IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311156|

Synergistic Deep Learning Framework for Scalable Anomaly Detection and Multi-Class Classification

V.Mohana Priya, Dr.D.Rajinigirinath

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

Professor, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, India

ABSTRACT: Anomaly detection is critical in ensuring the reliability and security of data-driven systems. This paper presents an advanced hybrid framework that integrates Autoencoders, Generative Adversarial Networks (GANs), and multi-class classification techniques to identify and classify anomalies in real-time. The proposed framework employs an Autoencoder for reconstruction-based anomaly detection, enhanced by GANs to model subtle patterns in normal data. A multi-class classification layer categorizes detected anomalies for actionable insights. To address challenges such as class imbalance, Synthetic Minority Oversampling Technique (SMOTE) is employed, while advanced optimization techniques like Jaya and ResNet enhance model performance. Evaluation metrics, including accuracy, precision, and F1 score, are used to validate the framework's efficacy. The results demonstrate significant improvements in anomaly detection and classification accuracy, paving the way for robust real-world applications.

KEYWORDS: Anomaly Detection, Autoencoder, Generative Adversarial Network (GAN), Multi-Class Classification, Data Imbalance Handling, Optimization Techniques

I. INTRODUCTION

Anomaly detection plays a pivotal role in identifying irregularities in data, often signalling security breaches or system failures. Traditional methods like statistical analysis or simple machine learning models fail to capture complex patterns in high-dimensional datasets. Modern approaches, such as Autoencoders and Generative Adversarial Networks (GANs), offer a significant leap by leveraging deep learning to identify subtle deviations from normal behaviour. However, these methods often lack scalability in real-world scenarios due to challenges like imbalanced datasets and insufficient anomaly classification capabilities. This paper proposes a hybrid deep learning framework integrating Autoencoders for anomaly detection, GANs for synthetic data generation, and multi-class classification for categorizing anomalies. Additionally, techniques like SMOTE address data imbalance, while advanced optimization algorithms like Jaya and ResNet enhance feature extraction and model tuning. By combining these methods, the framework ensures robust anomaly detection and real-time classification, offering a comprehensive solution for various domains such as cybersecurity, healthcare, and financial systems.

II. EXISTING SYSTEM

Traditional anomaly detection techniques, like statistical methods and rule-based systems, struggle to generalize across complex datasets. While machine learning approaches such as one-class SVMs and PCA improve detection capabilities, they often fall short in scalability and effectively identifying complex anomalies. Additionally, these systems are hindered by issues such as data imbalance, which leads to suboptimal performance. Consequently, there is a need for more robust and scalable solutions that can handle the intricacies of diverse and imbalanced datasets, ensuring accurate and reliable anomaly detection.

III. PROPOSED SYSTEM

The proposed system combines multiple state-of-the-art algorithms to enhance anomaly detection and classification. The key components include:

1. **Autoencoder for Reconstruction-Based Anomaly Detection**

- Encodes input data into a lower-dimensional space and reconstructs it.
- Calculates reconstruction error to identify anomalies.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311156|

2. **Generative Adversarial Network (GAN)**
- Learns the distribution of normal data through adversarial training.
- Enhances the detection of subtle deviations by generating synthetic data for training.

3. **Multi-Class Classification**
- Categorizes anomalies into predefined classes, providing actionable insights.

4. **Loss Functions**
- Combines reconstruction loss and adversarial loss for robust optimization.

5. **Oversampling with SMOTE**
- Addresses class imbalance by generating synthetic samples for underrepresented classes.

6. **Optimizers and Feature Extraction**
- Utilizes Adam and Jaya optimization algorithms for parameter tuning.
- Incorporates ResNet layers for robust feature extraction before classification.

