Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

An Integrative Computational Intelligence for Robust Anomaly Detection in Social Networks

Helina Rajini Suresh[1*], K.R.Harsavarthini[2], R. Mageswaran[3], Hirald Dwaraka Praveena[4], C. Gnanaprakasam[5], C. Sakthi Lakshmi Priya[6]

[1]Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai-600062, Tamil Nadu, India. Email
[2]PG Resident, Department of Community Medicine, Saveetha Medical College and Hospital,
Saveetha Institute of Medical and Technical Sciences (SIMATS), Saveetha University, Chennai, Tamil Nadu - 602105,India.
[3]Assistant Professor, Department of EEE, S.A. Engineering College, Anna University, Thiruverkadu, Tamil Nadu-600077, India
[4]Department of Electronics and Communication Engineering, School of Engineering, Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College), Tirupati-517 102, Andhra Pradesh, India,
[5]Department of Artificial Intelligence and Data Science, Panimalar Engineering College Poonthaomalli, Chennai – 600123.Tamil Nadu, India.
[6]Department of Computer Science and Engineering, P S R Engineering College, Sivakasi Tamil Nadu,

*Corresponding Author: Helina Rajini Suresh

DOI: https://doi.org/10.52866/ijcsm.2024.05.03.047
Received May 2024 ; Accepted June 2024; Available online August 2024

ABSTRACT: Anomaly detection is one of the most important tasks for maintaining the integrity, security, and trustworthiness of online communities in a social network. This paper proposes AdaptoDetect, which represents a new framework; it discusses a new anomaly detection approach called Pufferfish Optimization Technique for feature selection, together with a Graph Embedding Autoencoder for identifying anomalies. What makes AdaptoDetect special is that, with the use of POT, it has a distinctive capability in dynamic adaptation against network changes by selecting only the most relevant features in social network data. The technique for optimization underlines the important attributes for anomaly detection so as to allow a more fine-tuned and accurate identification process. Meanwhile, GEAE effectively learns low-dimensional representation of graph nodes, capturing complex patterns and interrelations in the structure of graphs. These graph embeddings further enhance anomaly detection by highlighting deviation from standard social network behaviors, hence making the detection of those irregularities more accurate. The novelty in this integration of POT and GEAE makes AdaptoDetect a strong, adaptive framework suited for tackling the dynamic nature of social networks. Extensive evaluations over various social network datasets and scenarios show the superior performance of AdaptoDetect compared to state-of-the-art methods, especially regarding its adaptiveness to the alteration in networks and detection of anomalies with high accuracy. Besides fortifying the security of social networks, making online environments much safer and more trustworthy will be contributed to by significantly enhancing resilience and reliability in social networks.

Keywords: Anomaly Detection, Deep Learning, Social Networks, Optimization, Computational Intelligence Models, and Classification

1. INTRODUCTION

Human connection, communication, and information sharing have seen a significant transition in the last few decades due to the widespread adoption of digital technologies. Social networks have grown exponentially from specialized online communities to omnipresent platforms that cut over national borders and cultural barriers, and this is a key component of the paradigm change [1-3]. The proliferation of mobile devices, advancements in internet infrastructure, and the fundamental human need for social interaction and connection in the digital age are all contributing causes to the emergence of social networks. With their ongoing proliferation and diversification, social networks have established themselves as essential elements of contemporary society, reshaping public discourse, forming social connections, and changing the global communication and collaboration landscape. Finding odd or unexpected patterns of behavior, interactions, or occurrences within a social network is known as anomaly detection. These anomalies may be indicative of a number of events, such as fraudulent activity, peculiar user behavior, network outages, or new trends. The dynamic and linked world of social networks offers a myriad of opportunities and problems due to the constantly changing nature of user interactions and content dissemination [4, 5]. These networks are made up

of complex networks of connections, routes of communication, and data exchanges that facilitate information flow and shape digital interactions globally. Anomalies, or departures from regular patterns of behavior or occurrences, can, nevertheless, appear within this enormous digital ecosystem and indicate possible risks, opportunities, or disruptions. One of the most important tasks in deciphering the complexity of these virtual worlds is anomaly detection in social networks [6]. Anomaly detection examines the multitude of interactions, content engagements, and network architecture in an effort to identify and describe anomalies that might represent different events. From dishonest behavior and spamming strategies to unexpected changes in user behavior and emerging trends that spread throughout the network, these anomalies include a wide spectrum of activities.

Moreover, a wide range of situations are included in the scope of anomaly detection in social networks, each with its own set of difficulties and ramifications. The integrity and reliability of online platforms are threatened by fraudulent actions, such as the spread of fake accounts, phishing scams, or misleading tactics. To protect user experiences and maintain community standards, unusual user behaviors—whether they are signs of malice or real anomalies—should be closely examined. In addition, anomalies may cause problems for the network itself, such as organized assaults, security lapses, and technological issues that cause delays in performance [7, 8]. Ensuring the resilience and dependability of social network infrastructures requires swiftly recognizing and addressing these disruptions. Furthermore, anomalies might be markers of new trends, providing insightful information about changing user preferences, social dynamics, and cultural phenomena. Numerous different approaches and techniques are used to navigate the complexity of anomaly identification in social networks. These methods, which range from statistical analysis and machine learning algorithms to graph mining and content analysis, take advantage of the massive amounts of data produced by social interactions to identify trends, anomalies, and patterns [9]. But even with the potential for improved detection powers, there are still many obstacles to overcome. These include issues with scalability, data quality, and algorithmic fairness and user privacy as well as ethical concerns.

Anomaly detection in social networks has great potential to promote a more secure, robust, and dynamic digital ecosystem, despite these obstacles [10]. This work gives platform operators, security specialists, and data scientists the ability to protect user experiences, reduce risks, and utilize social networks' revolutionary potential for the benefit of society by shedding light on the shadows created by anomalies [11, 12]. The different types of anomalies in social network can take many different forms, including:

- Detecting accounts or activities that participate in automated bot-driven interactions or spamming is known as spam and bot detection.
- Finding persons or content that substantially deviates from the usual patterns of behavior inside the network is known as "outlier detection."
- Event detection is the process of spotting abrupt increases or decreases in activity that are connected to certain events, such popular subjects or viral media.
- Community detection is the process of identifying irregularities in the network structure, like odd connections or outlier subgroups.

Social network anomaly detection is dependent on a number of data sources, such as user profiles, interactions (likes, shares, and comments), content attributes (text, photos), network architecture, temporal data, and metadata related to individuals and content [13]. Applications for anomaly identification in social networks include the following: Fraud detection is the process of spotting fraudulent activity, including click fraud, phishing scams, and fictitious accounts. Identifying malicious activity, coordinated attacks, or network intrusions is known as security monitoring [14]. Content moderation is the process of removing offensive, hateful, or spam content. Trend detection is the process of spotting new trends, popular material, or breaking news. Network maintenance includes tracking the health of the network, spotting performance snags, and figuring out connectivity problems. Using AI methods for anomaly detection in social networks [15], such as deep learning and machine learning, has many persuasive benefits and solves important issues that arise in this intricate field. To effectively detect anomalies in social networks, it is imperative to take advantage of computational intelligence for several reasons.

Social networks create a very big amount of data instantly, this makes manual or rule oriented methods not workable anymore. Artificial intelligence methods, particularly machine learning and deep learning, guarantee scalability and efficiency in detecting anomalies [9, 16]. These approaches allow for the automatic handling and examination of large-scale information. Rule-based techniques might struggle to identify fine or complex anomalies that deviate from established patterns. Deep learning methods, which can automatically identify complex features from raw data, are very good choices for recognizing irregularities that may not be easily noticed by humans. Since social network data is both dynamic and complex while also having the ability to scale up quickly, using AI methods in finding anomalies becomes very necessary [17, 18]. With the use of deep learning and machine learning techniques, companies can develop robust anomaly detection systems that have the capacity to recognize intricate irregularities in social network ecosystems. These systems enable quick response times which help safeguard safety as well as integrity of these networks. So, what this suggested work aims for is to build a special strong social network structure.

In the case of an anomaly in social networks, it has become very essential in order to maintain integrity, security, and trust among these communities. Social networks are growing and changing into big datasets; they can have

complex structures and user behaviors that constantly change. For both, conventional anomaly detection methods may usually fail to deal with scaling and heterogeneity in social network data, hence making them hardly able to find patterns effectively different from the usual course of events. Besides this, the rapid evolution of social networks is continuously creating new patterns and behaviors that come up very frequently and require highly adaptable systems for their detection. Most of the current approaches to anomaly detection lack the capability of scalability, precision, and flexibility in handling the unique complexities of social network data. This, therefore, calls for more sophisticated frameworks which are accurate and capable of detecting anomalies in these environments to ensure that the malicious activities, fraudulent activities, cyber-attacks, or even dissemination of misinformation, get detected timely and curbed with befitting ways.

AdaptoDetect proposes a new horizon for detecting anomalies in social networks by integrating Pufferfish Optimization Technique-POT, and Graph Embedding Autoencoder-GEAE. The proposed framework mainly deals with some of the major challenges inherent in state-of-the-art anomaly detection techniques, such as feature selection, scalability, and adaptability. POT is an innovative optimization technique that performs the selection of the most relevant features from big social network data, focusing the most on attributes most indicative of anomalies. This is accomplished by shrinking the feature space into these key aspects, hence boosting the general accuracy and efficiency of the detection process from POT. Thus, AdaptoDetect is capable of outperforming traditional methods effectively. Meanwhile, the Graph Embedding Autoencoder component of AdaptoDetect learns low-dimensional representations from graph nodes by modeling complex patterns and relationships in the social network. This ability is hugely important for the identification of complex anomalies that can otherwise hardly be detected using conventional methods of detection. By integrating POT and GEAE within AdaptoDetect, the solution becomes all-round and solid, which can only enable precise anomaly detection through the indication of deviations in typical graph structures and behaviors in real time.

