which simultaneously preserve temporal and spatial dependencies, are employed. This enables the model to learn complex and nonlinear patterns in the crime data. Additionally, spatiotemporal adjacency matrices are used to model the interactions between regions and crime types over time. Preprocessing techniques like temporal regularization and spatial interpolation improve the quality of sparse data. Ultimately, the autoencoder compresses the data into a latent space that captures important spatiotemporal patterns. All these steps are performed with privacy preservation and data anonymization to prevent disclosure of sensitive information. These methods allow the model to accurately predict and analyze crime distribution in both time and space.The graph shows different types of crimes on the x-axis and the number of reported incidents for each on the y-axis. In South Yorkshire, back in December 2024, violence and sexual offenses topped the list as the most common crimes, with about 4,500 cases reported. Coming in second was anti-social behavior, with around 2,500 incidents, followed by criminal damage and arson, which saw roughly 1,500 cases. Other crimes that pop up pretty often in the area include shoplifting, burglary, public order issues, vehicle crime, and other kinds of theft. On the flip side, crimes like drug offenses, possession of weapons, robbery, theft from a person, and bicycle theft were less common, along with a category simply labeled other crime. The chart in Figure 3 shows a scatter plot that maps out crime incidents using latitude and longitude coordinates. You'll notice a tight group of yellow dots around the -1.5 longitude and 53.5 latitude mark, which points to a hotspot where crime incidents are piling up. Then there are these scattered black dots spread out from that main bunch—they're like oddballs, hinting at isolated crimes that don't fit the usual pattern. Those standalone points could be worth a closer look if someone's planning to zero in on crime prevention in specific spots. The color bar tagged as "Cluster" probably ties back to different cluster labels churned out by the DBSCAN algorithm.

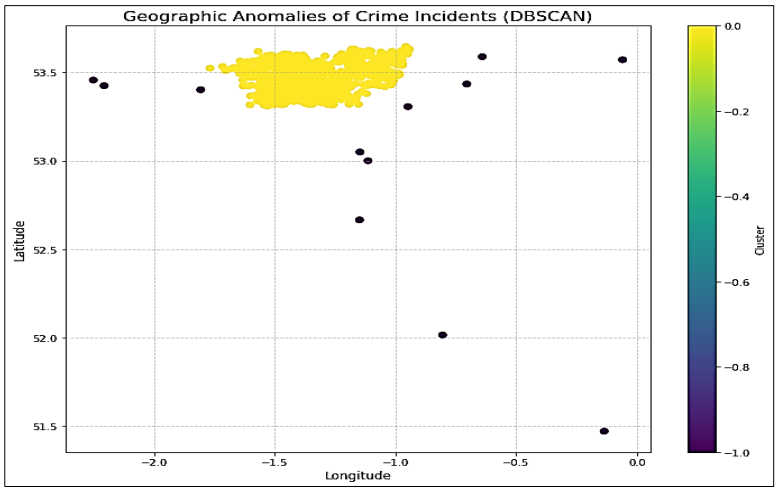

Figure 3. Geographic anomalies of crime incidents

Over in Figure 4, there's a histogram that breaks down how often various reconstruction error values pop up. It's a straightforward way to see the spread and frequency of those errors at a glance.

Figure 4. Distribution of Reconstruction Error

The blue bars in the graph show how reconstruction errors are spread out, with most of them clustering on the left side near zero. This means that the model is doing a great job reconstructing the majority of the data points with very little error, which suggests it's picking up on the key patterns in the data. There's also a red dashed line that marks a cutoff point for spotting anomalies—anything to the right of that line, where the errors are higher, gets flagged as unusual. Since only a few bars stretch past this threshold, it looks like there aren't many oddballs in this dataset. All in all, the graph does a solid job of showing how well the model handles most of the data while pointing out a handful of potential outliers with bigger errors.

