BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES,
DOI: 10.24425/bpasts.2024.152211



# HAIS-IDS:A Hybrid Artificial Immune System Model for Intrusion Detection in IoT

**Vineeta Soni**[1],**Devershi Pallavi Bhatt**[2] *, **Narendra Singh Yadav**[3]

[1,2,3] Manipal University Jaipur,Jaipur,India

**Abstract.** The application of the Internet of Things(IoT) is increasing exponentially, the dynamic data flow and distributive operation over low resource devices possesses huge threat to sensitive human data. This paper introduces an artificial immune system (AIS) based approach to intrusion detection in IoT network ecosystems, the proposed approach implements dual-layered AIS; which is robust to zero-day attacks and designed to adapt new types of attack classes in the form of antibodies.In this paper, a Hybrid method has been presented which uses Hybrid of Clonal Selection using Variation auto-encoders as Innate Immune Layer and Apaptive Dentritic Model for identifying intrusions over IoT Specific Datasets.Moreover we present extensive empirical analysis over six IoT network benchmark datasets for semi-supervised multi-class classification task and obtain superior performance compared to five state-of-the-art baselines. Finally, VC-ADIS achieves 99.83% accuracy over MQTT-set dataset.

**Key words:** Internet of Things; Artificial Immune System; Variational Clonal Selection; IoT Security.

## 1. INTRODUCTION

The Internet of Things (IoT) has experienced substantial growth in recent years. With the increasing number of devices integrated into daily life, there has been a rapid surge in the collection, transmission, and sharing of data from these devices. Ensuring the security of the IoT environment is a formidable challenge [1]. The IoT network functions on the principle of data exchange among compact devices, rendering it susceptible to advanced and zero-day attacks. While many existing security systems can handle common attacks, the unique nature of the IoT network involves multifaceted data streams and intricate devices optimized for energy efficiency.

### 1.1. Intrusion detection in IoT Network Ecosystem

An intrusion is characterized as any form of questionable activity that disrupts the normal data flow, aimed at compromising the network and illicitly acquiring data from the data stream [2]. Identifying intrusions in IoT environments involves various methods, including graph-based anomaly detection methods within the network, conventional machine learning techniques for classifying intrusion packets, and approaches based on matrix manipulation, among others. IoT network environments exhibit a multitude of vulnerabilities due to their complex layered structure and the energy-efficient nature of the devices they incorporate.

- Perception Layer: This Layer encompasses physical hardware like sensors and transmitters. T
- Network Layer: Responsible for managing message and data transmission throughout the network ecosystem,
- Application Layer: T The Application Layer plays a crucial role in offering essential services to users and facilitating user-IoT interactions within the environment.

Each layer contributes distinct functionalities to the IoT system and is susceptible to exploitation for network attacks [3]. Nonetheless, the surge in data-centric techniques, including machine learning and deep learning, introduces novel strategies for identifying intrusions within real-time network operations. AIS draws inspiration from natural immune systems [4] to establish resilient platforms capable of defending against advanced attacks. This paper utilizes an artificial immune system based on variational auto-encoders [5]. The objective is to leverage data representation learning and construct an efficient and robust security framework for IoT networks. The paper is organized as follows; starts with introducing background works and a relevant literature survey of the Immune system approaches in cyber-security, then our approach of variational clonal selection has been proposed with the self-adaptive mechanism which employs a self-learning paradigm for the adaption of new attacks. Finally, it compares with the standard data sets and other ML algorithms.

## 2. PRELIMINARIES, BACKGROUND AND RELATED WORK

Artificial Immune System (AIS) [6] Components and properties of AIS make it adaptable and efficiently secure data against potential attacks. Here are descriptions of some key AIS algorithms and their underlying mechanisms:

*2.0.1. Negative Selection for anomaly detection:* The Negative selection (NS) algorithm [7] draws inspiration from the acquired immunity mechanism of self-non-self discrimination.

The NS algorithm's primary goal is to establish a clear distinction between self and non-self entities. It achieves this by generating detector objects, akin to T-cells, that interact with and bind to non-self objects, thus enhancing system security.

*2.0.2. Clonal Selection Algorithm:* Built upon the principles of acquired immunity theory, the Clonal Selection Algorithm [8] focuses on creating receptors that progressively learn to respond to antigens over time. This process involves a delicate balance between receptor mutation and cloning. The algorithm effectively refines the receptor population, discarding

*e-mail: Vineeta.soni@jaipur.manipal.edu

those that compromise the environment's autoimmunity. .

***2.0.3. Artificial Immune Networks:*** Artificial Immune Networks (AIN) [6] are inspired by immunology's antibody theory and borrowing concepts from the clonal selection algorithm, this approach introduces antibodies present in pairs. These antibody pairs sustain immune memory regarding cellular interactions, even without external antigens. This enables the system to recognize potential threats and maintain a proactive stance. Unlike the basic Clonal Selection Algorithm, AIN focus on the interactions between antibodies themselves, not just between antibodies and antigens.

***2.0.4. Danger Theory Algorithm*** In biological terms, the Danger Theory suggests that the immune response is triggered not solely by the presence of foreign entities (non self) but by the danger or damage they cause to the host organism. This theory was proposed to explain certain immune responses that do not neatly fit into the self/non-self paradigm. This allows the system to become more or less sensitive to threats over time [9].These AIS algorithms encapsulate sophisticated immunological concepts within computationally efficient frameworks, aiming to enhance data security within the context of IoT networks. Through abstracting and adapting natural immune mechanisms [10].

## 3. PROPOSED SELF-ADAPTIVE ARTIFICIAL IMMUNE SYSTEM

This paper introduces a novel approach that revolves around prioritizing data-centric strategies for constructing a self-adaptive AIS. In Figure 1, offers an overview of the data pathway involved in securing the IoT landscape and surveilling potential attacks.

The proposed artificial immune system operates through two distinct layers of immunity: the innate layer and the adaptive immune layer. The underlying process of fortifying the IoT network ecosystem with this Artificial Immune System unfolds as follows:

***3.0.1. Data Capture and Preprocessing:*** The regular data flow is captured utilizing a tap connection between network nodes, and this data can be stored as a pcap file using wireshark [9]. This initial pcap file is then directed through a content feature extractor. The aim here is to derive a mapping of feature values that encapsulate the essence of the characteristics of Data. The left section of the figure delineates an IoT network cloud comprising multiple devices (D1-D5) and an identified Attacker Node, indicating the presence of potential security threats within the network topology. The data flow is captured in real-time, where it is subject to scrutiny by a Packet Capture (PCAP) Tap. This component's role in the architecture is critical as it enables the acquisition of network traffic data, which is essential for the subsequent analysis and identification of potential security breaches.