The novelty of AdaptoDetect is that it identifies anomalies in a holistic way; it seamlessly integrates feature selection and anomaly identification under the same framework. By doing so, it makes sure that AdaptoDetect is not only highly accurate but also adaptable to the ever-changing landscape of social networks. By fusing the strong feature selection of POT and the state-of-the-art graph embedding techniques of GEAE, AdaptoDetect can continuously monitor social network activity and update its detection concerning newly evolved patterns and behaviors. Indeed, such adaptiveness is crucial in social networks where rapid fluctuations in user behavior and the structure of the underlying network may render traditional detection methods void over time. When combined with the dynamic response to these changes by AdaptoDetect, this turns it into a powerful means for maintaining online communities secure and trustworthy. Moreover, the presented extensive framework evaluation was performed on the publicly available datasets of PubMed, Yelp, and ISA, which demonstrated superior performance in terms of accuracy, scalability, and flexibility compared to existing methods. These evaluations underlined the capability of AdaptoDetect to deal with a wide range of social network environments and positioned it as one of the most viable solutions within this sphere due to complex and dynamic data landscapes.

The following lists the main goals of the suggested work:

- This work introduced a novel framework named AdaptoDetect, it is the union of Graph Embedding Autoencoder (GEAE) with Pufferfish Optimization Technique (POT). This combination allows for effective identification of abnormalities in social networks. The method of AdaptoDetect also includes feature selection and anomaly detection algorithms, providing a complete solution to identify people's deviations from typical behavior within online communities.
- In the selection of relevant features from social network data, AdaptoDetect framework improves anomaly detection by using a technique known as POT. The use of features that have good potential for identifying anomalies combined with efficient narrowing of feature space brings about a more effective and efficient way to follow subsequent detection phases in AdaptoDetect.
- The selection is done by utilizing a specific feature-based method called GEAE. This mechanism has the ability to learn low-dimensional representations of nodes within social network graphs, thus helping in detecting complex linkages and patterns. By using these embeddings, GEAE makes sure that anomaly detection is precise enough to guarantee dependable recognition of deviations from usual actions in social networks.
- A wide-ranging performance study and comparison can be done by using public datasets that are known to everyone, such as PubMed, Yelp and ISA. This will help in measuring its strength and effectiveness for identifying abnormalities among online communities. It aims to show superiority, scalability and flexibility through the evaluation of performance on different social network datasets along with a comparison against existing methods.

The remaining information of this work has been separated into the following sections: In order to investigate various computational intelligence approaches currently in use for anomaly detection in social networks, a thorough overview of the literature is presented in Section 2. In order to facilitate precise analysis and problem characterization,

it also addresses the benefits and drawbacks of each model. Furthermore, the flow diagram, algorithms, and a comprehensive explanation of the suggested AdaptoDetect model are given in Section 3. In Section 4, the performance outcomes and results of the suggested AdaptoDetect model are verified through a number of assessment metrics. In Section 5, the results and future work are presented together with a summary of the entire research.

2. RELATED WORKS

The field of computational intelligence techniques used for social network anomaly detection is covered in this section. Through a review of recent developments in this area, we hope to clarify the effectiveness and applicability of different models in identifying anomalies within the complex dynamics of social interactions. Furthermore, a thorough examination of the benefits and drawbacks of each model is included, providing an understanding of its relative merits and weaknesses for anomaly identification in the intricate context of social networks. We hope that our investigation will shed light on the best practices for choosing and applying computational intelligence methods to improve anomaly identification in social network settings.

Anomaly Detection in social networks has recently become an active topic, as finding irregular activities within social networks is basically an indispensable way of maintaining online communities in respect to security and integrity. Various methods [19], developed over time, range from statistical techniques to machine learning-based methodologies, each trying to solve the unique challenges associated with the dynamic nature of social networks. The methods forming some of the earliest approaches used in anomaly detection include traditional statistical methods based on Gaussian mixture models and kernel density estimation. Most of these methods will assume that data points are generated from a known distribution, with an anomaly identified usually from points that show a significant deviation from a distribution that is expected. Though these methods are simple and easy to apply, more often than not, they fail in handling the high-dimensional and nonlinear nature of social network data, wherein relationships among data points are complex and mostly not captured by simple statistical distributions.

Machine learning techniques have been greatly explored for anomaly detection in social networks. There are several popular supervised learning methods for anomaly detection such as SVM and random forests where models that can differentiate between normal and anomalous behaviors are induced based on labeled datasets. These have often proved effective in applications within controlled environments where adequate labeled data is available. However, in social networks, labeled datasets are often scarce or imbalanced; hence, the application of supervised learning methods is limited. The approaches of unsupervised learning, including the methods of clustering technique-k-means, DBSCAN-and the dimensionality reduction approach-principal component analysis, PCA-would similarly look for anomalies in such data by searching for patterns and structures. Although these inherently fit better with the nature of social network data due to a lack of pre-labeling, these normally suffer from robustness issues when faced with noisy or incomplete data-the usual case in social networks [20].

Graph-based approaches have been popular recently because of their capability to model the relational nature of social networks. Graph convolutional networks and graph autoencoders constitute examples of methods that capture structural and relational information from social network data for the purpose of allowing accurate anomaly detection. These methods learn the representation of either graph nodes or edges to identify anomalies as deviations from common structures in graphs. While graph-based approaches have shown great potential in enhancing the accuracy of detection, their computational cost is usually very high and cannot be scalable for very large networks.

In all, different methods have been proposed to perform anomaly detection in social networks, but most of them fall short of covering all the dimensions of challenges these complex environments bring in. The traditional statistical approaches are not flexible for nonlinear and high-dimensional data analysis, while the machine learning methods suffer due to lack of labeled data and robustness for real-world applications. While the graph-based methods are indeed effective in modeling relational data, scalability and computational challenge is an open problem. Complete solutions are still needed that effectively include feature selection, adaptability, and efficiency for anomaly detection in social networks.

Xu, et al [21] presented a customizable Bayesian network model designed for detecting and identifying anomalies in social networks on a large scale. This model provides a strong structure that can effectively analyze complicated network structures and large amounts of social data, allowing for accurate anomaly detection on a large scale. The authors presented an interesting inference technique that determines, considering the parameters of a collection of binary data points observed from readily accessible sensors. The suggested methodology is capable of being applied to large-scale graph topologies because of its creative usage of Bayesian networks to bring together vectorization and parallelization. Cao, et al [22] examined how GPT-4V(ision), a strong visual-linguistic model, may be applied for broad anomaly detection applications. This study covers time series, logical industrial, point cloud, and other types of anomaly detection activities. Zardi, et al [23] presented a community-based method for identifying abnormalities in social networks, where user traits and network structure are analyzed using an efficient ranking-based methodology. Community-based approaches are more successful in spotting irregularities in graphs with attributes. This is because the node under investigation should share traits with other nodes in its community, and these methods determine a node's contextual environment based on the collective group of nodes. Scaling problems may arise when community-

based anomaly detection methods are used to large social networks with millions or billions of nodes and edges. The computational complexity of community detection techniques may become unmanageable when working with huge datasets. Guo, et al [24] developed a graph-based Generative Adversarial Network (GAN) for detecting abnormalities in social networks. In order to enhance the detection, they merged the prediction model with spatiotemporal logic. This approach considered the differences between random variables and data encoding, as well as the disparities between generated and real data. They also aimed to provide the generators with improved potential representations as input, stabilize their sample production, and bypass the expensive optimization process typically associated with traditional graph generative adversarial networks.

Kim, et al [25] carried out a thorough comparison analysis to look at several time series anomaly detection techniques for industrial control systems. The scoring process, which separates anomalous data items from the dataset, is the most important component of the unsupervised anomaly detection system. The main concept is to establish a scoring strategy that works well and enhances the difference among attack and normal data (i.e., anomalies), which improves prediction performance in the context of erroneous or incorrect detections. Chen, et al [26] established an insolation forest technique-based data anomaly detection method to guarantee the security of IoT devices. Furthermore, there are numerous types of anomaly detection algorithms, such as those based on statistics, clustering, proximity, and classification. This study shows that the majority of earlier methods struggled with issues such higher costs, the need for human parameter tuning, and complicated parameter selection. Elaziz, et al [27] used a deep reinforcement learning technique to detect and classify the many kinds of abnormalities found in the social network. The suggested framework aims to build an environment using training data. The DRL agent can interact with and learn from this environment. The environment's primary objective is to give the agent the ability to make use of the small number of anomalies that have been found and look for any more anomalies in the unlabeled data that might not be in the set. To strike a balance between exploitation and exploration, a mixed reward function integrates supervisory signals from both suspicious unlabeled anomalies and labelled anomalies. In the training phase, the agent discovers anomaly and gains the ability to distinguish between an anomalous and non-anomalous new trace through both exploitation and exploration.

Hayawi, et al [28] conducted a systematic literature review to investigate the different types of deep learning algorithms used for bot detection. Social media profiles that are automated but yet have human control are known as social bots. Positive functions for such bots include disseminating news updates and offering support when required. Bots have, however, also been employed maliciously, such as disseminating rumors and misleading information or interfering with political campaigns. Thankfully, there are currently processes in place to identify and eliminate dangerous bots automatically. Huang, et al [29] introduced an unsupervised outlier detection mechanism based on spectral clustering mechanism for social networks. In the field of data mining, identifying outliers is crucial for research, especially in relation to network security, credit card fraud detection, industrial problem detection, and other related fields. However, the three main challenges facing the current generation of outlier identification techniques are the curse of dimensionality, the lack of labelled data, and hyperparameter tweaking. Thudumu, et al [30] carried out an extensive analysis of the literature to look at several approaches for social network anomaly identification. The precise anomaly finding using AI algorithms was the main emphasis of this study's writers. The study concludes that in order to achieve better performance outcomes, the dimensionality of large-scale social data must be decreased by the application of optimization techniques.

Dealing with unlabeled data is frequent when discovering anomalies in social networks, wherein anomalies can take on a variety different patterns and characteristics. For this application, unsupervised machine learning methods like auto encoders and clustering work well because they can identify abnormalities even in the lack of labelled training data. Moreover, the AI models that are trained to detect anomalies may offer early alerts for a range of dangers, including planned assaults, misinformation operations, and the distribution of viral material. These technologies facilitate the prompt identification of anomalies, resulting in proactive mitigation and intervention strategies. AI-driven anomaly detection systems make use of sophisticated algorithms and computing power to improve efficiency and accuracy over conventional methods.

