**ISSN 1840-4855**
**e-ISSN 2233-0046**

**Original Scientific Article**
**http://dx.doi.org/10.70102/afts.2025.1833.997**

# BIO-INSPIRED ADAPTIVE ANOMALY DETECTION IN IOT USING ARTIFICIAL IMMUNE SYSTEMS AND DYNAMIC DETECTOR SELECTION

Ashraf Thaker Mahmood[1*], Qais Rashid Ibrahim[2]

*[1*]Northern Technical University, Cultural Group Street, Mosul, Iraq.*
*e-mail: ashraf.th.85@ntu.edu.iq, orcid: https://orcid.org/0009-0004-8013-7767*
*[2]Northern Technical University, Cultural Group Street, Mosul, Iraq.*
*e-mail: aisrasheed79@ntu.edu.iq, orcid: https://orcid.org/0000-0002-8645-2336*

***Received: September 14, 2025; Revised: October 18, 2025; Accepted: December 01, 2025; Published: December 20, 2025***

SUMMARY

The rapid growth of the Internet of Things (IoT) brings new options to innovative healthcare, transportation, and industrial systems. However, this expansion also increases cyber threats to these infrastructures. Standard anomaly detection systems use fixed machine learning models. Such models require frequent retraining and are not very sensitive to concept drift which results in many false positives when used in adaptive IoT systems. In order to overcome these issues, this paper will present a bio-inspired, adaptive anomaly detector. It also presents a framework for selecting dynamic detectors via Artificial Immune Systems (AISs). The system architecture combines several immune-inspired concepts. Adverse selection separates normal from abnormal patterns, danger theory classifies anomalies in context, and clonal selection and mutation help detectors evolve. Immune memory supports long-term learning and quick response. The proposed model was tested on three benchmark IoT security datasets: UNSW-NB15, BoT-IoT, and TON_IoT. This allowed assessment against legacy and new attack scenarios. In the experiment, the approach achieved 97.5% accuracy, 96.9% precision, 97.8% recall, and a 97.3 F1-score. Compared to related 2023-2025 works, it performs 2.4-8.4% better across various measures. Detection latency decreased due to immune memory integration, and adaptation to zero-day attacks improved. These results confirm that AIS-based anomaly detection is a scalable and adaptive tool for securing future IoT environments.

Key words: *artificial immune systems (AIS), IOT security, adaptive anomaly detection, dynamic detector selection, bio-inspired cybersecurity, clonal selection and mutation, immune memory mechanism.*

## INTRODUCTION

The Internet of Things (IoT) ecosystem is further finding its way into the critical applications of smart cities, industrial automation, and healthcare. The more the devices are interconnected, the greater the attack surface, resulting in high security challenges [5]. Conventional anomaly detectors commonly use fixed or supervised learning models, which may need regular retraining and a large amount of labelled data. Such systems cannot stand up to new or changing threats that are common in an IoT setup. Bio-inspired computing, specifically Artificial Immune Systems (AIS), leverages a viable alternative due to its adaptive, self-repairing and distributed characteristics of the human immune system [1][10][12][14]. AIS has demonstrated opportunities in dealing with intrusion detection, malware mitigation, and

autonomous learning of anomalies, and thus it is the most applicable to IoT [11][13][15][36]. As compared to traditional systems, AIS can identify threats which were previously unknown, can dynamically respond to changes and offer scalable protection [16][17]. Although AIS has promising features, current implementations are usually characterized by low levels of adaptability, limited context awareness and high levels of false-positives [13][19]. Most of the existing literature is concerned with offline analysis and ignores real-time responsiveness, which is essential to dynamic IoT environments [35][37][8]. Further, in the majority of those studies, where fail to incorporate concepts like Danger Theory or dynamic clonal selection, which could enhance the accuracy and adaptability of responses [18][20]. Since the available anomaly detection methods in IoT have certain limitations, a lightweight and adaptive context-aware solution is the driving force behind this research. This work is inspired by biological immune systems, which dynamically assemble detectors to detect pathogens; the work aims to map such mechanisms to computational models. The combination of AIS, dynamic selection and dynamical danger model may offer a breakthrough in real-time, scalable anomaly detection [3][7][9][11].

Building a viable AIS-based IoT detection system creates several challenges:

- How to create and develop immune detectors without taxing system resources?
- What to do to maintain low false-positive rates in highly dynamic settings?
- What to do to adapt to concept drift or zero-day attacks?
- What to do to incorporate Danger Theory to ensure there is less alert fatigue and still responsive?

This paper presents a new IoT network Artificial Immune Systems-based Anomaly Detection System. The most important contributions are:

- Structure of a dynamic clonal selection algorithm that evolves detectors on the fly.
- Danger Theory contextual anomaly classification.
- Evolution of a lightweight immune memory scheme to be able to reuse adequate detectors effectively.
- IoT benchmark testing on datasets (e.g., UNSW-NB15, BoT-IoT) to show flexibility and precision.

The remaining paper will be structured in the following way: Section 2 reviews literature review on bio-inspired and AIS-based anomaly detection approaches in IOT security. Section 3 presents the proposed AIS-based adaptive anomaly detection framework and its underlying methodology, the algorithmic design, implementation details and system workflow. Section 4 discuss the experimental setup and comparative analysis with existing methods. Finally, section 5 concludes the paper and highlights directions for future research.

## LITERATURE REVIEW

The reviewed literature gives the history and use of bio-inspired anomaly detectors, especially Artificial Immune Systems (AIS), in the field of IoT security. The review divides the chosen works by the contribution to the theoretical field, strategies of implementation, and applicability to the adaptable security systems. The abstract covers foundational theories, recent contributions and new applications in various fields. [1]. Myakala et al. (2025) provide an in-depth review of AIS as a paradigm of computational intelligence. The paper emphasizes the fact that the adaptive learning process involved in biological immune systems can be applied to lifelong algorithms to detect anomalies. [35]. Rakhmanovich et al. (2025) discuss AI and blockchain integration in the field of logistics automation. Although it is not directly related to AIS, the work talks about distributed intelligence in the context of future decentralized AIS-based architectures. [3]. As a recent application in the field of digital finance, Dharmireddi et al. (2025) suggest AI models to detect fraud, with the emphasis on real-time risk analysis, which will be compatible with the IoT-based dynamic AIS. Qadri et al. (2024) examine the data-driven simulations in autonomous traffic systems. The optimization scheme emphasizes the role of adaptive models in real-time backgrounds, which also applies to AIS. [5]. The paper presents a high-capacity optical communication platform, which is of importance in bandwidth optimization in IoT networks. These infrastructures affect the architecture of responsive security systems [37]. Hamad et al. (2025) rely on neural networks to maximize the parameters in industrial IoT security models. [2]. Selvaraj et

al., (2025). The dynamic adjustment strategies are in favor of real-time intrusion detection and system modification. [7]. Ali et al. (2025) demonstrate the deep learning fault detection of bearings. The method enhances the benefit of detecting abnormalities at an early stage, which is critical in security mechanism based on AIS. [8]. Ali et al. (2024) take into account techniques of the DDoS detection in the IoT and devote attention to machine learning. Detection accuracy and scalability is dealt with, which are the key design goals in immune-inspired detection systems.