***3.0.2. Innate Layer Processing:*** The processed data, now carrying the feature-value mapping, is subsequently channeled through the innate layer module of the AIS. This layer mimics the innate immunity found in natural systems [**?**], seeking to promptly recognize and respond to general patterns of intrusion or abnormal behavior. An integral part of the framework that categorizes network packets into 'Normal' and 'Antigen' packets. After classification, the Network Feature Extractor component extracts relevant features from the traffic data. The Preprocessing Network Data component suggests a refinement process to prepare the input for the Intrusion Detection System (IDS).

***3.0.3. Adaptive Layer Processing*** Following the innate layer, the processed data progresses into the adaptive immune layer module. Comparable to the adaptive immunity in natural systems [10], this layer evolves to discern and counter more specific threats, adjusting its responses as new challenges arise. The Self Adaptive IPS (Intrusion Prevention System), processes the 'Antigen Data' through what is labeled as the 'Primary Layer of Adaptive Security.' This nomenclature suggests that the system is capable of evolving its defensive mechanisms based on historical antigen data, indicative of a learning system that fine-tunes its responses to continually emerging threats. The Monitoring component is likely to provide essential feedback on the system's performance, including the efficacy of threat detection and the robustness of the adaptive responses [6].

### *3.1. Variational clonal selection as Innate Immune System*

We introduce a novel approach for generating clones of antigen features using a combination of variational autoencoders (VAEs) and regression of latent embeddings [11]. This process involves encoding the essential characteristics of antigens into a latent space using a VAE, followed by regression to produce accurate clones that capture the underlying patterns and variations. Figure 2 illustrates an innovative computational framework for generation of antigen clones using a hybrid method that combines the principles of Variational autoencoding and regression analysis. This framework is posited as an integral component of an artificial innate immune system, designed to enhance the recognition and response capabilities in digital security, health informatics, or other fields necessitating sophisticated pattern recognition and replication of complex features. Here we describe the components of the Variational Clonal selection mechanism as follows:

***3.1.1. Encoding and Latent Space Representation*** The process commences with the preparation of a dataset comprised of antigen features that encapsulate essential attributes pertinent to the domain of application. An encoder neural network is then employed to ingest these features and map them into a compressed, lower-dimensional latent space. This transformation is a probabilistic distribution, characterized by mean ($\mu$) and variance ($\sigma$) parameters. This distribution represents the inherent uncertainty and variability in the data,that allows for the subsequent generation of a diverse array of antigen clones. Latent Space Distribution: In a VAE, the encoder

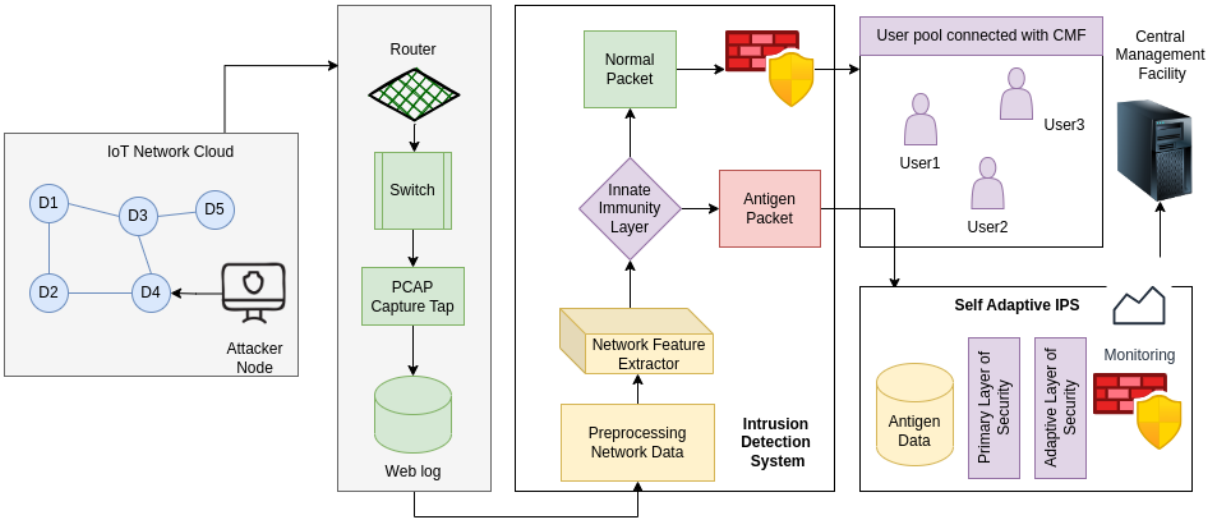


**Fig. 1.** A schematic diagram of our proposed architecture, VC-ADIS.

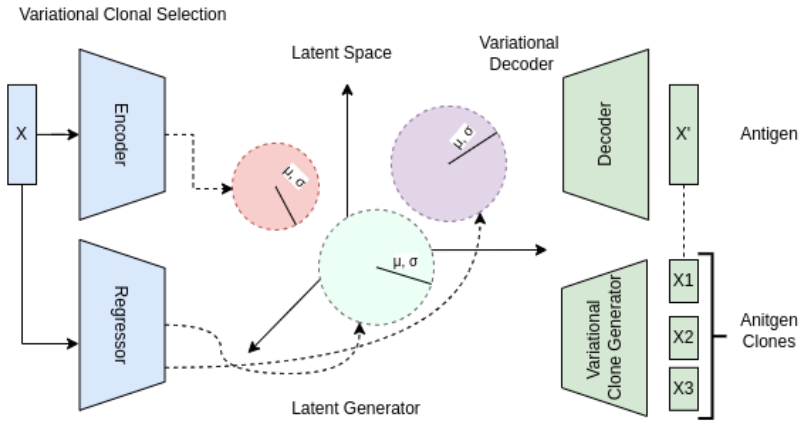


**Fig. 2.** Variational Clonal Selection in VC-AIS architecture

network produces a distribution (mean and variance) that describes the uncertainty of the encoding.

