Enhancing Dendritic Cell Algorithm by Integration with Multi-Layer Perceptron for Anomaly Detection

Yousra Abudaqqa, Zulaiha Ali Othman, Azuraliza Abu Bakar
Research Center for Artificial Intelligence Technology-Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, Bangi, Selangor 43600, Malaysia

Abstract*—Anomaly detection is crucial in a variety of areas, with the Dendritic Cell Algorithm (DCA) being one of the most used artificial immune systems (AIS) and introduced for binary classification of data. Both traditional and current perspectives on classification in DCA have primarily been threshold-based methods. Such approaches are limited in important ways, including inflexibility, manual tuning, and not being context-aware. The latest improvements in literature have provided adaptive dynamic threshold mechanisms that allow the system to adjust the sensitivity of the threshold using some statistical data of real-time observations. Although this is progress, the systems proposed are still based on rules, which have traditionally struggled with the more complex, higher-dimensional and nonlinear nature of data. This is common in most complex anomaly detection tasks today. In this study, we propose an improved DCA-MLP framework that uses a Multi-layer Perceptron (MLP) classifier replacing the thresholding phase. The MLP allows the DCA to learn from data context adaptively through a context-sensitive learning mechanism that can also change with the data distribution as it evolves, eliminating the need to robotically calibrate based on static or heuristic thresholds. The framework was tested thoroughly on fourteen benchmark datasets, and performance was evaluated against standard DCA in terms of accuracy, sensitivity and specificity measures. The performance results revealed considerable enhancements in DCA-MLP's performance: 12%–50% improvements in accuracy (increasing accuracy to 93%–99%), 46% improvements in sensitivity (sensitivity as 98%), and 39% improvements in specificity. This shows that DCA-MLP is better adaptable, with learning capacity and robustness - a paradigm shift away from thresholds or threshold-based systems to an intelligent self-adjusting anomaly detection classification scheme.

Keywords*—Dendritic Cell Algorithm (DCA); anomaly threshold; Multi-Layer Perceptron (MLP); anomaly detection

I. Introduction

Anomaly detection, or the process of identifying patterns that are identified as the unusual portion of normal behavior, is important across several domains, including cybersecurity, healthcare, finance, and industrial systems. Anomalies such as fraudulent financial transactions, malignant tumors in a medical image, and cyberattacks on network traffic, all signal important implications, transforming raw data into actionable insights [7, 24, 33, 37]. Traditional classification algorithms often falter on dynamic, high-dimensional data; so researchers have resorted to diagnostic and biologically inspired solutions, such as artificial immune systems (AISs).AISs emulate the human immune system's ability to distinguish self from non-self, offering unique advantages in adaptability and unsupervised learning [1]. Among AIS-based approaches, the Dendritic Cell Algorithm (DCA)[2]stands out for its success in anomaly detection, leveraging the biological "danger theory" to classify threats by monitoring antigen behavior through metrics like the Multi-Context Antigen Value (MCAV) [3].

Despite its effectiveness, the DCA faces significant limitations. Its reliance on fixed, empirically derived thresholds for anomaly classification introduces rigidity, as static parameters fail to adapt to evolving data patterns or outliers [4]. For instance, threshold-setting methods like try-and-test experiments or class distribution analysis depend heavily on historical data and expert input, limiting scalability and real-world applicability [4]. These constraints are particularly evident in complex tasks such as network intrusion detection or time-series analysis, where dynamic environments demand adaptive solutions [5].

To address these challenges, this study proposes a novel integration of the DCA with a Multi-Layer Perceptron (MLP), replacing the static threshold mechanism with a dynamic, data-driven classification framework. Inspired by the immune system's interaction between dendritic cells (DCs) and T-cells (TCs), our approach enhances the DCA's decision-making process by embedding an MLP to learn complex relationships within antigen signals. Unlike traditional threshold-based methods, the MLP adaptively adjusts classification boundaries, improving robustness against outliers and reducing false alarms. This integration leverages the MLP's capacity to handle non-linear patterns while preserving the DCA's unsupervised learning strengths.

The contributions of this work are threefold:

1) Improved accuracy: The MLP refines [6] anomaly classification through supervised learning on fused antigen signals (e.g., danger, safe, and co-stimulatory signals), achieving accuracy improvements of 12% to 50% across benchmark datasets.

2) Dynamic adaptability: By eliminating fixed thresholds, the DCA-MLP framework dynamically adjusts to new data patterns, enhancing resilience in evolving environments.

3) Scalability: Non-Negative Matrix Factorization (NMF) streamlines signal extraction, enabling efficient processing of high-dimensional data without compromising detection performance.

Experimental validation on fourteen datasets proves the framework's superiority over traditional DCA, with sensitivity

and specificity gains of up to 46% and 39%, respectively. These advancements position the DCA-MLP as a scalable, adaptive solution for complex anomaly detection tasks, bridging the gap between immune-inspired algorithms and modern machine learning.

The rest of this study is organized as follows: Section II reviews related work on AIS and DCA enhancements. Section III details the proposed DCA-MLP architecture, while Section IV presents the experiment setup. Section V details the experimental results. Section VI presents the discussion of the study. Finally in Section VII, the study concludes with implications and future research directions.

II. Related Work

Anomaly detection plays a crucial role in various fields, including network security, healthcare, and industrial systems, where identifying unusual patterns or behaviors is essential for maintaining system integrity and performance [7]. While traditional methods such as (MLP, KNN, SVM and Decision Tree) have been effective in specific contexts, they often face challenges when dealing with the complexity and dynamic nature of modern datasets [8]. Advanced algorithms like the Dendritic Cell Algorithm (DCA) have appeared as promising solutions to these challenges, offering improved capabilities for solving anomaly detection problems [4]. The DCA, introduced by [2] operates through four key phases [9], as illustrated in Fig. 1.

In the first phase**,** pre-processing, the algorithm performs two critical tasks: feature reduction and signal categorization. Feature reduction selects the most relevant attributes from the dataset, and these attributes are then categorized into three signal types: safe, danger, and Pathogen-Associated Molecular Patterns (PAMP). The most popular methods for feature reduction include Principal Component Analysis (PCA) and Non-Negative Matrix Factorization (NMF). While PCA is widely used, it can obscure data interpretation by transforming the dataset into components that may lose connection to the original features [10]. In contrast, NMF excels by identifying weakly correlated or uncorrelated factors, revealing hidden patterns, and transforming data into a reduced yet interpretable space [11]. This approach avoids overfitting, improves prediction accuracy, and effectively manages data sparsity. Furthermore, NMF operates without strict statistical assumptions, making it highly adaptable for large-scale datasets. By maintaining essential data characteristics, NMF simplifies computational demands related to time and storage while ensuring robust model performance.

