Integrating Novel Mechanisms for Threat Detection in Enhanced Data Classification using Ant Colony Optimization with Recurrent Neural Network

Vivek alias M. Chidambaram [*1], Karthik Painganadu Chandrasekaran[2]

[1] Research Scholar Department of Data Science and Business Systems, School of Computing, SRM Institute of Science and Technology, Kattankulathur.

[2] Associate Professor Department of Data Science and Business Systems, School of Computing, SRM Institute of Science and Technology, Kattankulathur.

Emails: vc8352@srmist.edu.in; karthikc@srmist.edu.in

Abstract

In new technologies like fog computing, edge computing, cloud computing, and the Internet of Things (IoT), cybersecurity concerns and cyber-attacks have surged. The demand for better threat detection and prevention systems has increased due to the present global uptick in phishing and computer network attacks. In order to identify irregularities and attacks on the network, which have increased in scale and prevalence, threat identification is essential. However, the community is forced to investigate and create novel threat detection approaches that are capable of detecting threats using anomalies due to the increase in network threats, the growth of new methods of attack and computations, and the requirement to ensure security measures. A novel mechanism is employed to identify threats in a data based on optimized deep learning. The main aim of this paper is the usage of data classification system based on Deep Learning (DL). The proposed mechanism employed the TCP (Transmission Control Protocol) communication protocol to extract data from loud IoT (Internet of Things) networks for the purpose of threat detection. To perform feature extraction an Ant Colony Optimization (ACO) is utilised, through Recurrent Neural Network (RNN), the attacks in data are classified and detected. Additionally, the suggested approach has been evaluated and trained using the BOUN DDoS contemporary dataset, which comprises a variety of attack types and allows for the effectiveness of the framework to be determined to compare it to previous approaches. The Findings indicate that the suggested approach achieved higher accuracy in DDoS attack identification in comparison with Traditional deep learning methods. The existing method detects the generic attack with lower efficiency however; the proposed mechanism achieves better accuracy in both the detection of the DDoS attack and the detection of regular traffic.

Keywords: Threat Detection; Data Classification; Deep Learning (DL); Recurrent Neural Network (RNN); Ant Colony Optimization (ACO)

1. Introduction:

Cybersecurity has benefited substantially from the advancement of Artificial Intelligence (AI) technologies in recent decades. DDoS attacks, which have increased over a period of time, are one important problem in cybersecurity(Nishant, Kennedy, and Corbett 2020). With the fast growth of technologies for networks like 5G, computing via the cloud, and Internet of Things (IoT), the enormous volume of data produced by the network has created significant issues and problems for network security, an area of study that has drawn greater attention (Wang et al. 2021). By immediately creating massive amounts of unauthorized traffic, DDoSattacks prevent genuine users from using services, affecting victims their credibility, goods, and prospective consumers(De Neira, Kantarci, and Nogueira 2023). Due to an increasing demand on the internet infrastructure brought on by the COVID-19 pandemic breakout in 2020, there has been a noticeable strengthen in DDoS attacks. As numerous companies offer services, they must continue operating without interruption. As a result, any interruptions brought on by a hacked technology can cause great financial and reputational harm(Shieh, Nguyen,

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

and Horng 2023). In the quarterly analysis of DDoS attacks, Cloudflare, a provider of Contents Delivering Network (CDN), claims that a sizable number of distributed denial of service (DDoS) assaults are launched every month(Najafimehr, Zarifzadeh, and Mostafavi 2023).