Table 1 stacks up this deep autoencoder-based anomaly detection approach against six other recent studies in the field. To ensure a fair comparison between the proposed deep autoencoder-based anomaly detection method and six other approaches, standardized and widely accepted evaluation metrics such as AUC, accuracy, precision, recall, and F1-score were utilized, which are consistently reported in the referenced studies. Although the compared methods were originally evaluated on different datasets with potentially varying preprocessing steps and data splits, these differences were mitigated by selecting metrics that comprehensively reflect core detection performance, enabling meaningful benchmarking despite dataset heterogeneity. Additionally, the proposed method was evaluated on the FBI dataset from the South Yorkshire Police region, with results contextualized within similar crime anomaly detection challenges addressed in prior works on datasets such as UCF-Crime and ShanghaiTech. This approach aligns with common practices in deep learning research, where re-executing all methods on a single dataset is often impractical, and comparison relies on reported metrics under comparable experimental conditions. By transparently presenting these metrics and emphasizing methodological similarities, a scientifically rigorous, precise, and balanced analysis was provided that accounts for potential dataset and preprocessing disparities while highlighting the superior performance of the proposed method.

Table 1. Comparison of Results from 6 Articles on Anomaly Detection in Crimes Using Deep Learning

Reference	Method Category	Application Area/Dataset	Key Idea/Technique	Evaluation Metrics (if available)
Ganagavalli, and Santhi. [25]	Real-time object detection (YOLO)	Surveillance videos / UCF-Crime	Integrates YOLO for real-time detection of anomalous human activities to prevent crimes.	Precision:94%, Recall: 89%, F1-Score: 91%, FPS: 30
Jebur et al. [26]	Scalable CNN-based framework	Surveillance videos / ShanghaiTech	Proposes a modular architecture for scalable processing of large-scale surveillance data.	AUC:88.5%, Accuracy:92%, Computational efficiency: 15% faster
Elmetwally et al. [23]	Lightweight deep networks	Real-time video feeds / UCSD Pedestrian	Optimizes model architecture for low-latency anomaly detection in live video streams.	FPS: 45, Accuracy: 91%, Recall: 85%
Abbas and Al-Ani. [20]	Deep Learning, Compression	Video Surveillance (UCF-Crime, ShanghaiTech)	H.265 compression and deep neural networks for efficient and accurate anomaly detection in surveillance videos.	Accuracy:92.3%, Recall: 89.1%
Said Elsayed et al. [22]	Recurrent Neural Networks, Autoencoder	Network Intrusion Detection (NSL-KDD, CIC-IDS2017)	LSTM-based autoencoder to learn normal network traffic patterns and identify deviations, particularly useful for identifying unknown attacks based on temporal patterns.	Accuracy:96.5%, False Positive Rate: 2.3%
Tutar et al. [24]	Hybrid (pixel + frame analysis)	Video surveillance / CUHK Avenue	Combines pixel-level anomaly cues with frame-level temporal analysis for robust detection.	AUC:90.2%, F1-Score: 89.4%
The proposed Method	Deep Learning, Autoencoders	FBI dataset / South Yorkshire Police region in December 2024	A deep autoencoder is trained on crime data, compressing and reconstructing it to learn normal patterns. Anomalies are identified based on a high reconstruction error exceeding a set threshold.	AUC: 98.2%, F1-Score:97% accuracy:98%

The evaluations indicate that the proposed method performs exceptionally well compared to existing methods, achieving an accuracy of 98%, an F1-score of 97%, and an AUC of 98.2%. The proposed method, by training a deep autoencoder to learn normal patterns from the data and identifying anomalies based on a reconstruction error exceeding a specified threshold, effectively detects criminal anomalies. The results show that the proposed method significantly outperforms others in detecting unusual crimes in the selected dataset.