In the second phase, detection**,** the DCA generates a signal database by combining the input signals with antigens, resulting in cumulative output signals. The third phase, context assessment, evaluates the context of antigens using the cumulative signals. If a Dendritic Cell (DC) collects more Mature Dendritic Cells (mDC) than Semi-Mature Dendritic Cells (smDC), the antigen is labelled as anomalous (1); otherwise, it is classified as normal (0) [12]. Finally, during the classification phase**,** the Mature Context Antigen Value (MCAV) is calculated for each antigen to assess the likelihood of an anomaly. The MCAV is determined by dividing the number of times an antigen appears in the mature context by the total number of antigen presentations. This value is then compared to a predefined anomaly threshold, classifying antigens with higher MCAV values as anomaly.

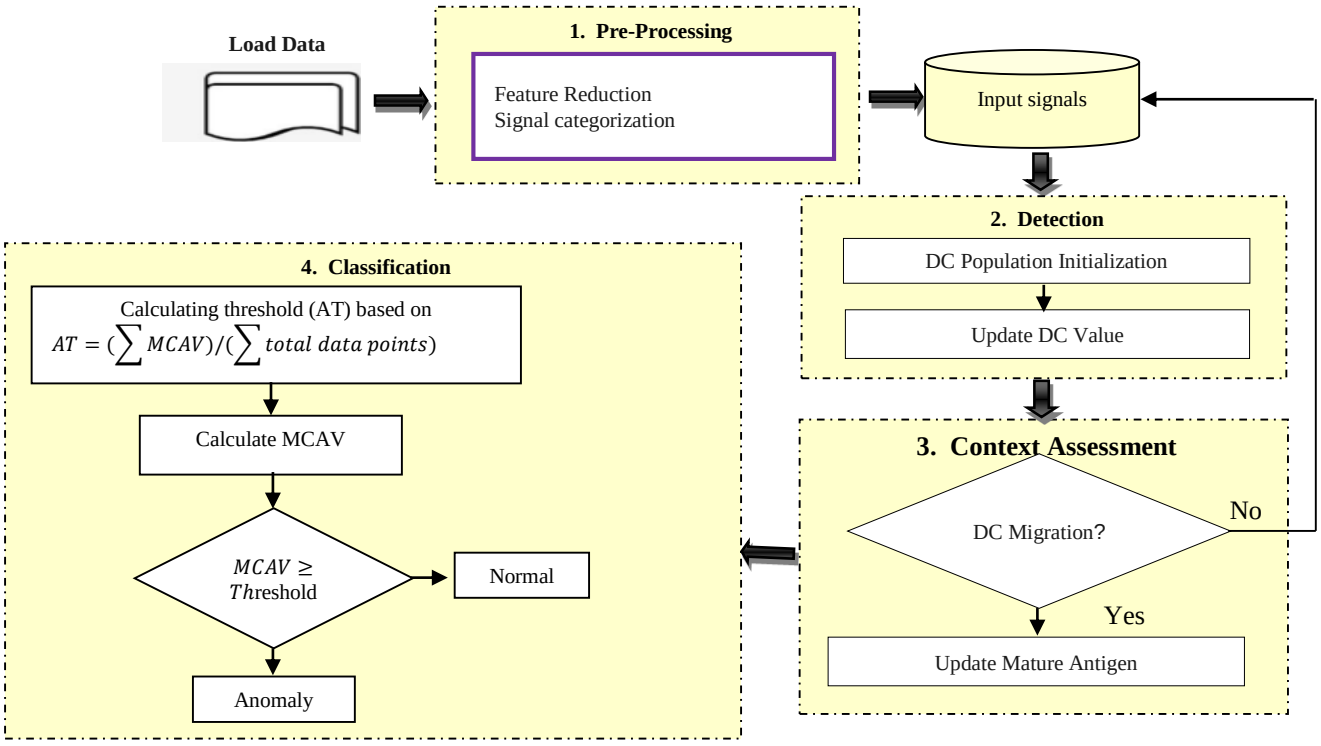


Fig. 1. The standard architecture of the Dendritic Cell Algorithm (DCA) diagram.

The MCAV plays a pivotal role in the DCA, representing the ratio of how often an antigen appears in a "mature context" compared to the total number of antigen presentations[13]. In the DCA, dendritic cells exist in two states**:** Mature Dendritic Cells (mDC)**,** which detect danger or anomalies, and Semi-Mature Dendritic Cells (smDC)**,** which reflect normal or non-threatening behavior. The MCAV measures how frequently an antigen is associated with dangerous contexts (mDC) versus normal ones (smDC), aiding in determining whether the antigen is more likely to be abnormal or normal. A higher MCAV indicates a higher likelihood of the antigen being anomalous, while a lower MCAV suggests it is normal. The MCAV is calculated as Eq. (1):

$$\text{MCAV} = (\text{Mature})/(\text{Semi Mature} + \text{Mature}) \quad (1)$$

The importance of the MCAV lies in its adaptive nature, allowing the DCA to assess anomalies based on the environment rather than static rules [14]. This flexibility makes the DCA highly capable of handling unfamiliar data points by evaluating how often an antigen appears in mature contexts, improving the algorithm's ability to classify new or unseen data accurately. Furthermore, combining the MCAV with a flexible anomaly threshold allows the DCA to adapt to different domains, such as network intrusion detection, spam filtering, and fault diagnosis, where normal and abnormal patterns vary significantly.

Anomaly Threshold (AT) is a default value used to differentiate between normal and abnormal antigens by comparing it to the MCAV of an antigen. If the MCAV exceeds the threshold, the antigen is considered abnormal or an anomaly. Currently, there are three primary strategies for determining the AT in DCA: 1) trial-and-error experimentation, 2) class distribution between normal and abnormal groups and 3) the average MCAV method [10]. The class distribution method is based on the ratio of normal to abnormal classes, requiring both classes to be balanced to generate a suitable threshold value, as shown in Eq. (2). However, achieving this balance is challenging, especially since anomalies are often rare and can create a significant gap between the two classes.

$$AT = (\sum MCAV)/(\sum total\ data\ points) \quad (2)$$

The anomaly threshold (AT) in standard DCA implementations has been applied across various domains with different strategies. In [15], the authors has enhanced the traditional DCA by introducing a migration threshold strategy that adapts to various attack scenarios, applied in network intrusion detection on the UNSW-NB15 dataset, achieving an anomaly value of 76.69% using the min MCAV approach. In [16], the authors also focused on network intrusion, using the NSL-KDD dataset to classify traffic as normal or anomalous based on immune-like danger signals. This approach identified DoS attacks through a class and min MCAV distribution strategy, providing scalability in dynamic network environments. Similarly, [17] employed a try-and-test approach in conjunction with min MCAV within a fuzzy logic system on the KDD99 dataset, enhancing adaptability to varied data types.

