IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 1 August 2022, accepted 15 August 2022, date of publication 24 August 2022, date of current version 2 September 2022.
Digital Object Identifier 10.1109/ACCESS.2022.3201332

RESEARCH ARTICLE

DVAEGMM: Dual Variational Autoencoder With Gaussian Mixture Model for Anomaly Detection on Attributed Networks

WASIM KHAN[1], MOHAMMAD HAROON[2], AHMAD NEYAZ KHAN[1], (Member, IEEE), MOHAMMAD KAMRUL HASAN[3], (Senior Member, IEEE), ASIF KHAN[1], (Member, IEEE), UMI ASMA MOKHTAR[3], AND SHAYLA ISLAM[4], (Senior Member, IEEE)
[1]Department of Computer Application, Integral University, Lucknow 226026, India
[2]Department of Computer Science and Engineering, Integral University, Lucknow 226026, India
[3]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Malaysia
[4]Institute of Computer Science and Digital Innovations, UCSI University, Kuala Lumpur 56000, Malaysia

Corresponding authors: Mohammad Kamrul Hasan (mkhasan@ukm.edu.my), Shayla Islam (shayla@ucsiuniversity.edu.my), and Mohammad Haroon (haroon@iul.ac.in)

This work was supported by Universiti Kebangsaan Malaysia under Grant GUP-2019-061 and Grant FRGS/1/2020/ICT03/UKM/02/6.

ABSTRACT A significant aspect of today's digital information is attributed networks, which combine multiple node attributes with the basic network topology to extract knowledge. Anomaly Detection on attributed networks has recently drawn significant attention from researchers and is widely used in several high-impact areas. Most current approaches focus on shallow learning methods such as community analysis, ego network or selection of subspace method. These approaches have network sparsity and data nonlinearity problems, and they do not even capture the intricate relationships between various information sources. Deep learning approaches like graph autoencoders are utilized to perform anomaly detection through obtaining node embeddings while dealing with the network nonlinearity and sparsity issues. However, they suffer from the problem of ignoring the latent codes' embedding distribution, which results in poor representation in many instances. In this paper, we propose a new framework called DVAEGMM to detect anomalies on attributed networks. First, our framework utilizes a dual variational autoencoder for capturing the complex cross-modality relationships between node attributes and network structure, like vanilla autoencoders, but it also considers the potential data distribution and makes use of a generative adversarial network (GAN) for an adversarial regularization approach. An adversarial mechanism makes the encoder make more accurate estimates of how potential features might be distributed. As a result, decoders can make graphs that are more like the original graph. Each input data point is represented by a low-dimensional representation and a probability of reconstruction by the algorithm. Lastly, the Gaussian Mixture Model, a distinct estimation network, is used to approximate the latent vector density, resulting in the detection of anomalies from measuring sample energy. They are trained jointly as an end-to-end framework. DVAEGMM helps in the simultaneous optimization of the mixture model, generative adversarial network, and variational autoencoder parameters. The joint optimization balances the reconstruction probability, the latent representation density approximation, and regularization. Extensive experiments on attributed networks prove that DVAEGMM significantly beats the existing methods, proving the efficiency of the presented approach. The AUC scores of our proposed framework for the BlogCatalog, Flickr, Enron, and Amazon datasets are 0.89380, 0.87130, 0.72480, and 0.75102, respectively.

INDEX TERMS Anomaly detection, attributed networks, deep learning, dual variational autoencoder, Gaussian mixture model, graph convolution network, unsupervised learning, generative adversarial network.

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Wei.

I. INTRODUCTION

Today, social networks are becoming an integral part of people's lives, allowing them to communicate and interact on a global level with those who share common values, views, and perspectives. People use social networking websites such as Twitter, Facebook, Myspace, Flickr, etc. to build professional and personal networks, gather valuable information, and exchange factual personal information with those around them [1], [2]. Anomalies on social networking sites pertain to odd and frequently illegal user behavior. All mainstream methods for anomaly detection assume that the samples are distributed uniformly and independently. However, in several real situations, cases are frequently linked to one another, forming a complicated network [3]. In the past few years, the topic of attributed anomaly detection in complicated networks has grown in popularity as a research topic. Compared to normal networks, which only use topology information to identify anomalies, attributed networks encode a wide variety of attribute characteristics for each node.

In the current world, attributed networks seem to be everywhere. Instead of observing interactions among nodes only, attributed networks contain a large set of characteristics or features for each node [4], [5]. Attributed networks are widely utilized to describe many complex systems because of the affinity between nodal properties and network architecture. There has been a significant increase in ongoing research to detect anomalies in attributed networks, which is a very critical problem due to its profound impacts in a wide range of real-world applications, including cyber-attack tracking in communications systems, social media spam detection, and fraud prevention, to name a few [6], [7], [8]. Attributed network anomaly detection is incredibly hard due to the consideration of attributes and structure both. Several methods for detecting anomalies in attributed networks have been presented recently. Many methods attempt to find abnormalities unsupervised since obtaining ground-truth anomalies is outrageously costly [9].

Some of them use only community-level structural information to conduct anomaly detection or by monitoring the adequacy of linked subgraphs [10], [11], [12]. A few of these investigate how to find feature-level anomalies in a subspace by selecting node features [13], [14]. Graph autoencoder based methods [4], [15], [16] and residual analysis-based methods [17], [18], use network reconstruction or residual assessment to detect node irregularities because they assume that anomalies will not be estimated by other reference nodes. Despite the fact that these innovative methods have had a lot of success, they still have some flaws. In high-dimensional, complex datasets, some of them rely on shallow practices that can't keep up with the numerous interactions between structure and attributes. A complicated issue in anomaly detection is combining the network's topology with nodes attributes. Established approaches to detect anomalies have relied heavily on structure-based (or community-based) methodologies [19], [20], [21]. As a result, it cannot be utilized for attributed network anomaly detection. Aside from this, the attribute-based model implies that highly complicated anomalies are present in the subgroup depending on user attributes. However, the traditional attribute-based approaches take into account the structure and attributes of the network only [22], [23], which leads to a lower detection rate. Furthermore, the description of anomalies varies across fields, indicating that there is no generally agreed anomaly definition. Furthermore, the description of anomalies varies across fields, indicating that there is no universally accepted definition of an anomaly [24], [25]. So, it's important to deal with the following challenges:

1) Data nonlinearity and network sparsity. The links and nodes' characteristics are extremely nonlinear, and the network's topology is extremely sparse in the current world [26].

2) *Unlabeled anomalies in the datasets.* The ineffectiveness of detecting anomalies through classification is exacerbated by the misclassification of abnormal and normal data. So, the methods to detect abnormalities are needed to find anomalies in attributed networks in an unsupervised way that is quick and easy [27].

3) *Homophily-based network smoothing.* It is possible to detect network anomalies by smoothing networks based on the homophily assumption. Unfortunately, these methods aren't very good at detecting anomalies because the results could be too smooth, making it hard to tell the difference between the majority of normal nodes and the abnormal ones.

4) *The deterministic nature of autoencoders.* Even though the autoencoder represents the latent variables as deterministic mappings, it is insufficient to deal with variation.

5) *Heterogeneous input and problems in setting an appropriate and precise reconstruction error threshold.* When the input variables are heterogeneous, it is challenging to compute anomaly scores using autoencoder-based anomaly detection. It is necessary to use a weighted sum. The problem is that there is no universally objective approach for determining the proper weight because the weights will differ based upon the data. Furthermore, once the weights have been determined, setting the reconstruction error threshold is time-consuming.

To address these challenges, we present the Dual Variational Autoencoder with Gaussian Mixture, DVAEGMM, a new framework to detect anomalies on attributed networks. The primary objective of our framework is to enforce the learnt latent embedding to match a prior distribution while simultaneously minimizing the reconstruction errors of the topological structure and node attributes. The following are the key aspects of this paper:

- Using a dual variational autoencoder to capture network sparsity and nonlinearity, DVAEGMM solves two problems at once: it captures cross-modality interactions between topological structure and node features, and it solves the problem of unlabeled anomalies.
- Our approach accomplishes joint learning on node features and network structure while adhering to anomaly detection requirements and eliminating homophily and over-smoothing issues.
- A Dual Variational Autoencoder based embedding framework is proposed that is based on probabilities instead of reconstruction errors, and the probabilities seem to be more systematic and objective than

reconstruction errors and therefore do not need model-dependent thresholds. As a stochastic generative model, VAE is also able to provide calibrated probabilities for dealing with the variability that is found in autoencoder based models.

- We include an adversarial component in the dual variational graph autoencoder to ensure that encoded data is distributed uniformly. This component would identify if the data comes from a low-dimensional representation of the graph network or from the genuine distribution of samples. Using a discriminator, the encoder can learn a better representation of the graph by creating low-dimensional variables with distributions that are closer to the distribution.
- We leveraged the Gaussian Mixture Model (GMM) across the learned low-dimensional space to tackle the density analysis problem for inputs having complicated structures. Our model combines the power of dimensionality reduction with density analysis. End-to-end optimization of both the deep autoencoder and the mixture model parameters has been achieved.
- In a unified framework, the dual variational autoencoder learning, adversarial regularization learning, and gaussian mixture models are jointly optimized such that each can complement the other and ultimately result in better anomaly detection.

The rest of this work is structured in the following manner. An analysis of the relevant literature on attributed network anomaly detection is provided in Section 2. The problem of anomaly detection on attributed networks is clearly stated in Section 3. Section 4 describes the preliminaries. Section 5 presents the proposed DVAEGMM anomaly detection framework in detail. Section 6 presents empirical proof of DVAEGMM's effectiveness for detecting anomalies in real-world networks using several assessment measures. Finally, in Section 7, we come to a logical conclusion.

II. RELATED WORK

Traditional anomaly detection and attributed anomaly detection are discussed in relation to each other in this section.

A. TRADITIONAL ANOMALY DETECTION

It has recently been found that most of the classic methods of anomaly detection use unsupervised approaches to discover anomalies in cases where there is just a limited number of labelled anomalous data and plenty of unlabeled data [28]. Conventional approaches to identifying anomalies are generally divided into clustering-based, reconstruction-based, and one-class classification-based methods. Data density is estimated using methods based on clustering [29], [30], [31]. Normal data is clustered to discover anomalies using a two-step process, starting with dimensionality reduction. Approaches based on reconstruction assume that anomalies cannot be adequately recreated from the latent representations, such as PCA-based algorithms [32], [33] and autoencoder-based methods [4], [15], [34], [35] that employ anomaly scores to detect them. For anomaly detection, one-class classification-based approaches [36], [37], [38], [39] differ from the previously described two categories in that they try to identify the line between normal and abnormal samples. In spite of their effectiveness in the typical anomaly detection area, these algorithms fail to scale effectively to graph data, because topological correlations between sample points are crucial. As a result, the detection of anomalies in graph data remains an open-ended issue.

B. ADVERSARIAL MODELS

Our method's adversarial approach relies on GAN [40], in which a generator and a discriminator compete in a minimax game to optimize each other. It was GraphGAN [41] that used the adversarial approach for graph learning for the first time. By imposing the distribution of the real data as a prior distribution on existing network embedding algorithms, ANE [42] views embedding vectors as the generated result and employs GAN as an additional regularization term. By incorporating the adversarial process into the autoencoder, Makhzani *et al.* presented an adversarial autoencoder to learn the latent embedding [43]. But this approach is intended for basic data, not graph data. Many adversarial models have been successful in computer vision, but the graph-structured data cannot be handled by them directly.