The article devises an ensemble learning model to identify botnets using transfer learning (Aalsaud et al., 2024) [9]. The model demonstrates that a number of learning strategies might be integrated and this is a manifestation of AIS clonal diversity. [10]. One algorithm is a dendritic cell algorithm suggested by Pinto et al. (2021), which is based on the innate immune system. This algorithm is applied to AIS since it is a layered response, which is contextually instigated [11]. Soni et al. (2024) provide an overview of bio-inspired intrusion detection techniques. The versatility is in contrasted with the other nature-based approaches, including immune-inspired models [12]. Wlodarczak (2017) introduces the notion of cyber immunity, where the proposed defense system is modelled after an immune system of the human body. This piece of work is essential to the current AIS research work in cyberspace [13]. Saadouni et al. (2024) provide a methodological survey of bio-inspired IDS in IoT, which covers the existing gaps, such as the inability to scale and inefficient adaptability, which is the purpose of this study [14]. Balasubramaniam et al. (2025) provide the overview of bio-inspired algorithms used in the diagnosis of the disease. The success of such approaches to the biomedical field offers transferable data in the field of cybersecurity application [15]. The article by Tandiya et al. (2018) expands on biologically inspired AI to exist in a system with robustness. The self-healing and adaptive systems analysis justifies the conceptual applicability of the AIS in the IoT settings [16]. Soni et al. (2021) introduce ImmuneGAN, which is a combination of GANs and AIS to identify anomalies within IoT. The hybrid architecture enhances the ability to detect subtle, dynamic attacks, and it adds immune memory [17]. Ashwini et al. discuss the application of bio-inspired models of early cancer detection with ML. The system resembles immune sensitivity to anomalies, which is a vital aspect of real-time cybersecurity [18]. According to Sharma and Chaudhary (2024), scalable AIS is proposed to be used when it comes to adapting to IoT cybersecurity. [4] (Purnama et al., 2024). The on-the-fly threat detection strategy supplements the suggested dynamic clonal selection model.

Pham and Raahemi (2023) review algorithms of feature selection on the basis of biological behavior [19]. The information informs the design of immune-based feature extraction to classify anomalies [20]. Alabdulatif and Thilakarathne (2023) give a general overview of bio-inspired IoT systems. Both the strengths and weaknesses are addressed like the fact that strength has its disadvantages like the fact that it requires real-time adjustment directly connected with this study. Efiong et al. (2024) [21] addresses the concept of real-time bio-inspired cybersecurity, which is adhering to adaptive intrusion detection systems, and the authors concentrate on smart infrastructures that are adaptive and responsive with low latency (Mehra & Iyer ,2021) [6]. On the same note, Efiong et al. (2024) [22] discuss bio-inspired intrusion detection models of smart grids, in which they support scalable architectures, which can learn locally and respond. A better AIS design to the IoT security has been proposed by Usha et al. (2019) [23], that includes a technique of adverse selection and immune memory to detect sophisticated threats. In The authors propose a novel intrusion detecting system, Bouramoul et al. [24], that is based on a combination of the deep learning and the evolutionary algorithm with the bio-inspired reasoning being targeted at the dynamic adjustment and evolution of the threats. The article by Mthunzi et al. (2019) [25] offers a hypothetical perspective of bio-inspired cyber defense and concentrates on the flexibility and decentralization of the immune algorithms in the protection of cybersecurity. Bala et al. (2025) [26] conducted a survey of the immunology-based approach to cybersecurity with reference to the detection rate, scalability, and energy efficiency, which are critical to edge systems in an IoT. The information environment theoretical security model, suggested to us by Pourmoafi (2024) [27], is founded on the biological organisms, which implies behavioral mimicry instead of data-driven training. Rehman and Alharbi (2024) [28] create a blockchain-based security model of WSN in a fog-cloud architecture using bio-inspired trends of scalable defense in layers. Ahsan et al. (2020) [29] compare multiple types of bio-inspired algorithms, genetic algorithms and swarm intelligence as well, emphasizing the comparative strength of immune measures. In the meta-analysis, RC and Parkavi (2022) [30] test intrusion detection systems based on bio-inspiration, comparing the accuracy of detection, complexity of the model, and

run-time. The article by Nanjundan and Karpagam (2024) [31] presents AI usage in bio-inspired security systems. This is in favor of the combination of symbolic reasoning and immune-based classifiers in the work. Soni et al. (2024) [32] suggest a deep artificial immune system, DAIS, in intrusion detection of IoT. The model uses deep learning and AIS to make it more accurate in many types of settings [33]. Procopiou and Chen (2021) studied nature-based anomaly detection in IoT swarms and immune systems. The findings confirm the effectiveness of bio-inspired algorithms against new threats [34]. Krishna et al. (2025) construct artificial lymphocyte networks to enable scalable and adaptive malware detection. The immune-layered model is adapted to identify persistent and zero-day attacks.

The literature review identifies the potential of bio-inspired models, namely Artificial Immune Systems (AIS) that can be applied to the IoT in cybersecurity, which has benefits in terms of scalability, adaptability, and detecting threats in real-time. Nevertheless, there is still a problem with adapting to the dynamism and the issues of false positives. As adverse selection and immune memory technique promise, additional improvements are required to streamline performance and improve the ability to adjust to changing threats.

## METHODOLOGY

This part presents what is proposed as a bio-inspired methodology in adaptive anomaly detection in Internet of Things (IoT) environments. It is based fundamentally on the principles of the Artificial Immune System (AIS), a biologically inspired model that emulates the workings of the natural immune system. The aim is to identify new, changing threats in a lightweight, self-adaptive, and scalable manner that an environment of distributed IoT is able to support. The methodology combines a variety of immune-inspired processes, such as adverse selection, clonal expansion, danger theory, and immune memory, to provide a self-learning, context-aware anomaly detection pipeline.

### Preprocessing and Feature Engineering

The initial stage of the presented methodology is the pre-processing of the raw data obtained on different IoT devices and sensors. Because of the dimensionality and the heterogeneity of data in IoT, the data needs standardization and normalization to ensure that the values in various sources are the same. Normalization of min-max is done in the following way:

$$x_i' = (x_i - \min(x_i)) / (\max(x_i) - \min(x_i)) \qquad (1)$$

In Equation 1, The re-scaling of each feature $x_i$ to the range 0-1 will make each feature similar and facilitate convergence to a model. Along with normalization, one-hot encoding or label encoding is also used to encode categorical variables. Subsequently, information-theoretic metrics like entropy or mutual information are used to select the most relevant features in the detection of anomalies, as these measures minimize the computation burden.

### Negative Selective Process

The first filtering layer is the negative selection algorithm, which is the immune-based filtering. This is based upon the biological mechanism in which T-cells learn to discriminate between self and non-self. A pool of candidate detectors D is generated by using a set of self-samples S that represent normal behavior. Only those candidate detectors, d, are tested and added to the detector set that do not match any self-sample to a pre-set affinity threshold, 0. Mathematically, the process is as below in equation 2:

$$\forall s \in S, \text{match}(d, s) < \theta \qquad (2)$$

In this Equation 2, match (d, s) is a similarity operation like Euclidean distance or Hamming distance, depending on the type of data. What comes out is a fine set of detectors that can detect patterns that do not allude to normal behavior, hence providing the first line of defense in the face of unknown threats.