In [7], the authors adopted a different method, using class distribution to determine AT by assessing the ratio of abnormal to normal traffic in the NSL-KDD dataset, achieving a 0.60% anomaly threshold. In [5], the authors applied min MCAV across general classification domains with datasets such as Sonar and GCD, adjusting the threshold based on dataset-specific characteristics. Finally, [10] utilized min MCAV for anomaly detection in medical diagnosis, using datasets like WBC and LDR, focusing on metrics such as Mean Correlation Activity Value to identify anomalies dynamically. This variety of approaches underscores the flexibility of DCA in different application areas, with each study refining AT to suit specific datasets and anomaly detection needs. Some investigations have focused on the DCA classification phase, aiming to refine and enhance its effectiveness. More precisely, researchers have explored ways to improve the decision-making process by optimizing how the algorithm classifies data points as either normal or anomalous. The traditional classification approach in the DCA relies on fixed thresholds based on the multi-context antigen value (MCAV) [16], which can be limited in applications such as network intrusion detection [13] and medical anomaly detection [17]. The core of this process revolves around the calculation of the Mature Context Antigen Value, handling complex or extreme data patterns. A critical stage for identifying anomalous patterns across different domains (MCAV) [8], which determines whether a pattern is a normal presentation. When the MCAV exceeds a predefined threshold, the pattern is classified as anomalous (depicted or anomalous. The MCAV is the ratio of antigen encounters in a mature context to the total number of antigens by the decision boundary in the figure). Otherwise, it is classified as normal [18]. This classification method, though effective in many cases, highlights the challenge of setting an appropriate threshold, which directly impacts the detection accuracy of the algorithm.

Several techniques have been proposed to establish the anomaly threshold for MCAV, each with its own limitations [19]. For instance, the try-and-test method involves iterative testing to find the optimal threshold, though this process is time-consuming and highly reliant on expert knowledge. Other approaches, such as the minimum MCAV threshold introduced by[7] and adaptive thresholds based on cumulative sum (CUSUM)[10], have also been explored. While these methods offer systematic approaches to threshold determination, they deal with outliers and data changes over time, which can limit their effectiveness for longer-term anomaly detection. However, the challenge remains that these methods still depend on historical data for initial threshold values may not be reliable in rapidly evolving datasets [10, 16, 20].

An effective method for enhancing the traditional threshold methods in the DCA is to adopt the Multi-Layer Perceptron (MLP) algorithm into the DCA. Unlike the standard method of comparing MCAV values to a predefined threshold for anomaly detection, the MLP algorithm learns from the data, adjusting its parameters to better manage outliers and extreme values. This adaptability enables the MLP-DCA combination to have greater accuracy and success in detecting and classifying anomalies. By leveraging the machine learning capabilities of MLP, this integration enhances the overall process, making it more resilient against unusual data points that might otherwise challenge a simple MCAV-based threshold approach.

Integrating the DCA with an MLP algorithm presents several key advantages. To begin with, it enhances system robustness by giving the MLP the ability to better deal with extreme values

and outliers. This ensures that the algorithm maintains reliable performance even when faced with unexpected data. Secondly, the learning capabilities in the MLP improve the ability to detect and classify anomalies by allowing the model to recognize complex patterns and associations in the data assignments. The MLP refines its understanding over time, it produces more precise and reliable results. Moreover, the adaptability of the MLP enables it to respond to evolving data patterns, making it a flexible and sustainable solution for anomaly detection.

This combination overcomes the limitations of traditional threshold-based approaches by introducing adaptive learning from data, making it a valuable advancement in the field of anomaly detection.

III. The Proposed Method

This study proposes an enhanced anomaly detection framework known as MLP-DCA**,** which integrates the Dendritic Cell Algorithm (DCA) with a Multi-Layer Perceptron (MLP) classifier to overcome critical limitations of traditional threshold-based decision-making in DCA. Two primary limitations of the standard DCA model motivate this integration:

1) Its reliance on a fixed threshold for anomaly classification, which leads to poor adaptability when handling datasets with imbalanced class distributions **or** dynamic patterns.

2) The manual effort and expert knowledge required to tune this threshold, making it impractical for real-world, large-scale, or evolving data environments.

To address these challenges, the proposed MLP-DCA model retains the original architecture of the standard DCA, which includes four primary phases: signal preprocessing, antigen processing, signal integration**,** and classification (see Fig. 1). The first three phases are preserved to leverage the biologically inspired behavior and contextual data fusion capabilities of DCA, which have proven effective in prior studies [11].

In the preprocessing phase, the model introduces Non-Negative Matrix Factorization (NMF) for automated feature transformation and signal categorization**.** This enhancement allows the model to handle high-dimensional datasets by reducing complexity and focusing on the most informative features. NMF serves as a dimensionality reduction technique, helping to categorize input attributes into the necessary signal types (PAMP, danger, and safe) without manual mapping.

The major innovation lies in the classification phase, where the traditional MCAV-based anomaly threshold (AT) is replaced with an MLP classifier (see Fig. 2). Instead of relying on static decision rules, the MLP dynamically learns non-linear and high-level feature relationships from the processed signals and antigen information. This adaptive learning approach enables the system to generalize better across diverse datasets, respond to class imbalance, and improve classification robustness On the whole, by combining context-aware processing capabilities of DCA with the learning power of MLP, we proposed model achieves a more flexible and scalable anomaly detection system. The MLP-DCA architecture in addition to completely removing threshold tuning, these powerful neurons improve the accuracy, sensitivity and specificity across many benchmark datasets, demonstrated in the experimental section.

As depicted in Fig. 2, the classification process begins the same as a standard DCA which is by calculating the MCAV [Eq. (1)]. The calculated MCAV values (acting as the independent variable) are fed into the MLP that classifies the antigens, as shown in Eq. (3):

$$f(MCAV) = (\sum_{i=1}^{m} w_i \,.\, MCAV_i) + b \qquad (3)$$

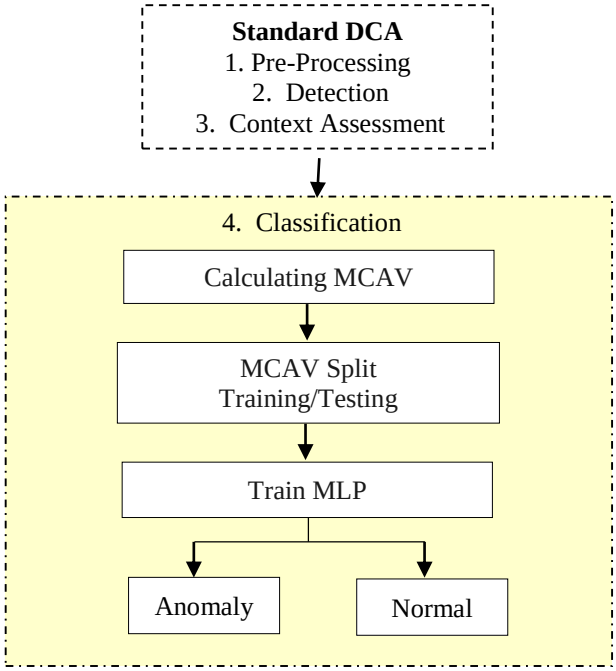


Fig. 2. Proposed method MLP_DCA.

where:

- $MCAV$: Represents the mean of context activation vectors
- derived from the inputs or data points.
- w_i: Weights assigned to each $MCAV_i$ during training.
- b: Bias term.
- m: Total number of MCAV inputs.
- The MLP leverages this transformation to predict the class of each antigen (e.g., normal or abnormal) based on learned parameters.

