

Integrated Deep Unsupervised Models Into An Advance Ensemble Framework For Detecting Anomalies In Attributed Social Networks

Sarfaraz Alam¹, Mohammad Faisal²

^{1,2} Department of Computer Application, Faculty of Engineering & IT, Integral University, Lucknow, India.

Abstract: Anomaly detection has become a major challenge in social network analysis, due to the significant applications of improper activity (such as fraud and spam detection), where the integration of graph topology and node attributes enables more accurate identification of anomalous nodes in networks with static characteristics. Although the rise of deep learning has occurred to overcome the scalability limitations of classical methods in the face of increasing volume and dimension of data, the major reliance on supervised techniques is still hampered by the lack of labeled data and the inherent unavailability of ground truth in anomaly detection tasks in the real world. Although unexplored strategies have been developed for using allele data, their efficacy is inherently limited by the diversity of anomaly types, as no single model can universally capture all possible aberrations. To overcome this fundamental limitation, we propose a new unsupervised ensemble framework that synergistically combines the representational capability of Autoencoder (AE), Variational Autoencoder (VAE) and Generative Adversarial Network (GAN), and incorporates a new weighting mechanism to dynamically aggregate the identities from each component model during the inference phase. Extensive evaluations on the BlogCatalog and Flickr datasets conclusively demonstrate that our ensemble approach is significantly superior to the performance of each individual state-of-the-art model used alone.

Keywords: Anomaly Detection, Social Network Analysis, Ensemble Learning, Deep Generative Models, Unsupervised Learning.

I. INTRODUCTION

The issue of identifying abnormal nodes and users is a big and continuous problem that threatens the integrity, accessibility and general reliability of the network. It is a complex task since modern network architectures are highly diverse given that there are unique characteristics of each network [1]. In the modeling of complex systems, like social media platforms, critical infrastructures and biological networks, attribute graphs are employed where node attributes are useful feature-level data that is needed to do precise analysis [2]. Following the heavy practical uses of the technique in fields like detection of fraud and spammer, network intrusion detection and system fault diagnosis, anomaly detection in these specific networks has become a key subject in research [3]. Nonetheless this task has its own set of challenges; This urges the need to integrate the structural information of the network intuitively with its nodal properties so as to successfully detect deviations [4]. One such major complication is presented by the existence of noisy and high-dimensional data of attributes which are structurally inconsistent, and therefore, hide true anomalies, which may result in large numbers of false positives and in-accurate conclusions that will have to be analyzed in highly complex modes [5-6].

As the prohibitive price and practical impossibility to find anomalies manually in increasingly big and complicated networks datasets, the approach of unsupervised learning becomes beneficial but also critical [7]. These tools are especially applicable in this task since they do not operate under the premise of pre-labeled data, but they do exploit the characteristics inherent in the data to learn deviations of the normal patterns [8-9]. This has led, in turn, to the development of modern methods of detecting social

network anomalies, which work to combine various types of information, the strong node features in a wholesale fashion with the subtler features, the structural features of the network [10]. Also, another important contribution to the field is the creation of more complex techniques to target and remove the effects of structurally irrelevant or noisy nodal features [11]. Such a refinement is significant, as it can guarantee that the model targets the most pertinent information which will improve detection accuracy, minimize false positives (false positives) and the overall reliability of the anomaly detection process [12-13].

Added to this fact, the remarkable achievement of the deep learning in a rather diverse field such as the computer vision, the natural language processing, and robotics has not only stimulated the interest of the academics but also that of the practitioners working in the industry who contemplate the potential of the method in the field of the social network security [14-15]. Anomaly detection is a significant part of the detection of criminal activity like spam, fraud, misinformation proliferation, and coordinated cyberattacks within this area [16-17]. Historically, anomaly detection models may be trained either by supervised, semi-supervised or unsupervised methods of learning. But supervised learning methods have a severe constraint in the quality of available labeled data in the first place it is computationally expensive to prepare a balancing dataset of benign and malicious examples, in the second place, it is also complicated by the fact that the abnormal phenomena are rare and in the third place the possibility to label accurately a range of negative actions [18]. To address the shortage of labelled data, unsupervised learning methods like autoencoders, variational autoencoders, and generative adversarial networks have been studied extensively, since they are based on generative models capable of learning representation using allele data [19]. These approaches have their potential, but it is often the dynamic and multifaceted nature of the adversarial approaches, fueled by advanced tools used by cybercriminals [20], that inhibits the effectiveness of such approaches since it is challenging to generalize to all possible types of anomalies any one approach. This problem reflects the basic disadvantage of the current strategy: Lack of a universal model, capable of identifying the whole range of abnormal actions within social networks. Having this constraint as motivation, [21] we introduce a novel framework of anomaly detectors leveraging an ensemble of models to outsource strengths of various technologies together to enhance robustness, flexibility as well as detection rates in the face of multidimensional and heterogeneous cyber-attacks. With the problem of anomaly detection on networks with static features, the work officially introduces the problem, and offers a solution through an innovative ensemble model, which is specifically aimed at defeating the intrinsic limitations and limited focus of individual identification algorithms [22]. Our key novelty is an advanced system of weighting (weighting mechanism) that smartly injects effect into the component models on the ensemble; The strategy offers a more comprehensive and holistic way of measuring node irregularity and this is due to the synthesis of varied detection strategies as seen in the ensemble [23]. The effectiveness of multi-modeling to serve one comprehensive and sophisticated goal is substantiated by the established feasibility of generalizability and replication of multi-modeling in the machine learning sphere [24]. With the advantages of unsupervised training, which is crucial in the absence of labeled abnormal data, our suggested ensemble models offer an effective and effective approach to detect high-level abnormalities in complex network models [25].

This paper has the following structure. Section 2 presents a review of the related works. Part 3's background offers the context of deep learning methodologies that are not analysed to detect anomalies. Section 4 discusses the proposed ensemble model in detail.

The analysis and the results of the experiments are given in Section 5, and the paper concluded.

II. RELATED WORKS

The rising popularity of attributed networks as a modeling tool to simulate complex systems from whose nodes are defined in both terms of relational relationships and rich attribute profiles has led to renewed research interest in them as a platform to detect anomalies. Early approaches to this challenge exploited particular structural or salient features: For example, the AMEN [26] approach finds unusual communities by considering how similar the values of attributes were within a node local ego-network. In the same vein, the RADAR [27] method explicitly use discrepancy-detection with a network structure by comparing residuals between the actual attribute values and those as predicted by the network structure, which effectively characterizes nodes that attributes do not match their structural form. Nevertheless, as network scale and complexity blow up exponentially, the concept of deep learning frameworks has proven to be a potent answer to learning non-linear, latent representations which intuitively combine both attribute and structural information. One of the key deep learning methods in this direction is that the graph convolutional network (GCN) encoder processes input data into a small latent encoded form that can be decoded back into input data by a decoder, the method is called as DOMINANT (Deep Anomaly Detection on Attributed Networks). It works on the assumption that if a model has been trained on the pattern (which is used by the rest of the network) that dominates, then it will successfully recreate normal nodes and not succeed at recreating the abnormal nodes, thus the identification of the outgoing points (outliers) is achieved by a high combined reconstruction error of the features of a node and its local network connections.

