IJARETY

# International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

IJARETY | ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106013

# A Hybrid Anomaly Detection System Using Autoencoders, Generative Adversarial Networks, and Multi-Class Classification for Intelligent Behaviour Analysis

**V.Mohana Priya[1], Dr.D.Rajinigirinath[2]**

PG Student, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, India[1]

Professor, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, India[2]

**ABSTRACT:** This paper proposes a novel anomaly detection system combining Autoencoders, Generative Adversarial Networks (GANs), and Multi-Class Classification to effectively identify and classify irregular patterns in system behaviour. The approach uses Autoencoders to reconstruct data and detect anomalies based on reconstruction errors, while GANs enhance anomaly detection by generating synthetic anomalies to improve model generalization. A multi-class classifier is employed to categorize various types of detected anomalies, including unauthorized access and unusual activity. The system also integrates advanced loss functions, oversampling techniques like SMOTE, and optimization strategies such as the Adam optimizer to ensure robust performance. Evaluation metrics, including accuracy, False Positive Rate (FPR), True Positive Rate (TPR), and F1 Score, are used to assess the effectiveness of the proposed system. This hybrid approach offers an effective solution for detecting complex anomalies across diverse datasets and use cases.

**KEYWORDS:** Anomaly detection, Autoencoder, Generative Adversarial Networks (GANs), multi-class classification, SMOTE, Optimization, Evaluation metrics

## I. INTRODUCTION

The identification of anomalies in complex systems is a critical task in fields such as cybersecurity, finance, and behaviour analysis. Unusual patterns of activity, such as unauthorized access or abnormal system behaviour, can indicate potential security threats or system malfunctions. Traditional methods of anomaly detection often struggle with high-dimensional data or fail to capture subtle anomalies due to insufficient training data. This paper proposes an advanced anomaly detection system that combines Autoencoders for unsupervised learning, Generative Adversarial Networks (GANs) for data augmentation, and Multi-Class Classification for accurate classification of various anomaly types.

The system leverages Autoencoders to detect discrepancies between normal and abnormal behaviour, while GANs generate synthetic anomalies to further enhance model robustness. A Multi-Class Classification layer is introduced to categorize detected anomalies into distinct classes, such as unauthorized logins or abnormal data access patterns. This hybrid approach addresses the limitations of traditional methods by incorporating both reconstruction-based anomaly detection and adversarial learning for improved generalization.

## II. EXISTING SYSTEM

Anomaly detection is a critical part of monitoring and securing systems in various fields such as cybersecurity, finance, and healthcare. Traditional approaches to anomaly detection include statistical methods like Gaussian Mixture Models (GMM), k-Nearest Neighbours (k-NN), and clustering techniques such as k-Means. While these methods have their merits, they often struggle with high-dimensional data, complex patterns, and evolving attack strategies. Additionally, many existing systems rely on predefined thresholds or rules to identify anomalies, which makes them ineffective against novel or unseen types of attacks.

Recent advancements in machine learning have led to the development of more sophisticated anomaly detection models. Autoencoders, Generative Adversarial Networks (GANs), and classification models have demonstrated promising results in identifying anomalies in high-dimensional data. These models can capture complex patterns in the data and generalize well, even when anomalies are subtle or previously unseen. However, existing systems often face challenges in balancing performance and accuracy, especially when dealing with imbalanced datasets or the need to classify multiple types of anomalies.

This paper presents a hybrid anomaly detection system that integrates Autoencoders, GANs, Multi-Class Classification, and SMOTE techniques to address these challenges. The proposed system aims to enhance detection accuracy, improve generalization, and classify different anomaly types effectively

## III. PROPOSED SYSTEM

The proposed hybrid anomaly detection system integrates advanced machine learning models and techniques to enhance the detection and classification of anomalies in high-dimensional data. It combines Autoencoders for reconstruction-based anomaly detection, Generative Adversarial Networks (GANs) for generating synthetic data and refining detection, and Multi-Class Classification for labelling anomalies.

To address imbalanced datasets, the system employs the SMOTE technique to oversample minority classes, ensuring effective training. Optimization algorithms such as Adam fine-tune model parameters, while combined loss functions (reconstruction and adversarial losses) ensure robust performance. The system evaluates its effectiveness using metrics like accuracy, precision, recall, and F1 score, making it suitable for detecting and classifying diverse anomaly types.
This architecture ensures a comprehensive approach to identifying and understanding anomalies, offering both precision and generalization in detection.