Fig. 3 illustrates the pseudocode for integrating the Dendritic Cell Algorithm (DCA) with a Multi-Layer Perceptron (MLP) during the classification phase. This integration comprises three primary steps:

1) Step 4.1 Calculation of MCAV values: Initially, for each antigen generated in prior stages, the Mature Context Antigen Value (MCAV) is computed using Equation (1). These MCAVs are then stored in the MCAV_values []. array for subsequent classification.

2) Step 4.2 Training the MLP model: After the MCAV values are recorded, and their labels normal or abnormal, we

can use those as inputs to train the MLP. The MLP contains three hidden layer sizes of 10, 10, and 5. Initial weights and biases are initialized random. Then the dataset is split into training and test data. The model trains through many epochs, and in each epoch all the samples will go through forward propagation in the layers of the MLP. The activations of the neurons are calculated using Eq. (3). The loss of the model is determined through cross entropy loss, and gradients are calculated by backpropagation for the weights and biases and updating them in many epochs until convergence.

3) Step 4.3 Prediction using the trained MLP: Finally, for each test sample, forward propagation is executed using the trained model to compute activations. The output activation is determined by Eq. (4):

$$MCAV(l) = f(W(l).MCAV(l-1)b(l) \qquad (4)$$

where, l indicates the output layer. A threshold of 0.5 is applied to classify the sample: outputs exceeding 0.5 are labeled as abnormal, while those below are labeled as normal.

This method uses the DCA's ability to generate MCAVs, and then it will be used as input to the MLP. The MLP is trained to classify the data into normal or abnormal categories, enhancing the overall classification performance by combining the strengths of both algorithms.

Phase 4: Classification
#Step 4.1: calculate MCAV values
1. For each antigen: // where antigen is the output of previous steps
2. Compute MCAV (antigen) using Equation 1
3. Append the computed MCAV (antigen) to the array MCAV_values [].

#Step 4.2: Feed MCAV Values into MLP for Classification
4. Train the MLP model as follow:
5. Input: MCAV_values []and their corresponding predefined labels (normal/abnormal).
6. Output: A trained MLP model with updated weights and biases.
7. Randomly initialize weights and biases for all layers based on the architecture (hidden layer sizes: 10, 10, 5).
8. Split the data into training and testing sets: X_{train}, X_{test}
9. Repeat the following steps until convergence:
10. For each epoch
11. For each training sample in X_{train}:
Perform forward propagation through the layers: Input Layer → Hidden Layers → Output Layer.
Compute activation for each neuron using equation (3)
Compute the loss between the predicted output and the actual label using across-entropy loss
Backpropagate the error using the chain rule to compute gradients of the loss with respect to the weight and biases.
Update weights and biases.
12 Store Final Weights and Biases:

#Step 4.3: Use trained MLP for prediction
13. For each test sample in X_{test}:
14. Perform forward propagation the trained model: Input Layer → Hidden Layers → Output Layer.
15. Compute activations for the output layer using
$$MCAV(l) = f(W(l).MCAV(l-1) + b(l))$$
16. Classify each test sample based on the output
If output > 05 → Assign ABNORMAL.
Else → Assign NORMAL.

Fig. 3. The pseudo-code for the proposed DCA_MLP algorithm.

The reason for the connection of the MLP to the DCA is that the MLP is a very strong learning procedure that can learn many complex, non-linear relationships from the data; without relying on any fixed decision rules. As a type of artificial neural network, the MLP classifier builds models through multiple interconnected layers of neurons, allowing it to capture intricate patterns between input features—such as the Mean Context Antigen Value (MCAV)and corresponding class labels (e.g., normal or anomalous).

During training, this MLP will repeatedly adjust its internal variables (weights and biases) to minimize overall classification error, in the hopes of maximizing performance across multiple types and dimensions of data. Unlike threshold methods, the dynamic nature of the learning process allows the model to learn and adjust to a number of data distributions with no need for human threshold adjustment. By combining MLP with the biologically inspired architecture of DCA—which is retained through its four-phase structure, the proposed MLP-DCA hybrid model enhances anomaly detection by preserving the contextual fusion strengths of DCA while improving classification robustness, generalization, and adaptability through machine learning.

IV. The Experimental Setup

As previously discussed, the standard Dendritic Cell Algorithm (DCA) [20] suffers from key limitations, particularly its reliance on manually defined, static thresholds for classification. This section details the experimental procedures undertaken to investigate these limitations and to validate the proposed enhancement of integrating a Multi-Layer Perceptron (MLP) into the DCA classification phase. The following hypotheses were formulated:

- H1: The performance of the standard DCA is significantly influenced by using static, predefined threshold values, particularly in datasets with varying class distributions.
- H2: Replacing the static threshold mechanism with an adaptive classifier, such as an MLP, improves classification performance by dynamically learning from the data.

To validate these hypotheses, we designed a two-part experimental framework. All experiments across both parts were conducted using a consistent set of fourteen benchmark datasets, listed in Table I, which span multiple domains including medical diagnosis, credit scoring, email classification, and network intrusion detection. These datasets were obtained from the UCI Machine Learning Repository[21], as well as widely used intrusion detection benchmarks—NSL-KDD [22] and UNSW-NB15[23].

1) Threshold sensitivity in the standard DCA model: To explore H1, we looked at the responsiveness of the standard DCA algorithm to different threshold values. For demonstrative purposes, the Wisconsin Breast Cancer (WBC) dataset was used under two distinct scenarios:

- Scenario A: Original dataset with 100% of the instances are anomalous.

- Scenario B: Modified version containing only 10% anomaly instances.

2) In each case, the DCA's decision threshold was manually tuned to maximize classification accuracy. The findings showed significant variability in performance depending on configuration of threshold which validated our assertion that the model was responsive and furthermore, not robust to changing class distributions. Evaluating the Proposed DCA-MLP Model.

