International Journal of Basic and Applied Sciences, 14 (4) (2025) 220-228

SPC

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/qw8xgz45
Research paper

Deep Learning Driven Anomaly Detection in Social Graphs by Using Anti-Corona Political Optimization

Dhanya. D. [1], N Krishnamoorthy [2], P S Ramapraba [3], Kancharla Nagababu [4], K. Balaji [5], M Koti Reddy [6], Win Mathew John [7], Sumit Chaudhary [8], Jayaram Boga [9], R G Vidhya [10] *

[1] Department of AI and Data Science, Mar Ephraem College of Engineering and Technology, Tamil Nadu 629171, India
[2] Faculty of Science and Humanities, Department of Computer Science and Applications (MCA), SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu 600089, India
[3] Department of EEE, Panimalar Engineering College, Chennai, Tamil Nadu 600123, India
[4] Department of Computer Applications, Aditya University, Surampalem, Andhra Pradesh 533437, India
[5] Department of CSE, SSM College of Engineering, Komarapalayam, Tamil Nadu 638183, India
[6] Department of ECE, Universal College of Engineering and Technology, Guntur, Andhra Pradesh 522438, India
[7] Department of Computer Applications, Marian College Kuttikkanam Autonomous, Kerala, 685531, India
[8] Department of CSE, Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, Uttarakhand 248007
[9] Department of CSE, Koneru Lakshmaiah Education Foundation, Hyderabad, Telangana 500043, India
[10] Department of ECE, HKBK College of Engineering, Bangalore, India
**Corresponding author E-mail: k20621092@gmail.com*

Received: June 26, 2025, Accepted: August 2, 2025, Published: August 9, 2025

Abstract

Anomaly detection in social networks is critical to identify abnormal behavior and prevent looming security attacks. Anti-Corona Political Optimization (ACPO) is a novel anomaly detection approach in social networks, utilizing advanced optimization techniques and deep learning models for high-precision anomaly detection. ACPO integrates Anti-Corona Virus Optimization (ACVO) and Political Optimization (PO) for efficient anomaly detection. The approach involves pre-processing to deal with missing values, noise, and inconsistencies; followed by taking features through the methodology of feature selection and data augmentation for enhanced robustness of the model, followed by clustering to find patterns and anomaly detection in discovered clusters. A combination of ACVO and PO enhances the detection of anomalies in ACPO; then deep learning architecture will provide strong and accurate detection. In general, ACPO offers a novel and effective approach with widespread applications in social network security and other fields. Experimental results verify the improved performance of ACPO_DRN, which achieved precision (0.813), recall (0.880), and F-measure (0.836) with K-Fold variations. The good performance of ACPO in social network anomaly detection is demonstrated by its ability to learn complex patterns and anomalies, and therefore, it is an effective tool for preventing possible security threats.

Keywords: *Anomaly detection; Political Optimization; Deep Residual Network; Anti-Corona Virus Optimization; Z-Score Normalization.*

1. Introduction

The evolution of the Web has revolutionized communication to enable the development of new technologies to facilitate the exchange of information among people and organizations. Social websites such as Facebook, Instagram, and Twitter are part of people's daily life, beginning as places to interact socially among friends, relatives, and professional networks. The rapid expansion of cyberspace and broader applications of the internet have empowered institutions and end users but brought significant challenges to governments and individuals alike. Online Social Networks (OSNs) have enabled the formation of virtual communities, where end users—consumers of content—and data generators—creators of content—are interacting with one another via online media [1]. A social network is often described as a graph that captures the relationships between people, groups, and social activities. OSNs are websites on which users form relationships due to their shared interests, views, and experiences [2]. While they offer improved communication and information exchange, they also open individuals up to misuse, like the posting of offensive or illegal content [3]. Social networking websites pose a threat to vulnerable groups like teenagers and children. Malware, unintentionally installed in most cases, can invade privacy data, leaving users and their families at risk of injury. Moreover, OSNs have become cyberbullying, youth violence, and gang cybercrime hotbeds, threatening public safety. With the growth of social media, OSNs are increasingly susceptible to spurious accounts. Spammers use bots to create and manage enormous quantities of spurious accounts to spread malware, disseminate phishing links, spread rumors, and tamper with essential systems such as elections or stock markets. These accounts also compromise privacy by scraping users' information [4]. An anomaly is usually referred to as any observation that does not conform to the norm. While normal patterns reveal what the system typically does, anomalies are likely to reveal important information regarding exceptional events. Anomaly detection has thus become a fundamental subject of research in data analytics, particularly in Machine Learning (ML) and statistics [5]. Anomaly detection (or outlier detection) in dynamically evolving networks is an ancient problem with long-reaching implications from security to social networks, public health, and computational biology. The identification of structural anomalies, e.g., unusual nodes or edges, can reveal valuable insights into network behavior [6]. Accurate anomaly detection allows early identification of malicious activity and enhances the performance of subsequent machine learning processes. Most recent efforts have focused on detecting spammers, social network spammers and fake users [7]. There is still a challenge posed by high-dimensional data (e.g., images and text), temporal dynamics, and scalability needs for big data [8]. Most existing approaches overlook the interdependency of the network elements and assign the same significance to features without knowledge of their relative importance. Deep learning has been an excellent feature extraction technique from highly interconnected data [9]. Traditional architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Stacked Autoencoders have been effectively utilized to safeguard multimedia services and websites [10]. This work proposes an enhanced Deep Residual Network (DRN) for anomaly detection in social networks. The proposed model uses an optimized training algorithm, ACPO, that combines Anti-Coronavirus Optimization (ACVO) and Political Optimization (PO). ACVO enables efficient anomaly localization and fast convergence to support timely intervention and risk minimization. The input data is enhanced, pre-processed, and clustered with techniques such as Fuzzy Local Information C-Means (FLICM) and oversampling to enhance the quality of data and the connectivity of the clusters.

Significant Contributions of this Work

- Design of a DRN architecture composed of multiple residual blocks, which utilizes batch normalization layers and convolutional layers for learning complex patterns of anomalies in social network data.
- Introducing the ACPO optimization algorithm—a hybrid of ACVO and PO—that maximizes training efficiency and improves the quality of anomaly detection. The hybrid strategy exposes increased accuracy and credibility in identifying out-of-pattern trends in social networks.