C. ANOMALY DETECTION ON ATTRIBUTEDNETWORKS

Auxiliary attribute data is common in real-world networks, hence attempts to identify anomalies in attributed networks have increased in recent years. For anomaly identification on attributed networks, four main categories may very well be outlined: community assessment, subspace identification, residual analysis, and deep learning techniques [44]. Community or ego-network anomaly detection approaches fall into the category of community analysis-based anomaly detection. CODA [10], for example, uses a cohesive predictive model to simultaneously detect communities and identify community abnormalities. AMEN [11] analyses each node's ego-network information and finds abnormal areas in attributed networks. In addition, there is a family of approaches that aim to identify anomalous nodes in a subspace of node characteristics [45], [46]. For example, GOutRank [45] uses subspace cluster analysis to identify anomalies in attributed networks. Prior to anomaly detection, ConSub [46] employs the selection method to choose subspaces. Residual analysis has also been a popular method for determining the abnormality of nodes in attributed networks, in addition to those already discussed. An anomaly is detected by RADAR [17] when residual feature data and its compatibility with the network show behavior that differs significantly from the normal. ANOMALOUS [18] is a combined anomaly detection system that uses matrices CUR reduction with residual extrapolation to maximize attribute selection and anomaly detection. Besides development, these approaches are constrained by inherent shallow modes and therefore unable to handle crucial attributed network challenges like network sparseness, data nonlinearity, and complicated modality connections among different data sources.

A lot of work has gone into building deep neural networks to detect anomalies on an attributed network due to the growing interest in deep learning research. Network embedding methods that assign nodes in a network to low-dimensional representations, are also getting a lot of attention since low dimensional representations can efficiently retain the topological structure [47], [48], [49]. Anomaly aware embedding on attributed networks is now the subject of several studies that take into account both network embedding and deep learning [4], [15], [16], [19], [38], [50], [51], [52], [53], [54]. Complex connections between a network's topology and node features are observed in AnomalyDAE [4], and both structural and attribute data are used to assess anomalies. A unique graph convolution encoder and decoder in SpecAE [16] to learn each node's local representations. The energy of each node's latent representation in the Gaussian mixture model determines its suspiciousness rating. DeepAD [19], an innovative hybrid embedding method, takes advantage of the strong non-linearity in both attributes and network structure to detect anomalies using reconstruction errors. A DUAL-SVDAE [38] is composed of a structure autoencoder and an attribute autoencoder to learn the embedding representation of the node, followed by a dual-hypersphere training algorithm for learning two normal node hyperspheres. Using GCN, the input network is reduced into low-dimensional embedding representations by DOMINANT [15], which it then uses to reconstitute the topological structure and nodal characteristics. Rather than reconstruction error, ResGCN [50] uses residual information from the input network to rank anomalies. GCN captures network sparsity and nonlinearity. Deep neural networks capture residual information, and residual-based attention lowers the impact of anomalous nodes.

III. NOTATIONS AND PROBLEM STATEMENT

In this section, we describe the common notations and concepts used in this paper. Table 1. summarizes the most significant notations.

Definition: An attributed network $\mathcal{G} = (\mathcal{V}, \varepsilon, \mathrm{X})$ contains: (1) Node Set $\mathcal{V} = \{v_1, v_2, \ldots v_N\}$, where $|\mathcal{V}| = \mathrm{N}$; (2) Edge set E, where $|\varepsilon| = \mathrm{E}$, and (3) Attribute Set $\mathrm{X} \in \mathbb{R}^{N\mathrm{x}M}$, where the r$^{\text{th}}$ row of X(r = 1,2,...M) represents the information for the attributes of the r$^{\text{th}}$ node in M dimension size. The Graph links are illustrated by an adjacency matrix $\mathrm{A} \in \mathbb{R}^{N\mathrm{x}N}$, that stores only binary values (i.e., 0 or 1) where $\mathrm{A}_{ij} = 1$ denoting a link between the node i and node j. Attributes latent embedding of nodes is represented as $\mathrm{Z}^{\mathcal{A}} \in \mathbb{R}^{N\mathrm{x}L}$ and $\mathrm{Z}^{\mathrm{S}} \in \mathbb{R}^{N\mathrm{x}L}$ respectively, where the embedding space dimension size is L.

Problem Statement: For a given attributed network G with X and A as the node attributed matrix and adjacency matrix respectively, anomaly detection for an attributed network is to find and rank all the rare nodes according to how they differ markedly from most of the other reference nodes from the perspective of both the attribute information and topological structure.

TABLE 1. Notations.

Notation	Description
G	Attributed Network
V	Node Set
E	Edge Set
X	Attribute Set
N	No of Nodes
M	Attribute Dimension
L	Embedding Dimension
$\mathrm{A} \in \mathbb{R}^{N\mathrm{x}N}$	Adjacency Matrix
$\mathrm{X} \in \mathbb{R}^{N\mathrm{x}M}$	Attribute Set
$\mathrm{Z}^{\mathcal{A}} \in \mathbb{R}^{N\mathrm{x}L}$	Node Embedding in Attribute Space
$\mathrm{Z}^{\mathrm{S}} \in \mathbb{R}^{N\mathrm{x}L}$	Node Embedding in Structure Space
$\mathrm{W}^{(l)}$	Trainable weight matrix in l-th layer

IV. PRELIMINARIES

A. GRAPH CONVOLUTIONAL NETWORKS (GCN)

GCNs are convolutional neural networks that intend to perform directly on graphs. The GCN, in particular, illustrates the topology and the interconnections among features and nodes through the node adjacent matrix A and the feature matrix X. It uses spectral convolution to apply the convolutional operation on graph data to generate the transformation:

$$\mathrm{Z}^{(l+1)} = \mathrm{f}\left(\mathrm{Z}^{(l)}, \mathrm{A} \mid \mathrm{W}^{(l)}\right) \tag{1}$$

where $\mathrm{Z}^{(l)}$ and $\mathrm{Z}^{(l+1)}$ are the convolutional input and output respectively in layer l. $\mathrm{W}^{(l)}$ is the layer-specific trainable weight matrix. The spectral convolution function is used to express each layer as follows:

$$\mathrm{f}\left(\mathrm{Z}^{(l)}, \mathrm{A} \mid \mathrm{W}^{(l)}\right) = \emptyset\left(\hat{D}^{-\frac{1}{2}}\hat{A}\hat{D}^{-\frac{1}{2}}\mathrm{Z}^{(l)}\mathrm{W}^{(l)}\right) \tag{2}$$

where $\hat{A} = \mathrm{A} + \mathrm{I}$, D and I are diagonal degree and an identity matrix, respectively. $\emptyset$ is an activation function and, based on previous research, we chose ReLU $(\cdot) = \max(0, \cdot)$ as the activation function [55]. $\mathrm{Z}^{(0)}$ is set as $\mathrm{X} \in \mathbb{R}^{N\mathrm{x}M}$ for the first layer. Therefore,

$$\mathrm{Z}^{(1)} = \emptyset\left(\hat{A}\mathrm{X}\mathrm{W}^{(0)}\right) \tag{3}$$

B. AUTOENCODERS (AE)

Autoencoder based Anomaly detection approaches have recently gained a lot of attention due to their ability to extract extremely non-linear connections. An autoencoder is a type of deep neural network that uses unsupervised learning to learn low-dimensional embedding representations of data. It has demonstrated convincing learning results in different areas. An encoder and a decoder are the main components

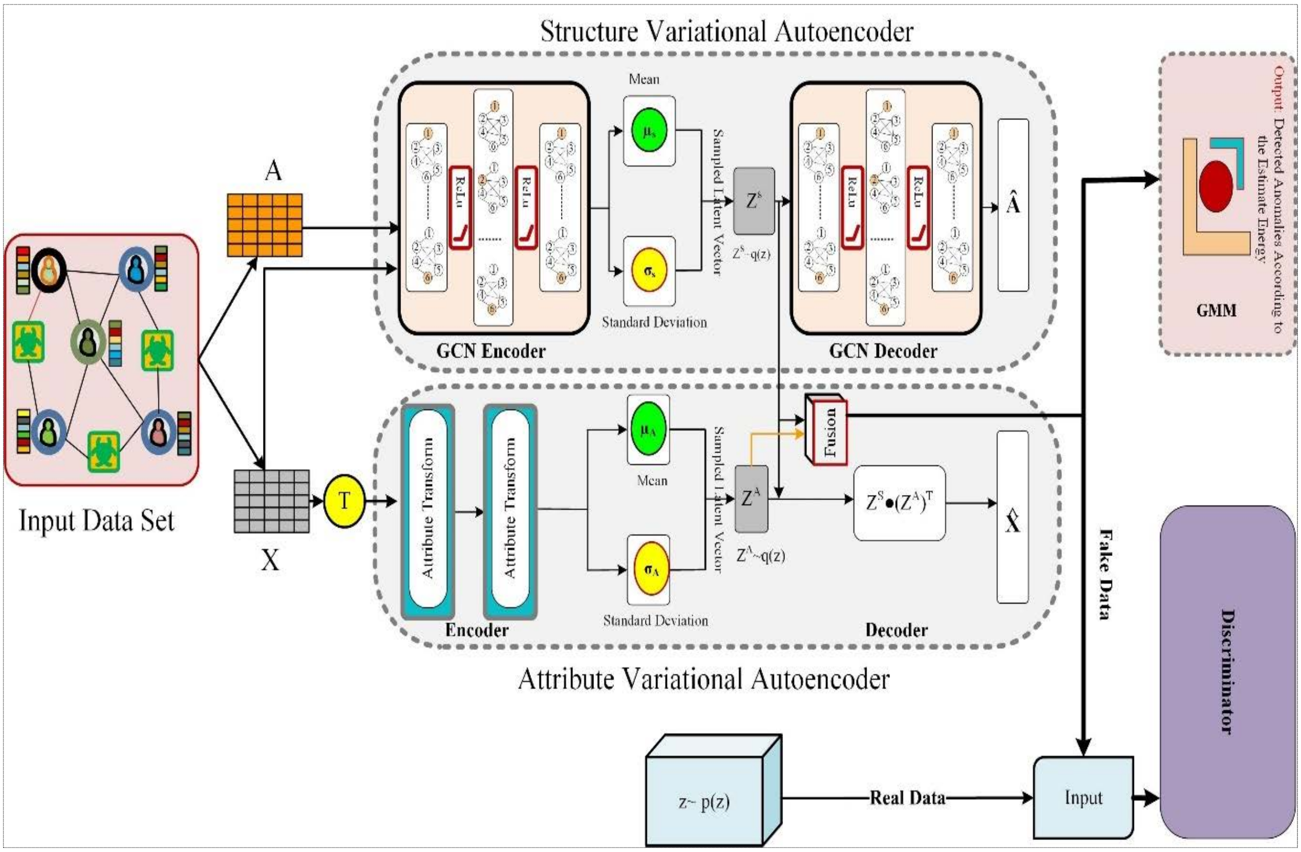

FIGURE 1. Proposed Framework DVAEGMM.

of an autoencoder. The node embeddings are obtained by the encoder using the attribute data and network structure as input. The decoder then uses these node embeddings as input to reconstruct the attribute data and also the network structure. Anomalies are then termed as inconsistencies between input and the reconstructed network [56], [57].