To test H2**,** we implemented the DCA-MLP model by integrating the Multi-Layer Perceptron classifier into the DCA's classification stage. Unlike static thresholding, the MLP enables adaptive and data-driven decision-making by learning complex, nonlinear relationships in the data.

For a comprehensive evaluation, we applied the DCA-MLP model to all fourteen benchmark datasets mentioned in Table I. These datasets were selected to ensure diversity in feature dimensionality, sample size, and application domain. The model's performance was compared to the standard DCA using metrics including accuracy, sensitivity, and specificity, demonstrating the robustness and generalizability of the proposed approach across different types of data distributions and class imbalances.

To assess the performance of the proposed DCA-MLP model, the following evaluation metrics were used:

- Accuracy (ACC): Overall classification correctness.
- Sensitivity (SNS): The ability to correctly identify abnormal (positive) instances.
- Specificity (SPS): The ability to correctly identify normal (negative) instances.
- False Discovery Rate (FDR): The proportion of abnormal predictions that are normal.

TABLE I. DATASET DESCRIPTION

Dataset	Source	Feature	Record	Target class	Class count
Sonar (sonar)	UCI	60	208	2	Normal (111), Abnormal (97)
Wisconsin Breast Cancer (WBC)	UCI	9	699	2	Normal (458), Abnormal (241)
Wisconsin Diagnostic Breast Cancer (WDBC)	UCI	30	569	2	Malignant (212 cases) or benign (357 cases)
Pima Indians Diabetes (PID)	UCI	8	768	2	500 (non-diabetic), 268 (diabetic).
Indian Liver Patient Dataset (ILPD)	UCI	10	583	2	**416** liver disease and **167** without liver disease
Horse Colic(horse)	UCI	28	368	2	**Survival (**204), **non-survival (**164)
German-Credit (GC)	UCI	20	1000		**Good** 700, **Bad 300**
Red-Win-quality(win)	UCI	13	6497		**Low quality (63, High quality (217))**
Ionosphere (ionosphere)	UCI	35	351	2	Normal (225), Abnormal (126)
Statlog (Heart)	UCI	16	270		**(105)** normal, **(165) abnormal**
Spambase (SP)	UCI	57	4601		**Spam (**1,813**), not spam (**2,788**)**
BUPA liver disorder (LDR)	UCI	7	345	2	Liver disorder present (145), Not present (200)
UNSW-NB15 (UNSW-NB15)	IDS	42	2007	2	Normal (243), Abnormal (1764)
NSL-KDD (NSL_KDD)	IDS	41	3577	2	Normal (1577), Abnormal (2000)

High values of ACC, SNS, and SPS indicate good performance, while a lower FDR reflects fewer false alarms. These metrics were computed as follows [see Eq. (5) to Eq. (8)] [24]:

$$ACC = TP + TN/(TP + TN + FP + FN) \quad (5)$$

$$SNS = TP/(TP + FN) \quad (6)$$

$$SPS = TN/(TN + FP \quad (7)$$

$$\text{FDR} = FP/(TP + FP) \quad (8)$$

To ensure statistical reliability, each experiment was repeated 30 times, and mean values of each metric were reported. The statistical significance of performance improvements (Δ) between the standard DCA and the proposed DCA-MLP was evaluated using p-values from independent t-tests.

3) Parameter configuration and preprocessing: In all the experiments we conducted, the setup for the Dendritic Cell Algorithm (DCA) included a population of 100 dendritic cells (DCs), and each iteration selected 10 DCs to sample the antigen vector. The migration threshold for each DC was set to 10 iterations. Signal classification employed a feature-based approach- the smallest standard deviation represented the PAMP and safe signals, while the largest standard deviation represented the n-NS signal. standard deviation was selected during preprocessing to prioritize informative features.

For the Multi-Layer Perceptron (MLP) classifier, we applied standard training approaches; adaptive learning rate, early stopping to prevent overfitting, and K-fold cross validation in order to ensure robust model evaluation. These parameters were not only chosen based on best practices in literature but were also found to significantly influence detection performance. For example, increasing the amount of DCs can increase the number

of antigen samples, but the cost of the computation may be increased. Likewise, if the migration threshold is lowered, it will improve the speed of classification but may decrease decision-making accuracy in noisy data. Within the MLP, we found that adaptive learning rate and early stopping had the most significant impacts, effectively allowing the MLP to converge without overfitting. While the proposed model demonstrated stability over a range of parameter values, a sensitivity analysis revealed that signal selection and learning rate had the most effect on classification accuracy and generalization capability.

Comparative Analysis of Benchmark Literature Finally, we validated the proposed DCA-MLP model by comparing its performance to established benchmark literature methods, including GA-DCA, dDCA, NMF, standard DCA, and COID-DCA, on several datasets (Sonar, NSL-KDD, UNSW-NB15, HC, GC, LR). Key metrics (Accuracy, Sensitivity, Specificity) were compared to confirm the superiority of the DCA-MLP model. In addition, Receiver Operating Characteristic (ROC) curve analysis was conducted to further highlight the performance robustness of the proposed method.

V. Experimental Results

A. Threshold Sensitivity in the Standard DCA Model

The traditional Dendritic Cell Algorithm (DCA) relies on a predefined threshold during the classification phase. While this threshold allows for the differentiation between normal and anomalous instances, its effectiveness is dataset dependent. Particularly in imbalanced datasets, a static threshold leads to suboptimal performance and reduced sensitivity.

As shown in Table II, reducing anomaly proportion to 10% results in a performance drop of 5% in accuracy. This demonstrates the sensitivity of standard DCA to class distribution, which compromises its generalizability across.

B. Performance of the Proposed DCA-MLP Model

To overcome the above limitations, we propose an enhanced DCA model by integrating a Multi-Layer Perceptron (MLP) classifier, replacing the static threshold with dynamic learning. We evaluated the proposed DCA-MLP on fourteen datasets, comparing its performance with the standard DCA using Accuracy (ACC), Sensitivity (SNS), and Specificity (SPS), alongside statistical significance (p-values).

As shown in Table III, DCA-MLP consistently outperforms the standard DCA across all datasets, with statistically significant improvements ($p < 0.001$) in all key metrics.

C. Comparative Evaluation with Benchmark Literature

To further validate the proposed model, we compared it with recent state-of-the-art DCA extensions and hybrid methods, as shown in Table IV.