***3.1.2. Decoding and Clone Generation:*** The decoder component of the VAE is tasked with the reconstruction of antigen features from the latent representations. To generate clones, the latent space is sampled, drawing vectors that represent the 'genetic code' of potential antigen variants. The decoder network then interprets these vectors, translating the encoded information back into a tangible feature set that closely resembles the original antigen, thereby producing viable clones.

***3.1.3. Regression-Enhanced Clonal Precision*** To refine the cloning process, a regression model is introduced. This model is trained to predict latent space encodings of antigens based on a chosen reference antigen's encoding. When presented with a new antigen's encoding, the regression model outputs a predicted latent encoding, which acts as the blueprint for the clone's features. These clones are not mere replicas but are nuanced variations of the reference antigen, capturing the underlying patterns and intricacies of the original features. The process for clonal preparation is employed as follows:

- Target Selection: we choose a reference antigen from the dataset for clone.
- Feature Regression: we train a regression model (a neural network) that takes the reference antigen's latent space encoding as input and aims to predict the latent space encoding of other antigens.
- Cloning Procedure: Given a new antigen's latent space encoding, we use the trained regression model to predict its corresponding latent space encoding based on the reference antigen's encoding. This predicted encoding serves as the "genetic code" for the clone.
- Decode Clones: Finally, decode the predicted latent space encoding through the decoder network to generate clones of the original antigen with characteristics similar to the reference antigen.

The algorithm 1 presents the pseudo-code for the variational clonal section.

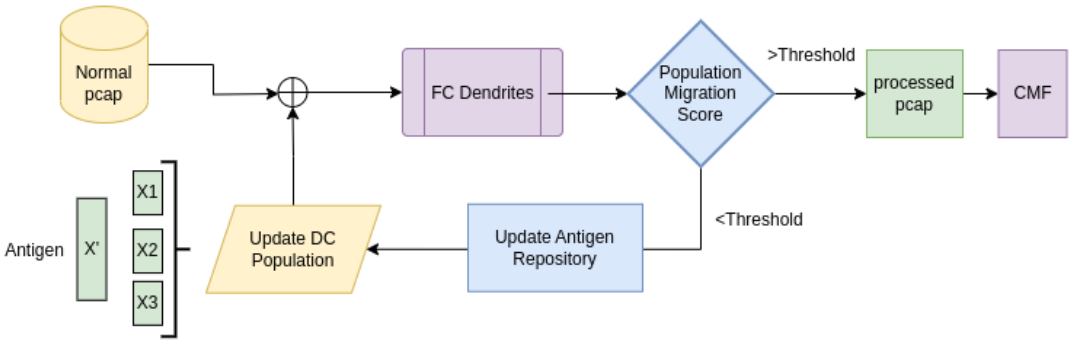


**Fig. 3.** Architecture for the training process of ADM.

**Algorithm 1** Training method for variational clonal selection

**Input** Process feature representations $X = x^1, x^2, ...., x^n$
Training class labels $C = c^1, c^2, ...., c^n$
**Output** Learned representations i.e. Antigen clones at time t

**for** i = 1 to num_epochs **do**

**Step 1:** Compute likelihood distribution of x assoc. with latent z
$p(x) = \int_z p(x,z,c)$, where $p(x,z,c) = p(x|z)p(z|c)p(c)$

**Step 2:** Compute regressor variables i using auxiliary function $q : q(z^i, c^i|x^i)$

**Step 3:** Compute pseudo variation for two time steps $logp(x) = \mathrm{D}_{\mathrm{KL}}(q(z^i, c^i|x^i)||p(z^i, c^i|x^i))$

**Step 4:** Approximate latent representations for time step $t+1$ $q(z|x) \sim N(z; f(x;\phi), g(x;\phi))$ where $\phi$ are network parameters

**Step 5:** Compute Loss
$L(x) = -\mathrm{E}_{z\sim q(z|x)}[logp(x)] + \mathrm{D}_{\mathrm{KL}}(q(z^i|x^i)||p(z^i))$

**Step 6:** Back-propagate weights

**end for**

### 3.2. *Adaptive Dendritic Module (ADM) for network anomaly adaptation and classification*

We propose a self-adaptive dendritic module for learning representations of antigens and the population cultivated by the variational clonal selection module. Figure 3 portrays an advanced self-adaptive dendritic cell (DC) [12] mechanism designed for the dynamic analysis and classification of network traffic, a core component of a cyber security framework. In the depicted module, the process initiates with the collection of standard network traffic data, represented here as 'Normal pcap'. This data encapsulates regular traffic patterns and serves as a baseline for comparison against potential threats. Simultaneously, the module receives an input stream of 'Antigen' data, which is a set of features identified by the variational clonal selection module as potential indicators of anomalies or security threats within the network. These antigen features, designated as X1, X2, and X3, are then integrated with the 'Normal pcap' to update the DC population, effectively merging the baseline of network behavior with the newly identified antigen characteristics. This neural network is tasked with classifying the combined features using cross-entropy loss [**?**], The outcome of this process is evaluated against a predefined threshold, which determines whether the traffic patterns are deemed normal or suspicious. If the classification score, termed 'Population Migration Score', exceeds the threshold, the traffic data is considered anomalous and is forwarded to the Central Management Facility (CMF). This implies that the system has identified a significant deviation from the normal traffic pattern, warranting further investigation or immediate action. Conversely, if the score falls below the threshold, the data is used to augment the 'Antigen Repository'. This repository serves as a knowledge base, contributing to the ongoing learning and adaptation of the system by updating the DC population with new antigen profiles. This iterative process allows the system to continuously refine its understanding of network behavior, adapting to new and evolving threats in real time. The elegance of this self-adaptive mechanism lies in its capacity to learn from the network environment actively and adaptively. This dendritic cell algorithm represents a significant step towards creating autonomous, intelligent systems are capable of safeguarding digital infrastructure against an ever-changing landscape of cyber vulnerabilities. The algorithm 2 presents the pseudocode for the ADM mechanism.