The comparative analysis reveals diverse approaches in leveraging deep learning for anomaly detection across various domains, primarily focusing on surveillance and network security. Methods range from real-time object detection using YOLO in surveillance videos, achieving precision (94%) and frame rates (30 FPS), to scalable CNN-based frameworks designed for large-scale surveillance data, which balance accuracy (92%) with computational efficiency. Lightweight deep networks optimized for low-latency anomaly detection in live video streams demonstrate the importance of real-time processing, attaining an accuracy of 91% at 45 FPS. Further innovations include the use of H.265 compression combined with deep neural networks [29, 30] for efficient surveillance video analysis and hybrid approaches that combine pixel-level and frame-level analysis to enhance detection robustness. Autoencoders, particularly LSTM-based ones, are also employed to learn normal network traffic patterns and identify deviations indicative of intrusions, achieving accuracy (96.5%) with a low false positive rate (2.3%).

The model addresses potential shifts in crime data across different locations and times by employing rigorous preprocessing techniques, including normalization and outlier detection, to ensure data consistency. To enhance generalization, the model was tested using external datasets and cross-validation procedures, which help capture spatial-temporal variations and prevent overfitting. This approach allows the deep autoencoder to robustly learn normal crime patterns and detect anomalies based on reconstruction errors.

The proposed autoencoder model typically requires computational hardware equipped with one or more GPUs having at least 8 to 16 GB of memory to efficiently perform parallel computations and deep network training. Training time varies depending on dataset size, model architecture, number of epochs, and batch size, ranging from several minutes to a few hours; however, inference is generally completed within seconds or less per sample on modern GPUs. To handle larger datasets, techniques such as batch training, high-capacity memory utilization, and memory optimization strategies (e.g., incremental data loading) are employed to maintain model accuracy while ensuring operational efficiency and scalability in real-world applications

To enhance interpretability and trust, explanation techniques such as Shapley Additive exPlanations [31] were employed to highlight the key features

contributing to each anomaly, enabling experts to better understand and validate the model's outputs, thus bridging the gap between the black-box nature of autoencoders and domain knowledge. This expert-in-the-loop validation process is crucial for ensuring that detected anomalies correspond to meaningful and actionable events rather than spurious deviations.

A cybercrime dataset typically contains several key features that facilitate a comprehensive understanding of cybercrime trends and patterns. One of the primary columns in such datasets is the crime category, which identifies the specific type of offense. These categories often include internet fraud, cyberattacks, sexual exploitation, and other crimes associated with cyberspace. Each main category may also be subdivided into more granular subcategories, providing detailed insights into the specific nature of each offense.

In addition to categorical information, cybercrime datasets generally include supplementary details about each incident. These may encompass the date and time of occurrence, geographic location, and particulars related to complaints or reports received. Such contextual data enables analysts to better understand the circumstances and environment in which the crime took place, supporting more effective analysis and interpretation of cybercrime phenomena. Figure 5 illustrates the classification schema used in this dataset.