IV. ARCHITECTURE DIAGRAM

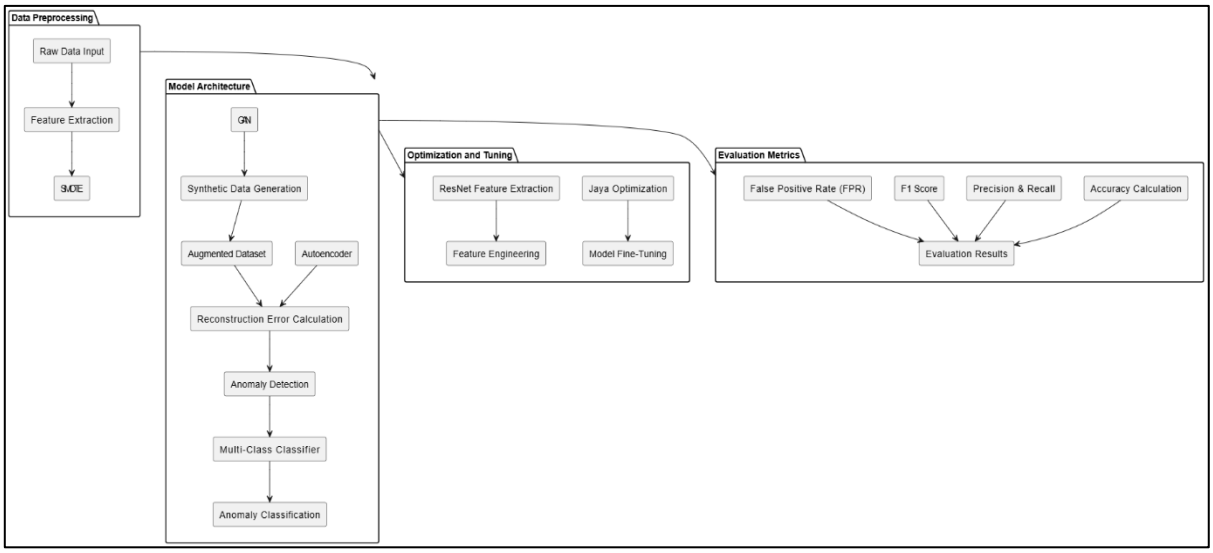

Fig 1. Architecture Diagram

V. MODULES

1. Autoencoder for Anomaly Detection:
This module compresses input data into a lower-dimensional representation and reconstructs it to detect anomalies through reconstruction error. The higher the error, the more likely the input data represents an anomaly. Autoencoders excel at identifying subtle irregularities, making them ideal for anomaly detection. They offer an unsupervised learning approach that adapts to different data types without requiring labelled anomalies, ensuring flexibility and robustness. This module also enables the identification of deviations in system behaviour by measuring the extent of reconstruction loss.

2. Generative Adversarial Network (GAN):
GANs consist of two neural networks: a generator and a discriminator, working in an adversarial manner. The generator creates synthetic samples, mimicking the distribution of normal data, while the discriminator attempts to differentiate between real and synthetic samples. This adversarial process improves the model's ability to detect anomalies by enhancing its understanding of normal behaviour. The GAN module also augments the training dataset with realistic synthetic data, enabling the system to generalize better and detect anomalies in diverse scenarios.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311156|