Generally, two parts make up the neural network. One is the encoder function $enc_w(.)$, and the other is the decoder function $dec_u(.)$. It tries to learn a code from the input by going through a pair of encoding and decoding processes.

$$\hat{X} = dec_u(enc_w(\mathrm{X})) \tag{4}$$

where X is the input data and $\hat{X}$ is the reconstructed input. The main concept is to find $enc_w(.)$ and $dec_u(.)$ so that the difference between X and $\hat{X}$ is as small as possible [58].

$$\min_{u,w} ||X - dec_u(enc_w(\mathrm{X}))|| \tag{5}$$

C. VARIATIONAL AUTOENCODERS (VAE)

Approaches that use autoencoders to extract highly non-linear connections for anomaly detection have recently attracted a lot of attention. In general, AE encoders provide discrete outcomes, and train a function to explicitly map the input results in coping with high-dimensional data is challenging. However, generating an embedding by integrating node semantics data and network topology is difficult, because the combined data has a significantly larger dimension than network topology alone [59]. To overcome this limitation, the Variational Auto-Encoder (VAE) was developed by incorporating a priori constraints into the embedding learning process. Rather than learning the discrete latent variables explicitly as seen in AE, the VAE encoder implies a posterior distribution of continuous latent variables based on a given input. So, it is preferable to handle complex and high-dimensional data, such as social networks [49], [60], [70].

The variational autoencoder (VAE) and its variants have seen a huge success, particularly in the creation of realistic data. Its structure is quite similar to that of a standard autoencoder. VAE models work as generative models, too, because they can produce new data from existing data. Initially, VAEs were intended for image analysis methods like denoising [61], but research on these models has expanded to various other areas, including anomaly detection. VAEs use in anomaly detection problems is anticipated since the primary concept of this approach is associated with a lower-dimensional representation, which has already been used in many anomaly detection methods [15], [16].

When utilizing variational autoencoders, the main advantage is that they are probabilistic. By combining the generative model P(X|z) with an inference model Q(z | X), the learning representation issue can be solved as a variational inference problem and comprehending latent representation of the data [62]. Each input data point is postulated to have a Gaussian distribution. It is possible to encode a Gaussian multivariate latent variable or hidden variable from the input x using the encoder $q_\theta(z\,|\,x)$. The decoder $p_\emptyset(x\,|\,z)$ takes samples for each data input and reconstructs the input x in x′. The basic concept is to determine the likelihood that x' was obtained through z. Variational lower bound optimization is done as follows in the variational graph encoder:

$$L = \mathbb{E}_{q(z\,|\,x)}\left[\log p\,(x\,|\,z)\right] - KL[q\,[z|x]\,||p\,(z)] \tag{6}$$

In the equation, KL stands for the Kullback-Leibler difference. $KL[q\,[z|x]\,||p\,(z)]$ is the regularization term.

D. GENERATIVE ADVERSARIAL NETWORKS (GAN)

A generative adversarial network (GAN) is a commonly employed deep generative model. The fundamental principle of GAN is to train a generator G and a discriminator D so that the generator learns to confuse the discriminator and the discriminator learns to differentiate between real and fake samples. Training improves both the discriminator's ability to discriminate between real and fake data and the generator's ability to produce realistic data, eventually to the point where the discriminator is no longer able to do so. This happens as a result of the generator's improved ability to produce data that resemble the genuine data seen in the training dataset. As a result, a GAN has been effectively trained and can now produce data that resembles those in the training set. The following minmax game is the objective function of GAN.

$$\min_G \max_D E_{x\sim p_{data}}\left[\log D\,(x)\right] + E_{z\sim p_z}\left[\log\left(1 - D(G\,(z)\right)\right] \tag{7}$$

E. GAUSSIAN MIXTURE MODELS (GMM)

In this model, we suppose that there exist a definite number of Gaussian distributions, each of which corresponds to a cluster. Consequently, a Gaussian Mixture Model is used to group together data points from a given distribution. In fact, these are probability models that spread out data points into different clusters using a soft clustering strategy. The main parameters that make up a Gaussian function are its mean, covariance, and mixing probability. The mean μ, and covariance Σ, are used to represent the center and width of the component, respectively, while the mixing probability π specifies the size of the Gaussian function. In general, the Gaussian density function can be expressed in the form of:

$$\mathcal{N}\,(x\,|\,\mu,\,\Sigma) = \frac{1}{2\pi^{(D/2)}\,|\Sigma|^{1/2}}\exp\left(-\frac{1}{2}\,(x-\mu)^T\,\Sigma^{-1}\,(x-\mu)\right) \tag{8}$$

where x specifies the data points and D represents the number of dimensions of each data point.

V. PROPOSED FRAMEWORK

The DVAEGMM anomaly detection framework for attributed networks is described in this section, which combines a dual variational autoencoder with a Gaussian mixture model. Figure 1 is an illustration of the DVAEGMM pipeline. This framework is divided into four significant components: a structure reconstruction variational autoencoder, an attribute reconstruction variational autoencoder, adversarial model, and a Gaussian Mixture model.

A. STRUCTURE RECONSTRUCTION MODEL

To obtain a significant number of prominent high-level node features, the structure variational autoencoder first converts the apparent node attribute X into a low-dimensional latent representation Z^S. The structure variational autoencoder uses a GCN encoder to learn the nodes' embedding and, subsequently, a GCN decoder is used to reconstruct the structure. For the encoding process, we use two-layer GCN to produce the parameters μ and σ:

$$\mu = GCN_\mu\,(X, A)\,, \tag{9}$$

$$\log\sigma = GCN_\sigma\,(X, A) \tag{10}$$

where μ and $\log\,\sigma$ are the matrices corresponding to μ_n and σ_n respectively. μ_n and σ_n are the mean and standard deviation vector of node v_j′s embedding z_j. Following that, sampling is used to determine the latent variables $\mathcal{N}\,(\mu,\sigma)$. As a result, the inference model is:

$$q(Z^S|X, A) = \prod\nolimits_{i=1}^{n} q(z_i|X, A), \tag{11}$$

$$q(z_i|X, A) = \mathcal{N}(z_i|\mu_i, \mathrm{diag}\left(\sigma_i^2\right)) \tag{12}$$

here, $\mu = Z^{(2)}$ represents the mean vector z_i matrix. When reconstructing the network's structure, two graph convolutional layers are utilized. Embedding output from the encoder will be fed to the decoder as input, and the GCN decoder is defined as:

$$Z^D = f_{linear} Z^S, A|W_s^{(1)}) \tag{13}$$

$$\hat{A} = f_{linear} Z^D, A|W_s^{(2)}) \tag{14}$$

where Z^S is the encoder's learned embedding while Z^D and $\hat{A}$ are the decoder outputs for the first and second layer, respectively. The number of dimensions in D is equal to the number of nodes.

B. ATTRIBUTE RECONSTRUCTION MODEL

Normal nodes' latent embeddings are learned by only using the attribute matrix as input. Two non-linear feature transform layers are employed in the encoder of the attribute variational autoencoder to learn a non-linear feature mapping of the node attributes, rather than relying on the structure information, as is the case with the structure autoencoder. In this example, the observed attribute data is mapped to the latent embedding Z^A, using two non-linear feature transform layers.

$$Z^{A(1)} = f\left(X^T W_A^{(1)} + b^{(1)}\right) \tag{15}$$

$$Z^A = [\mu_A, \sigma_A] = Z^{A(1)} W_A^{(2)} + b^{(2)}) \tag{16}$$

where $[\mu_{\mathbf{A}}, \sigma_{\mathbf{A}}]$ are the posterior approximation distribution parameters while $\mathbf{W}_{\mathbf{A}}^{(1)}$, $\mathbf{W}_{\mathbf{A}}^{(2)}$ are trainable weights and $\mathbf{b}^{(1)}$, $\mathbf{b}^{(2)}$ are the biases in two layers.

Finally, node structure embeddings $\mathbf{Z}^{\mathbf{S}}$ and node attribute embeddings $\mathbf{Z}^{\mathbf{A}}$ are fed as input to a simply inner product decoder, which reconstructs the $\hat{\mathbf{X}}$ as follows:

$$\hat{\mathrm{X}} = Sigmoid\left(\mathrm{Z}^{\mathrm{S}}\left(\mathrm{Z}^{\mathrm{A}}\right)^{\mathrm{T}}\right) \tag{17}$$

Following the attribute encoder, a feature fusion module is also built to fuse the learnt node embeddings Z^{S} from structure space and Z^{A} from attribute space into a fused embedding Z^{F}, which is accepted as input by the GMM to capture the relationship between structure and attribute. Here's how the fusion procedure works:

$$\mathrm{Z}^{\mathrm{F}} = Fusion\left(\mathrm{Z}^{\mathrm{S}}, \mathrm{Z}^{\mathrm{A}}\right) = \mathrm{Z}^{\mathrm{S}} \bullet \mathrm{Z}^{\mathrm{A}} \tag{18}$$

The element-wise plus operator of two matrices, which adds the corresponding elements in the same position of the two matrices, is represented by the $\bullet$ operator.

C. ADVERSARIAL MODEL

The core concept of our approach is to use an adversarial training model to induce latent representation Z^{F} to match a prior distribution. There are two major components to our adversarial model: The dual variational autoencoders serve as the generator of the adversarial network. The generator tries to fool the discriminator by producing fake data (latent variables generated by the input data from the dual variational autoencoders). The discriminator's goal is to determine if the samples come from real data or are artificially generated. Data from the prior distribution p_z output is considered positive by the discriminator, while data from the latent variable z output is considered negative, and its cost function is defined as follows:

$$-\frac{1}{2}\mathrm{E}_{z\sim p_z}\log(D\left(\mathrm{Z}^{\mathrm{F}}\right) - \frac{1}{2}\mathrm{E}_x\log(1 - D\left(G\left(X, A\right)\right)) \tag{19}$$

D. ANOMALY DETECTION WITH GAUSSIAN MIXTURE MODEL

The estimate network uses GMM to do density estimation based on low-dimensional representations of input data. In the training phase, GMM parameters are calculated using an unspecified distribution φ, mean μ, and covariance $\sum$ of mixture components. The estimation network evaluates the likelihood/energy for samples without alternate techniques like EM. The estimate network estimates mixture membership for each instance using a multi-layered model. An estimation network predicts mixture component membership using low-dimensional representations z and the number of mixture components N as follows:

$$\mathrm{NO} = \mathrm{MLN}\left(\mathrm{Z}^{\mathrm{F}};\alpha_m\right) \tag{20}$$

$$\hat{\beta} = \mathrm{softmax}\left(\mathrm{NO}\right) \tag{21}$$

where O is the network output parameterized by α_m, and $\hat{\beta}$ represents a P-dimensional vector to predict the membership of a soft mixture component. GMM model parameters can be further estimated using sample set of N size with their membership prediction, $\forall 1 \leq p \leq P$.

$$\hat{\varphi}_p = \sum_{i=1}^{N} \frac{\hat{\beta}_{ip}}{N} \tag{22}$$

$$\hat{\mu}_p = \frac{\sum_{i=1}^{N} \hat{\beta}_{ip} z_i}{\sum_{i=1}^{N} \hat{\beta}_{ip}} \tag{23}$$

$$\hat{\sum}_p = \frac{\sum_{i=1}^{N} \hat{\beta}_{ip}(z_i - \hat{\mu}_p)\left(z_i - \hat{\mu}_p\right)^T}{\sum_{i=1}^{N} \hat{\beta}_{ip}} \tag{24}$$

where $\hat{\beta}_{\mathrm{i}}$ is the membership prediction for z_i and $\hat{\varphi}_p$, $\hat{\mu}_p$ and $\hat{\sum}_p$ are mixture probability, mean and covariance for component p, respectively. Sample energy can be calculated using the estimated parameters by

$$\mathrm{E}\left(\mathrm{z}\right) = -\log\left(\sum_{p=1}^{P} \hat{\varphi}_p \frac{\exp\left(-\frac{1}{2}\left(\mathrm{z}-\hat{\mu}_p\right)^T \hat{\sum}_p^{-1}\left(\mathrm{z}-\hat{\mu}_p\right)\right)}{\sqrt{\left|2\pi\hat{\sum}_k\right|}}\right) \tag{25}$$

where |. | is matrix determinant.