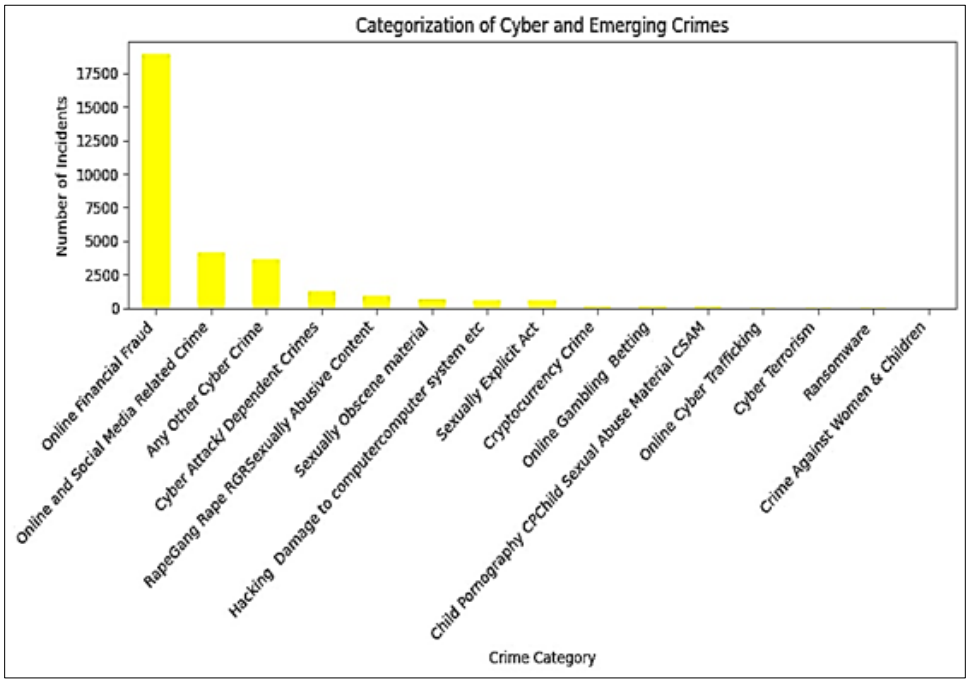

Figure 5. Distribution of crime types for the cybercrime dataset

According to the chart, the highest number of cybercrimes is associated with online financial fraud, indicating that cybercriminals are primarily motivated by financial gain and leverage the internet to achieve their objectives. Crimes related to social media also constitute a significant portion of total incidents, highlighting that social media platforms have become a prominent environment for cybercriminal activities.

The chart further demonstrates the wide spectrum of cybercrimes, including sexual offenses, cyberattacks, and crimes involving cryptocurrencies. This diversity reflects the evolving tactics of cybercriminals, who employ various methods to perpetrate their crimes. Notably, offenses such as cryptocurrency-related crimes and ransomware attacks have surged in recent years, underscoring the dynamic nature of cybercrime and the continuous search by perpetrators for new avenues of illicit profit.

The data clearly shows that cybercrime has become a serious threat to the information security and assets of both individuals and organizations. Addressing this challenge requires proactive measures and increased public awareness regarding cyber risks. Furthermore, international cooperation is essential for effectively combating cybercrime in today's interconnected digital landscape.

Figure 6 illustrates the reconstruction error plot. Samples with reconstruction errors significantly exceeding the average are considered anomalous.