## IV. ARCHITECTURE DIAGRAM

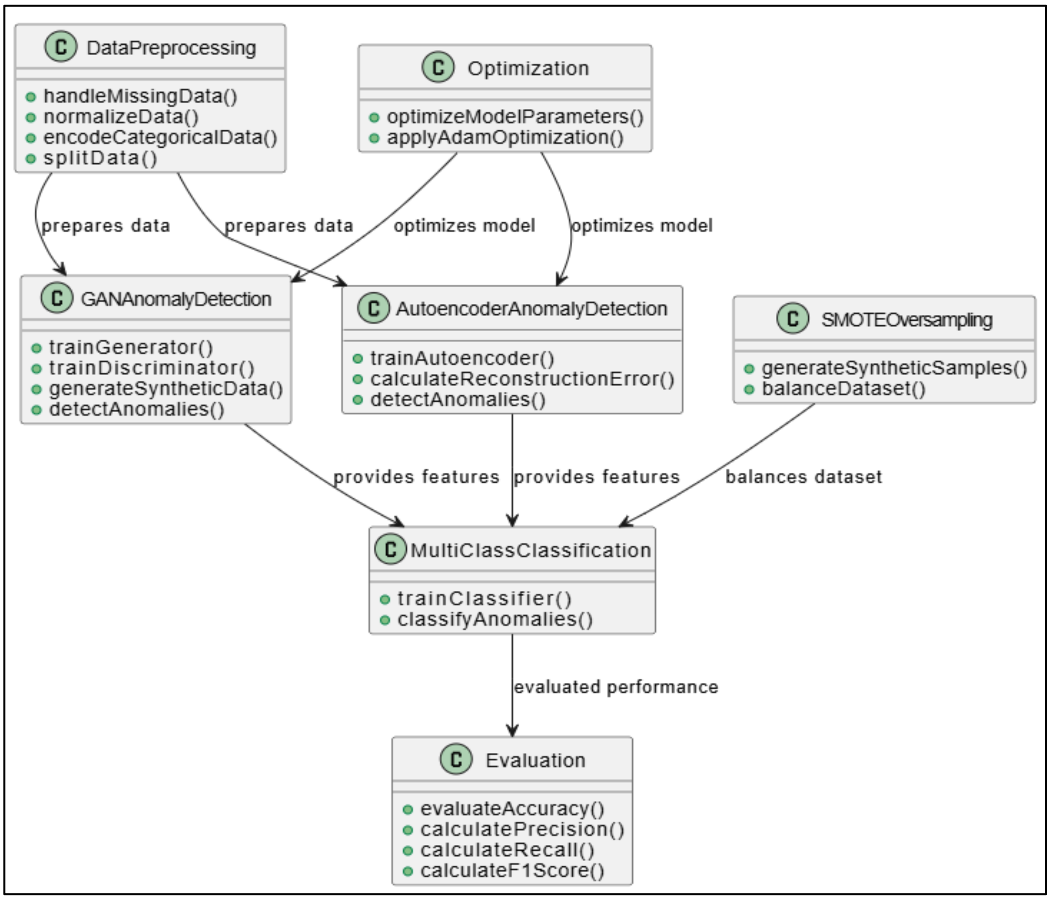

**Figure 1. Hybrid Anomaly Detection System Architecture**

## V. MODULES

**Data Preprocessing Module:**

The Data Preprocessing Module is responsible for cleaning and preparing the data before feeding it into the model. Raw data, particularly in real-world settings, is often noisy, incomplete, or unformatted. Therefore, preprocessing is a critical first step to ensure that the model receives high-quality input. This module performs several tasks:

- **Missing Value Handling**: Missing or incomplete data is handled using techniques such as mean imputation or using predictive models to estimate the missing values.
- **Normalization and Scaling**: Data is normalized or scaled to ensure that features with larger ranges do not dominate the model's learning process. Common techniques like Min-Max scaling or Z-score normalization are applied depending on the dataset.
- **Categorical Encoding**: Categorical variables are converted into numerical formats using encoding techniques such as one-hot encoding or label encoding, ensuring that all input data is in a format suitable for machine learning algorithms.
- **Data Splitting**: The module splits the data into training, validation, and test sets to evaluate the model's performance effectively. This splitting can be done randomly or through time-series cross-validation for sequential data.

Proper data preprocessing enhances the quality of input data and plays a significant role in the performance of the entire anomaly detection system.

**Autoencoder-Based Anomaly Detection Module:**

The Autoencoder-Based Anomaly Detection Module utilizes an Autoencoder to reconstruct input data and identify anomalies based on reconstruction errors. The Autoencoder is a neural network trained to compress the data (encode) and reconstruct it back to its original form (decode). Anomalies are detected by comparing the reconstruction error with a predefined threshold, where high reconstruction errors signify that the data point deviates significantly from the normal behaviour.