3. PROPOSED METHODOLOGY

In this part, the proposed framework for social network anomaly detection is explained in detail and with clarity. All suggested concepts for design, methodology, and implementation strategies are covered in detail. The article delves into the potential enhancement of anomaly detection skills in social network environments by utilizing the suggested paradigm. By describing the framework's adaptive features, use of cutting-edge computational intelligence techniques, and integration of instantaneous data processing, it also aims to shed light on and clarify the innovative approach presented by the suggested methodology. This proposed effort aims to develop a robust and scalable system for Social Network Adaptive Anomaly Detection (AdaptoDetect). The suggested structure was customized to accommodate the constantly evolving social media environment. AdaptoDetect aims to leverage state-of-the-art computational intelligence techniques to adaptively analyze large volumes of social network data, identify anomalous occurrences or behavior patterns, and promptly issue alerts or take appropriate action to mitigate any risks. With the addition of adaptation to the detection process, AdaptoDetect seeks to enhance anomaly detection in social networks. Long-term,

this will support preserving community safety, network integrity, and user trust. Fig 1 provides an overview of this framework, which uses unique and innovative computational algorithms for anomaly detection and categorization. As shown in Fig 2, the following is a list of the processing steps that this model uses:

- Data collection from social networks
- Data preparation & setup
- Pufferfish Optimization Technique (POT) for feature selection
- Graph Embedding Auto-Encoder (GEAE) for anomaly detection
- Testing performance & efficiency

The first step in this procedure is to collect data from different social networks, which are the main source of information for the model. Getting user profiles, posts, comments, network connections, and other pertinent social behaviors are a few examples of data collection techniques. The preparation stage makes sure the data is high-quality and appropriate for analysis. In this step, the raw data is cleaned, normalized, and transformed into a structured format that the model can use efficiently. Another crucial component of data preparation is splitting the dataset into appropriate subgroups for training, validation, and testing. The POT technique is then used for feature selection, which is more crucial for enhancing the anomaly detection system's overall effectiveness and performance. Additionally, it helps to properly identify and select the standout aspects from the social data that is presented. The data's total dimensionality has decreased as a result of the integration of this technology. As a consequence of this, the novel GEAE methodology has been implemented in this framework, which is the key element of AdaptoDetect that is more responsible for accurate anomaly detection. Moreover, it uses the graph embedding structure to get the meaningful data representations, while maintaining its structural relationships. Moreover, an autoencoder model has also been integrated with the graph architecture, and the hybrid model reconstructs the input data for recognizing the deviations and anomalies with reduced error rate. At the end of this process, the overall anomaly detection performance and efficacy of the proposed AdaptoDetect model has been validated using popular metrics and benchmarks. The primary advantages of the proposed AdaptoDetect model over other existing anomaly detection systems are high robustness, high efficiency, reduced error rate and low system complexity.

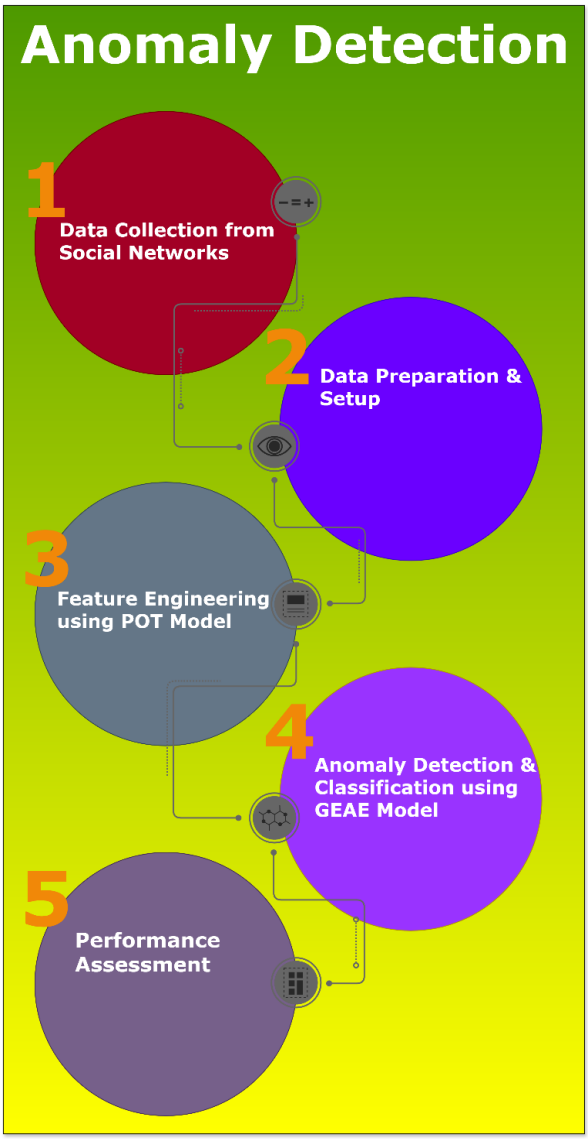


Figure 1. Overview of the proposed AdaptoDetect

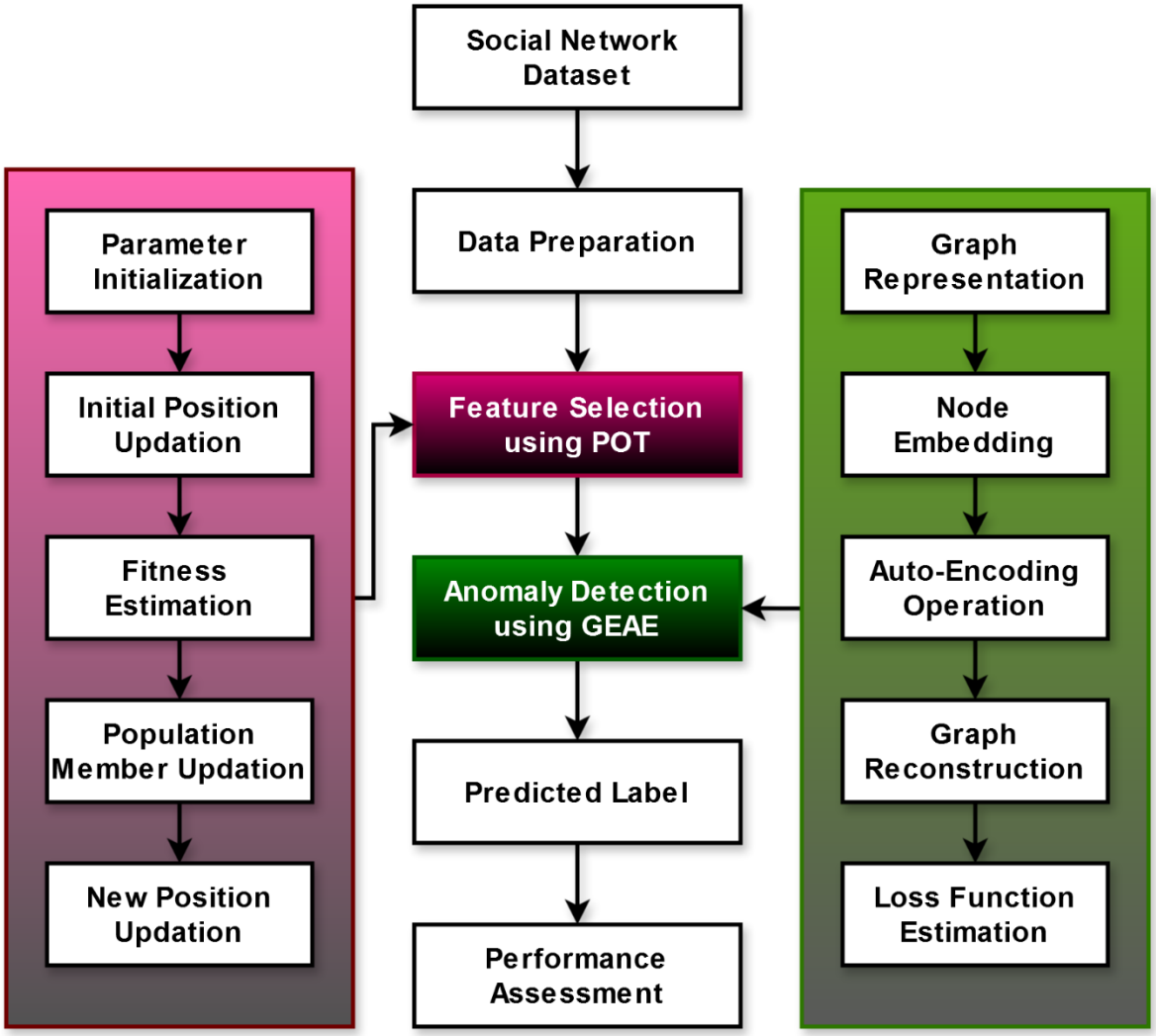


Figure 2. Flow of the proposed AdaptoDetect framework

A. Pufferfish Optimization Technique (POT) for Feature Selection

After data preparation, the next step involves feature selection using the POT technique, which is more important for improving the overall performance and effectiveness of the anomaly detection system. It also aids in correctly identifying and choosing the noteworthy features from the provided social data. The inclusion of this technology has reduced the total dimensionality of the data. The POT is a population-based technique that, through an iterative process, can effectively solve optimization problems by utilizing its population search power in the problem solving space. The values of the problem's decision variables are determined by each POT member based on the problem's location within the search space. Since a vector may be used to explain the problem mathematically and each element of the vector corresponds to a decision variable, each POT member is a potential solution to the problem. Algorithm population is made up of all POT members combined. Here, the position is performed based on the following equation;

$$p_{i,d} = l_{bd} + \alpha \times (u_{bd} - l_{bd}) \quad (1)$$

Where, p_i indicates the population, d is the dimensionality, l_{bd} denotes the lower bound, u_{bd} represents the upper bound, and α is the random number. The assessed values for the objective function serve as appropriate benchmarks to assess the caliber of potential solutions put up by every POT member. The optimal member, or the best candidate solution, is represented by the best evaluated value for the objective function, and the optimal member, or the worst candidate solution, is represented by the worst assessed value for the objective function. Every iteration updates the position of POT members in the problem-solving space; hence, every iteration should update the best member based on a comparison of newly evaluated values for the objective function. The suggested POT approach is constructed by updating the placements of population members in the problem-solving space using a simulation of the natural behaviors between pufferfish and their predators. In this natural process, the pufferfish is initially attacked by the predator. The pufferfish then uses its protection mechanism to transform into a ball of sharp spines, which threatens the predator and makes it retreat. Thus, every iteration updates the position of members of the POA population in two

stages: (i) exploration, which mimics a predator striking a pufferfish, and (ii) exploitation, which mimics a pufferfish employing its defense strategy.