The rising popularity of deep learning has spawned much interest in its use with graph-structured data, inspiring the creation of the advanced deep neural network infrastructure targeted at this space. One of the main areas that this study focuses on is network embedding where the goal is to learn low-dimensional representations that are effective at preserving the topological structure of a network. This has resulted in the expansion of novel models of anomaly detection. As an example, the SpecAE [29] approach employs an original and novel graph convolution encoder-decoder to learn local node representations and compute the doubtfulness score of a node as a function of the energy of its latent representation in a Gaussian mixture model. In the same manner, the DUAL-SVDAE [30] framework entails dual autoencoders in both structure and characteristics that combine the information in the dual-hypersphere training technology to describe generality. More methods are aimed at analyzing residual information about reconstruction error, which utilizes graph convolutional networks (GCN) to learn network sparsity and non-linearity; The effect of outgoing (outlier) nodes is additionally reduced on the effect of such residual data. Moreover, the astounding performances of Generative Adversarial Networks (GANs) [33], that have been demonstrated in scenarios like image processing and adversarial synthesis are also under investigation, highlighting a more general tendency of modifying advanced deep learning paradigms to the intricate issue of anomaly detection on special networks.

Ensemble learning is a potent machine learning model that harnesses the wisdom of a number of core learners to perform better prediction than a single model [34]. The recent developments have seen it prove to be useful in various fields especially in the area of anomaly detection and classification. A prominent method is sub-division of the locations of features to train neural networks on particular feature which leads to a set of, for example, classifiers with outputs concatenated to identify the occurrence of malicious activities. Density-based and rank-based approaches have been proven to be

effective with hybrid ensemble techniques that improve anomaly detection [35]. Ensemble structures Incremental ensemble structures have been studied, in which one prediction is further refined by other predictions over time. This has proposed a soft voting ensemble classifier to perform binary classification, which brings greater decision making when it comes to RFS, Logistic regression, and Naive Bayes. In cybersecurity, a three-step deep learning system with unsupervised, semi-supervised and supervised algorithms have been designed to address network intrusion. Likewise, in medical imaging, a boosted convolutional neural network (CNN) ensemble has been proposed to diagnose COVID-19 and is based on the segmentation, feature extraction with CNN, and end-stage voting. Deep Active Learning systems also achieve improvements in detecting anomalies by incorporation of human feedback on unsupervised and semi-supervised models, minimizing false positives without requiring labeled inputs. The other novel approach is to construct local models, by partitioning the data space, to run decision tree-based ensembles to find out the appropriate nuances in and around specific examples. Also, entropy-based ensemble algorithms have been used to detect anomalies in real-time forecasting in multidimensional time series, and assisted by visualization software tracking the behavior of nodes [37]. Taken together, these methodologies note the flexibility and usefulness of ensemble learning in addressing complex, data-hungry problems.

III. BACKGROUND OF RESEARCH

3.1 Autoencoder (AE)

Autoencoders are a type of artificial neural network, used in unsupervised learning. Their primary aim is to effectively encode data and acquire its representation. Their design is a symmetrical design, where there are two key blocks: One is the encoder that compresses the input data and transforms it into a low dimensional latent space (also known as code) and the other is the decoder that to the best of its ability gives the current compressed code back into its original data. The autoencoder is trained to discover salient features of the data and the underlying manifold rather than memorize the input by introducing some constraints on the network, e.g., through bottleneck layers or sparsity penalties. This is the reason why they are highly effective in such applications as dimensionality reduction, anomaly detection and noise denoising. Outside these, Variational Autoencoders (VAEs) build upon this set of encoders to an extent such that they are the foundation of deep generative modeling. Anyway, autoencoders are a crude and essential means to comprehend the inner. structure of complex and high-dimensional datasets.

3.2 Variational Autoencoder (VAE)

Variational autoencoders (VAEs) are an important advancement in the field of deep generative modeling. They have adapted the process of encoding-decoding to a probabilistic and Bayesian framework [39]. Moving away from conventional autoencoders, the encoder in VAE maps the input not directly to a point, but to a probability distribution in latent space. This distribution is usually defined by a mean and variance. Then a point from this same distribution is sampled and given to the decoder so that he can reconstruct it. This random sampling process, which is made capable of backpropagating the gradient with the help of the reparameterization trick, forces the latent space to become continuous and structured. This process is controlled by a regularization called the Kullback-Leibler divergence, which forces the posterior distribution to stay close to a pre-determined distribution (usually a standard Gaussian curve). So, VAEs are not only efficient encoders, but also powerful generative models.

With the help of these, you can create completely new, coherent and realistic data samples by taking samples from learned latent manifolds. That is why these have become indispensable tools for tasks like image generation, representation learning and Bayesian inference.

3.3 Generative adversarial networks (GAN)

In the framework of a generative adversarial network (GAN), the learning process is like a minmax game between two different neural networks: One is the generator and the other is the discriminator. This model, serving as our discriminator, denoted by $\text{Dis}(x)$ is a binary classifier. It is tasked with guessing whether or not the input point of the data (x) is part of the true data distribution or the generator has generated it. The discriminator is trained such that he is able to maximize the likelihood of correctly recognizing the positive as well as the negative samples. The generator network is, on the other hand, $\text{Gen}(z)$. It is a mapping process that samples z in a simple a priori distribution $p(z)$ (as the standard Gaussian distribution) to the complex data space. It attempts to make them look so lifelike that they are not recognized by the discriminator. It is the adversarial game - The generator always attempts to avoid the discriminator, and the discriminator adapts to finding and recognizing the generator it. In this process both the models keep on improving in turn, until the output distribution of the generator comes out to be almost completely equal to the real data distribution. Things work perfectly in the ideal case: the generator has grown too powerful to such an extent that the discriminator can hardly differentiate between real and fake.