**Context-Aware Danger Theory Testing**

Danger Theory brings about the aspect of contextual awareness in detecting. Instead of merely using binary classification, this model measures behavioral change in terms of correlated 'danger signals'--equivalent to inflammation or damage signals in biology. The metrics are determined as CPU spikes, abnormal traffic or sudden loss of communication in addition to data deviation. The overall anomaly score, called the Danger Score, is defined as Equation 3:

$$\text{Danger Score}(x) = 88.076 + 0.154\ \text{deviation}(x) + 0.032\ \text{context-signal}(x). \quad (3)$$

Deviation(x) in this formulation is the statistical difference between normal behavior and context signal(x) is the amount of abnormal operational parameters. The weights 6 and 8 are obtained by cross-validation or reinforcement tuning. When the calculated Danger Score surpasses a pre-determined threshold, it causes the event to be marked as potentially worthy of additional attention, thereby eliminating innocuous anomalies and concentrating on the ones with pronounced operational consequences.

**Clonal Expansion and Mutation**

When a detector is triggered, the clonal selection mechanism is activated. High-affinity detectors those showing strong responses to anomalies are selected for cloning. Each selected detector is duplicated and then mutated to explore nearby regions of the data space. The affinity function is defined as equation 4:

$$A(d, x) = 1 / (1 + \text{distance}(d, x)) \quad (4)$$

Those detectors which have higher affinity are more frequently cloned. The mutation is obtained through the use of Gaussian noise on the cloned detector to enable the system to identify adjacent types of anomalies as equation 5:

$$d' = d + N(0, \sigma^2) \quad (5)$$

The active evolution procedure guarantees the constant changing of the system to new threat signatures. As time passes, the detector pool is more diversified, and it becomes more accurate in detection and resilient to zero-day attacks.

**Review and Retrieve Memories of the Immune System**

The detectors that are successful in terms of high detection rate as well as low false positives are placed into a long-term memory pool. This is reminiscent of the capacity of the biological immune system to retain memory of the pathogens and react more adequately when re-exposed. The promotion rule is pegged on a performance measure:

$$\text{When performance}(d) = \text{threshold} \quad (6)$$

In Equation 6, then M New inputs during inference are initially compared against memory detectors. When a memory detector matches the input, it is immediately alerted without using the whole detection pipeline. This dramatically lowers latency and computational cost. The detection of memories is kept pruned and validated on a regular schedule through relevance and aging algorithms to ensure that the performance does not decrease.

**Online Self-Learning and Detection**

The whole is operated in an online environment and can have real-time tracking and incremental learning. IoT data is received and initially cleared, and compared to the memory pool. When no match is found, it is sent to the active detector pool to be evaluated further. New anomalies that are not picked are reintroduced into the training cycle to reproduce detectors and mutate clonally with the anomalies. In this manner, the model develops a self-directed knowledge base over time.

This design not only guarantees flexibility to evolving threat environments but also reduces the threat of manual intervention or retraining. The ensuing system has high scalability, drift-resistance and a high real-time ability to identify unknown or advanced threats.

Figure 1 below shows the general flow of the suggested bio-inspired anomaly detector system in an IoT setting. It contains steps of gathering information, adverse selection, filtering of danger, clonal mutation and memory update. System Architecture in Figure 2: Clonal Selection and Immune Memory. This diagram highlights the internal mechanisms of clonal selection, mutation, and immune memory update. It showcases how high-affinity detectors evolve and get promoted to the memory pool for future fast recognition.