During the first phase of POT, the positions of the population members are updated regularly. This is achieved by having the pufferfish imitate the predator's attack plan. Pufferfish's lazy, languid motions make them easy prey for ravenous predators. The placements of the POA members within the problem-solving environment are adjusted to correspond with the simulated position shift of the predator during the attack. This approach expands the scope of the global search by facilitating more investigation. To do this, the placements of the POA members are significantly altered by mimicking the predator's approach to the pufferfish. The location of other population members with a higher value for the objective function is taken into consideration while designing the POA for each member of the population acting as a predator. This position is known as the candidate pufferfish for attack. The following formula is used to determine each population member's set of pufferfish:

$$\mathfrak{B}_i = \{P_m : o_m < o_i \ and \ m \neq i\}, i = 1, 2 \ldots N \ and \ m \in \{1, 2 \ldots N\} \quad (2)$$

Where, $\mathfrak{B}_i$ represents the candidate population, P_m denotes the population member, o_m represents the objective function, and N is the total number of populations. Within the POT design, it is believed that the predator willfully chooses one pufferfish from the candidate population set of pufferfish; this pufferfish is referred to as the selected pufferfish. Each POT member is assigned a new position in the problem-solving space, as indicated by equation 3, based on the modelling of the predator's progress towards the pufferfish. The new position then replaces the associated member's prior position in accordance with equation 4 if the objective function value there is improved.

$$p_{ij}^G = p_{ij} + \partial_{ij} \times (\delta_{ij} - \kappa_{ij} \times p_{ij}) \quad (3)$$

$$P_i = \begin{cases} P_i^G, & \mathcal{F}_i^G \leq \mathcal{F}_i \\ \mathcal{F}_i & Else \end{cases} \quad (4)$$

Where, p_{ij}^G represents the new position, δ_{ij} is the selected pufferfish, ∂_{ij} denotes the random value [0, 1], and κ_{ij} is the random number (i.e. 1 or 2). Using a simulation of a pufferfish's defense mechanism against predator assaults, the position of population members is updated throughout the second phase of POT. A pufferfish fills its incredibly elastic stomach with water to defend itself from predators, turning it into a ball of sharp spines. Instead of taking advantage of the easy meal, the predator in this scenario flees from the pufferfish's location. The exploitation potential of the local search algorithm is increased by modelling the predator moving away from the pufferfish, which causes slight changes in the POT members' positions. The new location of each POT member is calculated in equation (5), which accounts for the predator's shift in position as it moves away from the prey. If the new position raises the value of the objective function, equation (6) is applied to replace the relevant member. Once the POT member has decided on a new position, the effectiveness of the new position is assessed by comparing its values to the aim function.

$$p_{ij}^T = p_{ij} + (1 - 2\partial_{ij}) \times \frac{u_{bdj} - l_{bdj}}{h} \quad (5)$$

$$P_i = \begin{cases} P_i^T, & \mathcal{F}_i^T \leq \mathcal{F}_i \\ P_i & Else \end{cases} \quad (6)$$

Where, p_{ij}^T is the newly updated position. The initial algorithmic iteration has been finished by adjusting the positions of all POT members according to the phases of exploration and exploitation. After that, the algorithm continues, changing the placements of POT members until the last algorithmic iteration. By using the best optimal value, the most significant features are selected from the social data, and these features are then used for classifier's training and validation processes.

B. Graph Embedding Auto-Encoder (GEAE) for anomaly detection

The Graph Embedding Auto-Encoder (GEAE) is a sophisticated learning method that can recognize abnormalities in datasets having complex relationship structures, like social networks. By blending graph embedding with autoencoder designs, the GEAE maintains the initial graph topology while gaining knowledge about data representations effectively. Turning nodes or other parts of a network into continuous vector space is called graph embedding. Why are the geometric aspects of these vectors important? They give understanding about the design of graph. Graph embedding assists the model in understanding characteristics of network, like relations and actions. This is used for anomaly detection and classification in social networks. Here, the output features from previous stage has been utilized for anomaly detection and classification. Typically, an autoencoder can handle complex data, thanks to the current advancement in deep neural networks. With deep neural networks serving as an encoder/decoder, one can reach to the latent space through multiple steps of nonlinear transformation, which can help unfold data with complex intrinsic structure and greatly facilitate the subsequent detection objective.

In the field of anomaly detection, GEAE combines autoencoder's ability to reconstruct input data with graph embedding's power in keeping relational information. In training, GEAE learns how to accurately rebuild normal or typical instances from the data set. Unusual instances that deviate from the norm generally have higher reconstruction errors because it is more difficult for the model to replicate these uncommon patterns precisely. The training stage works by adjusting the autoencoder network's parameters, making sure they lead to the least possible reconstruction

error on provided training data. When it is properly trained, we can apply GEAE for inference. This is done through providing fresh information to the model and computing reconstruction errors. Those examples that exhibit significantly heightened reconstruction error are identified as anomalies, indicating there could be abnormalities or doubtful actions occurring within social network systems. GEAE holds specific advantages for anomaly detection in social networks [31]. The model uses graph embedding, which helps it to understand the complicated relationship structures of social interactions. This results in more reliable detection of anomalies. Also, the design with autoencoder supports learning without supervision and this makes it appropriate for finding abnormalities when there is no need to have marked data. Moreover, the POT is skilled in picking out the most helpful features from high-dimensional datasets.

When it is combined POT with GEAE, it becomes possible to find and choose the important features from our social network data. This helps to decrease the size of input space, making it more efficient for computation while also improving model's capacity in identifying crucial aspects for detecting anomalies. Social networks naturally have intricate relationship structures, with interactions among users, groups and content. Incorporating graph embedding in the GEAE allows the model to comprehend and safeguard these relationship dependencies. Through using continuous vector space to embed nodes and edges, GEAE retains crucial data about network structure and connection which aids better anomaly identification. The integration of GEAE and POT makes it possible to do anomaly detection without supervision in social networks. The model can find out things that are different from the normal network activity by itself, not needing labeled data for this task. This is especially useful in analyzing social networks because it may be hard or not possible to label anomalies because of how social interactions keep changing all the time. There's a rise in these because of user actions, variety of content and changes in the network itself. The GEAE-POT model combines graph embedding with an autoencoder to deal with these challenges. It is made robust by using graph topology to highlight important features and represent the data's structure. Because it learns from significant characteristics while being shielded from noisy or variable elements through graph embedding for input representation, this model can effectively tell apart between normal and abnormal activities in a social network.

Usually, an encoder is a feed-forward neural network and has several layers in most practical scenarios. This is how the encoding process works:

$$\mathfrak{F} = a_{\varrho}(A) = x(\omega_{en}A + \mathfrak{b}_{en}) \tag{7}$$

$$\varrho = (\omega_{en}, \mathfrak{b}_{en}) \tag{8}$$

Where, a_{ϱ} is an encoding mechanism, ω_{en} is the weight value of the encoded data, $\mathfrak{b}_{en}$ is the bias value of the encoded data, $x(.)$ is the activation function, $\mathfrak{F}$ is the original data, and A is the reconstructed data. Decoder is like a different neural network, it rebuilds the main data and we can summarize this as:

$$A' = f_{\theta}(\mathfrak{F}) = x(\omega_{de}\mathfrak{F} + \mathfrak{b}_{de}) \tag{9}$$

$$\theta = (\omega_{de} + \mathfrak{b}_{de}) \tag{10}$$

For the autoencoder to work well in capturing an effective representation within the latent space, its design is based on minimizing a loss function. This function measures how much reconstruction error exists between the original data and recreated version from compressed form. The most commonly used loss function for this purpose is squared error loss, which can be expressed as follows:

$$\min_{\varrho,\theta} \mathbb{L}(A,A') = ||A - A'||_f^2 \tag{11}$$

In this algorithm, the graph regularization process is combined with minimum spanning tree idea. The distance calculation happens based on similarity measure in equation:

$$\omega_{ij} = \begin{cases} \frac{1}{\mathcal{S}_{ij}}, & if\ \mathcal{S}_{ij} > 0 \\ 0, & Otherwise \end{cases} \tag{12}$$

The suggested GEAE is given in terms of the joint loss function of the model. Also, the reconstruction error and minimum spanning tree-based embedding function are computed as shown in the following equation:

$$\min_{\varrho,\theta} \mathbb{L}(A,A') + \mathcal{G}(\mathfrak{F}) \tag{13}$$

$$\mathcal{G}(\mathfrak{F}) = \left\{\sum_{i<j}(\mathcal{S}_{ij} - \left|\left|\mathfrak{F}_i - \mathfrak{F}_j\right|\right|_2)^2 \right. \tag{14}$$

Then, its appropriate loss function is estimated as shown in the following equation:

$$\text{GEAE:} \min_{\varrho,\theta} \mathbb{L}(A,A') + \tau \times \frac{1}{2}\sum_{i<j}\left|\left|\mathfrak{F}_i - \mathfrak{F}_j\right|\right|_3^2 G_{ij} \tag{15}$$

Where, τ indicates the regularization parameter, and G_{ij} represents the similarity matrix. The use of this technique makes the anomaly detection successfully work in the suggested framework, showing low error rate and high precision.

It is hereby proposed that a new feature selection algorithm, to be called the Pufferfish Optimization Technique-POT in short-be specially designed with a view to enhancing effectiveness and efficiency in anomaly detection in social

networks. POT takes a cue from the self-defense mechanism used by pufferfish-to deter predators from attacks by inflating themselves-and, taking advantage of this metaphor, proceeds to inflate the relevance of important features while deflating the less important ones. The functionality of this optimization technique works in an iterative refinement of a set of candidate features by applying a fitness function that estimates the importance of each feature for discriminating anomalies from normal behavior. The key intuition behind POT is that its goal is to focus on a few features with high potential to indicate anomalies, which reduces the dimensionality of data and enhances the computational efficiency of subsequent phases of detection. The feature selection method used in AdaptoDetect is POT, because it can auto-update the set of features to conform with dynamically evolving patterns that appear in social network data. Preliminary experiments demonstrate that POT significantly reduces the number of features required for effective anomaly detection without compromising accuracy. This reduction in feature space not only accelerates anomaly detection but also avoids overfitting issues, which are common challenges when handling high-dimensional data. Theoretically, the analysis also indicates that POT can achieve a better trade-off between exploration and exploitation during the process of feature selection, which makes it robust in dynamically changing data characteristic environments such as social networks.