E. OBJECTIVE FUNCTION

The DVAEGMM objective function O(W) is generated as follows for a dataset of N samples:

$$\begin{aligned}
&\mathrm{O}\left(\mathrm{W}\right) \\
&= [\,(1-\theta)\,[\mathbb{E}_{q(\mathrm{Z}^{\mathrm{S}}|\mathrm{X},\mathrm{A})}(\log p(\mathrm{A}|\mathrm{Z}^{\mathrm{S}})] \\
&\quad +\theta[\mathrm{E}_{q(\mathrm{Z}^{\mathrm{A}}|\mathrm{X})} \\
&\quad \times\left(\log p(\mathrm{X}|\mathrm{Z}^{\mathrm{S}}, \mathrm{Z}^{\mathrm{A}})]] - \mathrm{KL}[(q\mathrm{Z}^{\mathrm{S}}|\mathrm{X}, \mathrm{A})||p(\mathrm{Z}^{\mathrm{S}}\right)] \\
&\quad -\mathrm{KL}[q(\mathrm{Z}^{\mathrm{A}}|\mathrm{X})||p\left(\mathrm{Z}^{\mathrm{A}}\right)] + [E_{x\sim p_{data}}\left[\log D\left(x\right)\right] \\
&\quad +E_{z\sim p_z}\left[\log\left(1 - D(G\left(z\right))\right)\right]] \\
&\quad +\frac{\gamma_1}{\mathrm{N}}\sum_{\mathrm{i=1}}^{\mathrm{N}} \mathrm{EN}(\mathrm{Z}_{\mathrm{i}}^{\mathrm{F}})+\gamma_2\sum_{\mathrm{p=1}}^{\mathrm{P}}\sum_{\mathrm{r=1}}^{\mathrm{d}}\frac{1}{(\sum_{pr})}
\end{aligned} \tag{26}$$

This objective function includes the following components:

- The first one is the loss function, which describes the dual variational autoencoder reconstruction error from both structure and attribute perspectives and θ is the parameter that regulates the balance between structure and attribute reconstruction.
- Second and third are KL divergence for structure and attribute variational autoencoders, respectively.
- The Forth component is used to jointly train the encoders of both variational autoencoders, and the discriminator via a minimax game such that they optimize each other.
- The fifth component EN (Z_{i}), represents the GMM estimation's sample energy of the latent representation Z_{i}, and models the probability that we could observe with

---

Algorithm 1 DVAEGMM Framework for Attributed Network Anomaly Detection

Input: An attributed network G, an attribute set $X \in \mathbb{R}^{N\text{x}M}$ and topology set $A \in \mathbb{R}^{N\text{x}N}$, with hyper-parameters θ, γ_1 and γ_2

Output: An L-node list with nodes ordered by normalcy.

1. Initialize O, θ, γ_1 and γ_2
2. k samples with normal behavior from n instances are chosen at random and used as training samples.
3. **for each** epoch = 1 to E do
4. Produce the structural space node embedding Z^S via Eq. (12);
5. Reconstruct A from the Z^S via Eq. (14);
6. Produce the attribute space node embedding Z^A via Eq. (16);
7. Reconstruct X from the Z^S and Z^A via Eq. (17);
8. Z^S and Z^A are fused into embedding Z^F via Eq. (18);
9. Update the adversarial model via Eq. (19);
10. Apply GMM on Z^F to get $\{\varphi, \mu, \sum\}$ via Eq. (22), (23) and (24);
11. Calculate the Objective function O according to (26);
12. Update the parameters $\{\varphi, \mu, \sum\}$ with backpropagation;
13. **end for**
14. As the normality score, estimate the sample energy of all n samples via Eq. (25);
15. Return the list of nodes L, sorted by normalcy score in decreasing order;

---

the input samples. We increase the likelihood of non-anomalous samples by reducing sample energy, and we identify samples with top-K high energy as anomalous.

- Sixth is covariance penalization, which penalizes the small values in the diagonal elements of the covariance matrix to solve the singularity problem in GMM.

Our proposed approach may be used to detect abnormalities in attributed networks after optimization of the objective function. The estimation energy in Eq. (25). is then used to evaluate the anomalous level of each node in our testing data. Nodes with higher rankings are more likely to be rated as anomalies. Our proposed approach is described in Algorithm 1.

VI. EXPERIMENTS

The performance of the DVAEGMM on various datasets is discussed in this part. Two of the most important evaluation tasks are anomaly detection performance analysis and model parameter sensitivity analysis. The four datasets are initially described in detail in this section. After that, the DVAEGMM is compared to the other baseline techniques, and the anomaly detection accuracy is given, as well as a comparison of the experimental data and analysis. Finally, we examine the experimental parameters' sensitivity.

A. DATASETS

In this paper, we perform experimentation on the following real-world attributed datasets: data with and without ground-truth anomalous labeling, in order to test the performance of our suggested approach. All networks have been extensively utilized in earlier research. Table 2. summarizes the detailed statistics of each dataset.

1) DATASETS WITHOUT GROUND-TRUTH ANOMALOUS LABELS

A BlogCatalog [15] is a website where bloggers can follow one another to create a social network. The blogger's features have been used to define the user and the blog, and the node attributes are composed of attribute information.

Flickr, like Instagram [63], is a photo-sharing website. People form social platform similar to BlogCatalog by connecting with each other. Tags, which reflect a user's interests, define their node attributes.

2) DATASET WITH GROUND-TRUTH ANOMALOUS LABELS

Enron [64] is an electronic mail communication system where edges denote the transfer of e-mails among individuals. Every node has 20 attributes that specify email content, such as the average content length and the number of people who receive mail. Spammers are considered anomalies, and this dataset is already widely used to detect anomalies.

Amazon is a copurchase network [45]. Each node has 28 attributes that describe various aspects of online commodities, such as price and rating. The term "anomalous nodes" refers to nodes that have the label "amazonfail."

We explicitly use the given labels to evaluate our approach for the networks that have ground truth anomaly labels. For unlabeled datasets, we must manually infuse anomalies into attributed networks for the evaluation task. To ensure a proper a common aberrant substructure in many specific circumstances in which a limited selection of nodes is significantly more clearly tied to each other than normal. As a result, after specifying the clique size as c, a total of r nodes is randomly picked from the network and connected all together, and then all the r nodes forming the clique are considered anomalies. This procedure is repeated indefinitely until the total number of c cliques has been generated. So, rxc are the total number of structural anomalies. An attribute perturbation method proposed by [66] is then used to find abnormalities viewed from the standpoint of an attribute. To verify that the attributed network contains an equivalent number of anomalies from structural and attribute perspectives, rxc nodes are chosen at random as attribute disruption targets. Then, additional t nodes are picked randomly from the network for each designated node n_i and the Euclidean distance between n_i and all the t nodes is computed. The node with the maximum distance is then elected as n_j, and the attribute X_j of the node

TABLE 2. Statistics of datasets.

Dataset	Vertices (V)	Edges (E)	Attributes (A)	Anomalies
BlogCatalog	5196	171743	8189	300
Flickr	7575	239738	12047	450
Enron	13533	176987	20	5
Amazon	1418	3695	28	28

n_j is changed to X_i of node n_i. Node n_j is regarded as the attribute anomaly. In our experiments, we also set r = 15 and c to 10 and 15 for BlogCatalog and Flickr, respectively, which are the same as [15] and [50].

B. EVALUATION INDICATORS

This paper evaluates the contribution of different anomaly detection methods using three commonly used evaluation indicators that have been extensively used in earlier anomaly detection methods [17], [18], [49], [67], [68], [69].

1) ROC-AUC

The ROC curve plots the true positive rate (an anomaly is identified as an anomaly) versus the false positive rate (normal is identified as anomalous) based on the ground truth and outcomes of detection. The AUC value represents the likelihood that a randomly picked anomalous node would be scored higher than a normal node. The approach is of high quality if the AUC value is close to one.

2) PRECISION@K

In order to quantify the percentage of true anomalies discovered by a specific detection scheme in its highest K ranked nodes, we use Precision@K, which ranks the nodes according to their anomalous scores.

$$Precision@K = \frac{|TRAnobyMethod| \cap |RankAno|}{|RankAno|} \tag{27}$$

where TRAnobyMethod denotes the true anomaly detected, while RankAno denotes anomalies in the Top-K ranking node.

3) RECALL@K

This evaluation indicator measures the percentage of true anomalies explored by a particular detection approach out of the total ground truth anomalies.

$$Recall@K = \frac{|TRAnobyMethod| \cap |RankAno|}{|AllTrueAnomalies|} \tag{28}$$

where AllTrueAnomalies refers to the entire dataset's true anomalies.

C. BASELINES

DVAEGMM is compared to the following techniques to demonstrate its ability to detect anomalies:

- LOF [23] defines how separated an object is in relation to its environment and locates anomalies on a contextual level. This method only considers nodal attributes.
- RADAR [17] is an unsupervised approach for finding anomalies in attributed networks. The residuals of attribute values and their similarity to network data are used to characterize anomalies whose behavior is very different from the majority's [70], [71]. This helps to identify anomalous behavior.
- DOMINANT [15] is a cutting-edge unsupervised approach based on deep learning to detect anomalies. Reconstructing the adjacency as well as the attribute matrix jointly is accomplished using a graph convolution autoencoder. It quantifies the weighted sum of reconstruction error terms to assess the irregularity of each node.
- DUAL-SVDAE [38] is composed of a structure autoencoder and an attribute autoencoder, which acquire the node's embedding in structure as well as in feature space, respectively. Then, from the structure and attribute viewpoints, a dual-hypersphere learning is imposed to learn two hyperspheres of normal nodes.
- ResGCN [50] In place of reconstruction errors, the residual information used to rank anomalies is generated from the input network. ResGCN uses GCN to capture network sparsity and nonlinearity, a deep neural network to collect residual information, and a residual-based attention mechanism to limit the negative impact of anomalous nodes.

TABLE 3. Parameters for experiment.