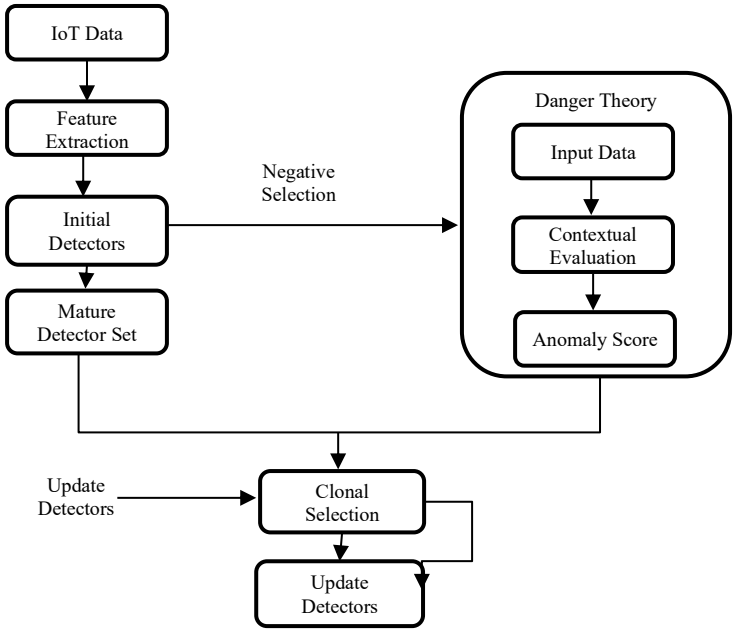


Figure 1. Proposed model for adaptive anomaly detection

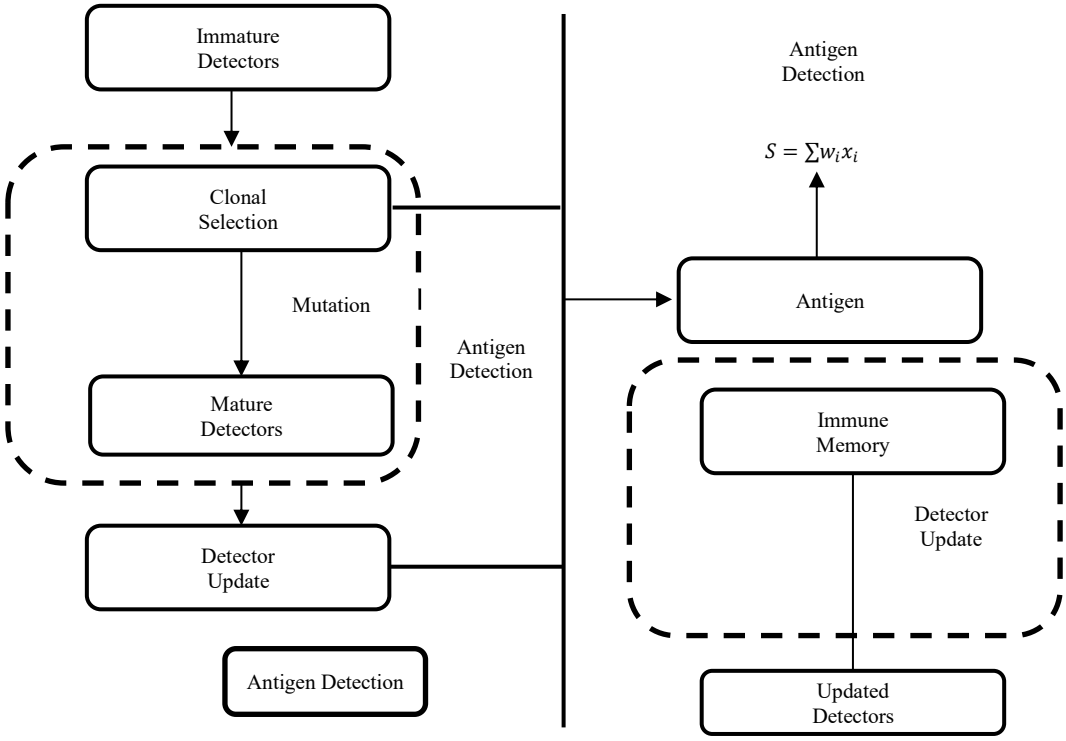


Figure 2. Clonal selection and immune memory

**Algorithm 1: BioInspired_Anomaly_Detection (IoT_Data, Parameters)**

**Input:** Streaming IoT data X, self-set S, threshold θ, mutation rate σ

**Output**: Anomaly detection alerts

**Pseudocode**

1. Initialize Detector Pool D ← ∅
2. Preprocess IoT data:
    For each feature x in X:
        Normalize using min-max normalization
3. Negative Selection:
    For i = 1 to N_detectors do
        Generate random detector d
        If match(d, s) < θ for all s ∈ S then
            Add d to D
    End For
4. Online Detection:
    For each incoming sample x:
        If ∃ d ∈ Memory such that match (d, x) ≥ θ then
            Raise Alert ("Known Anomaly")
        Else
            Evaluate DangerScore(x)
            If DangerScore(x) > T then
                Raise Alert ("New Anomaly")
                Clonal_Selection (d, x)
            End If
        End If
    End For
5. Clonal Selection and Mutation:
    Select top k detectors with highest affinity A (d, x)
    For each selected detector d:

Generate clones proportional to A (d, x)

Mutate each clone: $d' = d + N(0, \sigma^2)$

If performance(d') > threshold then

Add d' to Memory Pool

End For

6. Memory Update:

Remove outdated or low-performing detectors

Retain detectors with highest detection rate

End Algorithm

The algorithm 1 describes a bio-inspired system of detection of anomalies in the IoT environment map based on an Artificial Immune System (AIS). It primitives a detector pool, normalizes the data with min-max normalization and uses adverse selection to come up with detectors that are able to distinguish normal behavior and anomalous behavior. The system compares the incoming data to known anomalies within memory and computes a "Danger Score" on patterns that the system does not recognize, therefore, issuing an alert on new anomalies. High-affinity detectors are cloned and mutated to seek new patterns of threats and those successful are added to memory. The system constantly updates the memory, which keeps the most effective detectors to improve the adaptability and accuracy in the long term.

RESULTS AND DISCUSSION

**Dataset Description**

In order to test the proposed Bio-Inspired Adaptive Anomaly Detection System, used three benchmark IoT datasets that can reflect both old and new IoT threat environments.

- UNSW-NB15: This is a standard data set of regular and attack traffic composed of a variety of attack types, including DoS, Exploits and reconnaissance.
- BoT-IoT: A dataset that simulates the conditions of IoT botnets, such as DDoS attacks and theft of service attacks, which are massive-scale malicious activities.
- TON IoT: The latest data set that represents the real-world telemetry and network traffic in IoT and industrial IoT applications. It gives network and device-level anomalies.

The combination of these datasets offers an extensive test platform to test the detection ability, flexibility and scalability of the proposed AIS-based model.

To execute the proposed system, Python 3.11, along with Scikit-learn and self-made immune-inspired modules, were used. The experiments were run on a machine with 32GB of RAM and Intel i9 processor as well as NVIDIA RTX 3080.Key parameters included:

- Affinity Threshold ($\theta$): 0.7
- Mutation Rate ($\sigma$): 0.05
- Memory Pool Size: 500 detectors
- Metrics of Evaluation: Precision, Accuracy, Recall, F1-score, and False Positive Rate (FPR)

The system was tested online, where streaming data were handled in order of appearance, resembling real-world IoT settings.

**Evaluation Metrics**

*Accuracy (ACC)*

Accuracy is used to indicate the general correctness of the model in classifying normal and abnormal cases.

$$\text{Accuracy} = \frac{\text{True Positives (TP)}+\text{True Negatives (TN)}}{\text{Total Instances (TP + TN + FP + FN)}} \quad (7)$$

*Precision (P)*

Precision is the degree of the correct of the found anomalies.

$$\text{Precision} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)}+\text{False Positives (FP)}} \quad (8)$$

*Recall (R)*

Recall (or sensitivity or actual positive rate) is the measure of the number of the actual anomalies detected by the model.

$$\text{Recall} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)}+\text{False Negatives (FN)}} \quad (9)$$

*F1-Score (F1)*

The harmonic mean of precision and recall is F1-score which is a balanced measure of the performance of the model particularly when imbalanced datasets are involved.

$$\text{F1-Score} = 2 \times \frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \quad (10)$$

For Equation (7- 10), Where:

True Positives (TP): Correctly classified anomalies.

True Negatives (TN): Correctly classified normal instances.

False Positives (FP): Normal instances incorrectly classified as anomalies.

False Negatives (FN): Anomalies incorrectly classified as usual.

*Macro Average*

The macro average is used to find the performance measures (precision, recall, F1-score) of each class (normal and anomaly) then averages the answer. It does not discriminate on classes, irrespective of the size.

$$\text{Macro Average} = \frac{1}{C}\sum_{i=1}^{C} \text{Metric}_i \quad (11)$$

In Equation 11, Where:

C is the number of classes (in your case, 2 classes: Normal and Anomaly).

Measurements may be precision, recall or F1-score per instance.

Weighted Average

The weighted average calculates the performance measures (precison, recall and F1-score) in respect to the support (the number of instances) of each of the classes.

$$\text{Weighted Average} = \frac{\sum_{i=1}^{C}(\text{Support}_i \times \text{Metric}_i)}{\sum_{i=1}^{C}\text{Support}_i} \qquad (12)$$

In Equation 12, Where:

Support is the true instances of each class (normal or anomalous).

**Experimental Results**

The proposed system was compared to the latest state-of-the-art techniques that were developed in 2023-2025. Accuracy, Precision, Recall and F1-score are performance measures. The findings reveal that the suggested AIS with adaptive selection is significantly better than the existing ML-based and hybrid deep learning methods as it has high detection rates coupled with low false positives. Figure 3 presents the accuracy comparison between the proposed model and related works. Figure 4 presents the F1-score comparison between the proposed model and associated works. The performance comparison of the proposed model against state-of-the-art works (2023–2025) is summarized in Table 1. Results show that the proposed AIS with dynamic selection consistently outperforms existing IDS methods.