By contrast, AdaptoDetect uses Graph Embedding Autoencoder in order to learn complex relations and patterns within social network graphs. The GEAE is a neural network architecture designed to learn the low-dimensional representations or embeddings of nodes in graphs. These embeddings capture the structural and semantic properties of the nodes and their neighborhoods; hence, the model is able to spot those small anomalies that may denote malicious behavior or other forms of anomaly. Unlike traditional autoencoders that generally operate on vectorized data, the GEAE is tailored for graph-structured data, which makes it particularly fit for social networks, where the relationships between entities are as important as the entities themselves. It chooses between different GEA variants, and AdaptoDetect selects between them based on their well-documented performance at learning rich and meaningful graph representations that are relevant for modeling the subtle nature of social network behavior. Equipped with these graph embeddings, AdaptoDetect is able to detect anomalies more precisely that manifest themselves in the form of deviations from normal structures. Initial experiments on the GEAE already showed that it outperforms the conventional autoencoders not only in detection accuracy but also in generalization ability when unseen network topologies are presented. Theoretically, their derivations provided the effectiveness of GEAE to preserve the manifold structure during the process of graph embedding, a key factor to the integrity of the learned representation.

In this respect, the integration of POT and GEAE in AdaptoDetect is a strategic choice to possess the maximum strengths of both techniques while compensating for their respective limitations. The efficiency of POT in efficiently narrowing down the feature space is complemented by the capability of GEAE to learn comprehensive graph embeddings, resulting in a holistic anomaly detection framework that is scalable and adaptable. Algorithmic details of POT mainly involve initialization of the population of candidate feature sets and iterative refinement according to the fitness function that quantifies the effectiveness of a set of features in anomaly detection. It does include both local and global search strategies so that an extensive search through the feature space is performed. In contrast, the encoder-decoder structure of GEAE compresses the graph data into a lower-dimensional space, whereby the decoder will attempt to reconstruct the original graph from such embeddings. The reconstruction error is minimized by backpropagation, and the embeddings that result in the minimum reconstruction error will be considered to be optimal in capturing the network's inherent structure.

4. RESULTS AND DISCUSSION

In this section, an in-depth analysis of the performance outcomes and results of the AdaptoDetect framework is presented. Our evaluation plan focuses on studying various public social datasets to see how well it can handle different types of social network traits, actions and interactions. The selection of these datasets is important because it makes sure our examination covers a wide variety of scenarios found in real life. This allows us to make significant observations about how effective and strong the framework is for detecting anomalies within social network data. For measuring how well the AdaptoDetect framework works, we use a group of recognized evaluation measures. These are carefully picked to give detailed understanding into its performance across different aspects of finding anomalies. The assessment methods include precision, recall, F1-score, accuracy and analyses like receiver operating characteristic (ROC) curve analysis plus area under the curve (AUC). We also consider other relevant metrics for a thorough understanding.

First, three well-known datasets from PubMed, Yelp, and ISA were chosen to verify the performance of the AdaptoDetect framework in anomaly detection in social networks. They have been selected for presenting different social network scenarios regarding the size and structure of data, anomaly type, and characteristics. We present a thorough description of each dataset used, the settings of the parameters in our experiments, and the computational resources needed to ensure transparency and further facilitate the reproduction of the results shown.

The PubMed dataset is one of the benchmark datasets in the field of graph-based learning and anomaly detection; it has been derived from the citation network of PubMed papers. The nodes in this dataset correspond to documents, while edges correspond to citation relationships among them. It contains approximately 19,717 nodes and 44,338

edges, where each node is described by a 5,000-dimensional feature vector that represents word frequencies in the abstract of the paper. Regarding anomaly detection, the dataset has been labeled to identify outlier papers, defined as papers whose citation pattern differs considerably from the majority. The performance of the AdaptoDetect framework on this dataset was then demonstrated by applying POT for feature selection according to citation pattern and node attributes relevance while utilizing Graph Embedding Autoencoder to learn the low-dimensional embedding of graph nodes.

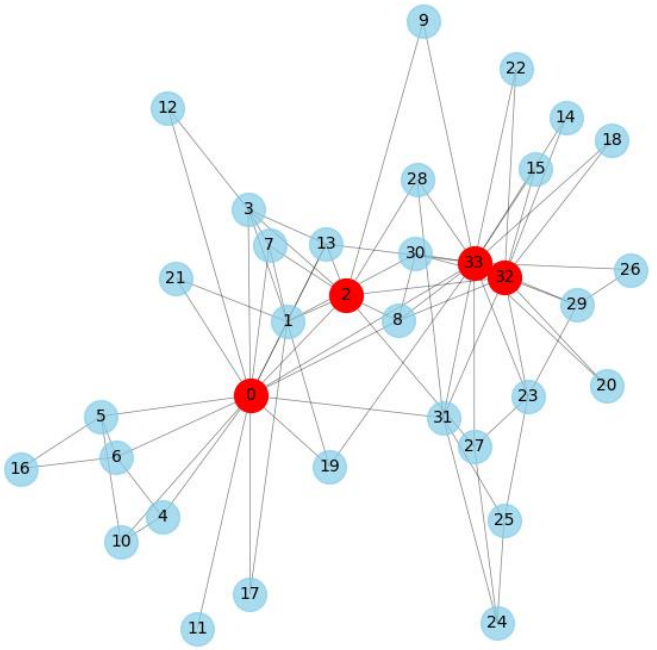
A node in the Yelp dataset represents a user, while the edges represent the social relationships among users. It also characterizes nodes with feature vectors that summarize user behavior, including review counts, average review length, and sentiment scores. Anomalies in this dataset include those users whose review or social patterns are abnormal, indicative of fraud or spam. An experimental study using the AdaptoDetect approach on the challenges of large-scale social networks with the Yelp dataset: in the dataset, the proposed approach with POT shrinks the high-dimensional feature space effectively by selecting features indicative of anomalous user behavior, while the embedding method GEAE is used to model complex social relationships and detect anomalies using deviations in learned embeddings.

Furthermore, each node has a feature vector comprising user role, activity level, and security classification. Anomalies in the ISA dataset are defined as interaction patterns or attributes highly conflicting with the normal regularities of individuals constituting those roles or clearance levels. The fact may point out insider threats or another security breach in the organization. Therefore, the ISA dataset is more effective in evaluating AdaptoDetect performance for sensitive security environments. While POT was leveraged to identify the salient features reflecting security-related anomalies, GEAE learned the graph embeddings indicative of usual interaction patterns and flagged deviations as the possible cause for security risks.

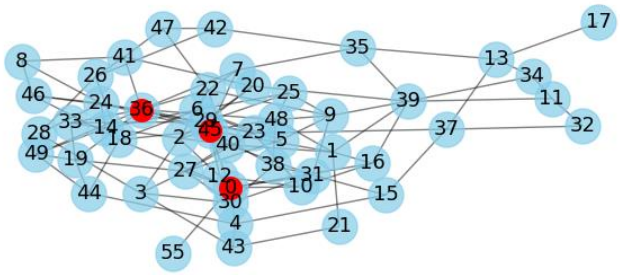
The parameter settings of the AdaptoDetect framework have been made with great care to be optimal in most different datasets. Hence, in the POT, parameters like population size, the number of generations, and mutation rate were tuned in view of some initial trials to balance the exploration and exploitation features in the selection process. The following hyperparameters were optimized for the GEAE algorithm: number of hidden layers, size of embeddings, learning rate, and number of training epochs were tuned with the grid search approach. The encoder-decoder architecture in GEAE was designed in such a way to retain the low reconstruction error while the learned embeddings still capture the essence of the graph structure.

The experiments were executed on a high-performance computing cluster equipped with several NVIDIA A100 GPUs with 40 GB each, supported by an Intel Xeon Platinum multi-core processor. In fact, this setup has provided the required computational power to handle extensive data processing and model training related to the large-scale Yelp dataset and complex graph structures of PubMed and ISA datasets. Each experiment has been replicated several times in order to ensure consistency and dependability in the results. Wherever applicable, average metrics are reported for accuracy, precision, recall, and F1-score. Most of the experiments were supported by detailed logging and check pointing to allow their easy reproduction and the creation of the same outcome under the same settings and by other researchers.

By using this variety in evaluation measures, our goal is to show many sides of framework's effectiveness and provide an overall view on how it performs. Finding anomalies in social networks refers to the task of recognizing odd or unexpected behavior, interactions, or events happening within the network. This is an important process as it helps to keep social network platforms honest, safe and dependable. Different methods are used for detecting anomalies in social network data such as statistical techniques, machine learning algorithms and graph-based approaches. In this way, identifying abnormalities like fraud, strange user actions or new patterns can help organizations lessen risks, increase trust from users and make better decisions. As shown in Fig 3, the anomalies are identified and discovered in the social networks using AdaptoDetect model.