Section 2: Literature review and critical analysis of previous work. Section 3: Comprehensive explanation of the proposed ACPO_DRN strategy, Section 4: Experimental results and discussion

Section 5: Conclusion and future research directions

2. Literature assessment

Anomaly detection in Online Social Networks (OSNs) has gained momentum as an immediate area of research due to newly emerging threats such as spam accounts, disinformation, and cyberattacks. Numerous machine learning and deep learning-based mechanisms have been proposed to counter such threats, each with advantages and limitations. Rahman et al. proposed an ML-based anomaly detection methodology that relies on statistical analysis and manual social network feature extraction. Their proposed model was effective in detecting unexpected anomalous patterns in typical OSNs, with potential use in cybersecurity. They further suggested a hybrid classification framework, DT-SVMNB, for detecting anomalous and suicidal users using behavioral and content features. While their model was very precise, it was also limited in scope, unable to handle dynamic user interests and not to explore temporal dynamics or complex network structures. Wang et al. [11] have introduced SeaDM, a structural evolution-driven anomaly detection framework particularly suited to dynamic social networks. SeaDM combines the Evolutional State Construction Algorithm (ESCA) and the Optimal Evolutional Observation Algorithm (OEOA), the latter founded upon a quantum-inspired genetic algorithm. SeaDM is well capable of detecting structural evolution and macro-level anomalies. SeaDM's domain specificity and reliance on network evolution, however, make it ineffective to be applied to static or heterogeneous networks where temporal evolution is not well defined. Khan and Haroon [12] illustrated an unsupervised ensemble approach aggregating five base learners, with a novel label consensus weighting mechanism. One key strength is that it does not require labeled training data. However, its performance has not been tested yet on sparse or low-dimensional data like Amazon and Enron, which could raise doubts about its robustness for different data environments. Further, the model lacks mechanisms to handle concept drift or changing user behavior. Li et al. [13] proposed RAU-GNN, a relevance-aware graph neural network framework for fine-grained identification of anomalous users. By building a multi-relational user graph and leveraging both GCN and GAT architectures, the model can effectively capture subtle inter-user relationships. While improving accuracy, RAU-GNN is computationally intensive and unsuitable for real-time applications. It also addresses anomaly detection to some extent because challenges remain in identifying previously unseen or ever-evolving threats. Garg et al. [14] suggested a hybrid deep learning model using enhanced Restricted Boltzmann Machines (RBMs) and Gradient Descent-based Support Vector Machines (GD-SVM) for anomaly detection. The model was further integrated with a Software-Defined Networking (SDN) module to satisfy rigorous Quality of Service (QoS) requirements. Although this system performs best in high-throughput environments, its generic design hinders domain-specific customization and explainability, which are essentials for security-oriented social applications. Yazdi and Bafghi [15] introduced the Online Fusion of Experts (OFE) model for addressing concept drift in online social network data streams. Through the application of a three-step error estimation process, posterior-based stream generation, and uncertainty modeling, OFE reacts to user behavior variation. Its accuracy, however, is lessened in initial-stage deployment, where it performs poorly at reliability and model stabilization.

Sudha and Valarmathi [16] proposed DBN-IAS, an Interactive Autodidactic School-based Deep Belief Network model to enhance the model's hidden layers. The model optimized undetected anomalies but did not enhance recall significantly, indicating vulnerability to false negatives—a security issue. Wanda and Jie [17] have suggested Deep Friend, a supervised neural network with labeled link features and dynamic architecture using Walk Pool pooling to enhance noise robustness. Although Deep Friend performed well in structured environments, it did not leverage generative models to predict hierarchical malware-account linkages, limiting its ability to generalize anomaly patterns in varied attack scenarios [18].

2.1. Existing approaches' limitations and gaps

Although recent research has yielded hopeful approaches for detecting anomalies in online social networks, several limitations exist in the existing models. Scalability is the largest issue; many approaches are not capable of handling the size and heterogeneity of real social networks with millions of members and mixed interactions. Besides, these networks are dynamic networks, where behavior and relationships keep changing, but most of the models cannot change to respond to such alterations and hence become useless in the event of concept drift or evolving abnormal patterns. Another significant issue is that social media data contains noise as well as sparsity [19], [20]. High-dimensional features such as text, image, and interaction logs typically hide underlying structures, which makes exact feature extraction hard. Also, class imbalance is the default for anomaly detection tasks because anomalous events typically constitute only a subset of the dataset, and models tend towards favoring normal behavior and dismissing small or infrequent deviations. Many supervised learning techniques rely heavily on labeled datasets, which are costly and difficult to obtain, particularly for security-related anomalies with sparse ground truth. Finally, interpretability is an ongoing problem. Deep learning models strong enough are typically black boxes, from which it is difficult for researchers and practitioners to understand or accept the model's predictions. Anomaly detection in real-time is also a relatively unexplored area; most methods available today operate in offline or batch mode and are unable to detect threats as they occur. Lastly, all these models are not generalizable across domains or capable of detecting new anomalies that do not correspond to learned patterns and hence limit their applicability in dynamic and varied domains.

2.2. Context and contribution

Relieving all the limitations discussed above in the current methods, this paper suggests an innovation in an anomaly detection framework called ACPO_DRN by combining Anti-Coronavirus Optimization (ACVO) and Political Optimization (PO) under an overarching optimization strategy called ACPO. This optimizer is utilized in the process of training a Deep Residual Network (DRN), which is particularly designed to learn rich representations from high-dimensional social network data. With the use of socio-inspired optimization techniques along with deep learning, the presented model gains improved adaptability and accuracy in identifying anomalous patterns, even previously unseen ones. Unlike traditional methods focusing on static analysis or relying on manually crafted features, ACPO_DRN supports data-driven dynamic feature learning through its residual structure. This allows it to learn shifting patterns of behavior and subtle abnormalities in real-time. Moreover, with the use of two distinct optimization paradigms—ACVO for global search and PO for local search—the model provides balanced and efficient training with enhanced convergence rate and detection accuracy. These contributions collectively complete key gaps in scalability, responsiveness, and novelty detection that position ACPO_DRN on solid and realistic foundations as an anomaly detection solution for dynamic and complex social network environments.

3. Proposed methodology

Once the social network dataset has been obtained, data pre-processing is the first task in the pipeline of anomaly detection. To standardize the input data and make it consistent, Z-score normalization is applied. This normalizes the data by shifting it to a mean of zero and scaling it based on standard deviation such that there is a uniform scale for all features. Normalization process ensures that all features will contribute to the model learning process equally, avoiding the impact of biases from differing ranges of values. After normalization, the dataset is better aligned with the following procedures, such as feature selection and model training. The ACVO and PO are combined to create the ACPO. The block diagram for the ACPO_DRN-based anomaly detection is given in Figure 1.