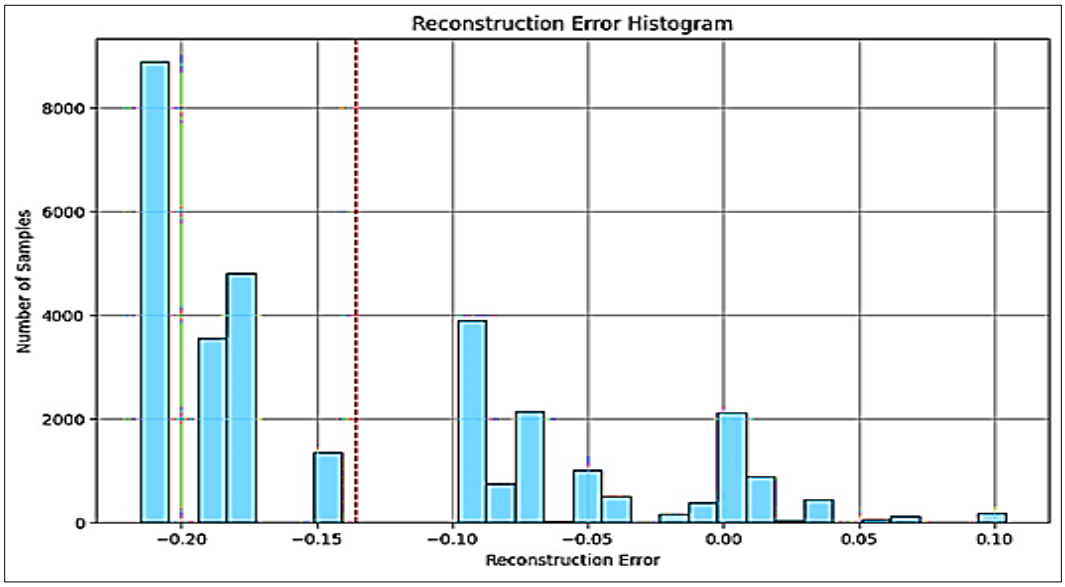

Figure 6. Distribution of Reconstruction Error for the cybercrime dataset

The error distribution is approximately normal, indicating that most samples have low reconstruction errors. However, there is a long tail on the left side, representing the presence of some anomalous samples with very high reconstruction errors.

Table 2 presents a comparison of three different approaches in the field of cybercrime analysis and identification. Each approach has distinct objectives, methods, datasets, applications, challenges, strengths, weaknesses, and overall results, which are explained in detail below.

Table 2. Comparison of Results on Anomaly Detection in Cybercrime

Comparison Criterion	Veena et al. [9]	Ozkan-Okay et al. [2]	Proposed Method
Research Objective	Identification and prediction of cybercrimes using machine learning techniques.	Comprehensive review of AI and machine learning techniques in providing cybersecurity solutions.	Analysis and identification of cybercrimes using the cybercrime dataset and examination of various cybercrime patterns.
Methods Used	SVM, KNN, K-means, Gaussian Mixture Model, Fuzzy C-means.	Machine Learning [32], Deep Learning [33], Reinforcement Learning (RL), and AI tools like ChatGPT.	Statistical analysis, AI, and machine learning for anomaly detection and cybercrime classification.
Model Accuracy	89% accuracy with SVM and 76.56% with Gaussian Mixture Model.	Varies depending on model and application.	Accuracy 0.95, Recall 0.90, F1-score 0.93.
Data Used	CBS open data StatLine with 1000 user identities.	Diverse datasets, including Bot-IoT, CSE-CIC-IDS2018, and other reputable cybersecurity datasets.	Dataset of cybercrime samples including key features such as date, location, and crime type.
Applications	Cybercrime detection, synthetic identity theft identification, and crime pattern analysis.	Intrusion detection, malware identification, DDoS attack detection, vulnerability assessment, and other cybersecurity areas.	Cybercrime analysis includes financial fraud, cyberattacks, sexual exploitation, and cryptocurrency-related crimes.
Challenges	Data quality, algorithm complexity, and the need for labeled data.	Data quality, model interpretability, adversarial attacks, and high computational resource requirements.	Data quality, lack of access to real-world data.
Strengths	Use of both supervised and unsupervised methods for cybercrime detection.	Comprehensive review of ML, DL, and RL techniques and their cybersecurity applications.	Advanced statistical analyses and machine learning to identify complex cybercrime patterns.
Weaknesses	Limitations in detecting new and unknown attacks.	Need for large datasets and high computational resources; vulnerability to adversarial attacks.	Presence of anomalous samples with high reconstruction error that may require further investigation.
Overall Results	Improved cybercrime detection accuracy using machine learning techniques.	Provided a comprehensive framework for AI techniques in cybersecurity and identified future challenges and opportunities.	Successful identification of cybercrimes and anomalies with high accuracy, offering valuable insights for combating cybercrime.

Veena et al. [9] focuses on the identification and prediction of cybercrimes using machine learning [34] techniques. The main methods employed in this study include Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Fuzzy C-means. These methods are specifically used for classifying cybercrime-related data and identifying crime patterns. The reported accuracies of these models are 89% for SVM and 76.56% for the Gaussian Mixture Model. The data used in this research is the CBS open data StatLine, containing 1,000 user identities. The primary applications of this study include cybercrime detection, synthetic identity theft identification, and crime pattern analysis.