(a)



(b)

Figure 3. Sample anomaly detection process in social network

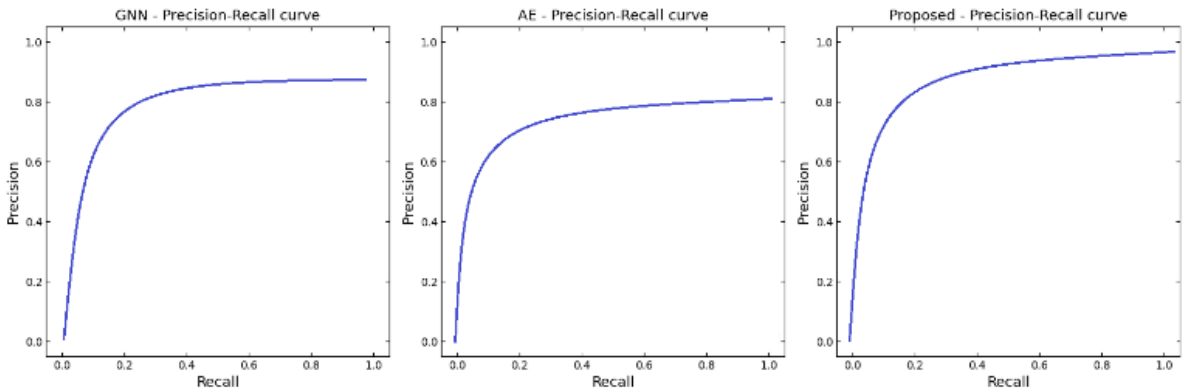


Figure 4. Precision-Recall curve

The curve of precision-recall shows the connection between precision (positive prediction value) and recall (true positive rate), for different thresholds. Recall gauges how many relevant results were found, while precision measures how many of the retrieved instances were actually relevant. The ROC curve shows how changing the false positive rate (1-specificity) influences the true positive rate (sensitivity). The false positive rate means wrongly identifying non-anomalies as anomalies, while the true positive rate is about correctly identifying actual anomalies. As shown in Fig 4 and Fig 5, it is determined that every model's performance (GNN, AE and GEAE) on a labeled dataset and calculate accuracy, recall, true positive rate as well as false positive rate at different threshold setups.

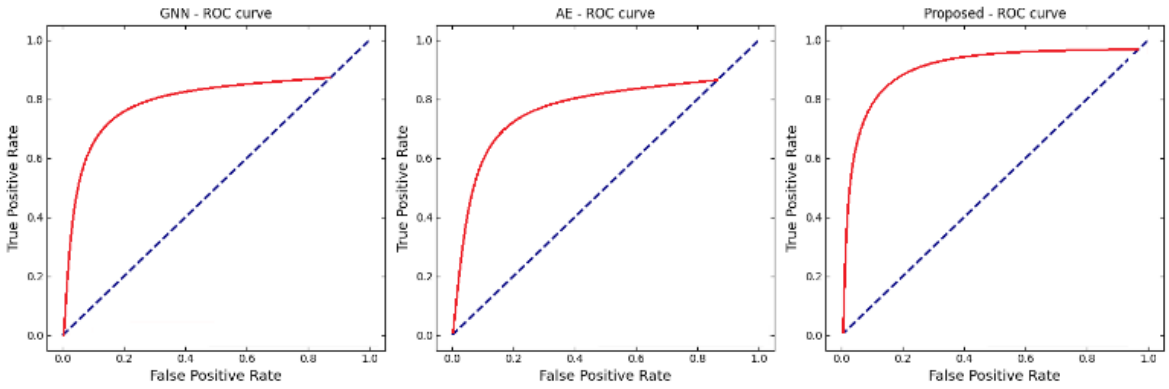


Figure 5. **ROC analysis**

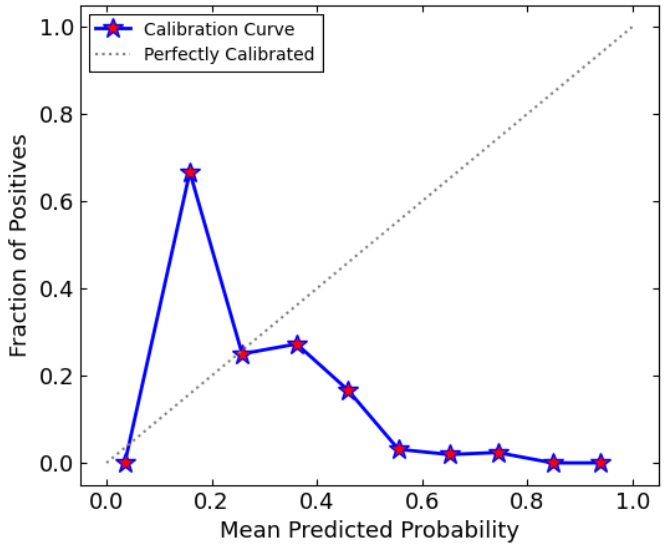


Figure 6. **Mean predicted probability Vs fraction of positives**

The graph of mean predicted probability and fraction of positives is a common visualization to evaluate the working of classification models like those used in detecting anomalies [32]. As represented in Fig 6, the average predicted probability shows the typical output from model for positive class (anomaly) over various threshold values. When we change the boundary for classification, mean forecasted likelihood shows how sure model thinks an instance is an anomaly or not. A higher mean predicted probability shows more sureness in identifying anomalies, but when it's lower this means there is less confidence. Also, the fraction of positives matches with how much instances are classified as positive (anomalies) by the model over different threshold values. This measures its ability to correctly recognize anomalies from all instances in dataset. A larger fraction of positives reveals that the model is correctly identifying more anomalies, whereas a smaller fraction implies less number of detected anomalies.

Precision is the ratio of retrieved instances that are relevant to all the instances that were retrieved. It shows how many of the results identified by the anomaly detection model are actually anomalies. High precision means there are less false positives, showing a better accuracy in identifying anomalies. Recall is defined as the ratio of relevant instances that have been retrieved over total amount possible; it shows how many anomalies were detected out of all possible ones present in dataset or area being examined (source). If the recall is high, it means that the model is recognizing more abnormalities. This results in less false negatives. F1-score calculates a balance between how precise and complete the model's results are. It gives a good overall gauge of how well the model performs. The F1-score considers both false positives and false negatives, making it useful to measure total effectiveness of a model. The parameters are calculated as shown in below:

$$\text{Accuracy} = \frac{Tp+Tn}{Tp+Fp+Tn+Fn} \tag{16}$$

$$\text{Precision} = \frac{Tp}{Tp+Fp} \tag{17}$$

$$\text{Recall} = \frac{Tp}{Tp+Fn} \tag{18}$$

$$F1-score=\frac{2Tp}{2Tp+Fp+Fn} \quad (19)$$

Where, Tp – true positives, Tn – true negatives, Fp – false positives, and Fn – false negatives. Fig 7 and Fig 8 confirm the correctness of accuracy, precision, recall and f1-score numbers for conventional and proposed anomaly detection methods using PubMed dataset. The right values are shown in Table 1 and Table 2 [33]. As per this comparison analysis, it is decided that AdaptoDetect performs well and gives better performance results than other current approaches. This decision is reached because merging POT with GEAE helps to get the desired outcomes.

The AdaptoDetect framework has performed outstandingly on the PubMed and Yelp datasets, respectively, in terms of accuracy, precision, recall, and F1-score. The superiority of the results can be summarized into several crucial factors. First is the very effectiveness of feature selection by POT, which contributes to enhancing the detection capability of the proposed framework. It allowed AdaptoDetect to target those most relevant features by only shrinking the feature space down to the ones that contributed a lot toward finding anomalies-for example, unusual citation patterns in PubMed and returning back to normal user behaviors in Yelp. This now becomes an issue of targeted approach rather than reduction of computational complexity. This increases the model's ability to identify minor deviations from regular behavior, which is usually a very important factor in complex social networks.

Besides, the ability of GEAE to learn the low-dimensional feature representations for nodes in a graph played an important role in modeling those complex patterns and relationships that are inherently embedded within the datasets. For example, in the PubMed dataset, whose edge relationships are defined by citations between nodes or papers, the capability of GEAE modeled these connections effectively by detecting nodes with different behaviors in terms of citations. Similarly, it has been a rich tapestry that GEAE was able to navigate around the Yelp dataset full of social networks with very detailed attributes of users in order to detect fraudulent activities and spam. These embeddings retain the essential structural and semantic properties of the original data points, thus enabling this framework to detect even the most subtle anomalies which usually go unseen when using traditional methods of detection.

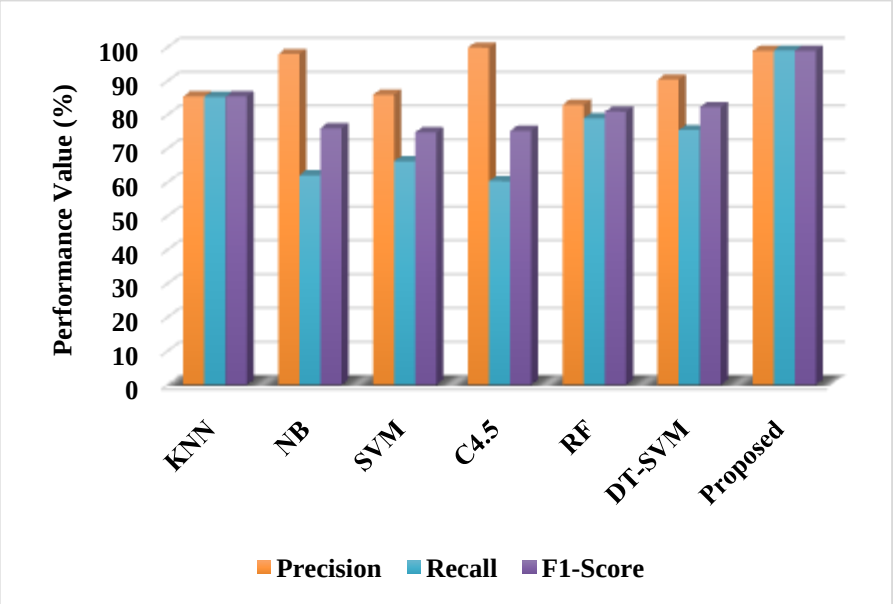


Figure 7. Comparative analysis using PubMed dataset

Table 1. Performance comparison using PubMed dataset

Methods	Precision	Recall	F1-Score
KNN	85.44	85.34	85.39
NB	97.97	62.05	75.98
SVM	85.95	66.19	74.77
C4.5	99.88	60.33	75.22
RF	82.97	78.96	80.92
DT-SVM	90.42	75.45	82.26
Proposed	98.9	99	98.9

Table 2. Accuracy comparison using PubMed dataset

Methods	Accuracy
KNN	83.83
NB	83.58
SVM	81.31
C4.5	82.38
RF	83.56
DT-SVM	85.57
Proposed	99