In the past, two main techniques have been used to identify network breaches and malware. The company network is equipped with an intrusion prevention system (IPS), which uses signature-based techniques to check network rules and patterns. It produces the necessary attack alarms, also known as safety incidents, and communicates the generated warnings to external structure, like SIEM. The security information and event management (SIEM) were concentrating on gathering and handling the IPS warnings. Amongst the different safety options, the SIEM is one of the most popular and reliable option for analysing the gathered security incidents and records. Additionally, security specialists work to evaluate abnormal alerts based on guidelines and thresholds and to find fraudulent behaviour by looking at correlations between occurrences and applying attack-related knowledge. However, because to the high percentage of false alarms and the vast volume of safety information, incursions over intelligent network infrastructures are still challenging to recognise and prevent(Lee et al. 2019). Even if the majority of fraudulent traffic reports are under 500 Mbps, this level of traffic has the power to momentarily disrupt several company systems. Attacks that are targeted with an optimal throughput of 100 Gbps happen every quarter, resulting in significant service outages, possible data centre delays, and ultimately lost income for vendors of services.

The existing research (Gaurav et al. 2022)demonstrates that DDoS attack tactics are always evolving. Protecting against new hazards with out-of-date remedies is inadequate(Sommese et al. 2022). A method that makes it easier for the current intrusion detection system (IDS) to identify unfamiliar data properties is therefore required. Telecom professionals could detect secret intrusion with the use of this method. Significant advancements in AI technology have been made in the last few decades, and the work that goes along with it is being used in a variety of fields, including cybersecurity(Mittal, Kumar, and Behal 2022). Deep learning-based IDSs are available in a variety of forms, and exhibit impressive accuracy. Studies that are relevant show that more than 90% of conventional DDoS can be correctly identified(Kim, Shin, and Choi 2019). Therefore, machine learning algorithms for identifying threats have received more attention in the most current research in the domain of security detection. The development of AI-related domains can help security experts investigate network attacks quickly and automatically.

A traditional IDS fails to classify new types of threats as unexpected and incapable of defending against them if it encounters them. As a result, an IDS is required that, rather than classifying data as either positive or negative, it can alert a telecommunication operator immediately of any strange traffic for analysis at the start of an assault (Yang and Lim 2021) . This is especially important when it is clear which hazards are present today and which ones were there in the past. In the case of an attack made up of distinct core elements, the defence technique's adaptation will be crucial. This can mean that the issue is no longer related to how effective the instruction was. The datasets used for training and testing might both be updated to address the current problem. The model has a sizable problem with respect to unidentified traffic, and the unidentified set provides a more complicated situation compared to the enclosed set. The integration of novel mechanisms entails exploring innovative approaches to enhance the feature extraction process, improve model interpretability, and strengthen the robustness of deep learning models against adversarial attacks. These mechanisms may include the incorporation of attention mechanisms, transfer learning(Ullah et al. 2022), generative adversarial networks (GANs) (Huang et al. 2021), multi-modal fusion techniques, and ensemble learning methods (Liu and Lang 2019). Additionally, optimization techniques such as network pruning (Rao et al. 2021), quantization (Arul and Punidha 2021), and architecture search will be explored to improve the efficiency and computational requirements of deep learning models without compromising performance.

The outcomes of research have significant implications for various real-world applications that rely on accurate threat detection. By improving the accuracy, interpretability, and resilience of data classification systems, the integration of novel mechanisms into optimized deep learning algorithms can enhance security measures, improve decision-making processes, and minimize false positives and false negatives. Furthermore, the insights gained from this research can drive advancements in other domains that rely on data classification, such as medical diagnostics, object recognition, and visual search. The contributions of the proposed mechanism for threat identification in a data classification system based on optimized deep learning are:

- ACO mechanism is applied for feature extraction in the data classification system which aims to enhance the performance of the deep learning model by extracting relevant features from the input data.
- The proposed approach employs RNN, a type of deep neural network that can effectively model sequential data, for the classification and detection of attacks in data.

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

- The suggested approach is evaluated and trained using the BOUN DDoS contemporary dataset, which encompasses various attack types and provides a benchmark for assessing the effectiveness of the framework.

The rest of the paper is structured as follows: Section 2 gives an overview of relevant studies and Section 3 covers the approach's research gap. The approach is presented in Section 4, which describes the structure of the proposed framework. Section 5 goes over the findings and performance analysis. Finally, Section 6 summarises the conclusion of research.