## 4. EXPERIMENTS

This section presents benchmark datasets, baseline methods, comparative analyses and ablation studies of our model. In figure 4 introduces a sophisticated self-adaptive dendritic cell (DC) algorithm that underpins an artificial immune system (AIS) for network security.Variable clonal selection modules improve the detection and response to network 'antigens'—like foreign pathogens—that present security risks. The operational flow within the self-adaptive DC mechanism commences with the acquisition of pcap (packet capture) data serves as a baseline for identifying deviations indicative of security threats. Concurrently, the variational clonal selection module processes data to identify unique or aberrant features—referred to as 'antigens'—that signify potential intrusions or anomalies in the network. These antigens, encoded as features X1, X2, and X3, are amalgamated with the normal pcap data to update the DC population, mirroring the bi-

**Table 1**
Performance comparison on the Bot-IoT and UNSW-NB15.

| **Dataset** | **The BoT-IoT** | | **UNSW-NB15** | |
|---|---|---|---|---|
| **Models** | Mean Acc | Macro F1 | Mean Acc | Macro F1 |
| **VC-ADIS** | **0.8906** | **0.8648** | **0.7512** | **0.6844** |
| TabNet | 0.8900 | 0.8492 | 0.7489 | 0.6755 |
| CNN-BiLSTM | 0.8636 | 0.8333 | 0.7211 | 0.5801 |
| LSTM | 0.8215 | 0.7824 | 0.6804 | 0.4315 |
| Deep NNs | 0.8824 | 0.8603 | 0.7254 | 0.5726 |
| Random Forest | 0.8797 | 0.8537 | 0.7248 | 0.5869 |
| Naive Bayes | 0.6532 | 0.6109 | 0.6528 | 0.5411 |
| Decision Tree | 0.8466 | 0.8134 | 0.7168 | 0.5731 |

[]

**Table 2**
Performance comparison on the MQTT-IoT-IDS and UNSW dataset.

| **Dataset** | **MQTT-IoT-IDS** | | **UNSW-NB15** | |
|---|---|---|---|---|
| **Models** | Precision | Recall | Precision | Recall |
| **VC-ADIS** | **0.8915** | **0.8802** | **0.6733** | **0.6904** |
| TabNet | 0.8701 | 0.8505 | 0.5347 | 0.5935 |
| CNN-BiLSTM | 0.8799 | 0.8433 | 0.6508 | 0.5504 |
| LSTM | 0.8305 | 0.7836 | 0.6001 | 0.5284 |
| Deep NNs | 0.8824 | 0.8603 | 0.7254 | 0.5726 |
| Random Forest | 0.8402 | 0.8655 | 0.5602 | 0.5829 |
| Naive Bayes | 0.5933 | 0.6237 | 0.5828 | 0.5108 |
| Decision Trees | 0.7824 | 0.8305 | 0.5534 | 0.6025 |

**Table 3**
Performance comparison on the benchmark IoT intrusion detection datasets.

| **Dataset** | **MQTT-IoT-IDS** | | **KDD-CUP-99** | | **MQTTset** | | **UFPI-NCAD** | |
|---|---|---|---|---|---|---|---|---|
| **Models** | Mean Acc | Macro F1 | Mean Acc | Macro F1 | Mean Acc | Macro F1 | Mean Acc | Macro F1 |
| **VC-ADIS** | **0.9211** | **0.9206** | **0.8764** | **0.8498** | **0.9983** | **0.9971** | **0.9592** | **0.9564** |
| TabNet | 0.9125 | 0.8966 | 0.8502 | 0.8375 | 0.9901 | 0.9925 | 0.9501 | 0.9463 |
| CNN-BiLSTM | 0.8801 | 0.7826 | 0.7911 | 0.8545 | 0.9628 | 0.9105 | 0.9274 | 0.9055 |
| LSTM | 0.8647 | 0.7405 | 0.7636 | 0.8205 | 0.9527 | 0.9148 | 0.8653 | 0.8155 |
| Deep NNs | 0.9184 | 0.917 | 0.8702 | 0.8311 | 0.9935 | 0.9943 | 0.9244 | 0.9188 |
| Random Forest | 0.8801 | 0.8732 | 0.8535 | 0.8472 | 0.9724 | 0.9967 | 0.9036 | 0.8961 |
| Naive Bayes | 0.9027 | 0.8946 | 0.8672 | 0.8568 | 0.9883 | 0.9910 | 0.9182 | 0.9134 |
| Decision Tree | 0.8632 | 0.8591 | 0.8592 | 0.8154 | 0.9689 | 0.9862 | 0.8942 | 0.8826 |

[]

**Table 4**
Performance comparison on the benchmark IoT intrusion detection datasets over Precision and Recall Values.

| Dataset | The Bot-IoT | | KDD-CUP-99 | | MQTTset | | UFPI-NCAD | |
|---|---|---|---|---|---|---|---|---|
| Models | Precision | Recall | Precision | Recall | Precision | Recall | Precision | Recall |
| **VC-ADIS** | **0.84** | **0.87** | **0.82** | **0.85** | **0.95** | **0.99** | **0.93** | **0.96** |
| TabNet | 0.83 | 0.78 | 0.80 | 0.74 | 0.94 | 0.96 | 0.91 | 0.83 |
| CNN-BiLSTM | 0.75 | 0.61 | 0.78 | 0.53 | 0.91 | 0.83 | 0.72 | 0.65 |
| LSTM | 0.80 | 0.43 | 0.65 | 0.48 | 0.82 | 0.71 | 0.64 | 0.57 |
| Deep NNs | 0.82 | 0.85 | 0.79 | 0.85 | 0.97 | 0.95 | 0.89 | 0.92 |
| Random Forest | 0.81 | 0.82 | 0.84 | 0.86 | 0.92 | 0.93 | 0.88 | 0.90 |
| Naive Bayes | 0.58 | 0.63 | 0.83 | 0.85 | 0.95 | 0.96 | 0.92 | 0.87 |
| Decision Tree | 0.80 | 0.78 | 0.77 | 0.80 | 0.88 | 0.92 | 0.86 | 0.89 |

**Table 5**
Ablation study to measure the impact of three blocks of – Feature Processing, Innate Immunity, and Adaptive Immunity

| Datasets | Performance | w/o Feature Processing | w/o Innate Immunity | w/o Adaptive Immunity |
|---|---|---|---|---|
| **MQTT-IoT-IDS2020** | 92.11 | 89.62 | 90.54 | 91.84 |
| **KDD-CUP- 99 dataset** | 87.64 | 83.45 | 82.12 | 87.02 |
| **MQTTset dataset** | 99.83 | 91.22 | 95.78 | 99.35 |
| **UFPI-NCAD-IoT-Attacks** | 95.92 | 90.84 | 91.64 | 92.44 |
| **The Bot-IoT** | 89.06 | 82.57 | 84.91 | 82.44 |
| **UNSW-NB15** | 75.12 | 70.64 | 71.45 | 72.54 |