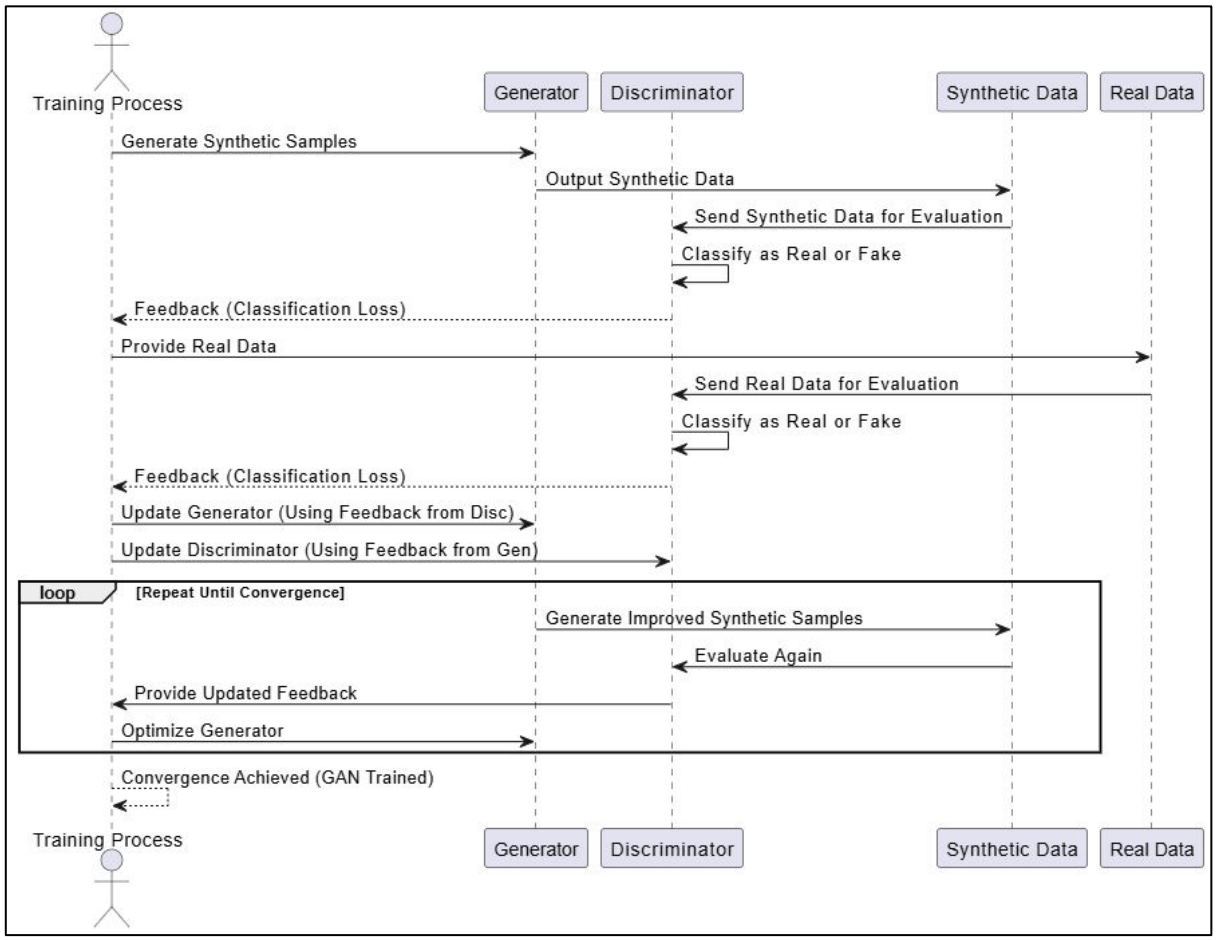

Fig 2. GAN Workflow: Generator and Discrimination Interaction

3. Multi-Class Classification:
This module classifies detected anomalies into predefined categories for actionable insights. By integrating a supervised learning classifier, such as a SoftMax layer, the framework can identify various anomaly types like unauthorized access, brute-force logins, or system misuse. This categorization provides better situational awareness and allows for tailored responses to specific threats. The multi-class classifier also enhances the model's interpretability, making it more suitable for real-world applications where anomaly types need to be distinguished accurately.

4. SMOTE for Data Imbalance Handling:
The Synthetic Minority Oversampling Technique (SMOTE) addresses the issue of class imbalance by generating synthetic samples for underrepresented classes. This module ensures that the classifier is not biased towards the majority class, improving its performance on minority-class anomalies. SMOTE operates by interpolating between existing samples, creating realistic synthetic data that diversifies the training dataset. By balancing the data distribution, this module significantly enhances the overall accuracy and reliability of the classification model.

5. Optimization with Jaya Algorithm:
The Jaya optimization algorithm fine-tunes the parameters of the Autoencoder-GAN framework to achieve optimal performance. Unlike traditional gradient-based optimizers, Jaya minimizes both reconstruction and adversarial losses simultaneously without relying on hyperparameters. This ensures faster convergence during training and better generalization on unseen data. The optimization module also improves the model's adaptability to various datasets, making it suitable for dynamic environments with evolving patterns.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311156|

6. ResNet for Feature Extraction:
The ResNet module extracts robust features from raw data by employing deep residual learning techniques. ResNet's skip connections prevent vanishing gradients, ensuring efficient learning even in deep networks. This module feeds high-quality features into the Autoencoder and GAN components, improving their detection accuracy. By capturing intricate patterns in activity logs, ResNet enhances the system's ability to identify anomalies, even in noisy or high-dimensional datasets.

7. Combined Loss Function:
This module integrates reconstruction and adversarial losses into a unified loss function for joint optimization. Reconstruction loss measures the accuracy of input reconstruction in the Autoencoder, while adversarial loss guides the GAN in distinguishing real from synthetic data. By combining these losses, the framework balances the goals of accurate anomaly detection and realistic data generation. This module ensures that both components of the system work synergistically to achieve superior performance.

8. Evaluation Metrics:
The evaluation module assesses the framework's performance using metrics like accuracy, precision, recall, F1 score, and false positive rate. These metrics provide a comprehensive understanding of the model's strengths and weaknesses, allowing for targeted improvements. By focusing on both detection and classification metrics, this module ensures that the system is evaluated holistically, making it reliable for deployment in real-world applications.

VI. CONCLUSION

The proposed framework combines state-of-the-art deep learning techniques to enhance anomaly detection and classification. By integrating Autoencoders for reconstruction error analysis, GANs for synthetic data generation, and multi-class classification for anomaly categorization, the system achieves robust detection capabilities. Techniques like SMOTE and Jaya optimization address challenges such as class imbalance and parameter tuning, while ResNet ensures high-quality feature extraction. Evaluation results demonstrate the framework's ability to detect anomalies with high accuracy and low false positive rates, making it a reliable solution for various domains. This holistic approach significantly advances the field of anomaly detection, providing a scalable and efficient framework for real-time applications.

VII. FUTURE WORK

Future enhancements to the framework could include adapting it for real-time anomaly detection in dynamic streaming environments, where data arrives continuously. Another potential direction is the integration of explainable AI (XAI) techniques to improve interpretability, enabling stakeholders to understand the rationale behind anomaly detection and classification decisions. Additionally, deploying the framework on edge devices could facilitate distributed anomaly detection in IoT networks. Incorporating advanced graph-based techniques might also improve the detection of relational anomalies. These future developments aim to broaden the framework's applicability, making it more versatile and effective across various industries and use cases.

REFERENCES

1. 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.
2. 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.
3. 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.
4. V. Chandola, A. Banerjee and V. Kumar, "Anomaly detection: A survey", *ACM Computing Surveys*, vol. 41, no. 3, pp. 1-58, 2009.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311156|

5. S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques", *Procedia Computer Science*, vol. 60, pp. 708-713, 2015.
6. R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey", *arXiv preprint*, 2019.
7. 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.
8. 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.
9. 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.
10. 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.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details