2. Related works:

The internet of things (IoT), cloud-based computing, and other remarkable breakthroughs in communication have created major issues with security. Currently, numerous artificial intelligence (AI) powered responses, involving recognition of intrusions, were developed for a variety of security-related uses. Fatani et al.(2021) proposed an effective AI-driven intrusion detection system (IDS) to safeguard IoT devices. We make use of deep neural networks and metaheuristic (MH) technique gains, which have been proven effective at addressing severe technical issues. Convolutional neural networks (CNNs) are used in this proposed feature extraction approach to retrieve pertinent characteristics. Additionally, using the parameters of the difference evolution (DE) technique, researcher create a novel choosing features technique employing a novel version for the transient search optimisation (TSO) procedure, termed TSODE. Eventually suggested that TSODE make greater usage of its DE to balance the exploring and exploiting stages. Further, research analyse the effectiveness of the created procedure, which attained enhanced accuracy in comparison with a number of current methodologies, using three open datasets and CICIDS-2017. For further development, various MH optimizers for IDS with various information will be taken into consideration.

Wu et al.(2022) suggests a Joint Semantic Transfer Network (JSTN) for successfully identifying intrusions into a massive, poorly tagged IoT environment. The JSTN combines a knowledge-rich network intrusion (NI) sector and modest IoT intrusion (II) sector as the source domains as part of the multi-source heterogeneous domain adaptation (MS-HDA) technique while maintaining basic cognitive characteristics in order to aid in targeted II domain detection of intrusions. To acquire a domain-invariant and selective description of features, the JSTN mutually transmits the three semantics listed below. In order to facilitate transmit of knowledge through a discriminator and classified distribute data conservation, the given situation semantics supplies source NI and II sector with features from one another. Additionally, it decreases the source-target disparity for achieving field invariance for the linked array of features. The starting point classified population is transferred to the desired area using its weighted implicitly semantics exchange, which also improves distinction through the retention of extremely fine information. The important ranking during the retention of knowledge is guided by the source-target dispersion that indicates the level of knowledge acquired. Extensive tests on a range of tasks demonstrate the JSTN's effectiveness over modern comparison techniques; on typical, an accuracy improvement of 10.3% is made. The computing expenses of the JSTN framework is relatively high considering that the algorithm training will be carried out on devices with relatively abundant resources

In view of the unique features of these systems and the discomfort of operators of Essential Infrastructure to perform actions indicating delay, the implementation of security tracking and control techniques is difficult. As precise virtual representations of actual processes, Sousa et al. (2021) digital twins can offer reliable platform for safety analysis or assessment of prospective mitigation approaches to be used in response to certain conditions. The article outlines an off-premises strategy for creating and deploying Digital Twins for safeguarding critical infrastructures that was developed as part of the ELEGANT project, despite the fact that on-premises distribution can be expensive. The creation of Digital Twins makes it easier to design and test machine learning algorithms to defend against security threats like Denial of Service (DoS) attacks. This is done in conjunction with adaptable and efficient data collection techniques. The Fed4Fire merged testing facilities were used in ELEGANT's testing method to assess the viability of applying cloudified Digital Twins. The obtained results show that, in DoS and Global Denial of Service attack situations, where huge amounts of data are created, the data pipelines supporting an ELEGANT Digital Twins exhibit a little effect on consumption of resources. More study is needed on how to implement the Digital Twin as a Service (DTaaS) with SmartGrids that are driven by 5G networks, related virtualization and edge computing.