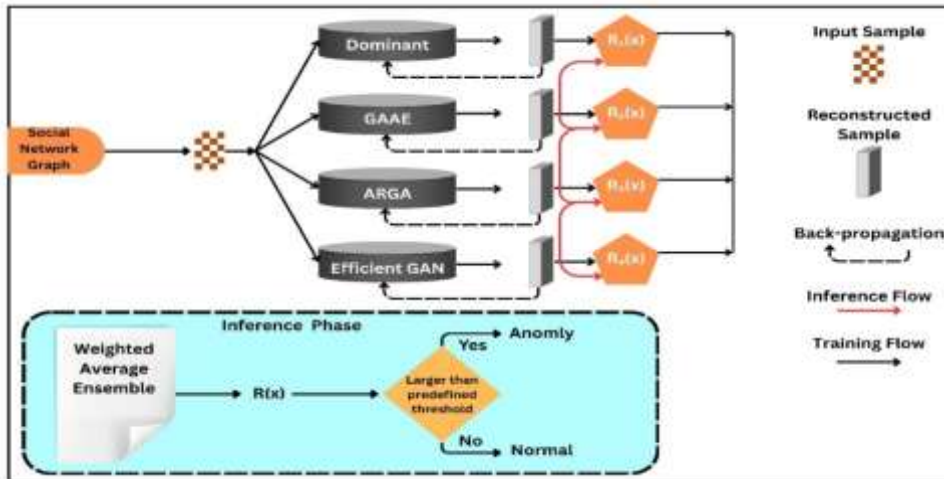
IV. DESIGN OF PROPOSED MODEL

Figure 1 shows the architecture of the advanced ensemble-based anomaly detection framework that we proposed. This model incorporates four different unsupervised learning approaches. Each of these approaches is designed to capture different structural and statistical properties of the data, thereby increasing robustness and reliability of identification. To combine the strengths of these different models, we have adopted a weighted average ensemble strategy. In this strategy, we aggregate the output of all the models (base learners), but give more weight to the models which perform better. This mechanism ensures that the final prediction for each sample is not dependent on any one model, but is made up of balanced contributions from all participating models. By taking advantage of the diversity among these unobserved methods and optimizing their collective judgment through weighted averages, our proposed ensemble seeks to achieve higher accuracy, less bias, and better generalization in anomaly detection tasks.

4.1 DOMINANT: DOMINANT is a state-of-the-art unsupervised anomaly detection framework, which leverages deep learning techniques to identify irregularities within graph-structured data [39]. The core of its architecture is a graph convolutional autoencoder, which is specifically designed to capture both structural and attribute-based information of nodes in a graph. This model reconstructs two things at once: adjacency matrix (which shows the connections between nodes) and attribute matrix (which encodes the attributes associated with each node). By learning to accurately reconstruct these matrices, the autoencoder develops a deeper understanding of common node behavior. Then the anomalies are detected by calculating the reconstruction error for each node, indicating the degree of deviation from the expected pattern. DOMINANT presents a weighted aggregation of these reconstruction errors, combining structural and characteristic anomalies to produce a comprehensive anomaly score. Nodes with high scores are marked as abnormal, indicating possible irregularities

in their connectivity, feature profile, or both. This combined reconstruction strategy allows DOMINANT to outperform traditional methods that treat structure and characteristics differently, making it particularly effective in complex, heterogeneous graph environments such as social networks, transactional systems, and cybersecurity applications.

Fig 1: Proposed Advanced Ensembled Framework



4.2 GAEE: Graph attentional autoencoders are a powerful extension of autoencoders, designed specifically for non-Euclidean graph-structured data. It integrates the representational capability of graph attentional layers into an encoder-decoder framework. The encoder uses masked self-attention layers (as introduced in Graph Attention Networks - GATs). These layers compute the node representation by dynamically weighting and aggregating the attributes coming from the neighboring nodes. This way the model understands the complex local dependencies present within the graph and the importance of each neighbor. The compressed latent node embeddings obtained from this process are then sent to a decoder. This decoder is usually designed to reconstruct the original graph structure, for which it often resorts to the method of link prediction - Like extracting the inner product between the latent representations. Learning two tasks simultaneously - on the one hand to encode topologically conscious node features and on the other hand to decode the adjacency matrix of the graph - This model learns a low-dimensional, semantically rich latent space. This latent space is extremely effective for tasks such as unsupervised node representation learning, graph clustering, and link reconstruction, and best of all, it also remains interpretable due to attention mechanisms.

4.3 ARGAs: Adversarial Regularized Graph AutoEncoder (ARGA) is a very generative model which is specifically tailored to the task of learning robust graph embeddings to perform an anomaly detector on attribute networks [42]. ARGAs also contains an adversarial regularization part, unlike conventional graph autoencoders. A discriminator is trained to differentiate two things: On one hand the latent representations produced by the encoder and on the other hand the samples of some pre-defined distribution (e.g. Gaussian distribution). On the other hand, the encoder tries to dodge this discriminator. This type of adversarial mechanism makes the latent space approximate that pre-determined distribution, making the model more

generalizable and prevents overfitting. To detect anomalies, ARGA captures both the structure of the graph and the distribution of the node attributes in the graph at the same time. Then the anomalies are determined by measuring high reconstruction errors or by looking at significant deviations in the embedding consistency. By integrating graph convolutional encoders with adversarial regularization, ARGA provides a theoretically robust way to create discriminative embeddings that explicitly expose irregularities in complex social and information networks.

4.4 EfficientGAN: The EfficientGAN framework is a generative adversarial network-based approach, designed to perform anomaly detection at low computational cost, while also maintaining high detection accuracy [43]. Unlike traditional GANs, which often suffer from training volatility and high resource demands, EfficientGAN includes architectural optimizations such as lightweight convolutional layers attention mechanisms, and efficient training strategies, so that high-quality reconstruction of input data can be performed. For anomaly detection, the generator learns to reconstruct normal samples, while reconstruction error or deviations in discriminator feedback highlight abnormal instances. By striking a balance between efficiency and representativeness, EfficientGAN enables scalable deployments on large, high-dimensional datasets, making it suitable for domains such as social networks, medical imaging, and cybersecurity, where timely and accurate anomaly detection is critical.

4.5 ResGCN: ResGCN is an anomaly detection framework that builds upon the residual learning concept to eliminate the drawbacks of the conventional graph convolutional networks (GCNs) [44-45] (including over-smoothing and gradient disappearance in deep networks). The ResGCN incorporates residual relationships amid layers to develop prolific networks that effectively learn neighborhood and long-distance structural connections in characteristic graphs. Regarding anomaly detection, ResGCN trains node embeddings conditioned on structural pattern and attribute data and detects anomalies by the reconstruction errors, inconsistencies in the learning of the embeddings, or anomalies in the learned graphs representations. This residual design training is more stable, has more features that are distributed across many layers, and enables this model to be more sensitive to subtle and more intricate anomalies in large-scale social and information networks.