Parameter Name	Value
Epochs	100
Learning Rate	0.002
Embedding Dimension	64
Balance Parameter(Θ)	0.6
Meta parameter γ_1	0.1
Meta parameter γ_2	0.005

D. EXPERIMENTAL DESIGN

In the experiment, we implemented DVAEGMM on Python language, and trained it with 100 training epochs for all the datasets. For optimization, the Adam algorithm with a learning rate of 0.002 is being used. Since, TensorFlow, Pytorch and others recommend a learning rate equal to 0.001, but we found the best result at 0.002. The embedding dimension has been fixed at 64 for all the datasets. Moreover, in all the DAGMM instances, we set parameters $(\theta, \gamma_1, \gamma_2)$ as (0.6, 0.1, 0.005) respectively, where θ is used to control the tradeoff between structure and attribute reconstruction, and γ_1 and γ_2 are meta parameters. We use the publicly accessible implementations from the source publications for the baseline techniques, and we fix the hyper-parameters to the recommended

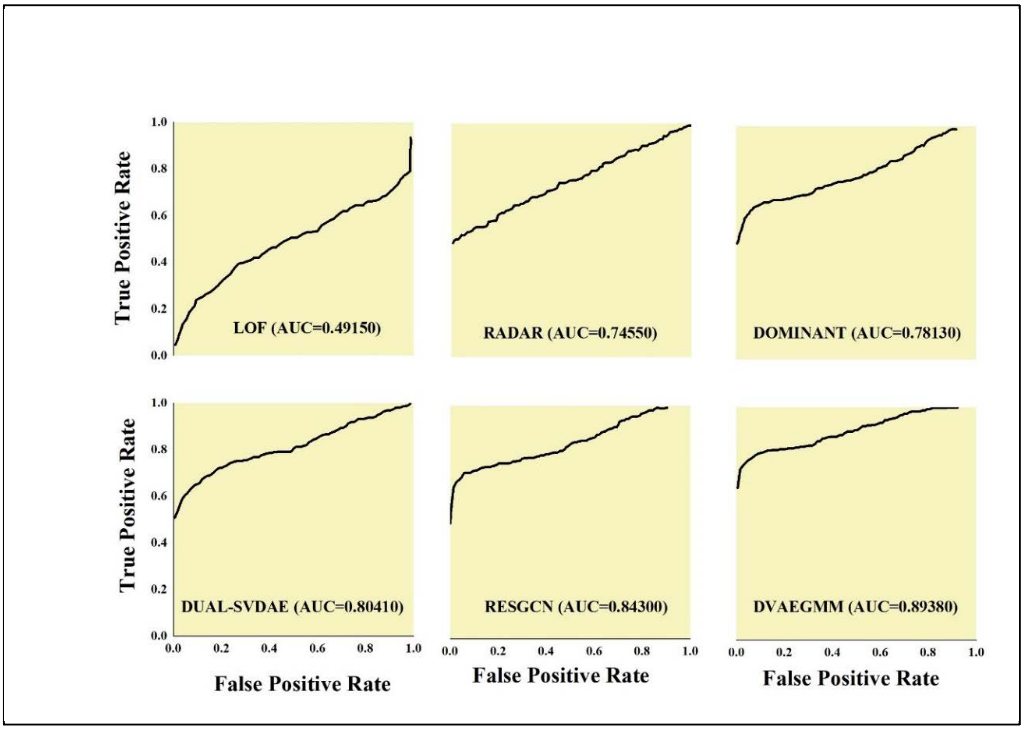

FIGURE 2. ROC Curve comparison on BlogCatalog.

TABLE 4. AUC results.

Method	BlogCatalog	Flickr	Enron	Amazon
LOF	0.49150	0.48810	0.46180	0.48620
RADAR	0.74550	0.72570	0.64200	0.67940
DOMINANT	0.78130	0.74900	0.68980	0.67150
Dual-SVDAE	0.80410	0.77100	0.64190	0.65120
ResGCN	0.84300	0.80570	0.66760	0.71920
DVAEGMM	0.89380	0.87130	0.72480	0.75102

values in the papers that presented the methods. Table 3. summarizes the values of different parameters.

E. EXPERIMENTAL RESULTS

A number of benchmarks are compared to the DVAEGMM's performance with respect to ROC-AUC. For each dataset, the AUC results of the methods are given in Table 4. In addition, the ROC curves of all the methods for the BlogCatalog, Flickr, Enron, and Amazon datasets are demonstrated in Figure 2, Figure 4, Figure 5, and Figure 6, respectively. The ROC curve demonstrates that our proposed framework outscored the other baseline anomaly detection methods. Compared to the second-best model, ResGCN, DVAEGMM increases AUC by at least 3.182%, and to the worst model, LOF, it increases AUC by 40.23% on the BlogCatalog dataset. Figure. 3 demonstrates the AUC performance comparison. The AUC results and the interpretation of ROC curves are explained as follows:

- A comparison of all datasets shows that the DVAEGMM outperforms all other baseline techniques. DVAEGMM's ability to combine the power of variational autoencoder and GMM for anomaly detection has been proven.
- In all three datasets, the AUC values of LOF are lower than the other four approaches that consider structural and attribute information to detect anomalies because LOF only evaluates attribute data.
- The residual analysis-based method, RADAR, outperforms the traditional method, LOF, However, because of their shallow mechanisms for dealing with network sparseness, data nonlinearity, and complicated modality connections, these approaches are still constrained.
- Dominant combines structural and attribute information for node embedding, but autoencoder based methods that use reconstruction errors cannot adequately measure the abnormality.
- Dual-SVDAE outperforms LOF, RADAR, and Dominant due to the use of a dual hypersphere learning mechanism.
- ResGCN outperforms all the other baseline methods except our DVAEGMM due to the attention based deep residual modeling approach.

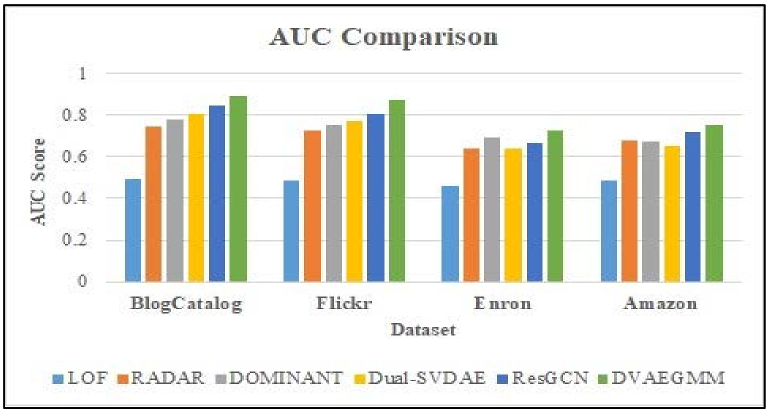

FIGURE 3. AUC performance comparison.

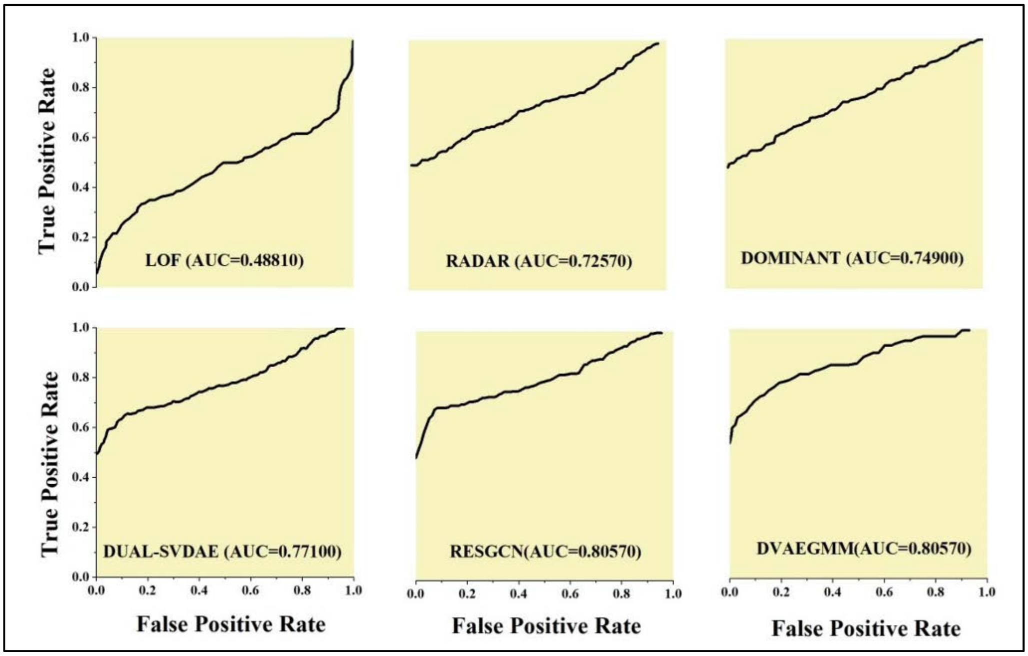

FIGURE 4. ROC Curve comparison on Flickr.

- The performance of our model is slightly worse in the datasets Enron and Amazon than in the other datasets. We speculate that this is most likely caused by the low dimensionality of the dataset.

As a result, we are certain that our model can detect more true anomalies in a ranking list with a limited length. Tables 5 and 6 provide the experimental findings for Precision@K and Recall@K, respectively. Figure. 7 and Figure. 8 demonstrate the Precision@100 and Recal@100 performance comparisons, respectively. Compared to the second-best model, ResGCN, DVAEGMM increases precision@100 by at least 6.7%, and to the worst model, LOF, it increases precision@100 by 70.7% on the BlogCatalog dataset. Similarly, it increases the recall@100 by 1.6% as compared to the ResGCN and 24.2% as compared to the LOF, on the BlogCatalog dataset. From this evaluation data, we derive the following conclusive results:

- With the exception of Precision@200 on BlogCatalog and Recall@200 on Flickr, the suggested DVAEGMM framework surpasses existing baseline approaches on all three attributed networks. It indicates the efficacy of our approach.
- Due to DVAEGMM's superiority in Precision@K and Recall@K compared to other methods, we believe our model can achieve higher accuracy and locate more real anomalies within a ranking list with a limited length.

F. PARAMETER SENSITIVITY

An anomaly detected is examined in this section according to the parameter sensitivity of different embedding

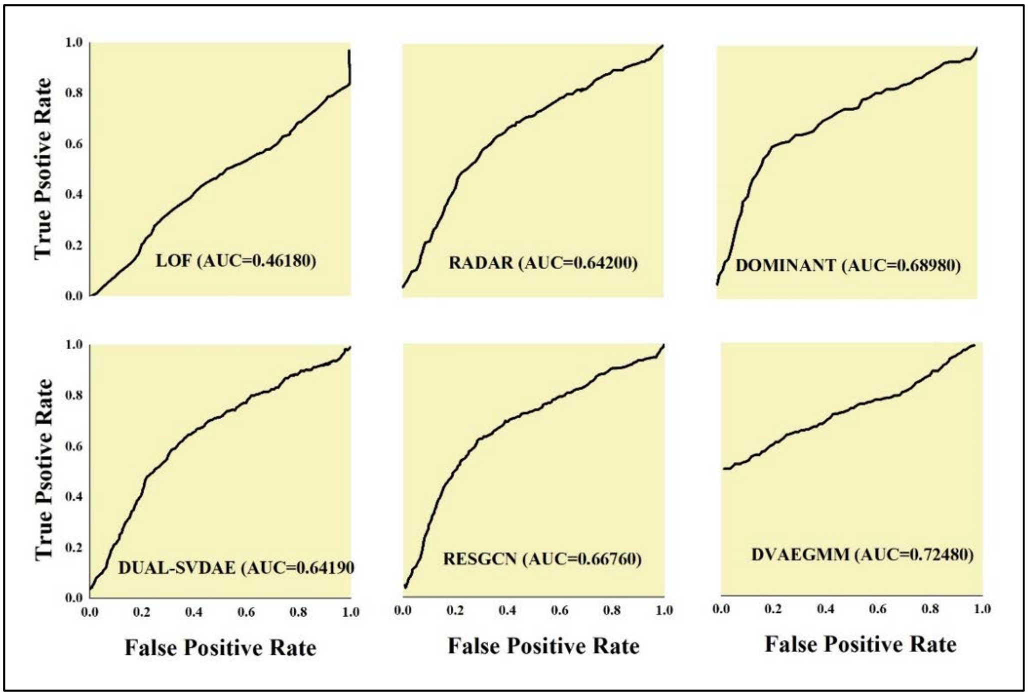

FIGURE 5. ROC Curve comparison on Enron.