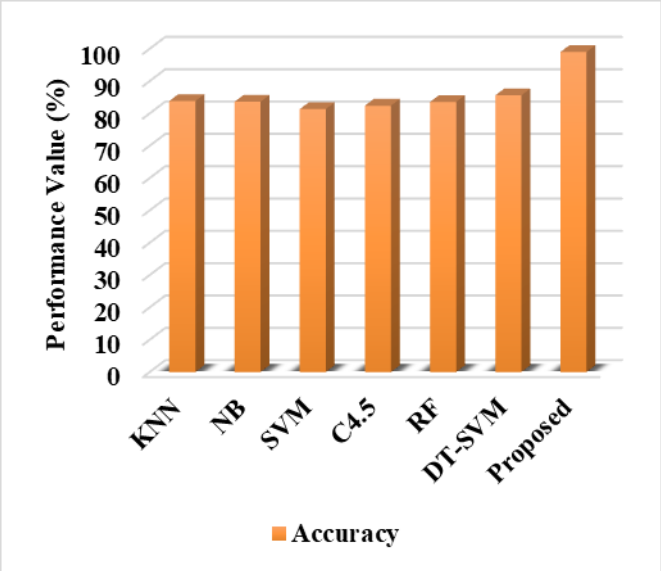


Figure 8. Comparison based on accuracy using PubMed dataset

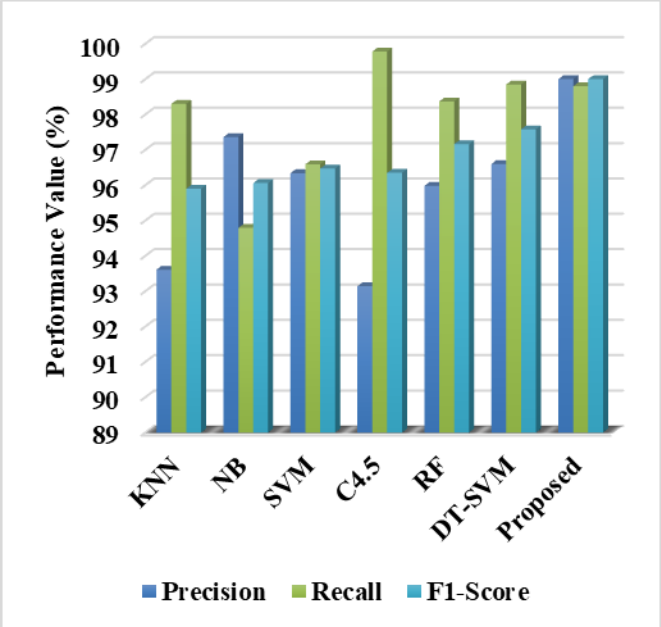


Figure 9. Comparative analysis using Yelp dataset

In a similar manner, Table 3 and Table 4 compares the conventional and proposed anomaly detection approaches with Yelp dataset. These can be seen in the graphical depiction of Fig 9 and Fig 10. The results show that this AdaptoDetect model gives more results compared to all existing approaches. By choosing good features and methods for detecting anomalies, it greatly enhances the overall effectiveness of our suggested AdaptoDetect model.

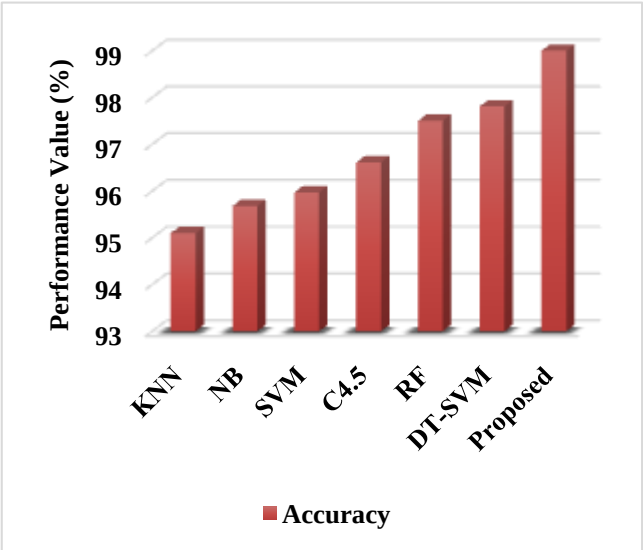


Figure 10. Comparison based on accuracy using Yelp dataset

Table 3. Performance comparison using Yelp dataset

Methods	Precision	Recall	F1-Score
KNN	93.61	98.30	95.90
NB	97.36	94.79	96.06
SVM	96.34	96.59	96.47
C4.5	93.14	99.78	96.35
RF	95.98	98.37	97.16
DT-SVM	96.60	98.85	97.58
Proposed	99	98.8	99

Table 4. Accuracy comparison using Yelp dataset

Methods	Accuracy
KNN	95.10
NB	95.68
SVM	95.97
C4.5	96.61
RF	97.50
DT-SVM	97.81
Proposed	99

Additionally, the AUC, PRC and f1-score figures are confirmed by comparing them with standard machine learning methods. This is demonstrated in Table 5 and Fig 11. These comparative results also indicate that the proposed AdaptoDetect is better than all existing approaches in terms of performance outcomes. Through the combination of POT and GEAE, an improved model has been created for this purpose.

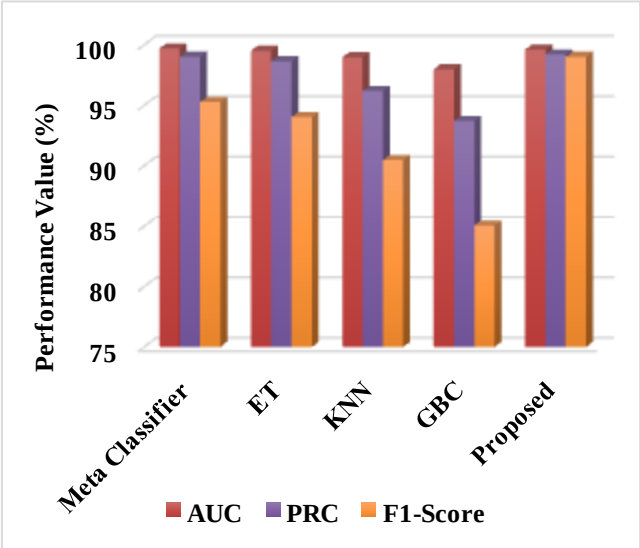


Figure 11. Comparative analysis using ISA dataset

Table 5. Performance comparison using ISA dataset

Methods	AUC	PRC	F1-Score
Meta Classifier	99.7	99	95.26
ET	99.5	98.63	94.02
KNN	98.96	96.17	90.46
GBC	97.98	93.69	85.04
Proposed	99.62	99.2	99

In this way, the performance achieved by the AdaptoDetect framework on the PubMed, Yelp, and ISA datasets bears a deep significance not only in its performance but also for practical anomaly detection in social networks. On the PubMed dataset, AdaptoDetect achieved a precision of 98.9%, a recall of 99%, an F1-score of 98.9%, while the overall accuracy was as high as 99%. These metrics indicate the great performance of the framework in detecting anomalies both with high precision and completeness. The former means that almost all of the detected anomalies are real, which is an important feature for keeping scientific research of high quality, as it effectively filters out most of the false positives. The recall rate can go up to 99%, indicating that the framework captures nearly all actual anomalies, therefore missing very few true cases. The F1-score, representing a balance between precision and recall, would be similarly high, establishing that AdaptoDetect reaches an appropriate balance between the identification of anomalies and their correct classification for it to be trusted in detecting unusual citation patterns and hence potential academic fraud. Also, it did very well on the Yelp dataset, with a precision of 99%, a recall of 98.8%, an F1-score of 99%, and an accuracy of 99%. These are consistent with the results for the efficiency of the framework in spam and fraudulent review detection with high dependability. The high precision underlines that most of the true anomalies were correctly identified by the system. The high recall hints that AdaptoDetect is able to detect almost all fraudulent activities, thus minimizing the chance of missing out on critical anomalies. The very high F1-score underlines the balanced performance of the framework and really robust capabilities regarding anomaly detection, important to ensure the authenticity and trustworthiness of user-generated content in social networks.

AdaptoDetect had an ISA dataset precision of 99.62%, a recall of 99.2%, and an F1-score of 99% to show how effectively it could detect security-related anomalies from within a complex cybersecurity network. The extremely high precision means the rate is exceptionally high of the detected anomalies are correctly identified, which is crucial for preventing insider threats and ensuring network security. The high recall further indicates that AdaptoDetect is knowledgeable in capturing most of the actual anomalies to bring security breaches and other critical issues under notice with immediate effect. A high F1-score further confirms that the framework will not compromise on a strong balance between precision and recall, even in high-stake environments, one case in point being cybersecurity. In general, such diverse datasets hint at the robustness of the performance metrics of AdaptoDetect across various social network contexts. The ability of the framework to maintain high precision, recall, and F1-scores in various applications underpins its contribution to anomaly detection research. AdaptoDetect enhances the security, trustworthiness, and

integrity of social networks by efficiently and effectively performing anomaly detection. It therefore forms a valuable tool to address a range of real-world challenges in the maintenance of quality and safety in online interactions.

5. CONCLUSION

In this paper, we presented and showed the efficacy of a new framework, AdaptoDetect; it is specifically designed for anomaly detection in social networks. The proposed framework leverages two innovative mechanisms: the Pufferfish Optimization Technique and the Graph Embedding Autoencoder. The effectiveness of anomaly detection is boosted because both techniques allow identification of feature selection as well as structural analysis. POT, developed from the foraging behavior in the pufferfish, is used here to appropriately select and rank the features out of the whole dataset, so that the detection process can concentrate on the most informative features. This meta-heuristic approach enhances accuracy and efficiency in anomaly detection by focusing only on those critical features that offer the richest contribution toward anomaly detection. Conversely, GEAE applies deep learning for the construction of low-dimensional representations for the nodes of a graph while preserving the most relevant structural information. The low-dimensional representations shall be used to identify anomalies by learning complex patterns and relationships across the network. AdaptoDetect re-constructs the graph using the constructed low-dimensional representations in order to correctly identify which node deviates from the normal, which results in highlighting potential anomalies with a high precision rate.