This architecture trains a collection of autonomously trained models with all of the component models learned independently, i.e. without interference with each other, allowing the parallel training of these models when the needed computational capabilities are available. The initial training time is a fixed cost which is paid once, however, model convergence to maximum efficiency can take a long time, and the overall time can highly depend on the model since the architectural design and hyperparameter choice can differ greatly. Throughout the inference stage each member of an ensemble packaging the models construct their respective reconstruction processing through the input sample. A discrepancy score of each of the models is then obtained by the average squared error between the input and its reconstruction. These personal scores are crunched into an overall, powerful discrepancy score through a weighted average ensemble operation, and ultimately the sample is classified as abnormal or normal by comparing this combined score to a predetermined threshold.

4.6 Weighted average ensemble for calculating final anomaly score

This paper is dealing with a severe shortcoming of ensemble-based anomaly detection systems, in which meaningful weights cannot be placed on individual models, because there is no abnormal data in the training stage. In a bid to get around this challenge we

have proposed a new weighting strategy which is founded on the measurement of equality and inequality using statistical correlation. Instead of using labeled discrepancies, our method measures the levels of consensus across model outputs in terms of computed pair-wise correlations, to capture how they consistently respond to normal data. Models with high interpersonal correlation - i.e. their behaviour and output patterns are similar - are assigned a larger weight (i.e. are more influential in the ensemble) whereas less correlated models are assigned an appropriate smaller weight. This weighting mechanism based on correlation guarantees that the ensemble favors models with the same decision boundary hence making it more robust and stable in the inference of anomalies. Our approach offers a statistical and data-saving alternative to conventional training-based ensemble weighting facilitating the statistical relationships of the model outputs. In ensemble-based anomaly detection, there are often significant disparities in the range of values of the outputs of different algorithms. Because of this, models whose outputs are numerically large can have a disproportionately high impact on the final ensemble decision. To reduce this bias and to ensure that every model has a balanced contribution, standardization as a normalization technique is widely adopted. In our approach, we use raw reconstruction error scores which are denoted by R_i .

R_i are converted into Z-scores using the formula:

$$Z_i = \frac{R_i - \mu}{\sigma}$$

Here μ denotes the mean of the error score and σ denotes the standard deviation. This transformation brings the output to a common scale, where the mean is zero and variance is unit (one). In this way, it ensures that the high discrepancy scores obtained from any individual method remain of relative importance, as well as they can be fairly integrated into the ensemble aggregation process.

After standardization of the reconstruction error score, we calculate the pairwise correlation between the authentic outputs of each model. This yields a correlation matrix, which is denoted by CM. The dimensions of this matrix are $m \times m$, where m represents the total number of models in the ensemble. As exemplified in equation (1), this matrix measures the degree of linear dependence between the error distributions of each model pair, which provides important insight into diversity and redundancy within the ensemble.

$$\begin{array}{ccccccc} & R_1 & R_2 & \dots & \dots & \dots & R_n \\ & CM_{11} & CM_{12} & \dots & \dots & \dots & CM_{1n} \\ R_1 & & & & & & \\ R_2 & CM_{21} & CM_{22} & \dots & \dots & \dots & CM_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ R_m & CM_{m1} & CM_{m2} & \dots & \dots & \dots & CM_{mn} \end{array} \quad \text{----(1)}$$

To refine the weight allocation process and to prevent inflationary bias generated by self-correlations - which are always absolute (value 1) and therefore useless for inter-model comparisons. We obtain a final weight matrix W through a normalized averaging procedure. For each model n , the sum of its correlations with all other models is extracted, excluding its own trivial self-correlation. Then this sum is divided by the total number of models minus one to get the mean inter-model correlation. This calculation is formally equivalent to extracting the average of each row of the correlation matrix and subtracting the identity matrix from it, thereby separating meaningful pairwise dependencies. The set of average correlations thus obtained for all models is then normalized to ensure that the sum of the weights is one. Thus, the final weight vector W

= $\{w_1, w_2, \dots, w_n\}$ is obtained, where each w_i proportionally represents the consensus of that model within the ensemble.

Finally, to compute the comprehensive anomaly score for a given sample x , the individual authentic reconstruction errors $R_j(x)$ obtained from all the N component models are aggregated into the integrated score $R(x)$. This aggregation is done through a weighted summation, which is formally defined as:

$$\sum_{j=1}^N W_j R_j(x)$$

where the optimal weights w_j are not determined by heuristic alone, but are closely optimized using the weighted ensemble method described earlier, which is designed to maximally discriminate between normal and abnormal examples. Next, a final determination of the nature of the sample (normal or abnormal) is made by comparing this combined anomaly score $R(x)$ to a pre-set threshold, thereby completing the proposed ensemble framework outlined in Algorithm 1.

Algorithm 1 Advance Ensemble framework.

Input:

- Given a dataset $D = \{d_1, d_2, d_3, \dots, d_m\}$ of size m , where d_i represent a specific observation.
- Algorithm set $A = \{A_1, A_2, \dots, A_N\}$, where each A_i is an anomaly detection algorithm.

Output:

- Final anomaly score $R(x)$ for each sample $x \in D$.
-

1. Base Anomaly Detection

For each algorithm $A_i \in A$:

- a) Apply A_i on D .
- b) Obtain the reconstruction (or detection) error score vector R_i .
- c) Normalize R_i to ensure comparability across algorithms.

2. Correlation Matrix Computation

Construct the correlation matrix $CM \in \mathbb{R}^{N \times N}$, where each entry CM_{mn} represents the correlation between R_m and R_n .

3. Weight Calculation

For each algorithm A_n :

- a) Compute its weight W_n as the average correlation of R_n with all other algorithms:

$$W_n = \frac{1}{N-1} \sum_{m=1}^N CM_{mn}$$

- b) Normalize weights so that $\sum_{n=1}^N W_n = 1$.

4. Final Anomaly Score Aggregation

For each sample $x \in D$, compute its final anomaly score as the weighted sum of base scores:

$$R(x) = \sum_{j=1}^N W_j \cdot R_j$$

5. Return

Output the anomaly score vector $R(x)$ for all samples $x \in D$.

V. EXPERIMENTAL RESULTS, ANALYSIS AND COMPARISON

5.1. Datasets

In this study, we perform a comprehensive empirical evaluation of our proposed model using two widely recognized real-world characteristic network datasets - Dataset 1 (Flickr) [46] and Dataset 2 (BlogCatalog) [47] -. These datasets were selected because they represent the standard benchmark in this field and have been used extensively in previous research on network analysis and anomaly detection, ensuring a robust and comparable basis for assessment. The detailed statistical properties of each dataset, including the number of nodes, edges, and attributes, are systematically summarized in Table 1 to provide a clear overview of their structural and feature-based characteristics.

- Dataset 1 is an online image and video hosting platform, where users build a social network by making connections to each other. In its network representation, nodes are users and are represented by attribute vectors made up of the tags they use to label their shared content; These tags collectively act as a proxy (parameter) of user's expressed interests and preferences.