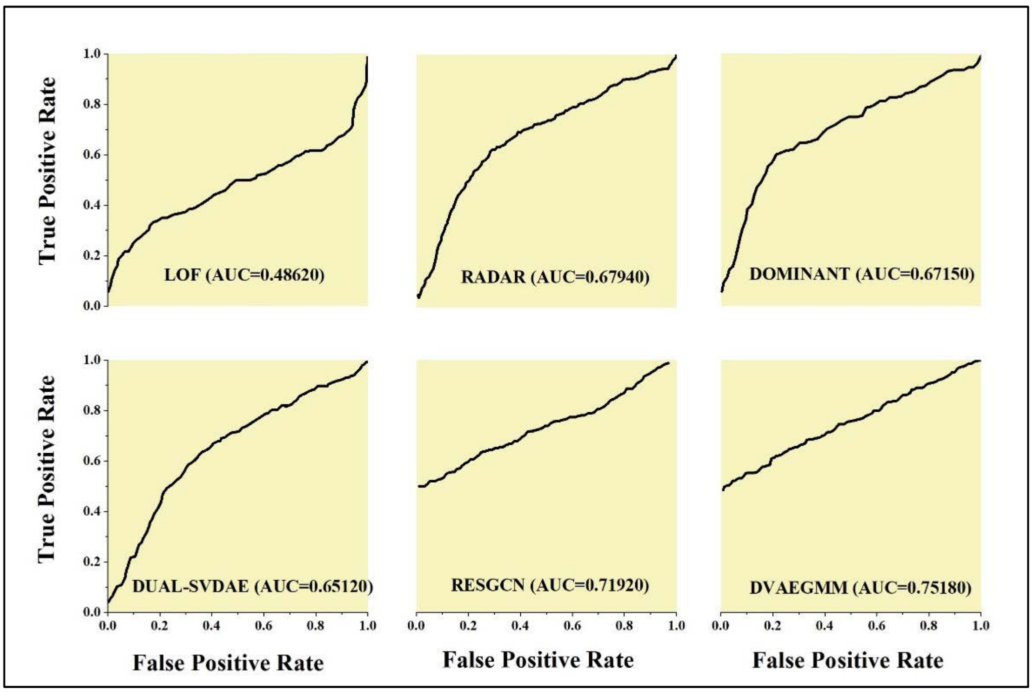

FIGURE 6. ROC Curve comparison on Amazo.

dimensions D and the balance parameter θ. The studies were performed on the BlogCatalog dataset. Figure 9 shows the trend of AUC under different dimensions of the embedding layer. We can observe that a higher dimensional embedding, such as 64 or 128 dimensions, provides good performance since higher dimensional embeddings can encode additional data. However, due to poor modelling capacity or over-fitting, the dimension with too low or too high a value would degrade the performance. For anomaly detection, it is clear that the interactions between the network structure

TABLE 5. Precision@K performance of different anomaly detection approaches.

Method	BlogCatalog			Flickr			Enron			Amazon		
K	**50**	**100**	**200**	**50**	**100**	**200**	**50**	**100**	**200**	**50**	**100**	**200**
LOF	0.300	0.220	0.180	0.420	0.380	0.270	0.049	0.048	0.036	**0.052**	0.045	0.039
RADAR	0.713	0.690	0.575	0.680	0.695	0.641	0.421	0.523	0.514	**0.496**	0.502	0.536
DOMINANT	0.760	0.710	0.590	0.770	0.730	0.685	0.510	0.612	0.589	**0.524**	0.584	0.592
Dual-SVDAE	0.792	0.810	0.640	0.769	0.780	0.650	0.592	0.710	0.675	**0.613**	0.675	0.695
ResGCN	0.848	0.860	0.670	0.780	0.830	0.875	0.623	0.730	0.712	**0.605**	0.746	0.703
DVAEGMM	0.896	0.927	0.675	0.825	0.878	0.910	0.667	0.818	0.768	**0.657**	0.775	0.682

TABLE 6. Recall@K performance of different anomaly detection approaches.

Method	BlogCatalog			Flickr			Enron			Amazon		
K	**50**	**100**	**200**	**50**	**100**	**200**	**50**	**100**	**200**	**50**	**100**	**200**
LOF	0.050	0.073	0.120	0.047	0.084	0.120	0.003	0.070	0.013	0.003	0.079	0.016
RADAR	0.123	0.195	0.315	0.069	0.126	0.259	0.036	0.078	0.091	0.035	0.081	0.094
DOMINANT	0.127	0.237	0.393	0.084	0.162	0.304	0.041	0.081	0.160	0.043	0.082	0.170
Dual-SVDAE	0.129	0.234	0.412	0.086	0.169	0.304	0.038	0.087	0.175	0.036	0.085	0.179
ResGCN	0.143	0.299	0.456	0.088	0.187	**0.393**	0.039	0.091	0.180	0.045	0.091	0.190
DVAEGMM	**0.172**	**0.315**	**0.461**	**0.092**	**0.191**	0.381	**0.041**	**0.101**	**0.195**	**0.047**	**0.093**	**0.214**

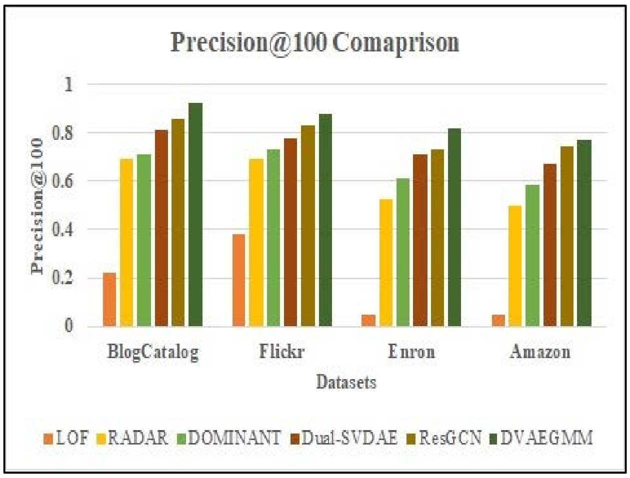

FIGURE 7. Precison@100 performance comparison.

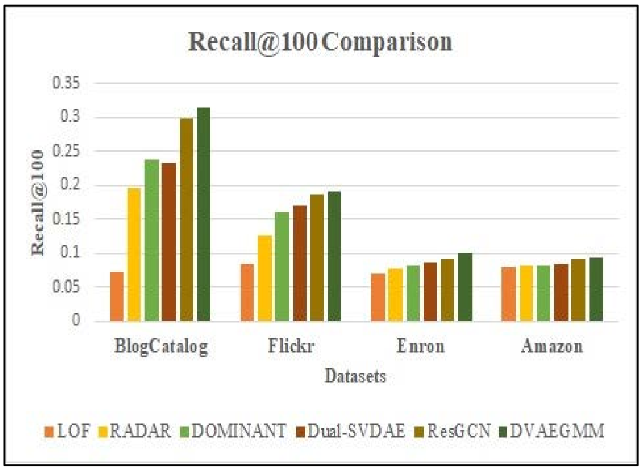

FIGURE 8. Recall@100 performance comparison.

and node attributes on the attributed network are critical, as only considering attribute reconstruction ($\theta = 0$) or structure reconstruction ($\theta = 1$) would result in low efficiency. Figure 10 shows the trend of AUC under different values of θ, indicating that a suitable balance factor can effectively improve performance.

G. ABLATIONS STUDY

In this section, using DVAEGMM for anomaly detection, we explore the effects of node attributes, network structure, adversarial training, and estimation density. Specific to DVAEGMM, each module's contribution is examined separately. The following are the specifics of the ablation settings:

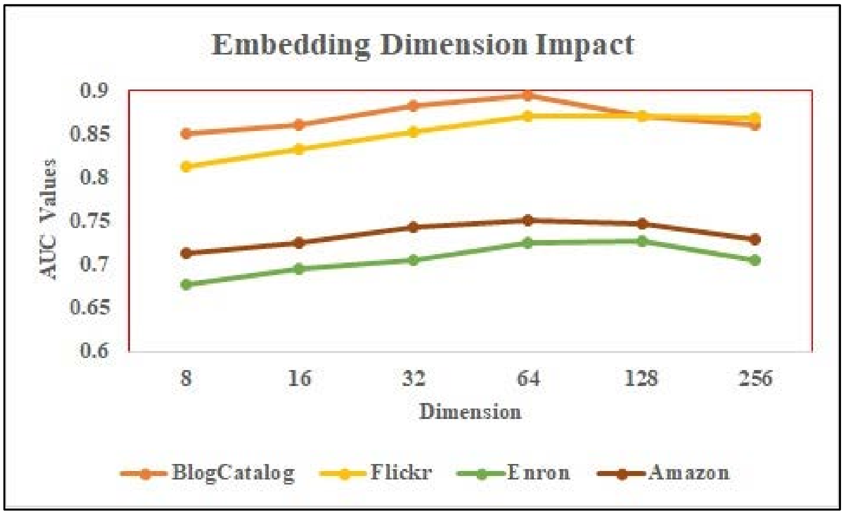

FIGURE 9. Embedding Dimension impact w.r.t. AUC values.

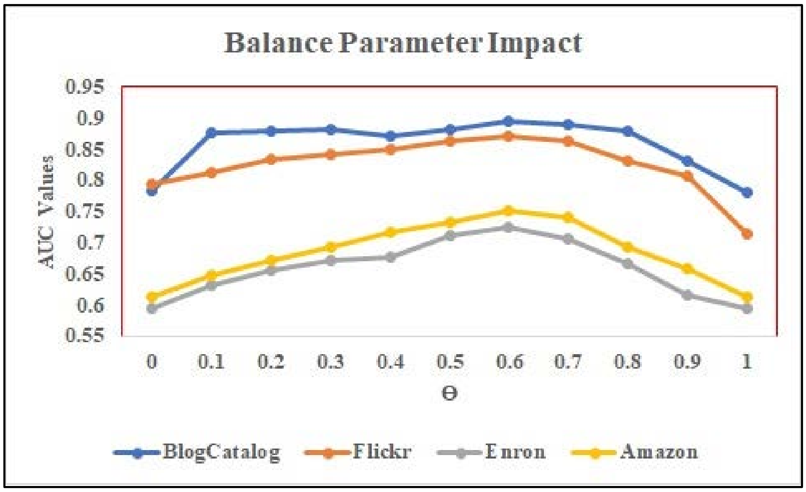

FIGURE 10. Balance parameter impact w.r.t. AUC values.

TABLE 7. Ablation study.

Method	BlogCatalog	Flickr	Enron	Amazon
DVAEGMM	0.89380	0.87130	0.72480	0.75102
WOGMM	0.51359	0.59618	0.37815	0.42345
WOSVAE	0.45731	0.47981	0.52988	0.46535
WOAVAE	0.62828	0.66727	0.45615	0.51235
ADGAN	0.83450	0.81575	0.69546	0.71245

- Without-GMM(WOGMM): To supervise model training, we drop the GMM module from DVAEGMM and substitute it with two reconstruction losses, one for network structure and the other for node attributes. Ultimately, reconstruction error is used as an anomaly score to detect anomalies.
- Without-StructuralVAE (WOSVAE): For training purposes, only attributed VAE is used, as the structural VAE module is eliminated, and finally detects anomalies by approximating the density using the GMM module.
- Without-AttributedVAE (WOAVAE): For training purpose, only structural VAE is used, as attribute VAE module is eliminated, and finally, anomalies are detected by approximating the density using the GMM module.
- Without GAN (WOGAN): Adversarial training component is removed, and dual variational autoencoders are used for the training, and anomalies are detected using the GMM module.
- Anomaly Detection with GAN (ADGAN) instead of GMM: We drop the GMM module and, by following the AnoGAN approach [68], the anomaly score is calculated

as the linear combination of reconstruction error and discriminator error.