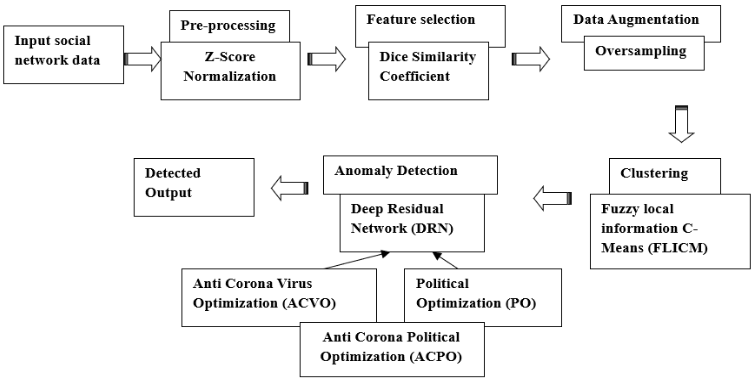

Input social network data
Pre-processing
Z-Score Normalization
Feature selection
Dice Similarity Coefficient
Data Augmentation
Oversampling
Clustering
Fuzzy local information C-Means (FLICM)
Anomaly Detection
Deep Residual Network (DRN)
Detected Output
Anti Corona Virus Optimization (ACVO)
Political Optimization (PO)
Anti Corona Political Optimization (ACPO)

Fig. 1: Preview of ACPO_DRN-Based Anomaly Detection.

To balance the data and diversify training samples, an oversampling-based data augmentation technique is used. Instead of collecting new data, this technique artificially expands the dataset by generating additional samples from the selected subset of features. The primary purpose of this technique is to minimize overfitting and maximize the generality of the detection model. The augmentation is performed by examining the existing data points in every class label and creating new instances within the range of the observed minimum and maximum. The dataset is thereby expanded in size and balanced, presenting the model with a more representative set of possible patterns, including those that are borderline or rare. The augmented dataset is subsequently passed to the clustering stage. After augmentation, the data is finally clustered using the Fuzzy Local Information C-Means (FLICM) algorithm. FLICM is an enhanced version of the traditional fuzzy cluster algorithms, which have been improved to the extent that they are resistant to noise while preserving meaningful structural information about the data. FLICM achieves this with the utilization of both spatial and local grey-level information for clustering. This renders it particularly effective in identifying coherent patterns in the augmented data. Unlike typical fuzzy clustering techniques, FLICM dynamically adjusts membership values based not just on the intensity of the data point but also on its spatial position, yielding better grouping. After the algorithm converges, fuzzy partitions are finally converted into hard clusters through defuzzification, where each data point is assigned to the cluster with which it has the strongest membership value. This crisp segmenting facilitates effective discrimination of regular and irregular behaviour, setting the stage for effective anomaly detection in the next step of classification. The clustered data generated here is carried as input to the Deep Residual Network (DRN) that has been trained on the ACPO optimization algorithm.

3.1. Clustering by FLICM

FLICM is used to cluster related data points or nodes after data augmentation to find patterns. In this scenario, the input is the output of data augmentation H . After data augmentation, the next process involves clustering the augmented data using the Fuzzy Local Information C-Means (FLICM) algorithm. FLICM is an effective enhancement of the traditional fuzzy c-means clustering algorithm. While conventional fuzzy clustering assigns data points to clusters solely based on feature similarity, FLICM integrates gray-level information and spatial proximity to possess the capability to maintain data integrity and be immune to noise—characteristics highly desirable when working with social network data that would normally exhibit overlapping or ambiguous patterns. The main advantage of FLICM is the application of a fuzzy local information model, which refreshes the membership degree of each data point dynamically according to the influence of its neighboring points. Such spatial consideration enhances the robustness of the model to distortions or outliers in the data and guarantees consistent clustering results. Following iteration and convergence of the FLICM algorithm, the fuzzy partition matrix obtained from it is converted to crisp partitions through a defuzzification process. This is typically carried out by using the maximum membership principle, i.e., by assigning each data point to the cluster to which it has the maximum degree of membership. The outcome is a nicely formed clustering of the input data into disjointed clusters, which can then be used for anomaly detection more accurately. The clustered data at this stage represents clear groupings of user behavior in the social network, making it easier for the DRN to learn discriminative features. The pseudocode detailing the step-by-step running of the FLICM algorithm is provided in Table 1.

Table 1: The Pseudocode Detailing the Step-by-Step Running of the FLICM Algorithm

Step	Description
1	Initialize the number of clusters, fuzzification coefficient, and stopping criterion.
2	Randomly assign initial membership values to each data point.
3	Repeat the following steps until convergence:
3.1	Compute cluster centres based on current membership values.
3.2	Calculate the local similarity measure by evaluating the spatial and grey-level information of neighbouring data points.
3.3	Update the membership values using both feature distance and local information.
3.4	Check convergence by comparing membership changes to the threshold.
4	Once convergence is achieved, perform defuzzification by assigning each data point to the cluster with the highest membership value.
5	Output the final clusters formed by the FLICM algorithm.

ACPO_DRN for anomaly detection is shown in this section. DRN accepts the clustered data as input and uses it for abnormality detection. In addition, the new ACPO design, which fuses PO [21] and ACVO [22] used for training the DRN. Convolutional layer, pooling, residual blocks, and linear classifier are the prominent layers of the DRN architecture [23], [24]. The DRN classifier is more effective in training and learning aspects if training data is limited [25], [26]. DRN is therefore effectively applied for anomaly detection with clustered data being considered as input [27], [28]. Figure 2 shows the DRN architectural framework.

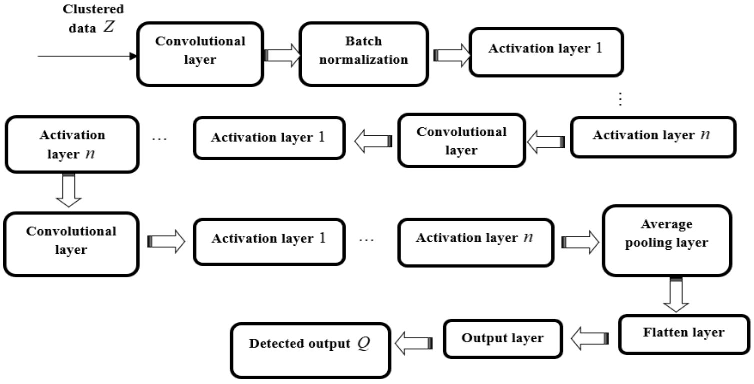


Fig. 2: DRN Structure.

3.2. Deep residual network architecture

The Deep Residual Network (DRN) utilized in this work is made up of several basic building blocks whose primary objectives are to optimize the learning process, reduce computational complexity, and achieve maximum anomaly detection accuracy [29], [30]. They are the convolutional layer, pooling layer, activation function, batch normalization, residual blocks, and linear classifier.

3.6.1. Convolutional layer

The convolutional layer is the core of the DRN and employs a two-dimensional structure in order to reduce the number of free parameters when trained. This is achieved by weight sharing and employing local receptive fields [31], [32]. The layer employs a series of filters, or kernels, to traverse the input data to compute the dot product. These computational operations help extract spatial features by detecting patterns within a local neighborhood of the input. Each kernel will interact with the input matrix to produce a feature map, allowing the model to effectively learn spatial hierarchies in a computationally efficient manner.