- Dataset 2 is a social media platform, where users (who are mainly bloggers) form a network by making connections to each other. The dataset representing this network consists of rich node attributes, which are feature vectors derived from descriptive information provided by users to characterize both their personal profiles and their blogs.

Table1: Statistics of dataset under test

Dataset	Vertices (V)	Edges (E)	Attributes (A)	Anomalies
Flickr Dataset1	7575	2,39,738	12,047	450
BlogCatalog Dataset2	5196	1,71,743	8189	300

5.2 Evaluation criteria and comparison

Accuracy is a widely used measure in classification, but cannot be relied upon with skewed datasets such as anomaly detection, where rare anomalies can be easily ignored. The aim is to identify as many abnormalities as possible and eliminating false positives. Therefore, accuracy and recall are desirable: precision is the fraction of correct anomalies of the predicted anomalies and recall is the fraction of predicted anomalies of the actual anomalies. This combined give more worth to model performance.

$$\text{Precision} = \frac{\text{TP}}{(\text{TP} + \text{FP})}$$

True Positives (TP) refer to correctly identified anomalies and False Positives (FP) are normal samples falsely identified as anomalies. Precision (a lower FP) is valuable, but cannot be utilized by itself, as a model may achieve good preciseness by identifying a few anomalies. This is achieved by recall, which counts the number of the actual anomalies that the model has correctly detected, which is a measure of sensitivity of the model. When Precision and Recall are both considered, it generates a more balanced and reliable. assessment of anomaly detection performance.

$$\text{Recall} = \frac{\text{TP}}{(\text{TP} + \text{FN})}$$

False negatives (FN) are discrepancies that the model does not recognize. The Receiver Operating Characteristic (ROC) curve evaluates performance by plotting the True Positive Rate (TPR) against the False Positive Rate (FPR), indicating a trade-off between sensitivity and specificity. Area Under the Curve (AUC) quantifies this performance, indicating the likelihood that an anomaly will receive a higher score than a typical example. An AUC that is close to one indicates the strong quality of the model and its ability to effectively distinguish between normal and abnormal samples.

Fig2 ROC curve on Dataset1

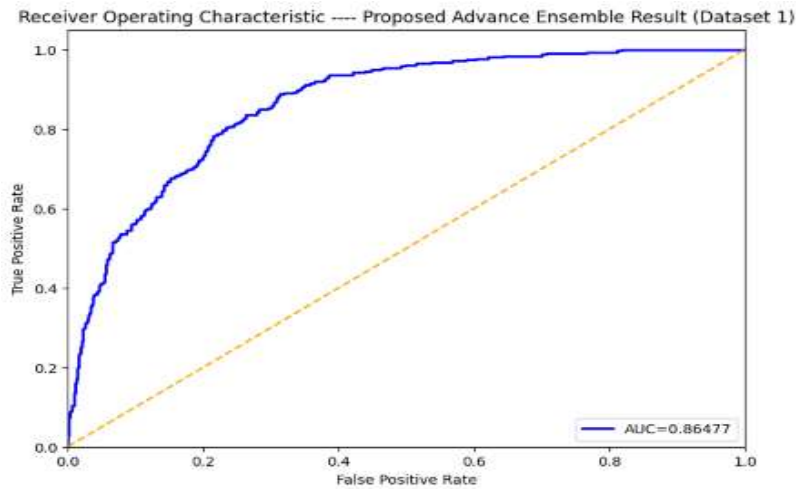


Fig3 ROC curve on Dataset2

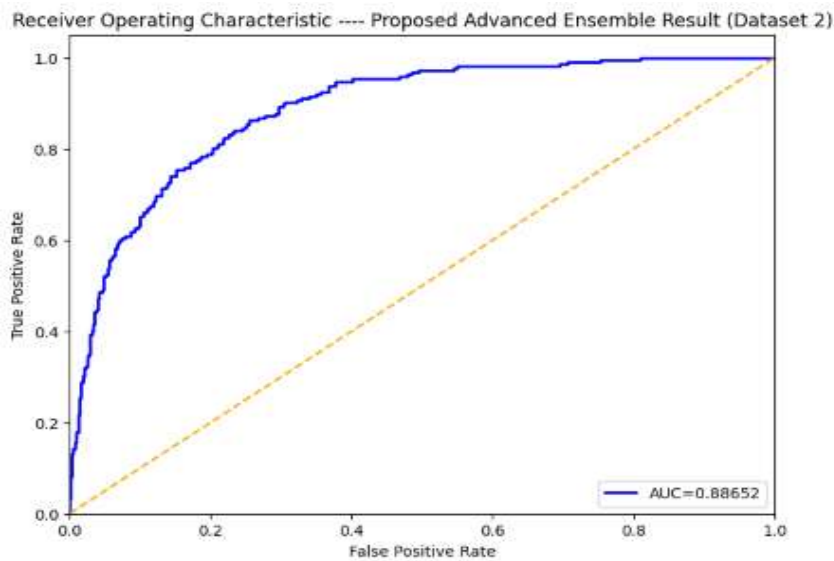
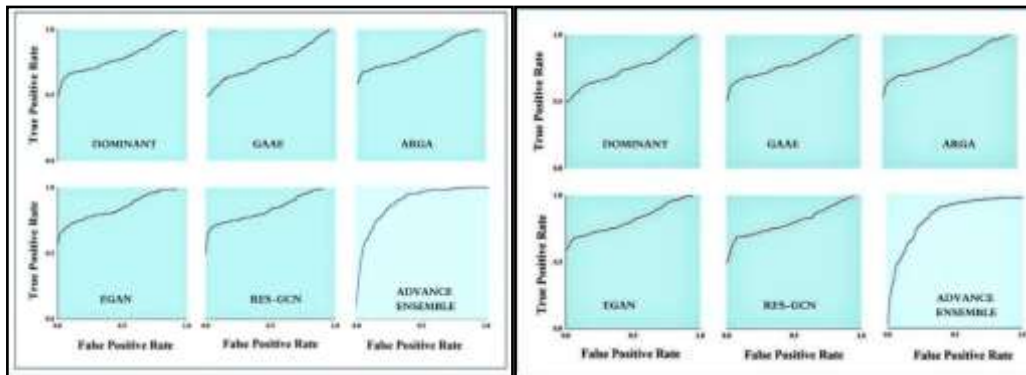


Table2: Result comparison

Method	Dataset1			Dataset2		
	AUC	Precision	Recall	AUC	Precision	Recall
DOMINANT	0.74900	0.70570	0.69560	0.78130	0.76530	0.71250
GAAE	0.73060	0.70820	0.70350	0.80360	0.77850	0.73520
ARGA	0.81100	0.78530	0.76590	0.82160	0.81150	0.80520
EfficientGAN	0.81640	0.79550	0.78530	0.81830	0.80950	0.79550
ResGCN	0.80570	0.79950	0.80160	0.84300	0.81570	0.80120
Ensemble	0.84180	0.82350	0.81350	0.85030	0.83250	0.81250
Proposed Advance Ensemble	0.86477	0.85438	0.84693	0.88652	0.86471	0.84581