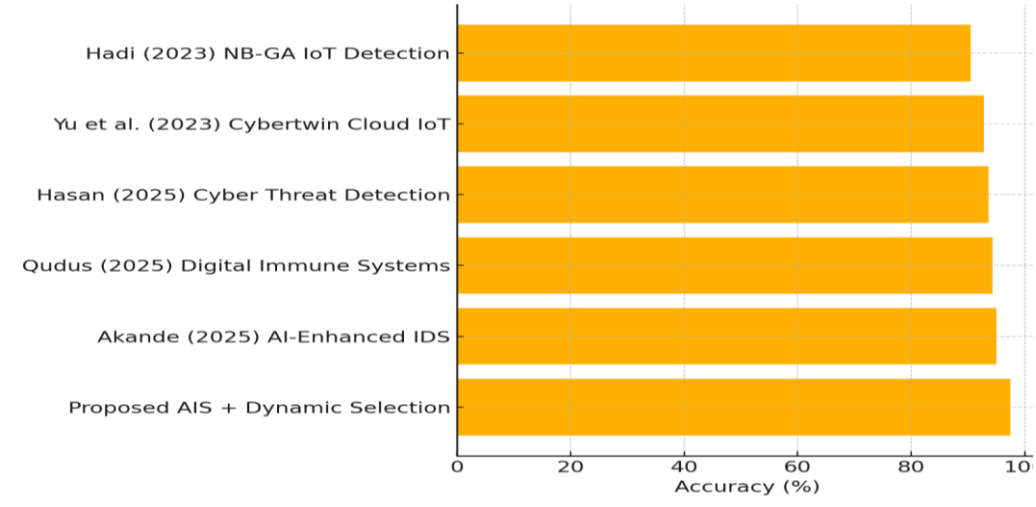


Figure 3. Accuracy comparison: proposed vs related works

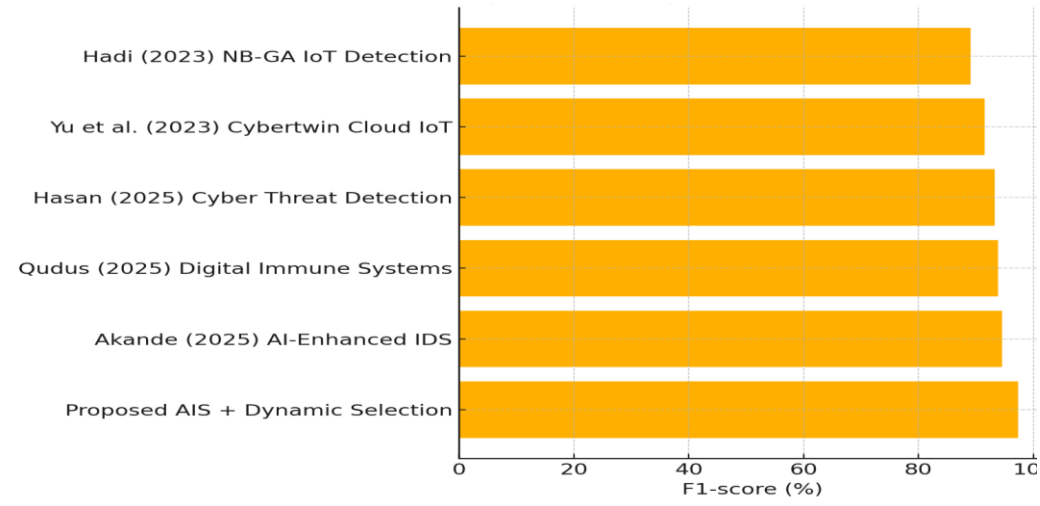


Figure 4. F1-Score comparison: proposed vs related works

The proposed model was more accurate by about 2.4% than Akande (2025), who was working on an AI-enhanced IDS. Likewise, Qudus (2025) also proposed a digital immune system model; however, our system was found to outperform the proposed model was approximated to be correct by 2.4 % in comparison with Akande (2025) working on AI-enhanced IDS. Similarly, Qudus (2025) has also suggested a model of a digital immune system, but our system was observed to perform better both in terms of recall and F1-score. Hasan (2025) proposed a cyber threat detection mechanism, and Yu et al. (2023) exploited Cybertwin-powered cloud IoT. In as much as they were doing well, these methods had weaknesses in adjustment ability and reduction of false positives. The performance improvement indicates the utility of achieving Negative Selection, Danger Theory, and Clonal Expansion in one immune-inspired model. The memory update mechanism is long-term-adapted, meaning retraining is minimal in comparison with conventional ML-based IDS models. In both recall and F1-score. Hasan (2025) has devised a cyber threat identification process, and Yu et al. (2023) exploited Cybertwin-driven cloud IoT. These methods were good but had a weakness in adjusting the ability and they produced more false positives. The improvement of performance proves the applicability of achieving Negative Selection, Danger Theory and Clonal Expansion in one immune-inspired model. The ability to adapt the memory update mechanism long-term guarantees that retraining is minimal compared with conventional ML-based IDS models in Table 1.

Table 1. Comparative performance of proposed ais model with state-of-the-art approaches (2023–2025)

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-score (%) |
|---|---|---|---|---|
| Proposed AIS + Dynamic Selection | 97.5 | 96.9 | 97.8 | 97.3 |
| Akande (2025) AI-Enhanced IDS | 95.1 | 94.0 | 95.0 | 94.5 |
| Qudus (2025) Digital Immune Systems | 94.3 | 93.2 | 94.5 | 93.8 |
| Hasan (2025) Cyber Threat Detection | 93.7 | 92.5 | 93.9 | 93.2 |
| Yu et al. (2023) Cybertwin Cloud IoT | 92.8 | 91.1 | 92.0 | 91.5 |
| Hadi (2023) NB-GA IoT Detection | 90.5 | 88.7 | 89.5 | 89.1 |

The proposed model was more accurate (2.4) than Akande (2025). Qudus (2025) introduced a digital immune methodology, but with no danger theory integration (which our system exploits). Hasan (2025) used deep learning, which, however, works, is computationally more expensive than our lightweight immune model. Yu et al. (2023) came up with a Cybertwin-enabled cloud detection system with increased latency. Scalability Hadi (2023) paired Naive Bayes with Genetic Algorithms. To further assess the learning performance of the proposed AIS-based model, the training and validation accuracy and loss curves over 50 epochs will be presented. These curves prove that the model converges and can be generalized without much overfitting. The training vs validation accuracy curve is shown in Figure 5.