**Algorithm 2** Self-adaptive dendritic cell algorithm

**Input** True legitimate pcap feature $P = p^1, p^2, ...., p^n$
Updated DC representations $X = x^1, x^2, ...., x^n$
True class labels $C = c^1, c^2, ...., c^n$
Threshold $e$ **Output** pcap label classification score

**for** i = 1 to num_epochs **do**

**Step 1:** Concatenate input pcap with DC population $\hat{x} = p^1, p^2, ...., p^n \cup x^1, x^2, ...., x^n$

**Step 2:**Compute classification score using FC layer assign $\hat{x}$

**Step 3:** Compute pseudo variation for two time steps $logp(x) = \mathrm{D_{KL}}(q(z^i, c^i|x^i)||p(z^i, c^i|x^i))$

**Step 4:** Approximate latent representations for time step $t+1$ $q(z|x) \sim N(z; f(x;\phi), g(x;\phi))$ where $\phi$ are network parameters

**Step 5:** Compute Loss $L(x) = -\mathrm{E}_{z\sim q(z|x)}[logp(x)] + \mathrm{D_{KL}}(q(z^i|x^i)||p(z^i))$

**Step 6:** Backpropagate weights

**end for**

ological process whereby dendritic cells capture and process antigens. Once integrated, the data traverses a fully connected neural network, emulating the dendritic structures in the immune system, where it undergoes classification. This classification employs a cross-entropy loss function to evaluate the probability of the data belonging to a class of normal or anomalous traffic. The outcome, manifested as a 'Population Migration Score', is compared against a predetermined threshold to ascertain the nature of the traffic. If the score is below the threshold, it indicates normality, and the data is relegated to the Antigen Repository. This repository acts as a cumulative knowledge base that informs the ongoing re-calibration of the DC population, fostering the AIS's capability to evolve its recognition and response patterns dynamically. By iterating this process, the system becomes increasingly sophisticated in recognizing and responding to complex and evolving cybersecurity threats, thereby enhancing the resilience and integrity of the network it protects.

#### *4.0.1. Experimental Setup*

#### *4.0.2. Benchmark Datasets*

We evaluate the proposed approach extensively on six publicly available datasets for intrusion detection. Here we provide a brief description of the datasets used for experiments:

- MQTT-IoT-IDS2020
- KDD-CUP- 99 dataset
- MQTTset dataset
- UFPI-NCAD-IoT-Attacks
- The BoT-IoT Dataset
- UNSW-NB15 Dataset

#### *4.0.3. Baseline Methods.*

We compare VC-ADIS with standard baselines designed for semi-supervised multi-class classification tasks in machine learning-based approaches. (i) Deep Neural Networks (DeepNNs) [9]: DNNs employ interconnected layers of neurons with weighted connections and activation functions. Back-propagation modifies these weights during training to reduce a loss function [9]. (ii) Random Forest [13]: A reliable and adaptable machine learning ensemble technique is random forests. During training, they build several decision trees [14], The end outcome is often an average or majority vote of the predictions from individual trees (regression or classification, respectively), with each individual tree then jointly contributing to creating predictions. (iii) Naive Bayes [15]: Naive Bayes is a straightforward probabilistic algorithm that is used for classification and text analysis.It computes the likelihood of a data point belonging to a specific class based on the conditional probabilities of each feature within that class. (iv) Decision Tree [14]: It is a tree-like model used in machine learning for classification and regression. Decision trees are frequently used due to their simplicity and capacity to handle both categorical and numerical data,but if not rigorously pruned or limited, they can be prone to over-fitting. (v) TabNet [16]: TabNet is a deep learning model designed specifically for tabular data, which uses sequential attention to choose which features to reason from at each decision step. This leads to improved interpretability and efficiency in handling high-dimensional data. (vi) CNN-BiLSTM [17]: This model combines Convolutional Neural Networks (CNNs) with Bidirectional Long Short-Term Memory (BiLSTM) networks. The CNN layers are used for feature extraction from the input data, while the BiLSTM layers capture temporal dependencies, making this architecture suitable for tasks requiring both spatial and sequential data analysis. (vii) LSTM [17]: Long Short-

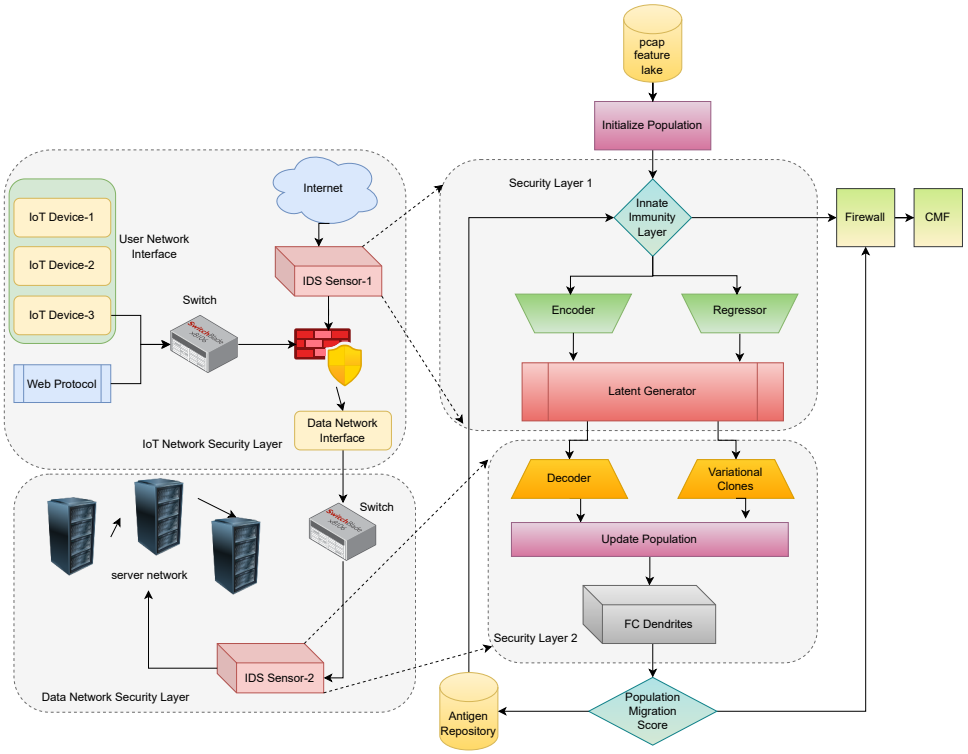


**Fig. 4.** Block diagram of the proposed VC-AIS algorithm

Term Memory (LSTM) networks are a type of recurrent neural network (RNN) capable of learning long-term dependencies. They are well-suited for sequence prediction problems because they can maintain information over long periods, making them useful for tasks where context and order are important.