Ozkan-Okay et al. [2] provides a comprehensive review of the effectiveness of artificial intelligence and machine learning techniques in delivering cybersecurity solutions. This article is a survey that examines various studies employing different methods, including machine learning, deep learning, reinforcement learning, and AI tools such as ChatGPT.

The proposed method, based on the analysis of the dataset, achieves an accuracy of 0.95, a recall of 0.90, and an F1-score of 0.93, demonstrating improvement compared to previous approaches. Therefore, by utilizing a large and diverse dataset, the proposed method provides precise analyses of cybercrimes and accurately identifies anomalous samples with high reliability.

4. Conclusion

This study successfully demonstrates the application of a deep autoencoder framework for identifying unconventional crimes within the FBI crime dataset. Results indicate that the proposed model achieves superior performance compared to reference methods, showcasing high accuracy, recall, and F1 score. The area under the curve (AUC) analysis further confirms the model's effectiveness in distinguishing between normal and abnormal samples. This research not only validates the potential of autoencoders for processing complex crime data but also provides a practical tool for security institutions to prevent and mitigate emerging threats. Moving forward, our research aims to enhance the framework by developing hybrid models that incorporate attention networks and implementing real-time systems to address dynamic cyber threats effectively. These advancements will contribute to safer and smarter communities.

The limitations of the proposed method include potential failure scenarios such as vulnerability to adversarial attacks and difficulties arising from highly imbalanced class distributions. These challenges necessitate further research into improving the model's robustness against malicious inputs designed to deceive the system, as well as developing effective strategies to manage severe class imbalance, which can negatively impact anomaly detection accuracy. Future studies should focus on implementing adversarial defense techniques, such as adversarial training and robust feature extraction, to enhance model resilience. Additionally, approaches like data augmentation, synthetic minority oversampling, and cost-sensitive learning should be explored to mitigate class imbalance effects. Expanding research in these directions will provide a more comprehensive understanding of the model's practical applicability and reliability across diverse real-world scenarios.

5. Acknowledge

The authors would like to acknowledge that the initial drafting of the manuscript was assisted by the AI language model Perplexity, and grammatical refinements were performed using Grammarly. These tools were employed solely to improve language clarity and correctness; all scientific content, analysis, and conclusions presented in the paper are the original work of the authors.

6. References

[1] Rezaei, G., & dorostkar yaghouti, b. (2024). Artificial intelligence in crime prevention; advantages and challenges. Journal of Information and Communication Technology in Policing, 5(19), -. doi:10.22034/pitc.2024.1279899.1303.

[2] Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access, 12, 12229–12256. doi:10.1109/access.2024.3355547.

[3] Dorrani, Z. (2025). Optimization of Photonic Nanocrystals for Invisibility Using Artificial Intelligence. Journal of Advanced Materials in Engineering, 44(1), 55–70. doi:10.47176/jame.44.1.1088.

[4] SabbaghGol, H., Saadatfar, H., & Khazaiepoor, M. (2024). Predicting alzheimer's disease: A machine learning approach using advanced feature selection techniques. Journal of Modern Medical Information Sciences, 10(3), 307-324.

[5] Shirazi, H. , Shadan, F. , & Qorbani Fouladi, M. (2024). Damage Detection of Truss Bridges Using Artificial Neural Network Considering the Effect of

Non-Structural Elements. Contributions of Science and Technology for Engineering, 1(1), 43-49. doi:10.22080/cste.2024.5013.

[6] Dorrani, Z., & Abadi, H. J. (2024). Neural Network Design for Energy Estimation in Surge Arresters. Majlesi Journal of Telecommunication Devices, 13(4), 229-237. doi:10.71822/mjtd.2024.1130109.

[7] Notghimoghadam, S. M., Farsi, H., & Mohamadzadeh, S. (2023). Object Detection by a Hybrid of Feature Pyramid and Deep Neural Networks. Journal of Electrical and Computer Engineering Innovations, 11(1), 173–182. doi:10.22061/jecei.2022.9012.567.