TABLE II. Effect of Threshold on Anomaly Detection Accuracy in DCA

Dataset	Total data		Threshold value	Result
WBC	Normal	Anomaly		Accuracy
Original (100% anomaly)	458	241	0.65	0.98
Reduced (10% anomaly)	241	40	0.26	0.93

TABLE III. The Results of Comprehensive Evaluation of Performance Metrics (ACC, SNS & SPS) with Statistical Significance (P-Values) for the Standard DCA and the Proposed DCA-MLP Across Datasets

Datasets	Accuracy (%)				Sensitivity (%)				Specificity (%)			
	DCA	DCA-MLP	Δ	pval	DCA	DCA-MLP	Δ	pval	DCA	DCA-MLP	Δ	pval
Sonar	0.88	0.99	0.11	2.26E-07	0.59	0.98	0.39	0.0004	0.78	0.98	0.2	0.000726
WBC	0.93	0.98	0.05	2.26E-07	0.90	0.98	0.08	0.0004	0.90	0.96	0.06	0.000726
WDBC	0.88	0.94	0.06	2.26E-07	0.39	0.86	0.47	0.0004	0.91	0.99	0.08	0.000726
PID	0.61	0.95	0.34	2.26E-07	0.39	0.87	0.48	0.0004	0.91	0.99	0.08	0.000726
ILPD	0.69	0.92	0.23	2.26E-07	0.57	0.77	0.20	0.0004	0.47	0.98	0.51	0.000726
horse	0.75	0.98	0.23	2.26E-07	0.95	0.99	0.04	0.0004	0.10	0.96	0.86	0.000726
GC	0.75	0.97	0.22	2.26E-07	0.95	0.99	0.04	0.0004	0.27	0.91	0.64	0.000726
win	0.70	0.91	0.21	2.26E-07	0.75	0.91	0.16	0.0004	0.42	0.91	0.49	0.000726
Ionosphere	0.75	0.95	0.20	2.26E-07	0.97	0.98	0.01	0.0004	0.88	0.9	0.02	0.000726
Heart	0.72	0.92	0.20	2.26E-07	0.25	0.85	0.60	0.0004	0.87	0.97	0.10	0.000726
SP	0.88	0.94	0.06	2.26E-07	0.84	0.90	0.15	0.0004	0.90	0.98	0.32	0.000726
LDR	0.67	0.97	0.30	2.26E-07	0.51	0.97	0.46	0.0004	0.79	0.95	0.16	0.000726
UNSW-NB15	0.86	0.98	0.12	2.26E-07	0.86	0.98	0.12	0.0004	0.60	0.99	0.39	0.000726
NSL-KDD	0.75	0.94	0.19	2.26E-07	0.82	0.84	0.02	0.0004	0.78		0.20	0.000726

TABLE IV. RESULT COMPARISON BETWEEN THE PROPOSED MODEL AND STATE-OF-THE-ART APPROACHES

Ref.	Method	Dataset	Results in percentage		
			Acc.	Sen.	Spe.
[5]	GA-DCA	Sonar	83.4	-	64.2
[7]	dDCA	NSL-KDD	93.29	-	88.93
		UNSW-NB15	97.25	-	95.01
[15]	DCA	UNSW-NB15	79.8	-	-
[25]	COID-DCA	HC	87.77	91.66	82.23
		GC	87.90	83.94	89.66
		LR	82.45	80.00	83.78
Proposed Model	MLP_DCA	Sonar	**0.99**	**0.98**	**0.98**
		NSL-KDD	**0.94**	**0.84**	**0.98**
		UNSW-NB15	**0.98**	**0.98**	**0.99**
		HC	**0.98**	**0.99**	**0.96**
		GC	**0.97**	**0.99**	**0.91**

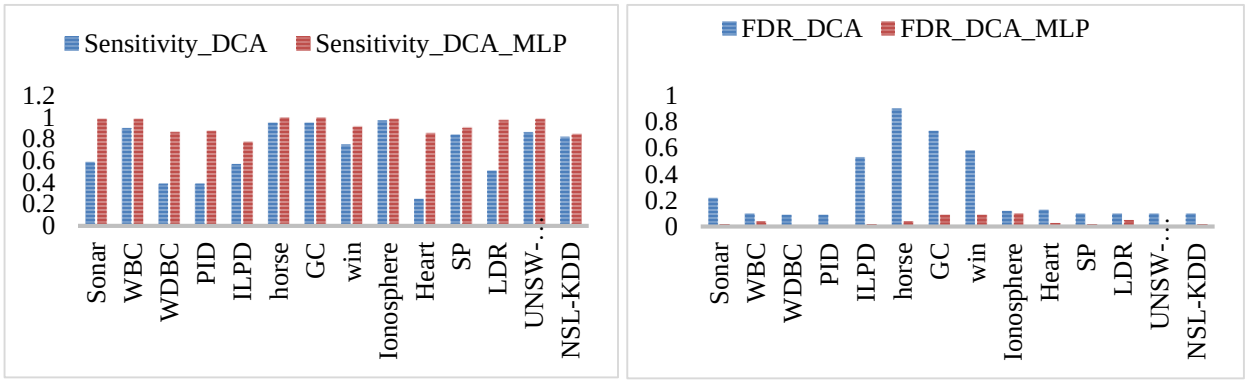
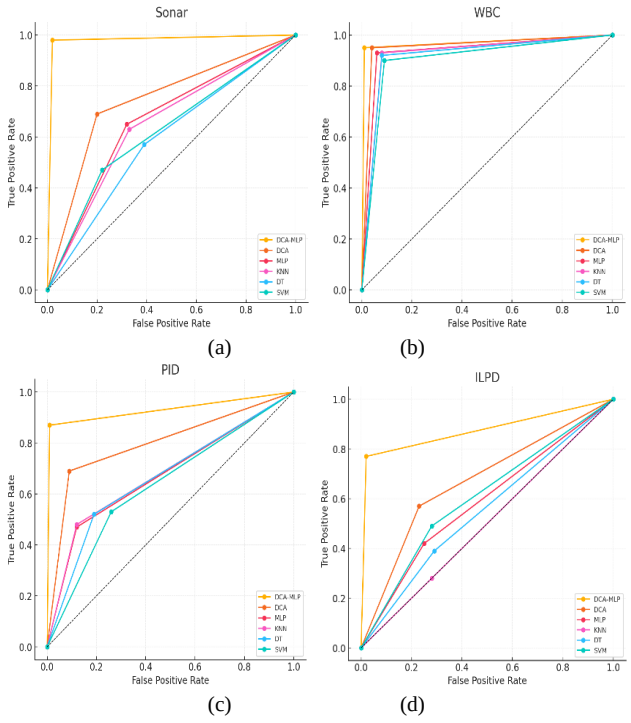


Fig. 4. The range between Sensitivity (SNS) and False Detection Rate (FDR) for DCA-MLP and DCA in benchmark datasets.