### *4.1. Performance Comparison*

We evaluate the model performance based on mean accuracy, macro F1-score, and micro F1-score. We report the average performance of the model over ten runs, along with the standard deviation as shown in table 1 and 2.

***4.1.1. Comparative Analysis:*** The table 3 presents a comparative analysis of the Variational Clonal-Artificial Dendritic Immune System (VC-ADIS) against several established machine learning models in IoT intrusion detection Domain.The datasets employed for this study are MQTT-IoT-IDS, KDD-CUP-99, MQTTset, and UFPI-NCAD, each representing a standard benchmark in the intrusion detection landscape.

VC-ADIS demonstrates superior performance across both metrics on the MQTT-IoT-IDS dataset, with a mean accuracy of 92.11% and a macro F1-score of 92.06%, closely followed by Deep Neural Networks (NNs) which showcase a slight decrement in performance. On the KDD-CUP-99 dataset, the performance of VC-AIS is competitive, achieving a mean accuracy of 87.64% and a macro F1-score of 84.98%, once again outperforming the alternative models. Notably, the margin of performance improvement with VC-ADIS is more pronounced on the MQTTset and UFPI-NCAD datasets, with mean accuracies of 99.83% and 95.92% and macro F1-scores of 99.71% and 95.64%, respectively as shown in table 3 and 4. These results underscore the robustness of VC-AIS in identifying and classifying network intrusions with high precision. The variational clonal approach allows VC-ADIS to adaptively learn and recognize diverse patterns of network traffic, which are crucial in the context of IoT security where the network behavior is highly dynamic and the threat landscape is continually evolving. The inclusion of dendritic mechanisms enables the VC-ADIS to efficiently process and integrate complex data representations, enhancing its detection capabilities.

When contrasted with traditional machine learning models such as Random Forests, Naive Bayes, and Decision Trees, VC-AIS not only achieves higher accuracy and F1-scores but also demonstrates an advanced ability to generalize across different types of network environments and attack vectors. Deep NNs, while performing comparably well, lack the biological inspiration that provides VC-AIS with its self-adaptive properties, essential for the rapidly changing domain of cybersecurity.

Moreover from the table 1 it is evident that VC-ADIS outperforms the other models across both datasets. Specifically, on The Bot-IoT dataset, VC-AIS achieves a mean accuracy of 89.06% and a macro F1-score of 86.48%. This is a notable improvement over traditional machine learning models such as Deep Neural Networks (NNs), Random Forests, Naive Bayes, and Decision Trees. The performance margin is particularly significant when compared to the Decision Tree model, which shows the lowest mean accuracy and macro F1-score of 84.66% and 81.34% respectively as shown in figure 5. Similarly, on the UNSW-NB15 dataset, VC-AIS again tops the

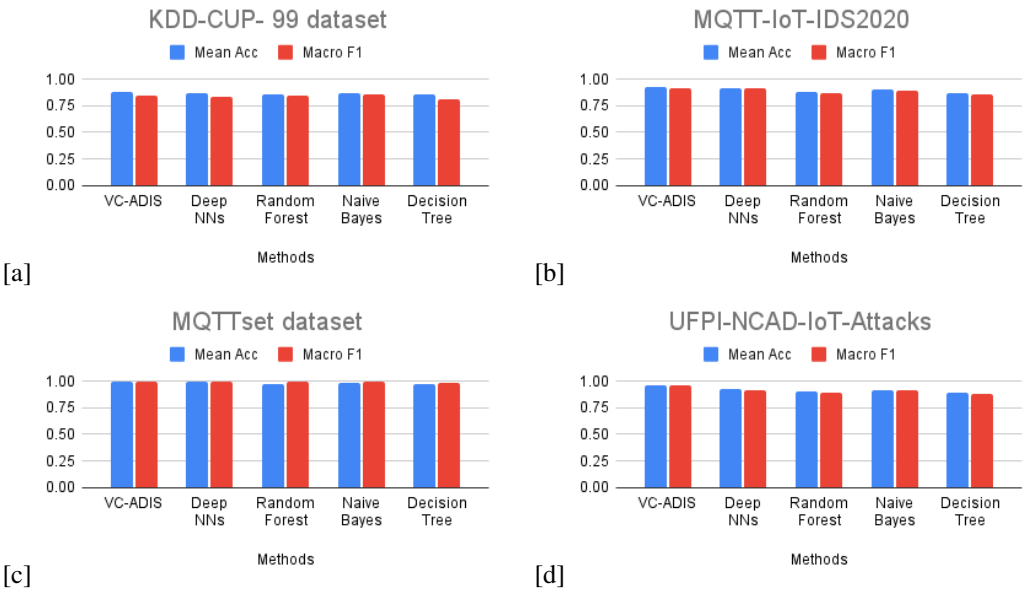


**Fig. 5.** Performance comparison of evaluation metrics and moving average of accuracy over (a) KDD-CUP-99 (b) MQTT-IoT-IDS-2020 (c) MQTTset (d) UFPI-NCAD-IoT Attacks.