3.6.2. Pooling layer

Then the pooling layer is employed to further reduce the spatial dimension of the feature maps. The down-sampling process reduces overfitting and improves generalization by retaining the most crucial features and eliminating less significant details. The pooling layer also reduces computation and memory needs by halving the size of the feature map, making it possible to train deeper network architectures effectively [33], [34].

3.6.3. Activation function

In order to introduce non-linearity to the model, DRN employs a non-linear activation function to enable the extraction of complicated relations from data [35]. ReLU is used because it can speed up convergence as well as suppress vanishing gradient issues. ReLU does this by retaining the positive values and eliminating the negative values, thus enhancing the discriminative capability of the network [36].

3.6.4. Batch normalization

Batch normalization is used to normalize the output of each layer to result in faster and more convergent training [37]. Normalizing the input layer from mini-batches reduces internal covariate shift, such that higher learning rates can be utilized and convergence is accelerated. Normalization scales and translates activations to improve uniformity and consistency during training, overall enhancing performance [38].

3.2.5. Residual blocks

One of the significant innovations of the DRN architecture is the use of residual blocks. Unlike regular convolutional networks, these blocks contain shortcut connections that directly link the input of a block and its output [39]. This identity mapping enables better gradient flow within the network and helps solve the degradation problem that is generally observed in deep models. For aligning the input and output dimensions whenever required, an element-wise matching factor is used so that residual learning remains effective even in deep configurations [40].

3.2.6. Linear classifier

The final part of the DRN is a linear classifier, usually consisting of a fully connected (FC) layer topped with Softmax activation [41], [42]. The FC layer consists of every neuron of one layer connected with every neuron in the next layer to facilitate global feature integration learned across the network. Softmax function then converts the raw output scores into class probabilities, enabling accurate classification of anomalous and normal instances[43], [44].

3.3. Training of deep residual network via ACPO

Training Deep Residual Network is via the Adaptive Coronavirus Political Optimizer (ACPO), a hybrid metaheuristic model that merges biological and political models to aid in optimization. ACPO is designed to successfully train the DRN for robust anomaly detection, particularly in imbalanced and complex data. ACPO takes inspiration from pandemic response strategy dynamics and political behavior dynamics. It has three main stages—quarantine, isolation, and social distancing—that metaphorically represent the reconfiguration of candidate solutions during optimization. At social distancing, spreading candidate solutions is facilitated by the algorithm in order to prevent convergence to local optima. During quarantine, low-performing solutions are segregated from the remainder of the population. The isolation stage is designed to reinforce poor solutions by reconceptualizing them in a way that they can be better accommodate within optimal regions of the solution space. The Political Optimizer (PO) is also reinforced with the inclusion of five new phases: party switching, party formation and constituency allocation, election control, inter-party choice, and parliamentary behavior. These stages simulate a political process where candidate solutions evolve and compete, sacrificing discovery of new solutions for using previously known good ones. While the PO component is more computationally intensive, coupling it with the Adaptive Coronavirus Optimization (ACVO) algorithm counteracts this cost by accelerating convergence. The ACPO algorithm begins by initializing a set of candidate solutions randomly over an n-dimensional space. Each member of the set is a potential solution and contains parameters for the DRN. The fitness of each member is determined based on how good the match is between the output predicted and the ground truth. Higher values of the fitness indicate higher compliance with the desired result. In the stage of social distancing, a random small subset of the population is selected to update their positions to minimize similarity and maximize diversity. The approach is significant for preventing premature convergence and enabling fuller exploration of the solution space. The selected members update their positions based on pre-defined rules that simulate the effect of maintaining physical distance. During the quarantine phase, low fitness score individuals are temporarily disallowed from influencing the optimization process. This will not allow weak solutions to lower the population's quality. On the other hand, in the isolation phase, the focus is to make these weak ones stronger by resetting their parameters to improve their fitness and reinserting them into the population. By combining social behavior modeling and political process simulation, ACPO is an effective optimization technique for training deep neural networks. Its dynamic adaptation mechanisms ensure that the DRN can learn useful patterns and yield high accuracy for anomaly detection even in challenging instances

$$qb_{my}^{f} = \begin{cases} \Delta - I_{my}^{f} & if\ \left(I_{my}^{f} < \Delta\right) \\ I_{my}^{f} & if\ \left(I_{my}^{f} \geq \Delta\right) \end{cases} \tag{1}$$

Where, Δ indicates the predetermined safe distance between individuals in each iteration and $I_{my}^{f} = \left\| G_{m}^{f} - G_{y}^{f} \right\|$ indicates the current distance between G_{m} and G_{y}. The transmission of disease declines when people move physically farther apart.

$$\Delta_{2}^{f} = \tau_{my}^{f} \times \mu \times \left(G^{*} - G_{m}^{f}\right) \tag{2}$$

Where, G^{*} is an ideal solution, μ is the step size, and τ_{my}^{f} is the infection effect of G^{*} on the G_{m}.

$$G_{m}^{f+1} = G_{m}^{f} + \kappa_{my}^{f} \times qb_{mu}^{f} \times K\left(-1,1\right) + \tau_{my}^{f} \times \mu \times \left(G^{*} - G_{m}^{f}\right) \tag{3}$$

$$G_{m}^{f+1} = G_{m}^{f}\left(1 - \tau_{my}^{f} \times \mu\right) + \kappa_{my}^{f} \times qb_{my}^{f} \times K\left(-1,1\right) + \tau_{my}^{f} \times \mu \times G^{*} \tag{4}$$

The global optimization problems are successfully handled by combining the ACVO with the PO, and the typical equation of the PO is as follows:

$$U_{z}^{j+1} = l^{*} + \left(2c - 1\right)\left|l^{*} - U_{z}^{j}\right| \text{if } U_{z}^{j-1} \leq l^{*} \leq U_{z}^{j} \text{ or } U_{z}^{j-1} \geq l^{*} \geq U_{z}^{j} \tag{5}$$