Fig 4 ROC Comparison of dataset1 and Dataset2



5.3 Result Analysis

The proposed model has been tested by its Receiver Operating Characteristic (ROC) curves on dataset 1 and dataset 2 (Figure 2 and Figure 3) respectively which suggest that the proposed model has a high level of differentiation. This model has scored high Area Under the Curve (AUC) scores of 0.86477 and 0.88652. The performance is reported with a detailed comparative analysis with various benchmark algorithm and the entire performance is described under Table 2 in terms of AUC, Precision and Recall. To provide a direct visual comparison between the predictive performance of all methods on a single dataset, we plot ROC curves of each method on the same plot and in Figure 4 (Dataset 1 and Dataset 2). Furthermore, AUC, Precision and comparison of Figures 5 (Dataset1) and Figure 6 (Dataset2) provide consolidated bar-chart comparisons.

Recall scores respectively that give an effective and prompt review of the excellence of the suggested ensemble model overall appraisal measures. These findings have been detailed by discussing them below.

Fig 5 Result Comparison of dataset1

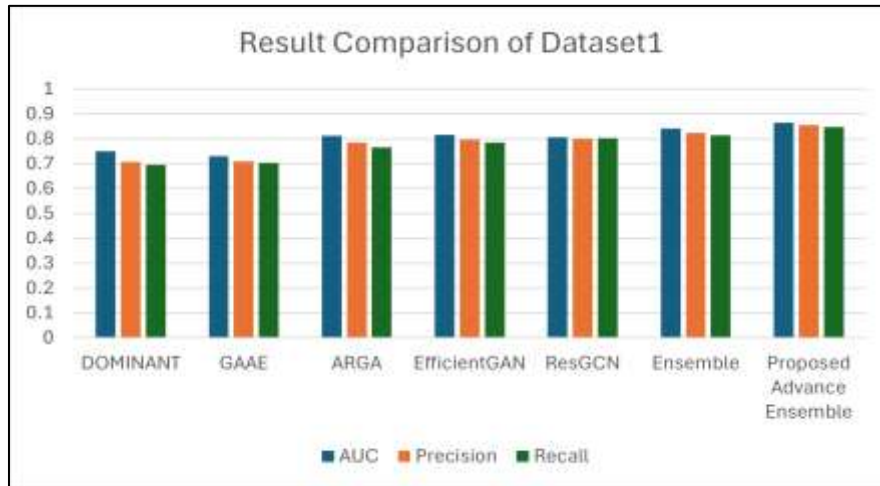
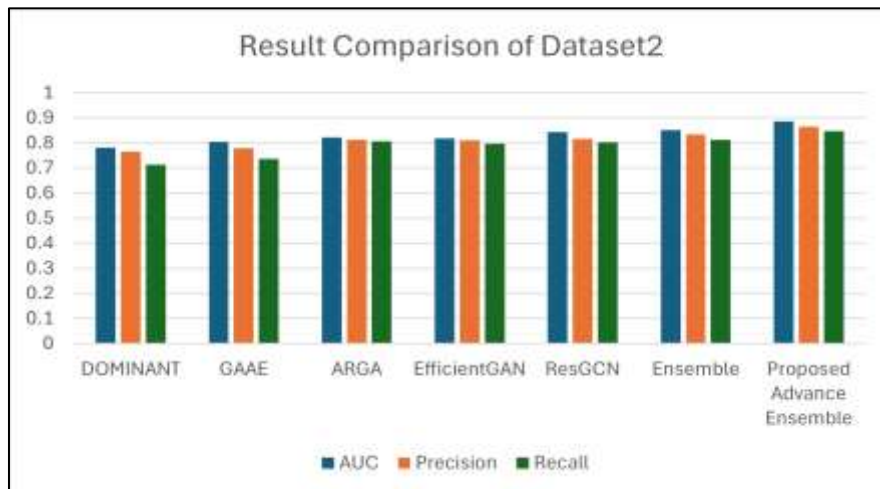


Fig 6 Result Comparison of dataset2



In the empirical evaluation, the performance of individual anomaly detection models in experimental evaluations showed remarkable variation on different datasets. Thus, model selection is a major challenge in graph-based anomaly detection since it is context-dependent. The Graph Attentional AutoEncoder (GAAE) surpassed the dominant model on dataset 2, but the order was reversed on dataset 1. This supports the hypothesis that one model is not universally optimal for all graph structures or data distributions. The resulting inconsistency can be taken as a justification for the proposed ensemble framework that achieves robust performance by effectively combining different base detectors. Furthermore, ARG and EfficientGAN yield better and relatively similar results due to their particular adversarial and generative regularization techniques. Both Dominant and GAAE demonstrate the effectiveness of these advanced learning frameworks. All said and done, the ensemble model we propose consistently outperforms all competitive methods, including these strong adversarial and generative baselines, in every evaluation metric and across all benchmark datasets.

VI. CONCLUSION

In this paper, we present an innovative unexplored advanced ensemble model for anomaly detection in social graphs, which intelligently integrates six different unexplored base models. The main innovation of our framework is a sophisticated weighting mechanism, which dynamically assesses the predictive quality of each component model for a given sample, leading to a more informed and stronger consensus for the final discrepancy score without the need for labeled data. This is an important advantage that increases its practical applicability. Extensive evaluation on real-world datasets, including Dataset 1 and Dataset 2, shows that our model performs significantly better than current state-of-the-art methods. Although these results are highly promising, we acknowledge that the performance of models on very low-dimensional datasets (such as Enron and Amazon) remains an area of future research. As a result, our next work will focus on optimizing the model to perform effectively across a broad range of data dimensions and extending its capabilities to more complex and dynamic network structures (such as heterogeneous, spatial-spatial, and time-evolving graphs), in order to further bridge the gap between theoretical development and real-world, large-scale deployment.

FINDING

The information used to support the article's conclusions is contained in this article.

ACKNOWLEDGMENT

This work is acknowledged under Integral University manuscript No IU/R&D/2026-MCN0004416.