Application and evaluation of AdaptoDetect to three diverse datasets, namely PubMed, Yelp, and ISA, reveal the superiority of this method with respect to the existing methods. In the case of the PubMed dataset, the proposed approach resulted in a high value of precision, amounting to 98.9%, recall of 99%, and an F1-score of 98.9%, whereas the overall accuracy was 99%. As for the Yelp dataset, this model reached a precision of 99%, a recall of 98.8%, an F1-score of 99%, and the accuracy amounted to 99%. On the ISA dataset, it returned a precision of 99.62%, a recall of 99.2%, and an F1-score of 99%, hence proving how sound this was for the detection of security-related anomalies. These truly bring out how effective the proposed framework has been in the correct detection of anomalies from diverse social network contexts, hence value addition in the anomaly detection domain.

Looking ahead, there are several directions of future work that could still extend both the capabilities and the applications of AdaptoDetect, for instance, the integration of new features and data types, such as temporal or contextual information, to enhance anomaly detection in social networks that dynamically and continuously evolve.There are several directions of future work that could be pursued in order to further develop both the capabilities and the applications of AdaptoDetect, for example, the integration of new features and data types, such as temporal or contextual information, for anomaly detection in social networks that dynamically evolve on a continuous basis. Other possible applications of AdaptoDetect to other network types, such as financial or communication networks, might give insights into the adaptability and performance of the approach across different domains. Other future directions include further studies of scalability on much larger and complex networks and real-time anomaly detection in a streaming data environment. Addressing these, in the future, work can be done on the extension of the range of applications for AdaptoDetect and go further in improving the state of the art in anomaly detection.

DECLARATION STATEMENT

ETHICAL STATEMENT

I will conduct myself with integrity, fidelity, and honesty. I will openly take responsibility for my actions, and only make agreements, which I intend to keep. I will not intentionally engage in or participate in malicious harm to another person or animal.

INFORMED CONSENT FOR DATA USED

All subjects gave informed consent for inclusion before participating in the study. The Declaration of Helsinki conducted the study.

I consent to participate in the research project and the following has been explained to me: the research may not be of direct benefit to me. my participation is completely voluntary. my right to withdraw from the study at any time without any implications to me.

DATA AVAILABILITY

- Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.
- The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.
- All data generated or analysed during this study are included in this published article

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

COMPETING INTERESTS

The authors have no competing interests to declare that are relevant to the content of this article.

FUNDING DETAILS

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGMENTS

I am grateful to all of those with whom I have had the pleasure to work during this and other related Research Work. Each of the members of my Dissertation Committee has provided me extensive personal and professional guidance and taught me a great deal about both scientific research and life in general.

REFERENCES

[1] X. Wan, "Anomaly detection method of social media user information based on data mining," *International Journal of Web Based Communities*, vol. 20, pp. 38-50, 2024.

[2] R. Doroudi, S. H. H. Lavassani, and M. Shahrouzi, "Optimal tuning of three deep learning methods with signal processing and anomaly detection for multi-class damage detection of a large-scale bridge," *Structural Health Monitoring*, p. 14759217231216694, 2024.

[3] N. Selvaganesh, D. Shanthi, and R. Pandian, "A Novel Biased Probability Neural Network (BPNN) and Regularized Extreme Learning Machine (RELM) based Hearing Loss Prediction System," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, pp. 56-71, 2023.

[4] A. Tüzen and Y. Yaslan, "Adversarial random graph neural network for anomaly detection," *Digital Signal Processing*, vol. 146, p. 104374, 2024.

[5] E. Aarthi, S. Jagan, C. P. Devi, J. J. Gracewell, S. B. Choubey, A. Choubey, *et al.*, "A turbulent flow optimized deep fused ensemble model (TFO-DFE) for sentiment analysis using social corpus data," *Social Network Analysis and Mining*, vol. 14, p. 41, 2024.

[6] J. Tang, F. Hua, Z. Gao, P. Zhao, and J. Li, "Gadbench: Revisiting and benchmarking supervised graph anomaly detection," *Advances in Neural Information Processing Systems*, vol. 36, 2024.

[7] H. Wang, Q. Gao, H. Li, H. Wang, L. Yan, and G. Liu, "A structural evolution-based anomaly detection method for generalized evolving social networks," *The Computer Journal*, vol. 65, pp. 1189-1199, 2022.

[8] A. O. Ibitoye, C. Onime, and N. D. Zaki, "Socio-Transactional Impact of Recency, Frequency, and Monetary Features oN Customers' Behaviour in Telecoms' Churn Prediction," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, pp. 101-110, 2022.

[9] Y. Zheng, M. Jin, Y. Liu, L. Chi, K. T. Phan, and Y.-P. P. Chen, "Generative and contrastive self-supervised learning for graph anomaly detection," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, pp. 12220-12233, 2021.

[10] J. Mao, H. Wang, and B. F. Spencer Jr, "Toward data anomaly detection for automated structural health monitoring: Exploiting generative adversarial nets and autoencoders," *Structural Health Monitoring*, vol. 20, pp. 1609-1626, 2021.

[11] X. Ma, J. Wu, S. Xue, J. Yang, C. Zhou, Q. Z. Sheng, *et al.*, "A comprehensive survey on graph anomaly detection with deep learning," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, pp. 12012-12038, 2021.

[12] G. Subburayalu, H. Duraivelu, A. P. Raveendran, R. Arunachalam, D. Kongara, and C. Thangavel, "Cluster based malicious node detection system for mobile ad-hoc network using ANFIS classifier," *Journal of Applied Security Research*, vol. 18, pp. 402-420, 2023.

[13] J. Wang, Y. Tang, S. He, C. Zhao, P. K. Sharma, O. Alfarraj, *et al.*, "LogEvent2vec: LogEvent-to-vector based anomaly detection for large-scale logs in internet of things," *Sensors*, vol. 20, p. 2451, 2020.

[14] T. Pourhabibi, K.-L. Ong, B. H. Kam, and Y. L. Boo, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," *Decision Support Systems*, vol. 133, p. 113303, 2020.

[15] P. Elamparithi, S. Kalaivani, S. Vijayalakshmi, E. Keerthika, S. Koteswari, and R. S. Raaj, "A Machine Learning Approach for Detecting DDOS Attack in IoT Network Using Random Forest Classifier," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, pp. 495-502, 2024.

[16] L. Erhan, M. Ndubuaku, M. Di Mauro, W. Song, M. Chen, G. Fortino, *et al.*, "Smart anomaly detection in sensor systems: A multi-perspective review," *Information Fusion*, vol. 67, pp. 64-79, 2021.

[17] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: A systematic review," *Ieee Access*, vol. 9, pp. 78658-78700, 2021.

[18] Y. Liu, Z. Li, S. Pan, C. Gong, C. Zhou, and G. Karypis, "Anomaly detection on attributed networks via contrastive self-supervised learning," *IEEE transactions on neural networks and learning systems*, vol. 33, pp. 2378-2392, 2021.

[19] G. Perumal, G. Subburayalu, Q. Abbas, S. M. Naqi, and I. Qureshi, "VBQ-Net: a novel vectorization-based boost quantized network model for maximizing the security level of IoT system to prevent intrusions," *Systems*, vol. 11, p. 436, 2023.

[20] M. S. Sheela, S. Gopalakrishnan, I. P. Begum, J. J. Hephzipah, M. Gopianand, and D. Harika, "Enhancing Energy Efficiency With Smart Building Energy Management System Using Machine Learning and IOT," *Babylonian Journal of Machine Learning*, vol. 2024, pp. 80-88, 2024.

[21] F. Xu and R. Moghaddass, "A scalable Bayesian framework for large-scale sensor-driven network anomaly detection," *IISE transactions*, vol. 55, pp. 445-462, 2023.

[22] Y. Cao, X. Xu, C. Sun, X. Huang, and W. Shen, "Towards generic anomaly detection and understanding: Large-scale visual-linguistic model (gpt-4v) takes the lead," *arXiv preprint arXiv:2311.02782*, 2023.

[23] H. Zardi and H. Alrajhi, "Anomaly Discover: A New Community-based Approach for Detecting Anomalies in Social Networks," *International Journal of Advanced Computer Science and Applications*, vol. 14, pp. 912-920, 2023.

[24] D. Guo, Z. Liu, and R. Li, "RegraphGAN: A graph generative adversarial network model for dynamic network anomaly detection," *Neural Networks*, vol. 166, pp. 273-285, 2023.

[25] B. Kim, M. A. Alawami, E. Kim, S. Oh, J. Park, and H. Kim, "A comparative study of time series anomaly detection models for industrial control systems," *Sensors*, vol. 23, p. 1310, 2023.

[26] J. Chen, J. Zhang, R. Qian, J. Yuan, and Y. Ren, "An Anomaly Detection Method for Wireless Sensor Networks Based on the Improved Isolation Forest," *Applied Sciences*, vol. 13, p. 702, 2023.

[27] E. A. Elaziz, R. Fathalla, and M. Shaheen, "Deep reinforcement learning for data-efficient weakly supervised business process anomaly detection," *Journal of Big Data*, vol. 10, p. 33, 2023.

[28] K. Hayawi, S. Saha, M. M. Masud, S. S. Mathew, and M. Kaosar, "Social media bot detection with deep learning methods: a systematic review," *Neural Computing and Applications*, vol. 35, pp. 8903-8918, 2023.

[29] Y. Huang, W. Liu, S. Li, Y. Guo, and W. Chen, "A Novel Unsupervised Outlier Detection Algorithm Based on Mutual Information and Reduced Spectral Clustering," *Electronics*, vol. 12, p. 4864, 2023.

[30] S. Thudumu, P. Branch, J. Jin, and J. Singh, "A comprehensive survey of anomaly detection techniques for high dimensional big data," *Journal of Big Data*, vol. 7, pp. 1-30, 2020.

[31] A. Mahalingam, G. Perumal, G. Subburayalu, M. Albathan, A. Altameem, R. S. Almakki, *et al.*, "ROAST-IoT: a novel range-optimized attention convolutional scattered technique for intrusion detection in IoT networks," *Sensors*, vol. 23, p. 8044, 2023.

[32] C. Meng, X. S. Jiang, X. M. Wei, and T. Wei, "A time convolutional network based outlier detection for multidimensional time series in cyber-physical-social systems," *IEEE Access*, vol. 8, pp. 74933-74942, 2020.

[33] C. Xiao, X. Xu, Y. Lei, K. Zhang, S. Liu, and F. Zhou, "Counterfactual graph learning for anomaly detection on attributed networks," *IEEE Transactions on Knowledge and Data Engineering*, 2023.