Consider, $U_{best} > U_{z}^{j}$ hence, equation (25) is given by,

$$U_z^{j+1} = U_{best} + (2c-1)(U_{best} - U_z^j) \tag{6}$$

Assume, $U_z^{j+1} = G_m^{f+1}$ and $U_z^j = G_m^f$ substitute in the above equation,

$$G_m^{f+1} = U_{best} + (2c-1)(U_{best} - G_m^f) \tag{7}$$

$$G_m^{f+1} = U_{best} + U_{best}2c - 2aG_m^f - U_{best} + G_m^f \tag{8}$$

$$G_m^{f+1} = U_{best}(1+2c-1) - G_m^f(2c-1) \tag{9}$$

$$G_m^f = \frac{2cU_{best} - G_m^{f+1}}{2c-1} \tag{10}$$

Substitute Equation (30) in (24),

$$G_m^{f+1} = \left[\frac{2cU_{best} - G_m^{f+1}}{2c-1}\right](1-\tau_{my}^f \times \mu) + \kappa_{my}^f \times qb_{my}^f \times K(-1,1) + \tau_{my}^f \times \mu \times G^* \tag{11}$$

$$G_m^{f+1} + \frac{G_m^{f+1}}{2c-1}(1-\tau_{my}^f \times \mu) = \left[\frac{2cU_{best}}{2c-1}\right](1-\tau_{my}^f \times \mu) + \kappa_{my}^f \times qb_{my}^f \times K(-1,1) + \tau_{my}^f \times \mu \times G^* \tag{12}$$

$$G_m^{f+1}\left[1 + \frac{(1-\tau_{my}^f \times \mu)}{2c-1}\right] = \left[\frac{2cU_{best}}{2c-1}\right](1-\tau_{my}^f \times \mu) + \kappa_{my}^f \times qb_{my}^f \times K(-1,1) + \tau_{my}^f \times \mu \times G^* \tag{13}$$

$$G_m^{f+1}\left[\frac{2c-1+1-\tau_{my}^f \times \mu}{2c-1}\right] = \left[\frac{2cU_{best}}{2c-1}\right](1-\tau_{my}^f \times \mu) + \kappa_{my}^f \times qb_{my}^f \times K(-1,1) + \tau_{my}^f \times \mu \times G^* \tag{14}$$

$$G_m^{f+1}\left[\frac{2c-\tau_{my}^f \times \mu}{2c-1}\right] = \left[\frac{2cU_{best}}{2c-1}\right](1-\tau_{my}^f \times \mu) + \kappa_{my}^f \times qb_{my}^f \times K(-1,1) + \tau_{my}^f \times \mu \times G^*\left[\frac{2c-1}{2c-\tau_{my}^f \times \mu}\right] \tag{15}$$

The above equation is the final updated equation of ACPO.
Update quarantine
It is the approach used by those who are suspicious during the quarantine period. To identify those who become infected, the individuals are categorized according to their level of fitness. The quarantine list is formed based on the most vulnerable people, and it includes suspected sick individuals who are kept under observation to determine their infection status.

$$\alpha^f = \left[\left(1-\left(1-(W^f)^2\right)q^f\right)X_0\right] \tag{16}$$

Where, α^f , X_0 are reproductive number, q^f denotes the percentage of people who distance themselves from others socially, and X is normal conditions.
Isolation
At this point, the equation below updates the chosen variables as,

$$G_{my}^{f+1} = \frac{1}{2}\left(G_{MY}^F + \left(\nu \times G_y^{*f}\right)\right) \tag{17}$$

Where, G_{my}^f is element y of G_m at iteration, G_y^{*f} is the fittest element individual G^* , and ν is a scaling factor.

$$\nu = 1 - \frac{\gamma}{U_b} \tag{18}$$

Where, γ ranges between 1 to U_b that is the highest isolation time.
Estimating feasibility
Every individual's fitness is updated depending on iterations, and an optimal value is determined by selecting the fitness that is the best.
Termination
Until a maximum repetition is reached, the processes are repeated.

4. Results and discussion

This section presents the experimental findings of the proposed anomaly detection framework, where the Deep Residual Network (DRN) is trained using the Adaptive Coronavirus Political Optimizer (ACPO). The analysis includes the implementation setup, dataset specifications, evaluation metrics, and a comprehensive comparative study to assess the effectiveness of the ACPO-DRN model.

4.1. Experimental setup

The ACPO-driven DRN model was implemented using the Python programming environment. All experiments were conducted on a personal computer running Windows 10 OS, equipped with an Intel Core i7 processor and 16GB RAM. The simulations were performed in a consistent and controlled environment to ensure reproducibility of the results.

4.2. Dataset description

For performance validation, the Mendeley dataset was employed [45]. This dataset comprises web pages categorized into two classes: malicious (phishing) and benign (legal). Each sample within the dataset contains 75 distinct attributes, capturing various features relevant to anomaly detection. This binary classification setting serves as a suitable benchmark for evaluating the detection capabilities of the proposed model. To examine the performance under varying data availability, the models were trained with different proportions of the training data, and the results were evaluated using precision, recall, and F1-score. In Precision Analysis (Figure 3i): When 50% of the dataset was used for training, ACPO-DRN achieved a precision of 0.746, outperforming the existing models DT-SVMNB (0.690), ESCA (0.711), GD-SVM (0.724), and DBN-IAS (0.730). This reflects improvements of 5.6%, 3.5%, 2.2%, and 1.6%, respectively. In Recall Analysis (Figure 3ii): At 60% training data, ACPO-DRN recorded a recall of 0.649, surpassing DT-SVMNB (0.619), ESCA (0.616), GD-SVM (0.610), and DBN-IAS (0.517). The relative improvements range from 1.5% to 3.4%. In F1-score Analysis (Figure 3iii): With 70% training data, the F1-score for ACPO-DRN was notably higher compared to DT-SVMNB (0.790), ESCA (0.737), GD-SVM (0.666), and DBN-IAS (0.676), highlighting its superior balance between precision and recall.