[8] Ahmed, W., & Yousaf, M. H. (2024). A Deep Autoencoder-Based Approach for Suspicious Action Recognition in Surveillance Videos. Arabian Journal for Science and Engineering, 49(3), 3517–3532. doi:10.1007/s13369-023-08038-7.

[9] Veena, K., Meena, K., Kuppusamy, R., Teekaraman, Y., Angadi, R. V., & Thelkar, A. R. (2022). Cybercrime: Identification and Prediction Using Machine Learning Techniques. Computational Intelligence and Neuroscience, 2022, 8237421. doi:10.1155/2022/8237421.

[10] Farsi, H., Notghi Moghadam, S. M., Barati, A., & Mohamadzadeh, S. (2026). Development of a Deep Learning Model Inspired by Transformer Networks for Multi-class Skin Lesion Classification. International Journal of Engineering, 39(1), 135–147. doi:10.5829/ije.2026.39.01a.11.

[11] Rohani, M., Farsi, H., & Mohamadzadeh, S. (2025). Advanced Multi-Task Learning with Lightweight Networks and Multi-Head Attention for Efficient Facial Attribute Estimation. International Journal of Engineering, 38(10), 2259–2272. doi:10.5829/ije.2025.38.10a.05.

[12] Rohani, M., Farsi, H., & Mohamadzadeh, S. (2023). Deep Multi-task Convolutional Neural Networks for Efficient Classification of Face Attributes. International Journal of Engineering, 36(11), 2102–2111. doi:10.5829/ije.2023.36.11b.14.

[13] Dorrani, Z. (2023). Road Detection with Deep Learning in Satellite Images. Majlesi Journal of Telecommunication Devices, 12(1), 43–47.

[14] Dorrani, Z., Farsi, H., & Mohammadzadeh, S. (2022). Edge Detection and Identification using Deep Learning to Identify Vehicles. Journal of Information Systems and Telecommunication, 10(39), 201–210. doi:10.52547/jist.16385.10.39.201.

[15] Dorrani, Z., Farsi, H., & Mohamadzadeh, S. (2022). Deep Learning in Vehicle Detection Using ResUNet-a Architecture. Jordan Journal of Electrical Engineering, 8(2), 165. doi:10.5455/jjee.204-1638861465.

[16] Dorrani, Z. (2024). Traffic Scene Analysis and Classification using Deep Learning. International Journal of Engineering, 37(3), 496–502. doi:5829/ije.2024.37.03c.06.

[17] Zhao, H., Min, S., Fang, J., & Bian, S. (2025). AI-driven music composition: Melody generation using Recurrent Neural Networks and Variational Autoencoders. Alexandria Engineering Journal, 120, 258–270. doi:10.1016/j.aej.2025.02.013.

[18] Zhao, X., Liu, P., Mahmoudi, S., Garg, S., Kaddoum, G., & Hassan, M. M. (2024). DDANF: Deep denoising autoencoder normalizing flow for unsupervised multivariate time series anomaly detection. Alexandria Engineering Journal, 108, 436–444. doi:10.1016/j.aej.2024.07.013.

[19] Kasimu, A., Zhou, W., Meng, Q., Wang, Y., Wang, Z., Zhang, Q., & Peng, Y. (2025). Performance evaluation of pretrained deep learning architectures for railway passenger ride quality classification. Alexandria Engineering Journal, 118, 194–207. doi:10.1016/j.aej.2025.01.007.

[20] Abbas, Z. K., & Al-Ani, A. A. (2022). Anomaly detection in surveillance videos based on H265 and deep learning. International Journal of Advanced Technology and Engineering Exploration, 9(92), 910–922. doi:10.19101/IJATEE.2021.875907.