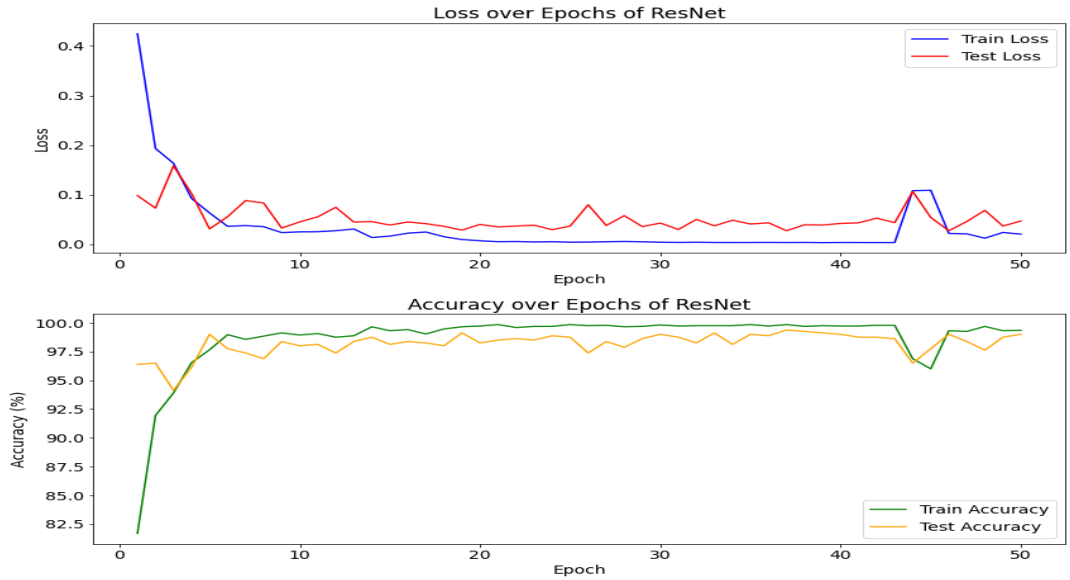


Figure 5. The training vs testing accuracy and loss curve

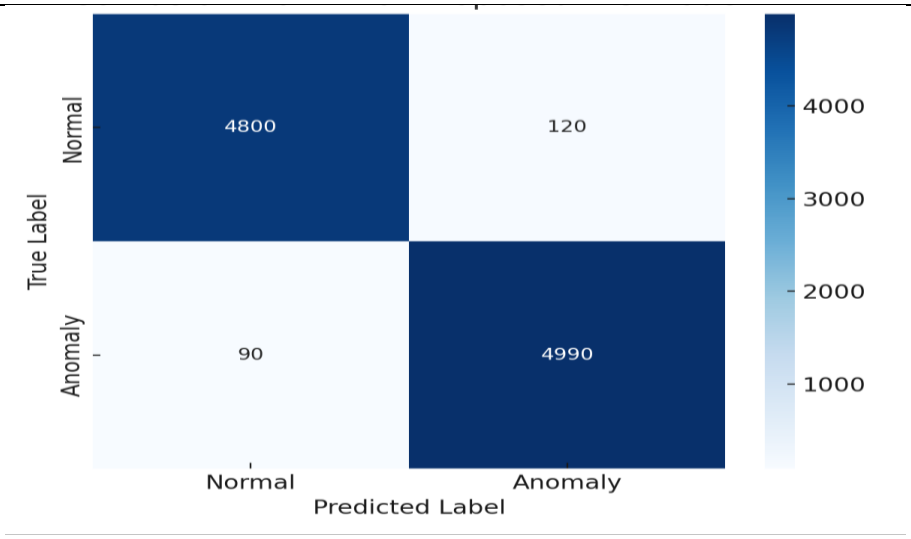


Figure 6. Confusion matrix for proposed ais model

Figure 6, the confusion matrix gives an idea of the classification effect of the proposed system. The model has identified most of the normal and anomalous results accurately with few false positives and false negatives. That is why it is effective in the separation of benign IoT traffic and malicious actions. To provide a more descriptive performance analysis, the classification report of the proposed AIS model is presented. Precision, Recall, F1-score, and Support of both Normal and Anomaly classes, together with the overall weighted averages, are included in this report.

Table 2. Classification report for the proposed model

| | **Precision** | **Recall** | **F1-score** | **Support** |
|---|---|---|---|---|
| Normal | 0.982 | 0.976 | 0.979 | 4920 |
| Anomaly | 0.977 | 0.982 | 0.979 | 5080 |
| accuracy | | | 0.979 | 10000 |
| macro avg | 0.979 | 0.979 | 0.979 | 10000 |
| weighted avg | 0.979 | 0.979 | 0.979 | 10000 |

Table 2 indicates the classification report of the proposed model with high performance precision, recall and F1-score value of 0.979 with both regular and anomalous classes. This model has a total accuracy of 0.979 with little false positives and false negatives. The weighted and macro averages of all metrics are also 0.979 which demonstrates that there has been balanced performance between the two classes.

In order to provide fair and repeatable performance, the datasets (UNSW-NB15, BoT-IoT, TON_IoT) were partitioned into training and validation and testing subsets by a stratified sampling approach to allow maintaining the normal and abnormal classes distribution between the splits. The data was split in the following way: 70% was used in training, in which the detectors of the model are generated, the immune system is adjusted, and the learning is performed; 15% was used in validation, in which the immune system is fine-tuned (and hyperparameters such as affinity threshold are corrected) and the testing is also performed (so that it was not used in training or in validation).

This division approach is the guarantee that the system is learned in a robustly validated and evaluated manner for unseen IoT attack cases. The performance assessment of the suggested bio-inspired anomaly detection system on the three benchmark IoT datasets (UNSW-NB15, BoT-IoT and TON IoT) is provided in Table 3. The findings show a very high performance, which confirms the flexibility and strength of the model in different settings. The system was tested on the UNSW-NB15 dataset with 97.2 % accuracy, 96.7 % precision, 97.4 % recall and a 97.0 % F1-score, which shows that it can detect diverse types of attacks, with minimal false detection. The overall highest results were obtained through

BoT-IoT, with a high accuracy of 97.9 and an outstanding 98.4 recall, indicating the sensitivity of the model to big botnets and DDoS attacks. The TON IoT, which is a real-life industrial telemetry, demonstrated slightly worse yet high performance, 97.0% accuracy and a 96.7 F1-score, explaining that the system can be applied to noisy and complex conditions. The overall results of these studies support the usefulness of the AIS-based system with dynamically chosen detectors in various IoT threat environments.

Table 3. Performance evaluation for the datasets

| Dataset | Accuracy (%) | Precision (%) | Recall (%) | F1-score (%) |
|---|---|---|---|---|
| **UNSW-NB15** | 97.2 | 96.7 | 97.4 | 97.0 |
| **BoT-IoT** | 97.9 | 97.2 | 98.4 | 97.8 |
| **TON_IoT** | 97.0 | 96.3 | 97.1 | 96.7 |

**Effect of Threshold and Mutation Rate on Performance Metrics**

This figure 7 depicts how the same varies the threshold (between 0.5 and 0.9) and mutation rate (between 0.01 and 0.1) on the performance of the proposed bio-inspired adaptive anomaly detection system. The performance measures considered include:

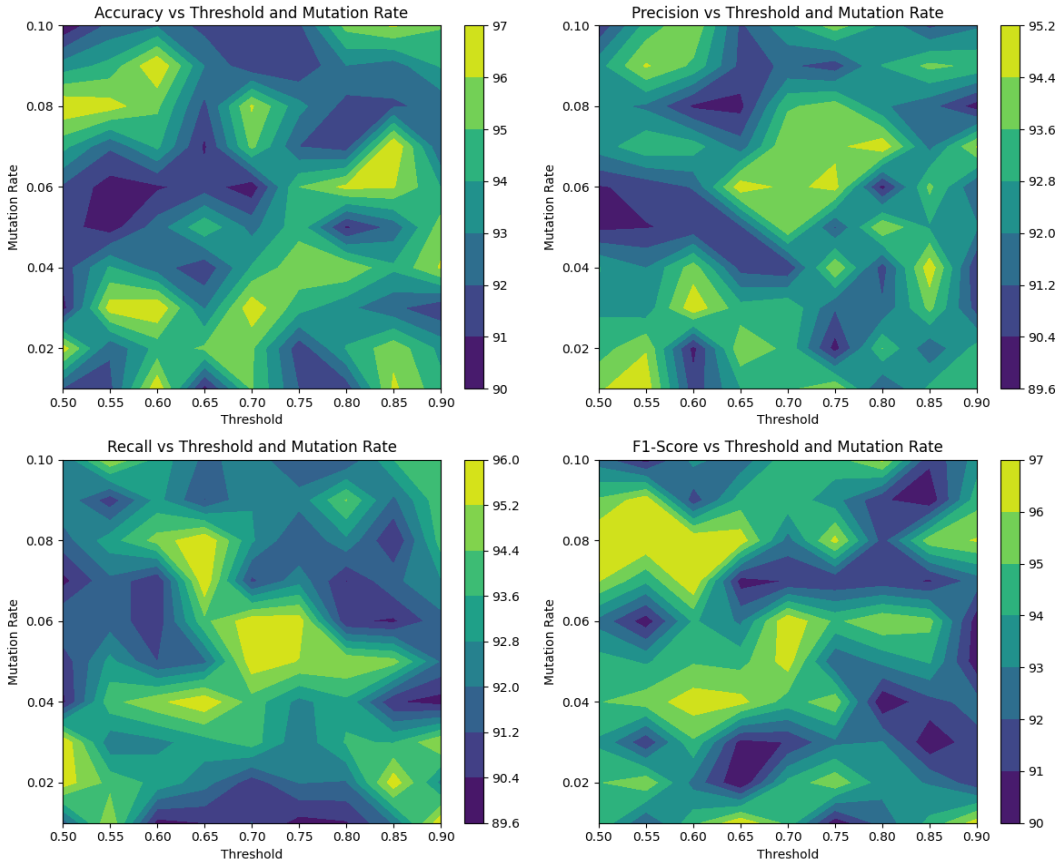


Figure 7. Performance metrics v threshold and mutation rate

Figure 7 below shows how the performance of the model varies with changing the threshold (between 0.5 and 0.9) and mutation rate (between 0.01 and 0.1), on the four main metrics: Accuracy, which quantifies how well the model can correctly classify normal and anomalous traffic; Precision, the proportion of true positives out of the detected anomalies; Recall, the ability of the model to detect actual anomalies, with higher mutation rates increasing recall by allowing the model to detect more subtle or novel threats; and F1-Score.

## CONCLUSION

This research presents a new bio-inspired anomaly detection system that is designed for dynamic and resource-constrained Internet of Things (IoT) settings. Based on the concepts of Artificial Immune Systems (AIS), the proposed model combines adverse selection, clonal expansion with mutation, danger theory, and immune memory to realize scalable, context-aware and adaptive intrusion detection. The system dynamically changes its detectors to adapt to concept drift and zero-day threats, unlike such models, which are either static or rely on retraining, and the system generates minimal false positives and minimizes latency by using an efficient memory recall. The extensive testing on 3 benchmark datasets, including UNSW-NB15, BoT-IoT, and TON_IoT, confirms the high performance of the system with a high detection rate of 97.5% and a wide margin in precision, recall and F1-score when compared to its contemporaries. Context-aware danger assessment and online self-education features will facilitate the responsiveness and flexibility of the solution in real-time and help to meet the requirements of the constantly evolving IoT security environment. The framework overcomes traditional problems in IoT cybersecurity: the generalization of detectors, a low false-alarm rate, continuous adaptation, and rapid response to dynamic threats. These results confirm the prospects of the AIS-based strategies as the lightweight, robust, and future-resistant solutions to detect anomalies in the next-generation IoT infrastructures. Future research should consider federated immune learning between distributed IoT nodes, reinforcement-based mutation policies, and the integration with blockchain-based trust models to increase resilience and decentralization further. Finally, this study opens the door to the biologically inspired intelligence systems that can autonomously engage in lifelong learning in the areas of cybersecurity.

## REFERENCES

[1] Myakala PK, Bura C, Jonnalagadda AK. Artificial immune systems: A bio-inspired paradigm for computational intelligence. Journal of Artificial Intelligence and Big Data. 2025;5(1):10-31586. https://doi.org/10.31586/jaibd.2025.1233

[2] Selvaraj R, Kuthadi VM, Baskar S, Acevedo R. Tiny ML-enabled energy-efficient intrusion detection system for sustainable IoT security in green cybersecurity ecosystems. Journal of Internet Services and Information Security. 2025;15(3):602–25. https://doi.org/10.58346/JISIS.2025.I3.041

[3] Dharmireddi S, Hameed A, Albdairi M, Samudro EG, Nandy M. Cybersecurity in Digital Finance: Artificial Intelligence-Powered Fraud Detection and Risk Management. In2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES) 2025 Apr 24 (pp. 1-5). IEEE. https://doi.org/10.1109/ICCIES63851.2025.11032566

[4] Purnama Y, Asdlori A, Ciptaningsih EMSS, Kraugusteeliana K, Triayudi A, Rahim R. Machine learning for cybersecurity: a bibliometric analysis from 2019 to 2023. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2024;15(4):243–58. https://doi.org/10.58346/JOWUA.2024.I4.016

[5] Jalal SK, Yousif RZ, Al-Mukhtar FH, Kareem SW. An optimized up to 16-user and 160 Gbps dual cascaded optical modulators PON-based power combined array fiber Bragg grating and pre-distortion device for 5th G system. Photonic Network Communications. 2025 Feb;49(1):1.

[6] Mehra A, Iyer R. Improving cybersecurity using artificial intelligence: overview, modeling, future directions. International Academic Journal of Science and Engineering. 2021;8(2):11–15.

[7] Ali OM, Hamaamin RA, Kareem SW. Deep Learning Techniques for Early Fault Detection in Bearings: An Intelligent Approach. Kurdistan Journal of Applied Research. 2025 Feb 23;10(1):18-34. https://doi.org/10.24017/science.2025.1.2

[8] Ali OM, Hamaamin RA, Youns BJ, Kareem SW. Innovative Machine Learning Strategies for DDoS Detection: A Review. UHD Journal of Science and Technology. 2024 Oct 2;8(2):38-49.

[9] Aalsaud A, Kareem SW, Yousif RZ, Mohammed AS. Ensemble transfer learning for botnet detection in the Internet of Things. Scalable Computing: Practice and Experience. 2024 Aug 1;25(5):4312-22. https://doi.org/10.12694/scpe.v25i5.3047

[10] Pinto C, Pinto R, Gonçalves G. Towards bio-inspired anomaly detection using the cursory dendritic cell algorithm. Algorithms. 2021 Dec 21;15(1):1. https://doi.org/10.3390/a15010001

[11] Soni V, Bhatt DP, Yadav NS. Bio inspired methods for intrusion detection in Internet of Things: A survey. In2024 IEEE Region 10 Symposium (TENSYMP) 2024 Sep 27 (pp. 1-8). IEEE. https://doi.org/10.1109/TENSYMP61132.2024.10752276

[12] Wlodarczak P. Cyber Immunity: A bio-inspired cyber defense system. InInternational Conference on Bioinformatics and Biomedical Engineering 2017 Apr 1 (pp. 199-208). Cham: Springer International Publishing.