- **Encoder**: The encoder network compresses the input data into a latent space representation, reducing its dimensionality while retaining the most important features of the data.
- **Decoder**: The decoder reconstructs the original input data from the encoded representation. The aim is to minimize the difference between the original data and the reconstructed output.
- **Reconstruction Error**: The difference between the original input and the reconstructed data is computed using metrics such as Mean Squared Error (MSE). A large error indicates that the data point does not conform to the normal behaviour, marking it as an anomaly.
- **Threshold Selection**: A threshold for anomaly detection is determined by analysing the distribution of reconstruction errors on normal data. Points with errors beyond the threshold are flagged as anomalies.

This module is highly effective for detecting subtle anomalies in data without relying on labelled datasets.

**GAN-Based Anomaly Detection Module:**

The Generative Adversarial Network (GAN) module enhances the anomaly detection process by introducing a generator and discriminator that help the model identify anomalies more accurately. GANs consist of two neural networks that compete against each other:

- **Generator**: The generator creates synthetic data that mimics the distribution of normal data, which helps the model better understand the underlying patterns in the data. The generator's goal is to produce realistic data that the discriminator cannot distinguish from actual data.
- **Discriminator**: The discriminator's task is to distinguish between real and synthetic data. It learns to identify discrepancies between the two, making it more sensitive to anomalies.
- **Adversarial Loss**: The generator and discriminator are trained in tandem, with adversarial loss guiding the training process. The generator improves by creating more realistic synthetic data, while the discriminator becomes better at detecting anomalies.
- **Synthetic Anomalies**: During training, the generator can also produce synthetic anomalies, which are used to train the discriminator to better recognize real anomalies in the data. This makes the system more robust and able to detect even rare or novel types of anomalies.

The GAN-based module improves the ability of the system to generalize and detect subtle anomalies that might be overlooked by other methods.

**Multi-Class Classification Module:**

The Multi-Class Classification Module is used to classify the anomalies detected by the Autoencoder and GAN modules into distinct categories. This module applies supervised learning techniques, typically using a SoftMax classifier, to label the anomalies based on their nature.

- **Feature Extraction**: Features extracted from the Autoencoder and GAN outputs are passed into the classifier. These features may include reconstruction errors, adversarial losses, and other statistics derived from the data.
- **Labelling Anomalies**: The classifier categorizes anomalies into different classes, such as unauthorized access, brute-force login attempts, or unusual changes in system behaviour. This classification is essential for understanding the type of threat or irregularity and taking appropriate action.
- **Training Data**: The classifier is trained on a labelled dataset that includes both normal and anomalous data, with corresponding labels for different anomaly types.
- **Model Evaluation**: The classification model is evaluated using metrics such as accuracy, precision, recall, and F1 score to assess its performance in distinguishing between different types of anomalies.

This module enhances the interpretability of the anomaly detection system by providing insights into the specific types of anomalies that have been detected.

**Oversampling with SMOTE Module:**

Class imbalance is a common challenge in anomaly detection, where anomalies are often underrepresented in training datasets. The Oversampling with SMOTE (Synthetic Minority Oversampling Technique) module addresses this issue by generating synthetic data points for underrepresented classes.

- **Synthetic Sample Generation**: SMOTE generates synthetic samples by selecting a minority class sample and creating new samples by interpolating between it and its nearest neighbours.
- **Balancing the Dataset**: By generating synthetic anomalies, SMOTE helps balance the dataset, ensuring that the model is trained on an equal number of normal and anomalous data points.
- **Improved Model Performance**: Balancing the dataset improves the model's ability to detect rare anomalies and reduces the likelihood of the model being biased toward the majority class.
- **Training Data Augmentation**: The module can augment the training data by generating additional samples, which is particularly useful in cases where the available labelled data is scarce or imbalanced.

SMOTE is essential for ensuring that the classifier learns to detect all types of anomalies effectively, even those that are underrepresented.

**Optimization Module:**

The Optimization Module ensures that the model parameters are tuned to achieve optimal performance. This module applies optimization algorithms such as Adam (Adaptive Moment Estimation) or Stochastic Gradient Descent (SGD) to minimize the combined loss function of the Autoencoder and GAN.

- **Gradient Descent**: Optimization algorithms adjust the weights of the neural network based on the gradient of the loss function with respect to the model parameters. Adam, for example, adapts the learning rate for each parameter, improving convergence speed and stability.
- **Learning Rate Adjustment**: The optimizer adjusts the learning rate dynamically, ensuring that the model can converge efficiently without overshooting the optimal solution.
- **Loss Function Minimization**: The optimization process aims to minimize both reconstruction loss (from the Autoencoder) and adversarial loss (from the GAN), resulting in better anomaly detection performance.
- **Hyperparameter Tuning**: The module also supports hyperparameter tuning, allowing for adjustments in the learning rate, batch size, and other parameters to improve the model's performance.