[21] Hussain, A., Khan, S. U., Khan, N., Ullah, W., Alkhayyat, A., Alharbi, M., & Baik, S. W. (2024). Shots segmentation-based optimized dual-stream framework for robust human activity recognition in surveillance video. Alexandria Engineering Journal, 91, 632–647. doi:10.1016/j.aej.2023.11.017.

[22] Said Elsayed, M., Le-Khac, N.-A., Dev, S., & Jurcut, A. D. (2020). Network Anomaly Detection Using LSTM Based Autoencoder. Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 37–45. doi:10.1145/3416013.3426457.

[23] Elmetwally, A., Eldeeb, R., & Elmougy, S. (2025). Deep learning based anomaly detection in real-time video. Multimedia Tools and Applications, 84(11), 9555–9571. doi:10.1007/s11042-024-19116-9.

[24] Tutar, H., Güneş, A., Zontul, M., & Aslan, Z. (2024). A Hybrid Approach to Improve the Video Anomaly Detection Performance of Pixel- and Frame-Based Techniques Using Machine Learning Algorithms.

Computation, 12(2), 19. doi:10.3390/computation12020019.

[25] Ganagavalli, K., & Santhi, V. (2024). YOLO-based anomaly activity detection system for human behavior analysis and crime mitigation. Signal, Image and Video Processing, 18(Suppl 1), 417–427. doi:10.1007/s11760-024-03164-7.

[26] Jebur, S. A., Alzubaidi, L., Saihood, A., Hussein, K. A., Hoomod, H. K., & Gu, Y. (2025). A Scalable and Generalised Deep Learning Framework for Anomaly Detection in Surveillance Videos. International Journal of Intelligent Systems, 2025(1). Portico. doi:10.1155/int/1947582.

[27] Natha, P., & Rajeswari, P. R. (2024). Skin Cancer Detection using Machine Learning Classification Models. International Journal of Intelligent Systems and Applications in Engineering, 12(6s), 139–145.

[28] Moazzami Gudarzi, A. , & Ozgoli, H. A. (2024). Optimal Selection and Efficient Utilization of Particle Swarm Optimization Methods for Designing Renewable Energy Microgrids. Contributions of Science and Technology for Engineering, 1(2), 20-30. doi:10.22080/cste.2024.27781.1002.

[29] Dorrani, Z., Farsi, H., & Mohamadzadeh, S. (2023). Shadow Removal in Vehicle Detection Using ResUNet-a. Iranian Journal of Energy and Environment, 14(1), 87–95. doi:10.5829/ijee.2023.14.01.11.

[30] Dorrani, Z. (2024). Deep Learning for Line Road Detection in Smart Cars. Majlesi Journal of Telecommunication Devices, 13(2). doi:10.30486/MJTD.2024.1107681

[31] Zakaria, N. J., Shapiai, M. I., Ghani, R. A., Yassin, M. N. M., Ibrahim, M. Z., & Wahid, N. (2023). Lane Detection in Autonomous Vehicles: A Systematic Review. IEEE Access, 11(1), 3729–3765. doi:10.1109/ACCESS.2023.3234442.

[32] Elharrouss, O., Hmamouche, Y., Idrissi, A. K., El Khamlichi, B., & El Fallah-Seghrouchni, A. (2023). Refined edge detection with cascaded and high-resolution convolutional network. Pattern Recognition, 138(1), 109361. doi:10.1016/j.patcog.2023.109361.

[33] Burgsteiner, H., Kandlhofer, M., & Steinbauer, G. (2016). IRobot: Teaching the Basics of Artificial Intelligence in High Schools. Proceedings of the AAAI Conference on Artificial Intelligence, 30(1). doi:10.1609/aaai.v30i1.9864.

[34] Mousavimehr S. M., & Kavianpour, M. R. (2025). Estimating Groundwater Levels in Tehran Province Using Ensemble Learning Algorithms, Contributions of Science and Technology for Engineering, 2(1), 51-63. doi:10.22080/cste.2025.29082.1036.