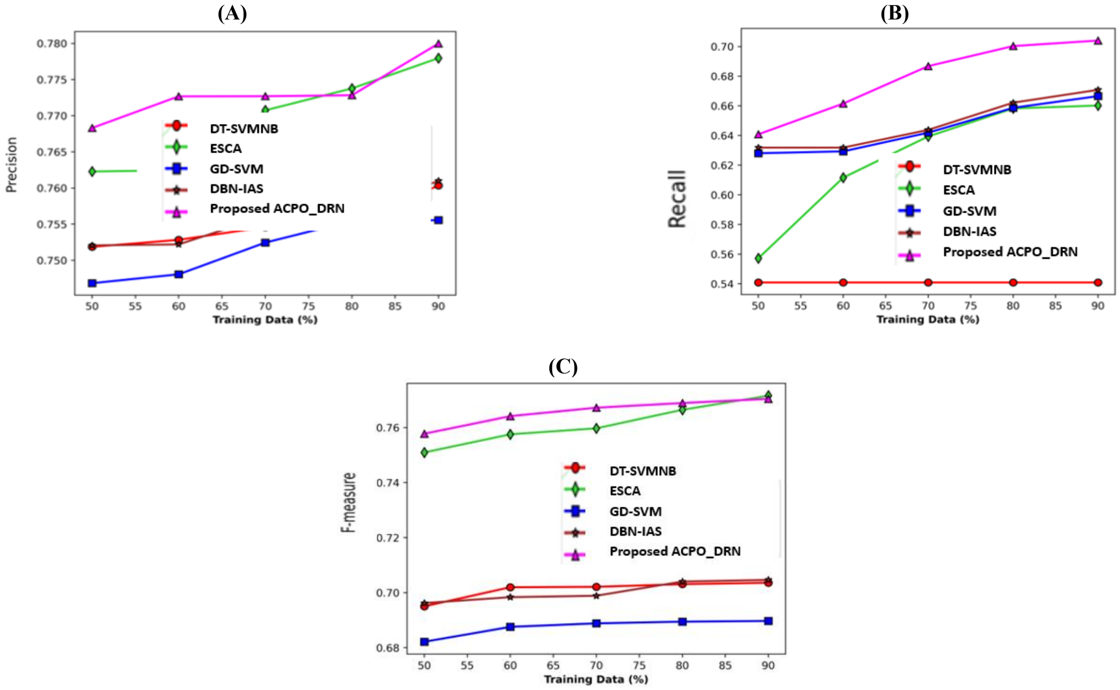
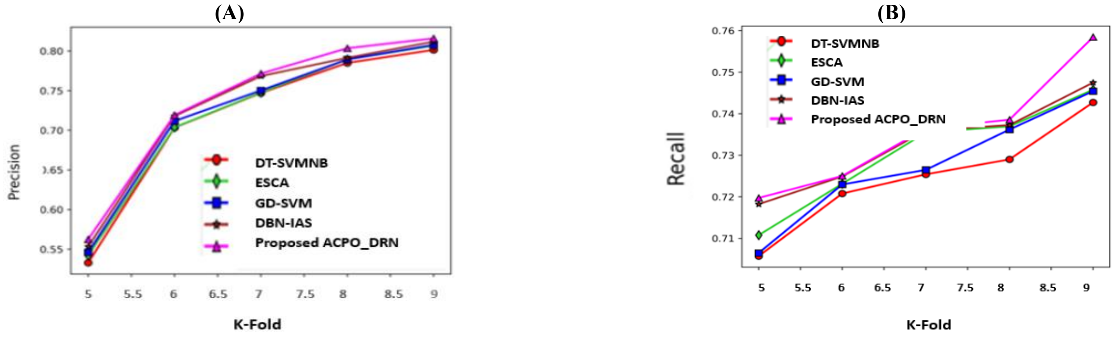


Fig. 3: Analysis Of The ACPO_DRN With Training Data Percentage Variation A) Precision. B) Recall. C) F-Measure.

4.3. K-Fold assessment

Figure 4 shows how the ACPO_DRN is evaluated for social network anomaly detection in connection to K-Fold variation measures. Figure 4i) displays the precision-based analysis. For the K-Fold 7, the accuracy values measured by the earlier methods (DT-SVMNB, ESCA, GD-SVM, and DBN-IAS) were 0.719, 0.725, 0.739, and 0.749, respectively; in contrast, the ACPO_DRN approach yielded a precision value of 0.759. Compared to the current methods, the created strategy produced a performance boost of 4.1%, 2.3%, 2.1%, and 1.1%. The Recall-based assessment is shown in Figure 4ii). When the K-Fold is 5, the recall value as reported by the DT-SVMNB is 0.683, ESCA is 0.698, GD-SVM is 0.709, DBN-IAS is 0.701, and ACPO_DRN is 0.716. The study based on F-Measure is shown in Figure 4iii). For the AVPO_DRN, the F-Measure value for the K-Fold 8 is 0.846, while the values for the DT-SVMNB, ESCA, GD-SVM, and DBN-IAS are 0.805, 0.807, 0.827, and 0.831, respectively.



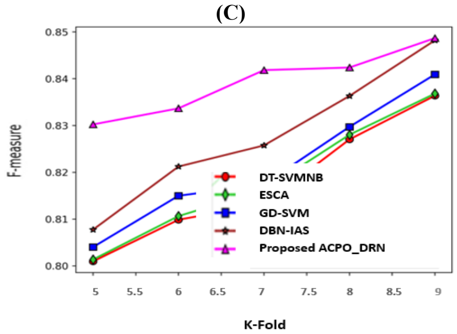


Fig. 4: Analysis of the ACPO_DRN with Varying K-Fold. A) Precision. B) Recall. C) F-Measure.

5. Conclusion

An Anomaly in an online social network means unusual or unexpected behavior deviating from typical user patterns, typically representing illegal or unusual activities. The increasing popularity of social networking websites such as Facebook and Twitter has introduced an increase in malicious activities, and, therefore, the detection of anomalies is a highly essential area of research.

We presented in this paper ACPO_DRN, a novel social network anomaly detection method. The approach begins with Z-score normalization as data preprocessing, followed by feature selection using the Dice similarity coefficient. Class imbalance is addressed using oversampling by data augmentation. Clustering is performed using the FLICM algorithm, and anomalies are detected through a Deep Residual Network (DRN) trained under the ACPO algorithm—a combination of ACVO and PO approaches. Because of the rising threats of criminal behavior from social media, ACPO_DRN offers a valuable approach to early warning detection and prevention of probable security dangers. Experimental results confirm that ACPO_DRN performs better with the best accuracy of 0.813, precision of 0.880, and F-measure of 0.836 using K-Fold cross-validation. Future research can continue to develop this work by studying the flexibility of ACPO_DRN across various datasets and application domains, and continuing to enhance its robustness and flexibility in anomaly detection.

References

[1] T. Al-Shehari, M. Kadrie, T. Alfakih, H. Alsalman, T. Kuntavai, et al., “Blockchain with secure data transactions and energy trading model over the internet of electric vehicles,” Sci. Rep., vol. 14, no. 1, p. 19208, Jan. 2024, https://doi.org/10.1038/s41598-024-69542-w.

[2] R. Vidhya, D. Banavath, S. Kayalvili, S. M. Naidu, et al., “Alzheimer’s disease detection using residual neural network with LSTM hybrid deep learning models,” J. Intell. Fuzzy Syst., vol. 45, no. 6, pp. 12095–12109, 2023. https://doi.org/10.3233/JIFS-235059.

[3] P. Selvam, N. Krishnamoorthy, S. P. Kumar, K. Lokeshwaran, M. Lokesh, et al., “Internet of Things Integrated Deep Learning Algorithms Monitoring and Predicting Abnormalities in Agriculture Land,” Internet Technol. Lett., Nov. 2024, https://doi.org/10.1002/itl2.607.

[4] S. S. F. Begum, M. S. Anand, P. V. Pramila, J. Indra, J. S. Isaac, C. Alagappan, et al., “Optimized machine learning algorithm for thyroid tumour type classification: A hybrid approach Random Forest, and intelligent optimization algorithms,” J. Intell. Fuzzy Syst., pp. 1–12, 2024.

[5] K. Maithili, A. Kumar, D. Nagaraju, D. Anuradha, S. Kumar, et al., “DKCNN: Improving deep kernel convolutional neural network-based covid-19 identification from CT images of the chest,” J. X-ray Sci. Technol., vol. 32, no. 4, pp. 913–930, 2024. https://doi.org/10.3233/XST-230424.