REFERENCES

- [1] L. Zhen, N. Hafizah Kamarudin, V. Jyn Kok and F. Qamar, "Anomaly Detection Model in Network Security Situational Awareness Based on Machine Learning: Limitation, Techniques, and Future Trends," in *IEEE Access*, vol. 13, pp. 126084-126129, 2025, doi: <https://doi.org/10.1109/ACCESS.2025.3589620>.
- [2] Kesavulu, D., R. K. Improved bio-inspired with machine learning computing approach for thyroid prediction. *Sci Rep* 15, 22524 (2025). <https://doi.org/10.1038/s41598-025-03299-8>
- [3] Schnoering, H., & Vazirgiannis, M. (2025). Bitcoin research with a transaction graph dataset. *Scientific Data*, 12(1), 404. doi : <https://doi.org/10.1038/s41597-025-04684-8>.
- [4] Khan, M. Z., Shahzadi, M., Khan, A., Ali, U., Hassan, M. A. S., & Hussain, M. (2025). Review on crack detection in civil infrastructure using structural health monitoring and machine learning techniques. *Innovative Infrastructure Solutions*, 10(8), 348. doi : <https://doi.org/10.1007/s41062-025-02147-y>.
- [5] Feng, C., Fan, J., Liu, Z., Jin, G., & Chen, S. (2025). Unmanned Aerial Vehicle Anomaly Detection Based on Causality-Enhanced Graph Neural Networks. *Drones*, 9(6), 408. doi : <https://doi.org/10.3390/drones9060408>.
- [6] Gad, I. (2025). TOCA-IoT: Threshold optimization and causal analysis for IoT network anomaly detection based on explainable random forest. *Algorithms*, 18(2), 117. doi : <https://doi.org/10.3390/a18020117>.
- [7] Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ... & Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. *IEEE access*, 7, 65579-65615, doi: <https://doi.org/10.1109/ACCESS.2019.2916648>
- [8] Mascali, L., Schiera, D. S., Eirauda, S., Barbierato, L., Giannantonio, R., Patti, E., ... & Lanzini, A. (2023). A machine learning-based Anomaly Detection Framework for

- building electricity consumption data. *Sustainable Energy, Grids and Networks*, 36, 101194, doi: <https://doi.org/10.1016/j.segan.2023.101194>.
- [9] Shrish Bajpai, "Low Complexity and Low Memory Compression Algorithm for Hyperspectral Image Sensors," *Wireless Personal Communications*, vol. 131, pp. 805-833, 2023.
- [10] Xing, L., Li, S., Zhang, Q., Wu, H., Ma, H., & Zhang, X. (2024). A survey on social network's anomalous behavior detection. *Complex & Intelligent Systems*, 10(4), 5917-5932, doi: <https://doi.org/10.1007/s40747-024-01446-8>.
- [11] Khosravi, P., Mohammadi, S., Zahiri, F., Khodarahmi, M., & Zahiri, J. (2024). AI-enhanced detection of clinically relevant structural and functional anomalies in MRI: Traversing the landscape of conventional to explainable approaches. *Journal of Magnetic Resonance Imaging*, 60(6), 2272-2289, doi: <https://doi.org/10.1002/jmri.29247>.
- [12] Zamanzadeh Darban, Z., Webb, G. I., Pan, S., Aggarwal, C., & Salehi, M. (2024). Deep learning for time series anomaly detection: A survey. *ACM Computing Surveys*, 57(1), 1-42, doi: <https://doi.org/10.1145/3691338>
- [13] Su, J., Jiang, C., Jin, X., Qiao, Y., Xiao, T., Ma, H., ... & Lin, J. (2024). Large language models for forecasting and anomaly detection: A systematic literature review. *arXiv preprint arXiv:2402.10350*, doi: <https://doi.org/10.1002/jmri.29247>.
- [14] Taye, M. M. (2023). Understanding of machine learning with deep learning: architectures, workflow, applications and future directions. *Computers*, 12(5), 91, doi: <https://doi.org/10.3390/computers12050091>.
- [15] Liu, R., Gupta, S., & Patel, P. (2023). The application of the principles of responsible AI on social media marketing for digital health. *Information Systems Frontiers*, 25(6), 2275-2299, doi: <https://doi.org/10.1007/s10796-021-10191-z>.
- [16] Baradaran, M., & Bergevin, R. (2024). A critical study on the recent deep learning based semi-supervised video anomaly detection methods. *Multimedia Tools and Applications*, 83(9), 27761-27807, doi: <https://doi.org/10.63313/JCSFT.9001>.
- [17] Divya Sharma, Y.K. Prajapati, and R. Tripathi, "Success Journey of Coherent PM-QPSK Technique with Its Variants: A Survey," *IETE Technical Review*, vol. 37, no. 1, pp. 36-55, 2020.
- [18] Shafi, M., Lashkari, A. H., Rodriguez, V., & Nevo, R. (2024). Toward generating a new cloud-based Distributed Denial of Service (DDoS) dataset and cloud intrusion traffic characterization. *Information*, 15(4), 195, doi: <https://doi.org/10.3390/info15040195>.
- [19] Berahmand, K., Daneshfar, F., Salehi, E. S., Li, Y., & Xu, Y. (2024). Autoencoders and their applications in machine learning: a survey. *Artificial intelligence review*, 57(2), 28, doi: <https://doi.org/10.1007/s10462-023-10662-6>.
- [20] Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *J. Sci. Technol*, 11, 001-024, doi: <https://doi.org/10.53022/oarjst.2024.11.1.0060>.
- [21] Xing, L., Li, S., Zhang, Q., Wu, H., Ma, H., & Zhang, X. (2024). A survey on social network's anomalous behavior detection. *Complex & Intelligent Systems*, 10(4), 5917-5932, doi: <https://doi.org/10.1007/s40747-024-01446-8>.
- [22] Liu, R., Shi, J., Chen, X., & Lu, C. (2024). Network anomaly detection and security defense technology based on machine learning: A review. *Computers and Electrical Engineering*, 119, 109581, doi: <https://doi.org/10.1016/j.compeleceng.2024.109581>.
- [23] Qiao, H., Tong, H., An, B., King, I., Aggarwal, C., & Pang, G. (2025). Deep graph anomaly detection: A survey and new perspectives. *IEEE Transactions on*