[13] Saadouni R, Gherbi C, Aliouat Z, Harbi Y, Khacha A. Intrusion detection systems for IoT based on bio-inspired and machine learning techniques: a systematic review of the literature. Cluster Computing. 2024 Oct;27(7):8655-81. https://doi.org/10.1007/s10586-024-04388-5

[14] Balasubramaniam S, Kadry S, TK MK, Kumar KS, editors. Bio-inspired Algorithms in Machine Learning and Deep Learning for Disease Detection. CRC Press; 2025 Mar 13.

[15] Tandiya N, Colbert EJ, Marojevic V, Reed JH. Biologically inspired artificial intelligence techniques. InCyber Resilience of Systems and Networks 2018 May 30 (pp. 287-313). Cham: Springer International Publishing.

[16] Soni V, Saxena S, Bhatt DP, Yadav NS. ImmuneGAN: Bio-inspired Artificial Immune System to Secure IoT Ecosystem. InInternational Conference on Cyber Security, Privacy and Networking 2021 Sep 9 (pp. 110-121). Cham: Springer International Publishing.

[17] Ashwini A, Balasubramaniam S, Sundaravadivazhagan B. Bio-Inspired Intelligence in Early Cancer Detection A Machine Learning Approach. InBio-inspired Algorithms in Machine Learning and Deep Learning for Disease Detection (pp. 122-140). CRC Press.

[18] Sharma P, Chaudhary K. Adaptive Cybersecurity for IoT Networks Using Artificial Immune Systems: A Scalable Approach for Real-Time Threat Detection. InInternational Conference on Artificial Intelligence on Textile and Apparel 2024 Aug 9 (pp. 733-746). Singapore: Springer Nature Singapore.

[19] Pham TH, Raahemi B. Bio-inspired feature selection algorithms with their applications: a systematic literature review. IEEE Access. 2023 May 2;11:43733-58. https://doi.org/10.1109/ACCESS.2023.3272556

[20] Alabdulatif A, Thilakarathne NN. Bio-inspired internet of things: current status, benefits, challenges, and future directions. Biomimetics. 2023 Aug 17;8(4):373. https://doi.org/10.3390/biomimetics8040373

[21] Efiong JE, Ajayi TO, Akinwale A, Olajubu EA. Towards a Bio-inspired Real-Time. ICT for Intelligent Systems: Proceedings of ICTIS 2024, Volume 1. 2024 Sep 26;403:289.

[22] Efiong JE, Ajayi TO, Akinwale A, Olajubu EA, Aderounmu GA. Towards a Bio-inspired Real-Time Intrusion Detection in the Smart Grid. InInternational Conference on Information and Communication Technology for Intelligent Systems 2024 May 22 (pp. 289-302). Singapore: Springer Nature Singapore. https://doi.org/10.3390/biomimetics8040373

[23] Usha G, Madhavan P, Kumar MR. A Novel Design Augmentation of Bio-Inspired Artificial Immune Technique in Securing Internet of Things (IOT). InInternet of Things for Industry 4.0: Design, Challenges and Solutions 2019 Dec 29 (pp. 103-114). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-32530-5_7

[24] Bouramoul IE, Zertal S, Derdour M, Zenbout I. Enhancing IoT Security Through Deep learning and Evolutionary Bio-Inspired Intrusion Detection in IoT systems. In2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS) 2024 Apr 24 (pp. 1-8). IEEE. https://doi.org/10.1109/PAIS62114.2024.10541160

[25] Mthunzi SN, Benkhelifa E, Bosakowski T, Hariri S. A bio-inspired approach to cyber security. InMachine Learning for Computer and Cyber Security 2019 Feb 5 (pp. 75-104). CRC Press.

[26] Bala A, Bahnasse A, El Bhiri B, Zegrari M, Tardif PM. Immunity-Inspired Approaches to Cybersecurity: A Review. Procedia Computer Science. 2025 Jan 1;257:274-81. https://doi.org/10.1016/j.procs.2025.03.037

[27] Pourmoafi S. A Solution for Securing the Information Environment Inspired by Living Organisms and Biology.

[28] Rehman A, Alharbi O. Bioinspired blockchain framework for secure and scalable wireless sensor network integration in fog–cloud ecosystems. Computers. 2024 Dec 26;14(1):3. https://doi.org/10.3390/computers14010003

[29] Ahsan MM, Gupta KD, Nag AK, Poudyal S, Kouzani AZ, Mahmud MP. Applications and evaluations of bio-inspired approaches in cloud security: A review. IEEE Access. 2020 Sep 30;8:180799-814. https://doi.org/10.1109/ACCESS.2020.3027841

[30] RC JS, Parkavi K. Investigations on bio-inspired algorithm for network intrusion detection–a review. Evol. Intell. 2022;9(4). https://doi.org/10.22247/ijcna/2022/214503

[31] Fatin M, Rahman M. Artificial Intelligence in Healthcare Systems: From Clinical Imaging to Epidemic Forecasting. Asia Pacific Journal of Surgical Advances. 2025 Oct 10;2(3):139-51. https://doi.org/10.70818/apjsa.v02i03.054

[32] Soni V, Bhatt DP, Yadav NS, Saxena S. DAIS: deep artificial immune system for intrusion detection in IoT ecosystems. International Journal of Bio-Inspired Computation. 2024;23(3):148-56. https://doi.org/10.1504/IJBIC.2024.137904

[33] Procopiou A, Chen TM. Malicious activity detection in IoT networks: A nature-inspired approach. InAdvances in Nature-Inspired Cyber Security and Resilience 2021 Oct 20 (pp. 55-83). Cham: Springer International Publishing.

[34] Krishna GB, Udayasri G, Devi KR, Gnaneshwar K, Rani DS, Ala R. Biologically-Inspired Artificial Lymphocyte Networks for Adaptive and Scalable Malware Detection Against Zero-Day and Persistent Threats. In2025 12th International Conference on Computing for Sustainable Global Development (INDIACom) 2025 Apr 2 (pp. 1-7). IEEE. https://doi.org/10.23919/INDIACom66777.2025.11115611

[35] Rakhmanovich IU, Hossein RR, Albdairi M, Omonov Q, Kumaraswamy B. Predictive Analytics and Automation: Transforming Logistics with Artificial Intelligence with Blockchain Intelligence. In2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES) 2025 Apr 24 (pp. 1-6). IEEE. https://doi.org/10.1109/ICCIES63851.2025.11033145

[36] Qadri SS, Albdairi M, Almusawi A, Kabarcik A, Abdulrahman HS. Optimization of Signalized Intersections: Analyzing Autonomous Vehicle Behaviors Through Data-Driven Simulations. InInternational Conference on Optimization and Data Science in Industrial Engineering 2024 Nov 7 (pp. 232-244). Cham: Springer Nature Switzerland.

[37] Hamad DM, Gwad WH, Fadaaq WH, Kareem SW. Dynamic Parameter Optimization for Industrial Internet Security Models Using Neural Networks. International Journal of Intelligent Engineering & Systems. 2025 Jun 1;18(6). https://doi.org/10.22266/ijies2025.0731.58