[6] K. Mannanuddin, V. R. Vimal, A. Srinivas, S. D. U. Mageswari, G. Mahendran, et al., “Enhancing medical image analysis: A fusion of fully connected neural network classifier with CNN-VIT for improved retinal disease detection,” J. Intell. Fuzzy Syst., vol. 45, no. 6, pp. 12313–12328, 2023. https://doi.org/10.3233/JIFS-235055.

[7] T. A. Mohanaprakash, M. Kulandaivel, S. Rosaline, P. N. Reddy, S. S. N. Bhukya, et al., “Detection of Brain Cancer through Enhanced Particle Swarm Optimization in Artificial Intelligence Approach,” J. Adv. Res. Appl. Sci. Eng. Technol., vol. 33, no. 3, pp. 174–186, 2023. https://doi.org/10.37934/araset.33.2.174186.

[8] Wange N. K., Khan I., Pinnamaneni R., Cheekati H., Prasad J., et al., “β-amyloid deposition-based research on neurodegenerative disease and their relationship in elucidate the clear molecular mechanism,” Multidisciplinary Science Journal, vol. 6, no. 4, pp. 2024045–2024045, 2024. https://doi.org/10.31893/multiscience.2024045.

[9] Anitha C., Tellur A., Rao K. B. V. B., Kumbhar V., Gopi T., et al., “Enhancing Cyber-Physical Systems Dependability through Integrated CPS-IoT Monitoring,” International Research Journal of Multidisciplinary Scope, vol. 5, no. 2, pp. 706–713, 2024. https://doi.org/10.47857/irjms.2024.v05i02.0620.

[10] Balasubramani R., Dhandapani S., Sri Harsha S., Mohammed Rahim N., Ashwin N., et al., “Recent Advancement in Prediction and Analyzation of Brain Tumour using the Artificial Intelligence Method,” Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 33, no. 2, pp. 138–150, 2023. https://doi.org/10.37934/araset.33.2.138150.

[11] Chaturvedi A., Balasankar V., Shrimali M., Sandeep K. V., et al., “Internet of Things Driven Automated Production Systems using Machine Learning,” International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 642–651, 2024. https://doi.org/10.47857/irjms.2024.v05i03.01033.

[12] Saravanakumar R., Arularasan A. N., Harekal D., Kumar R. P., Kaliyamoorthi P., et al., “Advancing Smart Cyber Physical System with Self-Adaptive Software,” International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 571–582, 2024. https://doi.org/10.47857/irjms.2024.v05i03.01013.

[13] Vidhya R. G., Surendiran J., Saritha G., “Machine Learning Based Approach to Predict the Position of Robot and its Application,” Proc. Int. Conf. on Computer Power and Communications, pp. 506–511, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072031.

[14] Sivanagireddy K., Yerram S., Kowsalya S. S. N., Sivasankari S. S., Surendiran J., et al., “Early Lung Cancer Prediction using Correlation and Regression,” Proc. Int. Conf. on Computer Power and Communications, pp. 24–28, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072059.

[15] Vidhya R. G., Seetha J., Ramadass S., Dilipkumar S., Sundaram A., Saritha G., “An Efficient Algorithm to Classify the Mitotic Cell using Ant Colony Algorithm,” Proc. Int. Conf. on Computer Power and Communications, pp. 512–517, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072277.

[16] Sengeni D., Muthuraman A., Vurukonda N., Priyanka G., et al., “A Switching Event-Triggered Approach to Proportional Integral Synchronization Control for Complex Dynamical Networks,” Proc. Int. Conf. on Edge Computing and Applications, pp. 891–894, 2022. https://doi.org/10.1109/ICECAA55415.2022.9936124.

[17] Vidhya R. G., Rani B. K., Singh K., Kalpanadevi D., Patra J. P., Srinivas T. A. S., “An Effective Evaluation of SONARS using Arduino and Display on Processing IDE,” Proc. Int. Conf. on Computer Power and Communications, pp. 500–505, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072229.

[18] Kushwaha S., Boga J., Rao B. S. S., Taqui S. N., et al., “Machine Learning Method for the Diagnosis of Retinal Diseases using Convolutional Neural Network,” Proc. Int. Conf. on Data Science, Agents & Artificial Intelligence, 2023. https://doi.org/10.1109/ICDSAAI59313.2023.10452440.

[19] Maheswari B. U., Kirubakaran S., Saravanan P., Jeyalaxmi M., Ramesh A., et al., “Implementation and Prediction of Accurate Data Forecasting Detection with Different Approaches,” Proc. 4th Int. Conf. on Smart Electronics and Communication, 2023, pp. 891–897. https://doi.org/10.1109/ICOSEC58147.2023.10276331.

[20] Mayuranathan M., Akilandasowmya G., Jayaram B., Velrani K. S., Kumar M., et al., “Artificial Intelligent based Models for Event Extraction using Customer Support Applications,” Proc. 2nd Int. Conf. on Augmented Intelligence and Sustainable Systems, 2023, pp. 167–172. https://doi.org/10.1109/ICAISS58487.2023.10250679.

[21] Gold J., Maheswari K., Reddy P. N., Rajan T. S., Kumar S. S., et al., “An Optimized Centric Method to Analyze the Seeds with Five Stages Technique to Enhance the Quality,” Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2023, pp. 837–842. https://doi.org/10.1109/ICAISS58487.2023.10250681.

[22] Anand L., Maurya J. M., Seetha D., Nagaraju D., et al., “An Intelligent Approach to Segment the Liver Cancer using Machine Learning Method,” Proc. 4th Int. Conf. on Electronics and Sustainable Communication Systems, 2023, pp. 1488–1493. https://doi.org/10.1109/ICESC57686.2023.10193190.

[23] Harish Babu B., Indradeep Kumar, et al., “Advanced Electric Propulsion Systems for Unmanned Aerial Vehicles,” Proc. 2nd Int. Conf. on Sustainable Computing and Smart Systems (ICSCSS), 2024, pp. 5–9, IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10625489.

[24] Jagan Raja V., Dhanamalar M., Solaimalai G., et al., “Machine Learning Revolutionizing Performance Evaluation: Recent Developments and Breakthroughs,” Proc. 2nd Int. Conf. on Sustainable Computing and Smart Systems (ICSCSS), 2024, pp. 780–785, IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10625103.

[25] Sivasankari S. S., Surendiran J., Yuvaraj N., et al., “Classification of Diabetes using Multilayer Perceptron,” Proc. IEEE Int. Conf. on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2022, pp. 1–5, IEEE. https://doi.org/10.1109/ICDCECE53908.2022.9793085.