- Knowledge and Data Engineering, pp 5106 – 5126, doi:
<https://doi.org/10.1109/TKDE.2025.3581578>.
- [24] Rane, N., Choudhary, S. P., & Rane, J. (2024). Ensemble deep learning and machine learning: applications, opportunities, challenges, and future directions. *Studies in Medical and Health Sciences*, 1(2), 18-41, doi:
<https://doi.org/10.48185/smhs.v1i2.1225>.
- [25] Iqbal, A., Amin, R., Alsubaei, F. S., & Alzahrani, A. (2024). Anomaly detection in multivariate time series data using deep ensemble models. *Plos one*, 19(6), e0303890, doi: 10.1371/journal.pone.0303890.
- [26] Lapid, S., Kagan, D., & Fire, M. (2023). Co-membership-based generic anomalous communities' detection. *Neural Processing Letters*, 55(5), 5619-5651, doi:
<https://doi.org/10.1007/s11063-022-11103-1>.
- [27] Veeram, S. B., Satish, A. R., Tupakula, S., Chinnam, Y., Prakash, K., Bansal, S., & Faruque, M. R. I. (2025). Design of an integrated model with temporal graph attention and transformer-augmented RNNs for enhanced anomaly detection. *Scientific Reports*, 15(1), 2692, doi: <https://doi.org/10.1038/s41598-025-85822-5>.
- [28] Huang, H., Wang, P., Pei, J., Wang, J., Alexanian, S., & Niyato, D. (2025). Deep learning advancements in anomaly detection: A comprehensive survey. *IEEE Internet of Things Journal*, pp 1-1, doi: <https://doi.org/10.1109/JIOT.2025.3585884>.
- [29] Liu, J., Liu, Y., Lin, J., Li, J., Cao, L., Sun, P., ... & Leung, V. C. (2025). Networking systems for video anomaly detection: A tutorial and survey. *ACM Computing Surveys*, 57(10), 1-37, doi: <https://doi.org/10.1145/3729222>.
- [30] Bhatti, U. A., Tang, H., Wu, G., Marjan, S., & Hussain, A. (2023). Deep learning with graph convolutional networks: An overview and latest applications in computational intelligence. *International Journal of Intelligent Systems*, 2023(1), 8342104, doi: <https://doi.org/10.1155/2023/8342104>.
- [31] Fan, H., Wang, R., Huang, X., Zhang, F., Li, Z., & Su, S. (2024). Deep joint adversarial learning for anomaly detection on attribute networks. *Information Sciences*, 654, 119840, doi: <https://doi.org/10.1016/j.ins.2023.119840>.
- [32] Khan, W., Mohd, A., Suaib, M., Ishrat, M., Shaikh, A. A., & Faisal, S. M. (2025). Residual-enhanced graph convolutional networks with hypersphere mapping for anomaly detection in attributed networks. *Data Science and Management*, 8(2), 137-146, doi: <https://doi.org/10.1016/j.dsm.2024.09.002>.
- [33] Dash, A., Ye, J., & Wang, G. (2023). A review of generative adversarial networks (GANs) and its applications in a wide variety of disciplines: from medical to remote sensing. *IEEE Access*, 12, 18330-18357, doi:
<https://doi.org/10.1109/ACCESS.2023.3346273>.
- [34] Rane, N., Choudhary, S. P., & Rane, J. (2024). Ensemble deep learning and machine learning: applications, opportunities, challenges, and future directions. *Studies in Medical and Health Sciences*, 1(2), 18-41, doi:
<https://doi.org/10.48185/smhs.v1i2.1225>.
- [35] Ginni, G. R., & Lade, S. C. (2025). A Learning-Based Ensemble Algorithm with Optimal Selection for Outlier Detection. *Informatica*, 49(14), doi:
<https://doi.org/10.31449/inf.v49i14.7439>.
- [36] Nur-A-Alam, M., Nasir, M. K., Ahsan, M., Based, M. A., Haider, J., & Kowalski, M. (2023). Ensemble classification of integrated CT scan datasets in detecting COVID-19 using feature fusion from contourlet transform and CNN. *Scientific Reports*, 13(1), 20063, doi: <https://doi.org/10.1038/s41598-023-47183-9>.
- [37] Oladejo, A. O., Sch, J. W. M., Oluwabukunmi, F., Olufemi, D., McClure, J. W., Oladipo, K., ... & Lateef, A. Smart Spectrum Intelligence: AI-Guided Quantum Sensing in

- Terahertz-Enabled Broadband Networks, Volume 14–Issue 06, 181 – 206, 2025, ISSN: -2319–8656 doi: <https://doi.org/10.7753/IJCATR1406.1012>.
- [38] Berahmand, K., Daneshfar, F., Salehi, E. S., Li, Y., & Xu, Y. (2024). Autoencoders and their applications in machine learning: a survey. *Artificial intelligence review*, 57(2), 28, doi: <https://doi.org/10.1007/s10462-023-10662-6>.
- [39] Vishnu Shankar, S., Naffees Gowsar, S. R., & Manjubala, M. (2025). Variational Autoencoders (VAEs). In *Revolution with Generative AI: Trends and Techniques* (pp. 43-64). Cham: Springer Nature Switzerland, doi: https://doi.org/10.1007/978-3-031-91660-1_3.
- [40] Chaudhary, A., Rastogi, R., Mattoo, A., Kumar, P., Kumari, T., & Dubey, D. (2025). Generative Adversarial Networks (GANs). *Generative AI: Disruptive Technologies for Innovative Applications*, 29-55, doi: <https://doi.org/10.1002/9781394302932.ch2>.
- [41] Lagogiannis, I., Meissen, F., Kaissis, G., & Rueckert, D. (2023). Unsupervised pathology detection: a deep dive into the state of the art. *IEEE transactions on medical imaging*, 43(1), 241-252, doi: <https://doi.org/10.1109/TMI.2023.3298093>.
- [42] Bekkair, A., Bellaouar, S., & Oulad-Naoui, S. (2025). Unsupervised graph attention autoencoder clustering-oriented for community detection in attributed networks. *International Journal of Data Science and Analytics*, 1-14, doi: <https://doi.org/10.1007/s41060-025-00800-4>.
- [43] Tian, C., Zhang, F., & Wang, R. (2024). Adversarial regularized attributed network embedding for graph anomaly detection. *Pattern Recognition Letters*, 183, 111-116, doi: <https://doi.org/10.1016/j.patrec.2024.05.004>.
- [44] Li, H., & Li, Y. (2023). Anomaly detection methods based on GAN: a survey. *Applied Intelligence*, 53(7), 8209-8231, doi: <https://doi.org/10.1007/s10489-022-03905-6>.
- [45] Rajmohan, R., Kumar, T. A., Sandhya, S. G., & Hu, Y. C. (2024). R-GCN: A residual-gated recurrent unit convolution network model for anomaly detection in blockchain transactions. *Multimedia Tools and Applications*, 83(40), 87527-87551, doi: <https://doi.org/10.1007/s11042-023-17942-x>.
- [46] Al-Tameemi, I. K. S., Feizi-Derakhshi, M. R., Pashazadeh, S., & Asadpour, M. (2024). A comprehensive review of visual–textual sentiment analysis from social media networks. *Journal of Computational Social Science*, 7(3), 2767-2838, doi: <https://doi.org/10.1007/s42001-024-00326-y>.
- [47] Jain, S., & Sinha, A. (2023). TriBeC: identifying influential users on social networks with upstream and downstream network centrality. *International Journal of General Systems*, 52(3), 275-296, doi: <https://doi.org/10.1080/03081079.2023.2194642>.