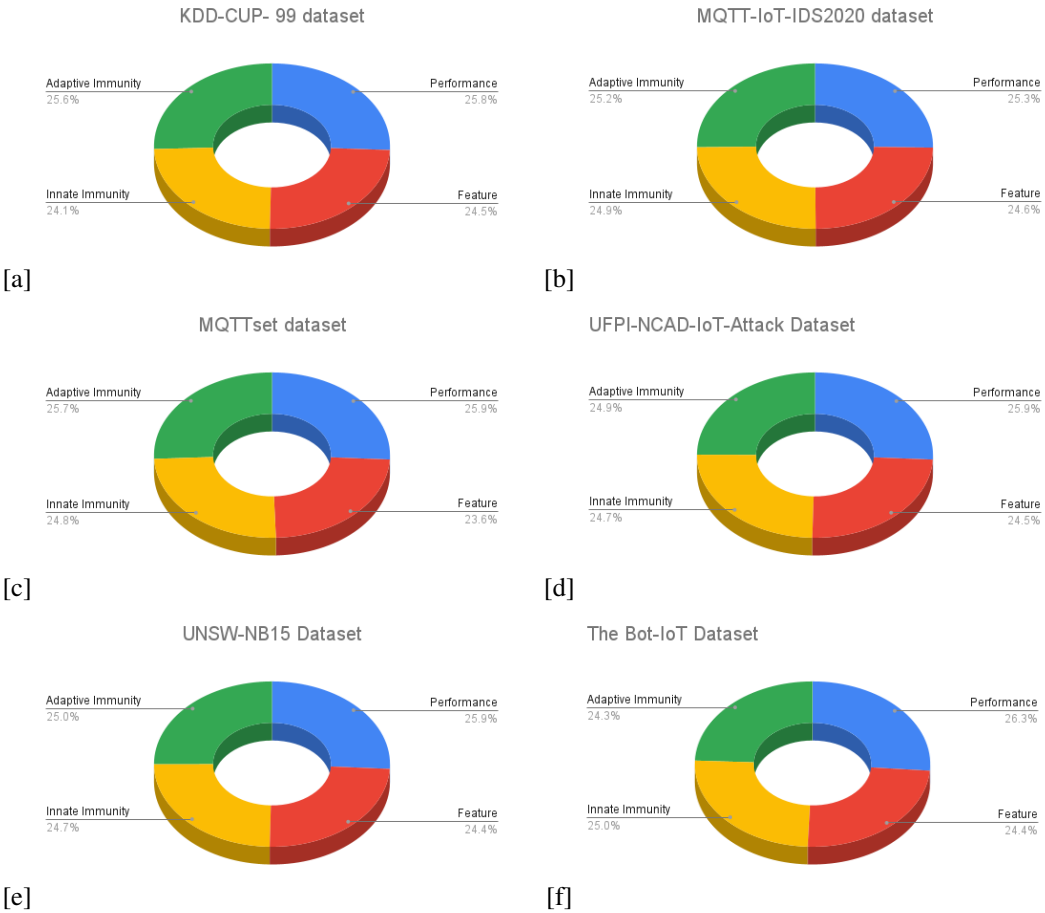


**Fig. 6.** Ablation study accuracy over (a) KDD-CUP-99 (b) MQTT-IoT-IDS-2020 (c) MQTTset (d) UFPI-NCAD-IoT Attacks (e) UNSW-NB15 (f) The Bot-IoT

chart with a mean accuracy of 75.12% and a macro F1-score of 68.44%, whereas the other models exhibit substantially lower performance metrics.

The superior performance of VC-ADIS can be attributed to

its advanced design, which incorporates concepts from the biological immune system, particularly the functionalities of dendritic cells. These cells are critical to the immune response, and adept at identifying and presenting antigens. In the VC-AIS model, this biological analogy is used to create a system that can effectively learn and recognize the complex patterns associated with network intrusions. The variational aspect of the model allows for the handling of uncertainties inherent in network traffic, providing a robust means to adapt to the dynamic nature of cyber threats, which is crucial in the rapidly evolving landscape of IoT security.

The comparative results underscore the effectiveness of VC-ADIS in accurately detecting a wide range of intrusions. Its biologically inspired components confer a strategic advantage over more traditional models, enabling it to dynamically adapt and maintain high performance even in the face of sophisticated and novel attack strategies. This study highlights the potential of leveraging biological mechanisms within artificial intelligence frameworks to enhance cyber security measures in complex network environments. VC-ADIS emerges as a potent solution, demonstrating that the integration of variational and clonal principles with dendritic cell-inspired algorithms can significantly advance intrusion detection systems' capabilities.

The study emphasizes the efficacy of VC-AIS in accurately detecting diverse intrusions. Its biologically inspired elements provide a strategic edge, enabling dynamic adaptation and sustained high performance against sophisticated attacks. By leveraging biological mechanisms in AI frameworks, this research underscores the potential for enhancing cyber security in complex networks. VC-ADIS stands out as a powerful solution, showcasing how integrating variational and clonal principles with dendritic cell-inspired algorithms can significantly boost intrusion detection system capabilities.

***4.1.2. Comparative analysis over recent baselines:*** The VC-ADIS model demonstrated superior performance across all datasets, consistently achieving Mean Accuracy and Macro F1-scores exceeding 0.90. Notably, for the MQTT-IoT-IDS dataset, VC-ADIS attained a Mean Accuracy of 0.9211 and a Macro F1-score of 0.9206, underscoring its robustness and generalization capabilities. In contrast, traditional algorithms such as Decision Trees and Naive Bayes exhibited comparatively lower performance metrics. The observed performance variability among different models highlighted the challenges posed by imbalanced datasets in the domain of network intrusion detection. Models like TabNet and CNN-BiLSTM demonstrated moderate performance, with Mean Accuracy and Macro F1-scores typically ranging from 0.80 to 0.90. However, their Precision and Recall metrics showed significant variability across datasets, suggesting potential overfitting issues. For instance, the CNN-BiLSTM model achieved a Precision of 0.91 and Recall of 0.83 on the MQTTset dataset, but its performance declined on the KDD-CUP-99 dataset, with Precision and Recall values of 0.78 and 0.53, respectively as shown in table 4. These discrepancies emphasize the critical need for robust data processing techniques and judicious feature selection to mitigate overfitting and enhance model generalization across diverse network intrusion datasets.

***4.1.3. Ablation Study:*** The table 5 shows that the ablation study quantifies the contribution of feature processing, innate immunity, and adaptive immunity components by comparing the performance of the complete system against versions with each of these elements removed (Fig. 6). The datasets used for this evaluation include MQTT-IoT-TDS2020, KDD-CUP-99, MQTTset, UFPI-NCAD-IoT-Attacks, The Bot-IoT, and UNSW-NB15, which are benchmark datasets in the domain of network security, particularly focusing on intrusion detection in IoT environments.

The 'Performance' column indicates the effectiveness of the full VC-ADIS module, with all features and mechanisms operational. The subsequent columns show the system's performance without feature processing, without innate and adaptive immunity, Adaptive immunity respectively. A noticeable decline in performance across all datasets when these modules are disabled demonstrates their individual and collective importance to the system's overall effectiveness.