[26] Anushkannan N. K., Kumbhar V. R., Maddila S. K., et al., “YOLO Algorithm for Helmet Detection in Industries for Safety Purpose,” Proc. 3rd Int. Conf. on Smart Electronics and Communication (ICOSEC), 2022, pp. 225–230, IEEE. https://doi.org/10.1109/ICOSEC54921.2022.9952154.

[27] Reddy K. S., Vijayan V. P., Das Gupta A., et al., “Implementation of Super Resolution in Images Based on Generative Adversarial Network,” Proc. 8th Int. Conf. on Smart Structures and Systems (ICSSS), 2022, pp. 1–7, IEEE. https://doi.org/10.1109/ICSSS54381.2022.9782170.

[28] Joseph J. A., Kumar K. K., Veerraju N., Ramadass S., Narayanan S., et al., “Artificial Intelligence Method for Detecting Brain Cancer using Advanced Intelligent Algorithms,” Proc. Int. Conf. on Electronics and Sustainable Communication Systems, 2023, pp. 1482–1487. https://doi.org/10.1109/ICESC57686.2023.10193659.

[29] Surendiran J., Kumar K. D., Sathiya T., et al., “Prediction of Lung Cancer at Early Stage Using Correlation Analysis and Regression Modelling,” Proc. 4th Int. Conf. on Cognitive Computing and Information Processing, 2022, pp. 1–.https://doi.org/10.1109/CCIP57447.2022.10058630.

[30] Goud D. S., Varghese V., Umare K. B., Surendiran J., et al., “Internet of Things-based Infrastructure for the Accelerated Charging of Electric Vehicles,” Proc. Int. Conf. on Computer Power and Communications, 2022, pp. 1–6. https://doi.org/10.1109/ICCPC55978.2022.10072086.

[31] Vidhya R. G., Singh K., Paul J. P., Srinivas T. A. S., Patra J. P., Sagar K. V. D., “Smart Design and Implementation of Self-Adjusting Robot using Arduino,” Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2022, pp. 1–6. https://doi.org/10.1109/ICAISS55157.2022.10011083.

[32] Vallathan G., Yanamadni V. R., et al., “An Analysis and Study of Brain Cancer with RNN Algorithm-based AI Technique,” Proc. Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2023, pp. 637–642. https://doi.org/10.1109/I-SMAC58438.2023.10290397.

[33] Vidhya R. G., Bhoopathy V., Kamal M. S., Shukla A. K., Gururaj T., Thulasimani T., “Smart Design and Implementation of Home Automation System using Wi-Fi,” Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2022, pp. 1203–1208. https://doi.org/10.1109/ICAISS55157.2022.10010792.

[34] Vidhya R., Banavath D., Kayalvili S., Naidu S. M., Prabu V. C., et al., “Alzheimer’s Disease Detection using Residual Neural Network with LSTM Hybrid Deep Learning Models,” J. Intelligent & Fuzzy Systems, 2023; vol. 45, no. 6, pp. 12095–12109. https://doi.org/10.3233/JIFS-235059.

[35] Balasubramaniyan S., Kumar P. K., Vaigundamoorthi M., Rahuman A. K., et al., “Deep Learning Method to Analyze the Bi-LSTM Model for Energy Consumption Forecasting in Smart Cities,” Proc. Int. Conf. on Sustainable Communication Networks and Application, 2023, pp. 870–876https://doi.org/10.1109/ICSCNA58489.2023.10370467.

[36] Somani V., Rahman A. N., Verma D., et al., “Classification of Motor Unit Action Potential Using Transfer Learning for the Diagnosis of Neuromuscular Diseases,” Proc. 8th Int. Conf. on Smart Structures and Systems (ICSSS), 2022, pp. 1–7, IEEE. https://doi.org/10.1109/ICSSS54381.2022.9782209.

[37] Vidhya R. G., Saravanan R., Rajalakshmi K., “Mitosis Detection for Breast Cancer Grading,” Int. J. Advanced Science and Technology, 2020; vol. 29, no. 3, pp. 4478–4485.

[38] Gupta D., Kezia Rani B., Verma I., et al., “Metaheuristic Machine Learning Algorithms for Liver Disease Prediction,” Int. Res. J. Multidisciplinary Scope, 2024; vol. 5, no. 4, pp. 651–660. https://doi.org/10.47857/irjms.2024.v05i04.01204.

[39] Sudhagar D., Saturi S., Choudhary M., et al., “Revolutionizing Data Transmission Efficiency in IoT-Enabled Smart Cities: A Novel Optimization-Centric Approach,” Int. Res. J. Multidisciplinary Scope, 2024; vol. 5, no. 4, pp. 592–602. https://doi.org/10.47857/irjms.2024.v05i04.01113.

[40] Vidhya R. G., Batri K., “Segmentation, Classification and Krill Herd Optimization of Breast Cancer,” J. Medical Imaging and Health Informatics, 2020; vol. 10, no. 6, pp. 1294–1300. https://doi.org/10.1166/jmihi.2020.3060.

[41] Chintureena Thingom, Martin Margala, S Siva Shankar, Prasun Chakrabarti, RG Vidhya, “Enhanced Task Scheduling in Cloud Computing Using the ESRNN Algorithm: A Performance-Driven Approach”, Internet Technology Letters, vol. 8, no. 4, 2025, pp. e70037. https://doi.org/10.1002/itl2.70037.

[42] V. V. Satyanarayana, Tallapragada, Denis R, N. Venkateswaran, S. Gangadharan , M. Shunmugasundaram, et.al.,” A Federated Learning and Blockchain Framework for IoMT-Driven Healthcare 5.0”, International Journal of Basic and Applied Sciences, vol. 14, no. 1, 2025, pp. 246-250. https://doi.org/10.14419/n1npsj75.

[43] Thupakula Bhaskar, K. Sathish, D. Rosy Salomi Victoria, Er.Tatiraju. V. Rajani Kanth , Uma Patil, et.al.,” Hybrid deep learning framework for enhanced target tracking in video surveillance using CNN and DRNN-GWO”, International Journal of Basic and Applied Sciences, vol. 14, no. 1, 2025, pp. 208-215. https://doi.org/10.14419/wddeck70.

[44] Thupakula Bhaskar, Hema N, R.Rajitha Jasmine , Pearlin , Uma Patil , Madhava Rao Chunduru , et.al.,” An adaptive learning model for secure data sharing in decentralized environments using blockchain technology”, International Journal of Basic and Applied Sciences, vol. 14, no. 1, 2025, pp. 216-221. https://doi.org/10.14419/9f4z3q54.

[45] B. Ramesh, V. V. Kulkarni, Ashwini Shinde, Dinesh Kumar J. R, Prasanthi Kumari Nunna, Rajendiran M, “Optimizing EV Energy Management Using Monarch Butterfly and Quantum Genetic Algorithms” International Journal of Basic and Applied Sciences, vol. 14, no. 2, 2025, pp. 311-318. https://doi.org/10.14419/xaqk1294.