Efficient optimization is crucial for training complex models like Autoencoders and GANs, ensuring that the system performs well in real-world applications.

**Evaluation Module:**

The Evaluation Module assesses the performance of the anomaly detection system by applying several key metrics. The evaluation process provides insights into how well the model detects and classifies anomalies.

- **Accuracy**: The overall percentage of correctly identified instances (both normal and anomalous).
- **True Positive Rate (TPR)**: The proportion of actual anomalies correctly identified by the system.
- **False Positive Rate (FPR)**: The proportion of normal behaviour incorrectly flagged as anomalies.
- **Precision, Recall, and F1 Score**: Precision measures the proportion of correctly identified anomalies out of all flagged anomalies, while recall measures the proportion of correctly identified anomalies out of all actual

anomalies. The F1 score is the harmonic mean of precision and recall, providing a balanced measure of performance.

- **ROC Curve**: The Receiver Operating Characteristic curve is used to evaluate the trade-off between true positive and false positive rates across different threshold values.

The Evaluation Module plays a crucial role in validating the system's accuracy and ensuring its reliability for deployment in real-world scenarios.

## VI. CONCLUSION AND FUTURE WORK

This paper presents a robust hybrid approach to anomaly detection using Autoencoders, Generative Adversarial Networks (GANs), and Multi-Class Classification. By combining these techniques, the system is capable of detecting subtle anomalies in complex datasets while classifying them into different categories for further analysis. The use of advanced loss functions, SMOTE for handling class imbalance, and optimization techniques ensures that the model performs efficiently and accurately. Evaluation metrics demonstrate that the proposed system achieves high performance in detecting and classifying anomalies, making it a valuable tool for various applications requiring intelligent behaviour analysis and anomaly detection.

Future work will focus on improving the system’s scalability and real-time performance, as well as exploring additional optimization techniques and advanced classification methods. This hybrid approach can be extended to various domains, including cybersecurity, finance, and healthcare, where anomaly detection is crucial for identifying potential threats or system failures.

## REFERENCES

1. S. Rezaei, N. Masoud and A. Khojandi, "GAAD: GAN-Enabled Autoencoder for Real-Time Sensor Anomaly Detection and Recovery in Autonomous Driving," in *IEEE Sensors Journal*, vol. 24, no. 7, pp. 11734-11742, 1 April1, 2024.
2. F. Carrara, G. Amato, L. Brombin, F. Falchi and C. Gennaro, "Combining GANs and AutoEncoders for efficient anomaly detection," *2020 25th International Conference on Pattern Recognition (ICPR)*, Milan, Italy, 2021, pp. 3939-3946.
3. P. Bergmann, M. Fauser, D. Sattlegger and C. Steger, "Mvtec ad-a comprehensive real-world dataset for unsupervised anomaly detection", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 9592-9600, 2019.
4. T. Schlegl, P. Seebock, S. M. Waldstein, U. Schmidt-Erfurth and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery", *International conference on information processing in medical imaging*, pp. 146-157, 2017.
5. D. Subudhi, R. K. Venkatesan, K. Devi and M. Manivannan, "Finger Induced Auto-Thermogenesis," *2021 IEEE 3rd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*, Tainan, Taiwan, 2021, pp. 33-37.
6. Z. Li, D. Xu, Y. Li, T. Chai and T. Yang, "OSVAE-GAN: Orthogonal Self-Attention Variational Autoencoder Generative Adversarial Networks for Time Series Anomaly Detection," *2023 IEEE Symposium Series on Computational Intelligence (SSCI)*, Mexico City, Mexico, 2023, pp. 19-24.
7. S. P. Aly, K. Chapaneri, J. J. John, G. Mathiak and M. A. Alarm, "Retrofitting the Translation Equations of the One-Diode Model for Photovoltaic Modules," *2023 Middle East and North Africa Solar Conference (MENA-SC)*, Dubai, United Arab Emirates, 2023, pp. 1-4.
8. V. Chandola, A. Banerjee and V. Kumar, "Anomaly detection: A survey", *ACM Computing Surveys*, vol. 41, no. 3, pp. 1-58, 2009.
9. S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques", *Procedia Computer Science*, vol. 60, pp. 708-713, 2015.
10. R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey", *arXiv preprint*, 2019.

IJARETY

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com