For instance, the MQTT-IoT-TDS2020 dataset shows a marked decrease in performance from 92.11% with the full system to 89.62% when feature processing is omitted, suggesting that pre-processing of input data plays a significant role in preparing the data for effective pattern recognition and anomaly detection. The further reduction to 90.54% without innate immunity indicates that the system's ability to rapidly identify and respond to known threats based on predefined rules is crucial. The performance drop to 91.84% without adaptive immunity underscores the importance of the system's ability to learn and adapt over time to evolving threats.

Similarly, on the KDD-CUP-99 dataset, there is a significant performance decline from the full system's 87.64% to 83.45% without feature processing, illustrating that raw data may contain noise or irrelevant information that, unless processed, can hinder the system's detection capabilities. The innate immunity's impact is also notable, with performance falling to 82.12%, which could indicate the importance of having predefined rules or patterns for quick identification of common threats. The adaptive immunity's contribution is confirmed by a decrease to 87.02%, suggesting that learning from past experiences and adapting to new types of attacks is essential for maintaining high performance in anomaly detection.

The variations in performance across different datasets also provide insights into the nature of each dataset and the types of attacks or anomalies present within them. For datasets where the decline is less pronounced when a module is removed, it may suggest that the specific threats present in that dataset are less reliant on the capabilities provided by the removed module.

In conclusion, the ablation study within this table illustrates the vital roles that feature processing, innate immunity, and adaptive immunity play in the VC-AIS module's operation. Each component contributes to the system's robustness and accuracy, ensuring comprehensive threat detection and enhancing the VC-ADIS module's reliability as a security mechanism

in IoT networks.

## 5. CONCLUSION AND FUTURE DIRECTIONS

VC-ADIS's Variational Clonal Selection Method may adapt to different network traffic patterns. Dendritic processes help the VC-ADIS interpret and integrate complicated data representations, improving detection and make it adaptive for the new types of attacks.In comparison with Random Forests, Naive Bayes, and Decision Trees, VC-ADIS has greater accuracy, F1-scores, and generalization across network settings and attack vectors. Deep NNs operate similarly but lack in VC-ADIS's self-adaptive features, important for Security in a Dynamic IoT Environment.

Experimental Results show VC-ADIS demonstrates superior performance compared to the other models in Different Benchmark Datasets dataset such as KDD-CUP- 99 dataset,MQTT-IoT-IDS2020, MQTTset dataset, UFPI-NCAD-IoT-Attacks and UNFW-NB-15 mainly for MQTT-IOT-IDS 2020 and The Bot-IoT dataset, VC-ADIS gets a mean accuracy of 89.06% and a macro F1-score of 86.48%.

We are also trying to develop a more efficient non-data-based innate immunity mechanism so that intrusion in the normal data flow can be flagged in O(1) time and monitored in real-time by a moderator. Our research aims to improve the architecture of IoT devices to provide a low-cost security module based on cached memory mechanisms [18], reducing the time between AIS layers and ensuring data security without human intervention.

## REFERENCES

[1] B. Thakur, "A survey on internet of things (iot) security : Challenges and current status," 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:245903650

[2] O. Lifandali and N. Abghour, "Deep learning methods applied to intrusion detection: Survey, taxonomy and challenges," *2021 International Conference on Decision Aid Sciences and Application (DASA)*, pp. 1035–1044, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:246289590

[3] X. Liang and Y. Kim, "A survey on security attacks and solutions in the iot network," *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0853–0859, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:232316944

[4] T. Kumar, A. Sharma, S. Dutta, J. Sachin, G. Dutta, and R. P. Sharma, "A concise review of immune system and natural immune modulators," *International Journal of Pharmaceutical Sciences Review and Research*, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:238824403

[5] D. P. Kingma and M. Welling, "An introduction to variational autoencoders," *ArXiv*, vol. abs/1906.02691, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:174802445

[6] J. M. Vidal, A. L. S. Orozco, and L. J. G. Villalba, "Adaptive artificial immune networks for mitigating dos flooding attacks," *Swarm Evol. Comput.*, vol. 38, pp. 94–108, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:36071267

[7] C. Ramdane and S. Chikhi, "Negative selection algorithm : Recent improvements and its application in intrusion detection system," 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:53349523

[8] R. K. Das, S. Dash, R. K. Mishra, and A. Panigrahy, "E-clonalg: A classifier based on clonal selection algorithm," *Transactions on Machine Learning and Artificial Intelligence*, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:64343503

[9] D. P. B. S. S. Vineeta Soni, Narendra Singh Yadav, "Dais: deep artificial immune system for intrusion detection in iot ecosystems," *International Journal of Bio-Inspired Computation*, vol. 23, pp. 148–156, 2024. [Online]. Available: https://doi.org/10.1504/IJBIC.2024.137904

[10] É. Vivier, D. H. Raulet, A. Moretta, M. A. Caligiuri, L. Zitvogel, L. L. Lanier, W. M. Yokoyama, and S. Ugolini, "Innate or adaptive immunity? the example of natural killer cells," *Science*, vol. 331, pp. 44 – 49, 2011. [Online]. Available: https://api.semanticscholar.org/CorpusID:15163504

[11] D. P. Kingma and M. Welling, "An introduction to variational autoencoders," *ArXiv*, vol. abs/1906.02691, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:174802445

[12] R. Pinto, G. Gonçalves, J. Delsing, and E. Tovar, "Incremental dendritic cell algorithm for intrusion detection in cyber-physical production systems," in *Sai*, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:237962691

[13] L. Breiman, "Random forests," *Machine Learning*, vol. 45, pp. 5–32, 2004. [Online]. Available: https://api.semanticscholar.org/CorpusID:89141

[14] J. R. Quinlan, "Induction of decision trees," *Machine Learning*, vol. 1, pp. 81–106, 1986. [Online]. Available: https://api.semanticscholar.org/CorpusID:13252401

[15] H. Zhang, L. Jiang, and L. Yu, "Attribute and instance weighted naive bayes," *Pattern Recognit.*, vol. 111, p. 107674, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:224953147

[16] K. Wawryn and P. Widuliński, "Detection of anomalies in compiled computer program files inspired by immune mechanisms using a template method," *Journal of Computer Virology and Hacking Techniques*, vol. 17, pp. 47–59, 2021.

[17] J. Sinha and M. Manollas, "Efficient deep cnn-bilstm model for network intrusion detection," in *Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition*, 2020, pp. 223–231.

[18] Y. Lu and J. Lu, "A universal approximation theorem of deep neural networks for expressing probability distributions," *Advances in neural information processing systems*, vol. 33, pp. 3094–3105, 2020.