As illustrated in Fig. 4**,** the results are summarized in terms of SNS and FDR, which are critical performance metrics for anomaly detection models. The increased distance between the two metrics for the DCA-MLP model demonstrates its improved ability to clearly distinguish between normal and abnormal data groups. This larger gap indicates that the DCA-MLP not only increases the detection of actual anomalies but also appropriately limits false positives, leading to more accurate and dependable classification results. This capability is essential in high-stakes domains like cybersecurity, healthcare, or fraud detection, where accuracy and reducing false alarms are crucial.

Across all fourteen datasets, the proposed MLP-DCA model consistently achieved the highest Area Under the Curve (AUC) values when compared to other DCA variants and traditional classifiers, including stand-alone MLP, K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Decision Tree. As illustrated in Fig. 5, this robust and consistent performance highlights the superior generalization capability of the MLP-DCA model. Furthermore, the statistically significant improvement over both the standard DCA and conventional classifiers underscores the effectiveness of integrating adaptive learning through MLP into the biologically inspired DCA framework.



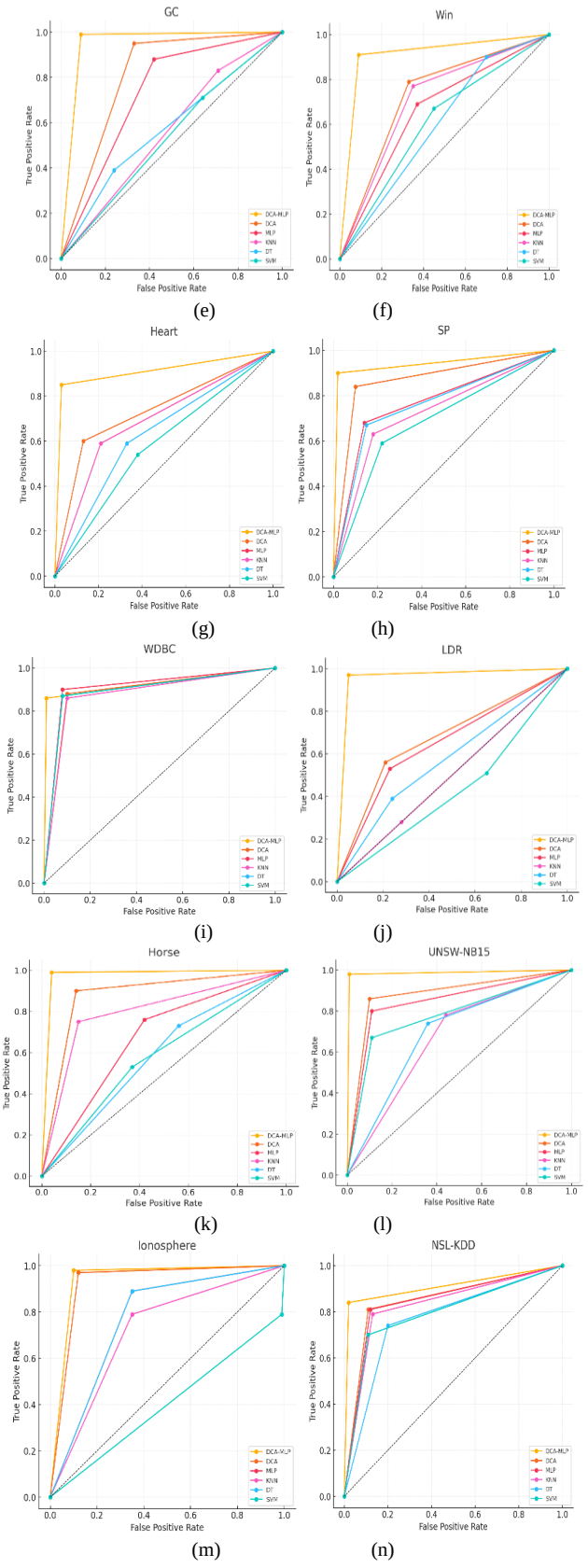


Fig. 5. Illustrates the comparative classification performance of the various DCA expansions and traditional classifiers in terms of ROC analysis across multiple datasets.

VI. Discussion

The experimental results provide ample evidence for the effectiveness and robustness of the proposed DCA-MLP model against the traditional Dendritic Cell Algorithm (DCA) model. One of the major limitations of a standard DCA is that it relies on a fixed threshold value during classification. As the results show, the fixed threshold is very sensitive to dataset specific distributions, especially with class imbalance (which is typically the case with anomaly detection tasks). The static nature of the threshold often results in decreased detection accuracy and increased false negatives when applied to datasets with evolving or uneven data distributions.

Integrating a Multi-Layer Perceptron (MLP) into the DCA framework, the model overcomes this threshold sensitivity and gains the ability to learn and generalize complex decision boundaries. The MLP enables dynamic classification by continuously adjusting to the patterns within the input data. This adaptability significantly improves classification performance across a wide variety of datasets. For example, substantial improvements were observed in both sensitivity and specificity on datasets like Sonar, PID, and NSL-KDD, which are known for their variability and complexity.

Another important aspect highlighted by the results is the consistent superiority of the DCA-MLP model across different domains and data types, including medical (WBC, WDBC), cybersecurity (NSL-KDD, UNSW-NB15), and signal processing (Sonar). This indicates that the proposed hybrid model is not only effective for a single category of data but is also generalizable and robust across diverse anomaly detection scenarios. The model's capacity to handle both structured and unstructured features contributes to its high adaptability and makes it suitable for real-world applications where data distributions are not always known in advance.

Moreover, the comparison with recent state-of-the-art approaches further supports the DCA-MLP model's effectiveness. When evaluated against various DCA variants—such as GA-DCA, COID-DCA, and dDCA—as well as conventional classifiers, the DCA-MLP consistently achieved higher accuracy and demonstrated better sensitivity-specificity trade-offs. These improvements are statistically significant, with p-values well below the 0.01 threshold, indicating that the observed performance gains are not due to random variation but rather a result of the model's enhanced learning capabilities.

The model also shows strong capability in minimizing false positives, a critical factor in anomaly detection systems. The analysis of sensitivity versus false detection rate (FDR), as shown in the experimental figures, illustrates a wider performance gap for the DCA-MLP model. This means it not only detects true anomalies more accurately but also avoids misclassifying normal instances as abnormal, thereby improving the reliability and precision of the system. Such performance is particularly crucial in high-stakes applications such as fraud detection, network intrusion prevention, and medical diagnosis, where incorrect predictions can lead to severe consequences.

VII. Conclusion

This research presents an enhancement of the Dendritic Cell Algorithm (DCA) aimed at improving anomaly detection

performance. The new approach utilizes a Multi-Layer Perceptron (MLP) embedded into the DCA framework, thereby eliminating the threshold-based classification reliant exclusively on the multi context antigen value (MCAV). This innovation solves the fundamental problems of fixed thresholds, which generally perform badly when measured with extreme values and bad from the perspective of typically improving the accuracy of anomaly detection. By leveraging the adaptive learning capabilities of the MLP, the enhanced MLP-DCA model demonstrates increased robustness and adaptability. Experimental results conducted on fourteen benchmark datasets validate that the MLP-DCA model significantly outperforms the conventional DCA, showing notable improvements in sensitivity, specificity, and overall accuracy.