Table 7 shows the results of the ablation study on all the datasets. We find that DVAEGMM achieves the best results. The efficiency of the DVAEGMM is demonstrated by the poor results of the WOGMM, WOSVAE, WOAVAE, and ADGAN. In addition, the model's performance degrades when we rely solely on the structure or attribute features. One potential reason for this is that considering only the attribute or structure information compromises the attributed network data integrity. Therefore, anomaly detection on an attributed network necessitates both structure information and attribute information.

VII. CONCLUSION

This research proposes a Dual variational Autoencoder with Gaussian Mixture Model (DVAEGMM) framework to solve the issue of anomaly detection in attributed networks. In contrast to prior techniques, DVAEGMM effectively addresses the shortcomings of previously proposed methods. Dual variational autoencoders address the complicated cross-modality connections between network structure and node attributes while incorporating the prospective distribution of data, thus reflecting the sparsity and nonlinearity of networks. GAN provides the adversarial power to the dual variational autoencoders. The Gaussian Mixture Model (GMM) is then applied to density estimation problems for input data with complex structures over the learned low-dimensional space. The sample energy is used to identify anomalies. Two datasets without ground truth anomalies, BlogCatalog and Flickr, and two datasets with ground truth anomalies, Enron and Amazon, were evaluated for the comparison. The results of the experiments show that DVAEGMM is a viable alternative to the approaches that had previously been offered. The performance of our proposed method is higher than baselines, i.e., it outperforms LOF by 40.23%, Radar by 14.83%, Dominant by 11.25%, Dual-SVDAE by 8.97%, and ResGCN by 2.68%, respectively on AUC for the BlogCatalog dataset. Each DVAEGMM component's efficiency is demonstrated via ablation analysis. Our suggested model, however, needs to be tested in real-world large-scale operational network scenarios before it can be used in the real world. The performance of our model is slightly worse in the datasets Enron and Amazon than in the other datasets. We speculate that this is most likely caused by the low dimensionality of the dataset. In the future, we will try to incorporate changes in our proposed framework to perform efficiently on datasets with low dimension. We also plan to explore DVAEGMM extensions for dynamic or time-series networks. The detection of anomalies in more complicated networks and graphs, such as heterogeneous graphs, spatial-temporal graphs, and dynamic graphs, will be one of our research priorities.

REFERENCES

[1] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 1–33, 2013.
[2] M. Rasool and W. Khan, "Big data: Study in structured and unstructured data," *Int. J. Technol. Innov. Res.*, vol. 14, pp. 1–6, Apr. 2015.
[3] L. Xue, Y. Chen, M. Luo, Z. Peng, and J. Liu, "An anomaly detection framework for time-evolving attributed networks," *Neurocomputing*, vol. 407, pp. 39–49, Sep. 2020.
[4] H. Fan, F. Zhang, and Z. Li, "AnomalyDAE: Dual autoencoder for anomaly detection on attributed networks," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2020, pp. 5685–5689, doi: 10.1109/ICASSP40776.2020.9053387.
[5] W. Khan, "An exhaustive review on state-of-the-art techniques for anomaly detection on attributed networks," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, pp. 6707–6722, 2021.
[6] T. Bai, Y. Zhang, B. Wu, and J.-Y. Nie, "Temporal graph neural networks for social recommendation," in *Proc. IEEE Int. Conf. Big Data*, Dec. 2020, pp. 898–903, doi: 10.1109/BigData50022.2020.9378444.
[7] Z. Liu, C. Chen, X. Yang, J. Zhou, X. Li, and L. Song, "Heterogeneous graph neural networks for malicious account detection," in *Proc. 27th ACM Int. Conf. Inf. Knowl. Manag.*, Oct. 2018, pp. 2077–2086, doi: 10.1145/3269206.3272010.
[8] M. K. Hasan, A. F. Ismail, S. Islam, W. Hashim, and B. Pandey, "Dynamic spectrum allocation scheme for heterogeneous network," *Wirel. Pers. Commun.*, vol. 95, no. 2, pp. 299–315, 2017.
[9] X. Zhang and A. A. Ghorbani, "An overview of online fake news: Characterization, detection, and discussion," *Inf. Process. Manag.*, vol. 57, no. 2, Mar. 2020, Art. no. 102025.
[10] J. Gao, F. Liang, W. Fan, C. Wang, Y. Sun, and J. Han, "On community outliers and their efficient detection in information networks," in *Proc. 16th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2010, pp. 813–822.
[11] B. Perozzi and L. Akoglu, "Scalable anomaly ranking of attributed neighborhoods," in *Proc. SIAM Int. Conf. Data Mining*, Jun. 2016, pp. 207–215.
[12] B. Perozzi and L. Akoglu, "Discovering communities and anomalies in attributed graphs: Interactive visual exploration and summarization," *ACM Trans. Knowl. Discovery Data*, vol. 12, no. 2, pp. 1–40, Mar. 2018.
[13] B. Perozzi, L. Akoglu, P. I. Sánchez, and E. Müller, "Focused clustering and outlier detection in large attributed graphs," in *Proc. 20th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2014, pp. 1346–1355.
[14] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 303–336, 1st Quart., 2014.
[15] K. Ding, J. Li, R. Bhanushali, and H. Liu, "Deep anomaly detection on attributed networks," in *Proc. SIAM Int. Conf. Data Mining*, 2019, pp. 594–602, doi: 10.1137/1.9781611975673.67.
[16] Y. Li, X. Huang, J. Li, M. Du, and N. Zou, "SpecAE: Spectral autoencoder for anomaly detection in attributed networks," in *Proc. 28th ACM Int. Conf. Inf. Knowl. Manag.*, Nov. 2019, pp. 2233–2236, doi: 10.1145/3357384.3358074.
[17] J. Li, H. Dani, X. Hu, and H. Liu, "Radar: Residual analysis for anomaly detection in attributed networks," in *Proc. 26th Int. Joint Conf. Artif. Intell.*, Aug. 2017, pp. 2152–2158.
[18] Z. Peng, M. Luo, J. Li, H. Liu, and Q. Zheng, "ANOMALOUS: A joint modeling approach for anomaly detection on attributed networks," in *Proc. 27th Int. Joint Conf. Artif. Intell.*, Jul. 2018, pp. 3513–3519, doi: 10.24963/ijcai.2018/488.
[19] D. Zhu, Y. Ma, and Y. Liu, "DeepAD: A joint embedding approach for anomaly detection on attributed networks," in *Proc. Int. Conf. Comput. Sci.*, 2020, pp. 294–307.
[20] T. M. Ghazal, M. A. M. Afifi, and D. Kalra, "Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications," *Solid State Technol.*, vol. 63, pp. 2513–2521, Oct. 2020.
[21] H. Kundra, W. Khan, M. Malik, K. P. Rane, R. Neware, and V. Jain, "Quantum-inspired firefly algorithm integrated with cuckoo search for optimal path planning," *Int. J. Mod. Phys. C*, vol. 33, no. 2, Sep. 2021, Art. no. 2250018, doi: 10.1142/S0129183122500188.
[22] X. Xu, N. Yuruk, Z. Feng, and T. A. J. Schweiger, "SCAN: A structural clustering algorithm for networks," in *Proc. 13th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2007, pp. 824–833.
[23] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying density-based local outliers," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, 2000, pp. 93–104.
[24] K. G. Mehrotra, C. K. Mohan, and H. Huang, *Anomaly Detection Principles and Algorithms*, vol. 1. New York, NY, USA: Springer, 2017.