Technology has advanced dramatically in recent years, making it possible for businesses to operate smoothly and revolutionising global connections. In intelligent settings Wi-Fi networks are used by the gadgets for communication. These electronic devices not only offer advantages but also security risks. Rahman et al. (2021) explore and make use of efficient selection of features strategies to enhance IDS by ML approaches. The deep feature extraction generates new features for the network's traffic using deep learning methods from artificial

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

based neural networks in a kind of independent autoencoder. The framework then uses a variety of wrapper-based feature selection approaches, such as Naive Bayes, SVM and decision trees to choose highly-ranked features depending on the presence of cumulative features. These features are subsequently merged as well as fed into a neural network-based classifier to differentiate between attack and usual behaviours. The research results demonstrate the efficiency of the suggested approach on Aegean Wi-Fi Attack Dataset, achieving high recognition precision of a maximum of 99.95%, which is reasonably comparable to the previous method used on the dataset. Further studies could improve the method to recognise more types of attacks other than the impersonation attack which has been detected.

To improve the capability of machine learning algorithms to detect threats in Internet of things (IoT) data from networks analysis, research is done by Alwasel et al. (2023) merging graph theory along with it. To determine if graph theory modelling is effective in enhancing the precision of classification, method that included data pretreatment, representation, feature evaluation, and artificial intelligence technique comparison. This study invented a graph-based format of network-related data, where node represented by devices and edges for communication events. These graph properties were subsequently included ML frameworks. The results show that the studied ML models, such as SVM, K-means clustering and LR perform modestly better when graph theory is applied to the study of network data. The outcomes highlight the importance of graph theory representation for boosting machine learning capacity for discrimination when used with network data. Future work should focus on refining the categorization technique to better discriminate between legitimate and malicious network traffic.

To early protect IIoT systems the researcher suggests a powerful and autonomously threat identification technique. Bibi, Akhunzada, and Kumar (2023) proposed unique Cuda-enabled Convolutional LSTM2D (ConvLSTM2D) method is extremely scalable and has the ability to self-optimize to effectively counter many dynamic versions of growing IIoT complex attacks and threats. 21 million instance, state-of-the-art dataset that included a variety of attack types and common vectors of threat for a thorough examination were used. The suggested method is also contrasted with benchmark methods and process that we have built. With a negligible loss in speed efficiency, the suggested method surpasses threat intelligence and has high detection accuracy. research must increase detection precision and reduce computational difficulty is required.

3. Problem statement:

The problem addressed in the above research works is the need for effective security measures emerging technologies such as the Internet of Things (IoT) and cloud-based computing. These technologies have introduced significant security challenges, requiring robust intrusion detection systems (IDS) to protect IoT devices and secure crucial infrastructures. The research work proposes data classification system based on Deep Learning (DL), thus to perform feature extraction an Ant Colony Optimization (ACO) is utilised. Through Recurrent Neural Network (RNN) the accuracy and efficiency of intrusion detection is enhanced. The goal is to develop advanced systems that can effectively identify and mitigate intrusions, improve recognition of different types of attacks, and provide reliable security analysis and assessment for real-world scenarios.

4. Proposed Threat Detection in Data Classification approach:

The model execution takes six essentials into account. The suggested hybrid model's overarching structure for identifying and categorising attacks is summarised in Figure 1. To create a normalised, balanced, and diversified dataset to use in training the suggested model, the data must first be cleaned. The strategy is to keep the highly variable features while applying a dimension reduction. Following data cleansing, assaults are categorised in order to aggregate attacks with comparable impacts on network behaviour or damage and to categorise cyberattacks of a similar type under a single label. In order to equalise the dataset and produce a number of datas, feature normalisation and data generation are later assumed. This is done by converting every traffic record into an 8*8 data with an 8-bit depth. To put into practise a mixed intrusion detection model that combines the ACO and RNN algorithms, using the former for feature extraction and the latter for threat categorization and detection. The efficiency of the proposed approach is then assessed by contrasting it with earlier strategies.