These updates suggest that there is a good reason to believe that combining the strong principles of anomaly detection in the DCA with the extremely capable pattern detection and recognition advantages of the MLP. However, this study also has certain limitations**.** First, while the current model maintains consistent performance across many datasets, its effectiveness will vary when used on large-scale or highly imbalanced real-world data where rare anomalies are often prevalent. Second, the model's performance depends on hyperparameter configurations in both the DCA and MLP components, which may require manual tuning or additional optimization for each dataset. To add, the current model has not yet taken streaming or online data into account so there is no direct application of it towards real-time anomaly detection. As a result, the MLP-DCA model may have significant advantages for complex classification tasks, specifically for anomaly detection, which is characterized by non-linear data distributions or imbalances related to classes. Future research could explore integrating the Dendritic Cell Algorithm with advanced deep learning architectures or reinforcement learning-based decision modules. Hybrid approaches have the capacity to further improve performance on the class of complex datasets, which can be found in time-series anomaly detection, streaming data environments, and image-based pattern identification applications.

REFERENCES

[1] D. Wang, Y. Liang, H. Dong, C. Tan, Z. Xiao, and S. Liu, "Innate immune memory and its application to artificial immune systems," The Journal of Supercomputing, vol. 78, no. 9, pp. 11680-11701, 2022.

[2] J. Greensmith, "The dendritic cell algorithm," Citeseer, 2007.

[3] R. Pinto, G. Gonçalves, J. Delsing, and E. Tovar, "Incremental dendritic cell algorithm for intrusion detection in cyber-physical production systems," in Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3, 2021: Springer, pp. 664-680.

[4] C. A. Winanto, P. Putra, D. P. Rini, O. Arsalan, S. K. Ningrum, and M. Q. Rizqie, "A Comparative Analysis of Snort and Dendritic Cell Algorithm in Intrusion Detection Systems," in 2024 11th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), 2024: IEEE, pp. 282-287.

[5] D. Zhang, Y. Zhang, and Y. Liang, "A genetic algorithm-based dendritic cell algorithm for input signal generation," Applied Intelligence, vol. 53, no. 22, pp. 27571-27588, 2023.

[6] M. F. M. Mohsin, A. A. Bakar, and A. R. Hamdan, "An Adaptive Anomaly Threshold in Artificial Dendrite Cell Algorithm."

[7] D. Limon-Cantu and V. Alarcon-Aquino, "Multiresolution dendritic cell algorithm for network anomaly detection," PeerJ Computer Science, vol. 7, p. e749, 2021.

[8] L. An et al., "Challenges, tasks, and opportunities in modeling agent-based complex systems," Ecological Modelling, vol. 457, p. 109685, 2021.

[9] B. Boudoua, M. Roche, M. Teisseire, and A. Tran, "EpiDCA: Adaptation and implementation of a danger theory algorithm for event-based epidemiological surveillance," Computers and Electronics in Agriculture, vol. 229, p. 109693, 2025.

[10] M. F. M. Mohsin, A. A. Bakar, A. R. Hamdan, and M. H. A. Wahab, "An improved artificial dendrite cell algorithm for abnormal signal detection," Journal of Information and Communication Technology, vol. 17, no. 1, pp. 33-54, 2018.

[11] M. Belhadj, F. Cherif, and M. Cheriet, "NMF-DCA: An efficient dendritic cell algorithm based on non-negative matrix factorization," International Journal of Computing and Digital Systems, vol. 10, pp. 575-583, 2021.

[12] Z. C. Dagdia, "A scalable and distributed dendritic cell algorithm for big data classification," Swarm and Evolutionary Computation, vol. 50, p. 100432, 2019.

[13] M. F. M. Mohsin, A. A. Bakar, A. R. Hamdan, M. Sahani, and Z. M. Ali, "Dengue Outbreak Detection Model Using Artificial Immune System: A Malaysian Case Study," Journal of Information and Communication Technology, vol. 22, no. 3, pp. 399-419, 2023.

[14] C. Pinto, R. Pinto, and G. Gonçalves, "Towards bio-inspired anomaly detection using the cursory dendritic cell algorithm," Algorithms, vol. 15, no. 1, p. 1, 2021.

[15] E. Farzadnia, H. Shirazi, and A. Nowroozi, "A new intrusion detection system using the improved dendritic cell algorithm," The Computer Journal, vol. 64, no. 8, pp. 1193-1214, 2021.

[16] K. Arora and S. Mahajan, "Detecting denial-of-service attack using dendritic cell approach," in Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI 2020, 2021: Springer, pp. 509-516.

[17] N. Elisa, J. Li, Z. Zuo, and L. Yang, "Dendritic cell algorithm with fuzzy inference system for input signal generation," in Advances in Computational Intelligence Systems: Contributions Presented at the 18th UK Workshop on Computational Intelligence, September 5-7, 2018, Nottingham, UK, 2019: Springer, pp. 203-214.

[18] N. Elisa, L. Yang, F. Chao, N. Naik, and T. Boongoen, "A secure and privacy-preserving e-government framework using blockchain and artificial immunity," IEEE Access, vol. 11, pp. 8773-8789, 2023.

[19] M. F. M. Mohsin, A. A. Bakar, and A. R. Hamdan, "Integration of the dendritic cell algorithm with K-means clustering," Int. J. Adv. Soft Compu. Appl, vol. 6, no. 3, 2014.

[20] J. Deng, D. Wang, J. Gu, C. Chen, and C. Xie, "NK-DCHS: An Adaptive Hybrid Immune Model for Imbalanced Anomaly Detection," Expert Systems with Applications, p. 128704, 2025.

[21] A. Frank and A. Asuncion, "UCI machine learning repository, url= http://archive. ics. uci. edu/ml," Accessed: June, vol. 59, pp. 80-85, 2013.

[22] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in 2009 IEEE symposium on computational intelligence for security and defense applications, 2009: Ieee, pp. 1-6.

[23] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in 2015 military communications and information systems conference (MilCIS), 2015: IEEE, pp. 1-6.

[24] F. Gu, J. Greensmith, R. Oates, and U. Aickelin, "Pca 4 dca: The application of principal component analysis to the dendritic cell algorithm," arXiv preprint arXiv:1004.3460, 2010.

[25] Z. Chelly Dagdia and Z. Elouedi, "A hybrid fuzzy maintained classification method based on dendritic cells," Journal of Classification, vol. 37, no. 1, pp. 18-41, 2020.