[25] W. M. H. Azamuddin, R. Hassan, A. H. M. Aman, M. K. Hasan, and A. S. Al-Khaleefa, "Quality of service (QoS) management for local area network (LAN) using traffic policy technique to secure congestion," *Computers*, vol. 9, no. 2, p. 39, May 2020.
[26] Y. Pan, J. Zou, J. Qiu, S. Wang, G. Hu, and Z. Pan, "Joint network embedding of network structure and node attributes via deep autoencoder," *Neurocomputing*, vol. 468, pp. 198–210, Jan. 2022.
[27] P. Shi, Z. Zhao, H. Zhong, H. Shen, and L. Ding, "An improved agglomerative hierarchical clustering anomaly detection method for scientific data," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 6, p. e6077, Mar. 2021.
[28] M. Goldstein and S. Uchida, "A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data," *PLoS ONE*, vol. 11, no. 4, Apr. 2016, Art. no. e0152173.
[29] L. Xiong, B. Póczos, and J. Schneider, "Group anomaly detection using flexible genre models," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 24, 2011, pp. 1–9.
[30] Z. Zhang, L. Liu, J. Qin, F. Zhu, F. Shen, Y. Xu, L. Shao, and H. T. Shen, "Highly-economized multi-view binary compression for scalable image clustering," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, 2018, pp. 717–732.
[31] M. K. Hasan, M. Shafiq, S. Islam, B. Pandey, Y. A. B. El-Ebiary, N. S. Nafi, R. C. Rodriguez, and D. E. Vargas, "Lightweight cryptographic algorithms for guessing attack protection in complex Internet of Things applications," *Complexity*, vol. 2021, pp. 1–13, Apr. 2021.
[32] C. Pascoal, M. R. De Oliveira, R. Valadas, P. Filzmoser, P. Salvador, and A. Pacheco, "Robust feature selection and robust PCA for internet traffic anomaly detection," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1755–1763.
[33] E. R. Ziegel, "Principal component analysis," *Technometrics*, vol. 45, no. 3, pp. 276–277, 2003.
[34] C. Zhou and R. C. Paffenroth, "Anomaly detection with robust deep autoencoders," in *Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2017, pp. 665–674.
[35] S. Zhai, Y. Cheng, W. Lu, and Z. Zhang, "Deep structured energy based models for anomaly detection," in *Proc. Int. Conf. Mach. Learn.*, 2016, pp. 1100–1109.
[36] R. Sadeghi and J. Hamidzadeh, "Automatic support vector data description," *Soft Comput.*, vol. 22, no. 1, pp. 147–158, Jan. 2018.
[37] R. Perdisci, G. Gu, and W. Lee, "Using an ensemble of one-class SVM classifiers to harden payload-based anomaly detection systems," in *Proc. 6th Int. Conf. Data Mining (ICDM)*, Dec. 2006, pp. 488–498.
[38] F. Zhang, H. Fan, R. Wang, Z. Li, and T. Liang, "Deep dual support vector data description for anomaly detection on attributed networks," *Int. J. Intell. Syst.*, vol. 37, no. 2, pp. 1509–1528, Feb. 2022.
[39] X. Wang, B. Jin, Y. Du, P. Cui, Y. Tan, and Y. Yang, "One-class graph neural networks for anomaly detection in attributed networks," *Neural Comput. Appl.*, vol. 33, pp. 12073–12085, Mar. 2021.
[40] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 27, 2014, pp. 1–9.
[41] H. W. Wang and X. Wangjl, "GraphGAN: Graph representation learning with generative adversarial nets," 2017, *arXiv:1711.08267*.
[42] B. Hu, Y. Fang, and C. Shi, "Adversarial learning on heterogeneous information networks," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Jul. 2019, pp. 120–129.
[43] A. Makhzani, J. Shlens, N. Jaitly, I. Goodfellow, and B. Frey, "Adversarial autoencoders," 2015, *arXiv:1511.05644*.
[44] X. Ma, J. Wu, S. Xue, J. Yang, C. Zhou, Q. Z. Sheng, H. Xiong, and L. Akoglu, "A comprehensive survey on graph anomaly detection with deep learning," *IEEE Trans. Knowl. Data Eng.*, early access, Oct. 8, 2021, doi: 10.1109/TKDE.2021.3118815.
[45] E. Müller, P. I. Sanchez, Y. Mulle, and K. Bohm, "Ranking outlier nodes in subspaces of attributed graphs," in *Proc. IEEE 29th Int. Conf. Data Eng. Workshops (ICDEW)*, Apr. 2013, pp. 216–222.
[46] P. I. Sanchez, E. Müller, F. Laforet, F. Keller, and K. Bohm, "Statistical selection of congruent subspaces for mining attributed graphs," in *Proc. IEEE 13th Int. Conf. Data Mining*, Dec. 2013, pp. 647–656.
[47] D. Zhang, J. Yin, X. Zhu, and C. Zhang, "Network representation learning: A survey," *IEEE Trans. Big Data*, vol. 6, no. 1, pp. 3–28, Mar. 2020.
[48] A. U. Haq, J. P. Li, B. L. Y. Agbley, A. Khan, I. Khan, M. I. Uddin, and S. Khan, "IIMFCBM: Intelligent integrated model for feature extraction and classification of brain tumors using MRI clinical imaging data in IoT-healthcare," *IEEE J. Biomed. Health Informat.*, early access, Mar. 3, 2022, doi: 10.1109/JBHI.2022.3171663.
[49] M. K. Hasan, S. Islam, I. Memon, A. F. Ismail, S. Abdullah, A. K. Budati, and N. S. Nafi, "A novel resource oriented DMA framework for internet of medical things devices in 5G network," *IEEE Trans. Ind. Informat.*, early access, Feb. 4, 2022, doi: 10.1109/TII.2022.3148250.
[50] Y. Pei, T. Huang, W. van Ipenburg, and M. Pechenizkiy, "ResGCN: Attention-based deep residual modeling for anomaly detection on attributed networks," *Mach. Learn.*, vol. 111, no. 2, pp. 519–541, 2021.
[51] D. Kumar, C. Verma, S. Dahiya, P. K. Singh, and M. S. Raboaca, "Cardiac diagnostic feature and demographic identification models: A futuristic approach for smart healthcare using machine learning," *Math. Comput. Sci.*, vol. 19, Jun. 2021, Art. no. 6584.
[52] N. Varish, A. K. Pal, R. Hassan, M. K. Hasan, A. Khan, N. Parveen, D. Banerjee, V. Pellakuri, A. U. Haqis, and I. Memon, "Image retrieval scheme using quantized bins of color image components and adaptive tetrolet transform," *IEEE Access*, vol. 8, pp. 117639–117665, 2020.
[53] M. R. Kadis and A. Abdullah, "Global and local clustering soft assignment for intrusion detection system: A comparative study," *Asia–Pacific J. Inf. Technol. Multimed*, vol. 6, no. 1, pp. 30–38, 2017.
[54] L. Akoglu and C. Faloutsos, "Anomaly, event, and fraud detection in large network datasets," in *Proc. 6th ACM Int. Conf. Web Search Data Mining*, 2013, pp. 773–774.
[55] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in *Proc. 5th Int. Conf. Learn. Represent.*, 2017, pp. 1–14.
[56] G. V. Daniel and M. Venkatesan, "Robust graph based deep anomaly detection on attributed networks," in *Proc. 11th Int. Conf. Cloud Comput., Data Sci. Eng.*, 2021, pp. 1029–1033, doi: 10.1109/Confluence51648.2021.9376881.
[57] M. K. Hasan, M. M. Ahmed, and S. S. Musa, "Measurement and modeling of DTCR software parameters based on intranet wide area measurement system for smart grid applications," in *Proc. Int. Conf. Innov. Comput. Commun.*, 2021, pp. 1139–1150.
[58] Z. Cheng, S. Wang, P. Zhang, S. Wang, X. Liu, and E. Zhu, "Improved autoencoder for unsupervised anomaly detection," *Int. J. Intell. Syst.*, vol. 36, no. 12, pp. 7103–7125, Dec. 2021, doi: 10.1002/int.22582.
[59] D. Jin, B. Li, P. Jiao, D. He, and W. Zhang, "Network-specific variational auto-encoder for embedding in attribute networks," in *Proc. 28th Int. Joint Conf. Artif. Intell.*, Aug. 2019, pp. 2663–2669, doi: 10.24963/ijcai.2019/370.
[60] D. P. Kingma and M. Welling, "Auto-encoding variational Bayes," in *Proc. 2nd Int. Conf. Learn. Represent.*, 2014, pp. 1–14.
[61] D. J. Im, S. Ahn, R. Memisevic, and Y. Bengio, "Denoising criterion for variational auto-encoding framework," in *Proc. 31st AAAI Conf. Artif. Intell.*, 2017, pp. 2059–2065.
[62] A. Asperti and M. Trentin, "Balancing reconstruction error and Kullback–Leibler divergence in variational autoencoders," *IEEE Access*, vol. 8, pp. 199440–199448, 2020, doi: 10.1109/ACCESS.2020.3034828.
[63] H. Virtanen, P. Björk, and E. Sjöström, "Follow for follow: Marketing of a start-up company on Instagram," *J. Small Bus. Enterprise Develop.*, vol. 24, no. 3, pp. 468–484, Aug. 2017.
[64] V. Metsis, I. Androutsopoulos, and G. Paliouras, "Spam filtering with naive Bayes-which naive Bayes?" in *Proc. CEAS*, vol. 17, 2006, pp. 28–69.
[65] K. Ding, J. Li, and H. Liu, "Interactive anomaly detection on attributed networks," in *Proc. 12th ACM Int. Conf. Web Search Data Mining*, 2019, pp. 357–365, doi: 10.1145/3289600.3290964.
[66] X. Song, M. Wu, C. Jermaine, and S. Ranka, "Conditional anomaly detection," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 5, pp. 631–645, May 2007.
[67] L. Gutiérrez-Gómez, A. Bovet, and J.-C. Delvenne, "Multi-scale anomaly detection on attributed networks," in *Proc. AAAI Conf. Artif. Intell.*, 2020, vol. 34, no. 1, pp. 678–685.
[68] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," in *Proc. Int. Conf. Inf. Process. Med. Imag.*, 2017, pp. 146–157.
[69] S. A. Lashari, R. Ibrahim, N. S. A. M. Taujuddin, N. Senan, and S. Sari, "Thresholding and quantization algorithms for image compression techniques: A review," *Asia–Pacific J. Inf. Technol. Multimedia*, vol. 7, no. 1, pp. 83–89, 2018.
[70] Z. R. Mahayuddin and A. S. Saif, "A comprehensive review towards segmentation and detection of cancer cell and tumor for dynamic 3D reconstruction," *Asia–Pacific J. Inf. Technol. Multimedia*, vol. 9, no. 1, pp. 28–39, 2020.
[71] M. I. A. Latiffi and M. R. Yaakub, "Sentiment analysis: An enhancement of ontological-based using hybrid machine learning techniques," *Asia–Pacific J. Inf. Technol. Multimedia*, vol. 7, pp. 61–69, Dec. 2018.

WASIM KHAN received the B.Tech. degree in IT and the M.Tech. degree in CSE from A. P. J. Abdul Kalam University, Lucknow, Uttar Pradesh, India. He is currently pursuing the Ph.D. degree with Integral University, Lucknow. He is also working with Integral University as an Assistant Professor. He has over 15 years of teaching experience. His current research interests include machine learning, deep learning, social network analysis, anomaly detection, and network intrusion detection.

MOHAMMAD HAROON received the B.Tech. degree in computer science from Dr. Bhim Rao Ambedkar University, Agra, Uttar Pradesh, India, the M.Tech. degree from the Allahabad Agriculture Institute Deemed University Allahabad, Uttar Pradesh, and the Ph.D. degree from Teerthankar Mahaveer University, Moradabad, in 2016. He is currently working as an Associate Professor with the Computer Science and Engineering Department, Integral University, Lucknow, Uttar Pradesh. He has over 15 years of experience in academics. His research interests include deep learning, social network analysis, anomaly detection, and distributed systems.

AHMAD NEYAZ KHAN (Member, IEEE) received the B.Sc. (Hons.) and master's degrees in computer applications from Aligarh Muslim University, India, in 2009 and 2012, respectively, and the Ph.D. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. He is currently an Assistant Professor with Integral University, India. His research interests include information security, machine learning, and reversible data hiding in the encrypted domain.

MOHAMMAD KAMRUL HASAN (Senior Member, IEEE) received the Doctor of Philosophy (Ph.D.) degree in electrical and communication engineering from the Faculty of Engineering, International Islamic University, Malaysia, in 2016. He is currently working with the Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), as a Senior Lecturer. He is specialized with elements pertaining to cutting-edge information centric networks, computer networks, data communication and security, mobile network and privacy protection, cyber-physical systems, the Industrial IoT, transparent AI, and electric vehicles networks. He has published more than 150 indexed papers in ranked journals and conference proceedings. He is a member of Institution of Engineering and Technology (MIET 1100572830) and a member of Internet Society (198312). He is also a Certified Professional Technologist (P.Tech./Ts.), Malaysia. He also served the IEEE Student Branch as the Chair, from 2014 to 2016. He has actively participated in many events/workshops/trainings for the IEEE and IEEE humanity programs in Malaysia. He works as the editorial member in many prestigious high-impact journals, such as IEEE, IET, Elsevier, Frontier, and MDPI, and the general chair, the co-chair, and a speaker for conferences and workshops for the shake of society and academy knowledge building and sharing and learning. He has been contributing and working as a Volunteer for Under Privileged Children for the Welfare of Society.

ASIF KHAN (Member, IEEE) received the B.Sc. (Hons.) and Master of Computer Science and Application (M.C.A.) degrees from Aligarh Muslim University, India, and the Ph.D. degree (Hons.) in computer science and technology from the University of Electronic Science and Technology of China (UESTC), China, in 2016. He was an Adjunct Faculty with the University of Bridgeport, USA, for China Program, in Summer 2016. Previously, he was a Visiting Scholar in big data mining and application at the Chongqing Institute of Green and Intelligent Technology (CIGIT), Chinese Academy of Sciences, Chongqing, China. He done a Postdoctoral Scientific Research Fellow with UESTC. He is also holding a position of an Assistant Professor with Integral University, India. He is a contributor to many international journals with robotics and vision analyses about the contemporary world in his articles. His research interests include machine learning, robotics vision, and new ideas regarding vision-based information critical theoretical research. He awarded by the UESTC Academic Achievement Award and the Excellent Performance Award, from 2015 to 2016.

UMI ASMA MOKHTAR is currently a Senior Lecturer in information science at the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. In 2012, she was awarded the Oliver Wendell Holmes Travel Award by the Society of American Archivists. Her research interests include electronic records management, function-based classification, information policy, and information security. Her articles have appeared in international and national periodicals, such as the *International Journal of Information Management* and the *Records Management Journal*. She is currently the Malaysian Team's Lead Researcher of the Inter PARES Trust AI Project.

SHAYLA ISLAM (Senior Member, IEEE) received the B.Sc. degree in computer science and engineering from International Islamic University Chittagong, Bangladesh, and the M.Sc. and Ph.D. degrees in engineering from the Electrical and Computer Engineering (ECE) Department, International Islamic University Malaysia (IIUM), in 2012 and 2016, respectively. She is currently an Assistant Professor with UCSI University, Malaysia. She has awarded a Silver medal for her research work at International Islamic University Malaysia. In consequences, she has also awarded the Young Scientist Award for the contribution of Research Paper at Second International Conference on Green Computing and Engineering Technologies and 2016 (ICGCET'16), Organized by the Department of Energy Technology, Aalborg University, Esbjerg, Denmark. She received the Malaysian International Scholarship (MIS) for the Ph.D. degree.