5. Data Collection

Researchers chose the entire BOUN DDoS the data set, which is divided into two classes: DDoS attacks created by floods TCP SYN and assault-free network traffic, for the suggested approaches' evaluation. The above can be used to efficiently test network-based DDoS detection methods or systems. The attacks are directed at the lone victim’s server, which is a part of the campuses' backbone router. Attack packets comprised IP addresses used as spoof sources that were chosen at randomly. The information in the trace, which was captured on the backbone,

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

includes over 4000 active hosts. The BOUN DDoS database contains a staggering amount of NTF records (9,335,605 records overall), which is a lot over nine million records. In order to decrease the amount of observations, we suggest using the NTF records frames method. Assuming the fact that are using a four-node federalism and that each node has a unique localised dataset (in this instance, a partition of the entire BOUN DDoS dataset), construct four dataset divisions using the entire BOUN DDoS dataset to mimic federation with its nodes (Toldinas et al. 2022).

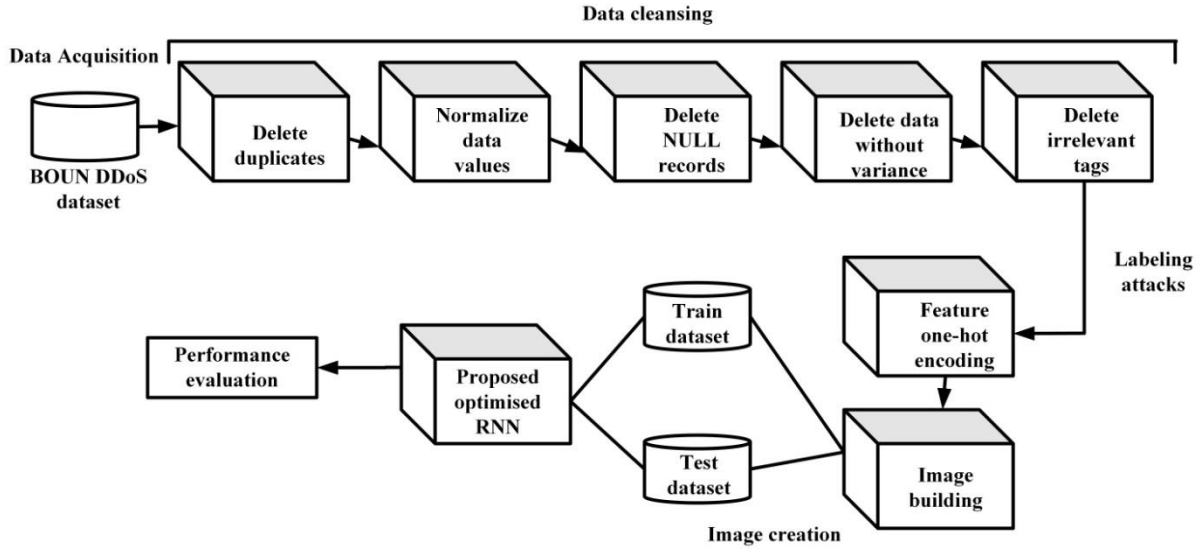

Figure 1: Overall workflow of the proposed system.

The proposed mechanism employed the TCP (Transmission Control Protocol) communication protocol to extract data from loud IoT (Internet of Things) networks for the purpose of threat detection. In this scenario, IoT devices generate a significant amount of network traffic, making it challenging to identify potential threats within the data stream. By utilizing TCP, which provides reliable and ordered transmission of data, the mechanism establishes a robust and consistent connection with the IoT devices. This enables the systematic collection of data packets from the noisy IoT network, allowing for efficient analysis and identification of potential threats. By employing TCP-based data extraction, the mechanism enhances threat detection capabilities, enabling real-time monitoring and response to security incidents in IoT environments.

6. Normalization of Data

It is believed that several characteristics' maximum and lowest value ranges are excessively wide and require some pre-processing before dataset normalisation. First, the range is shortened using a function that is logarithmic. Due to the fact that all features' measures are based on lengths, times, or quantities, they are all in the positive domain. Zero value is yet conceivable. Therefore, a unit is added to each number before using the logarithmic function. The next thing to do is to use Eqn (1) to produce a linear normalisation.

$$x''_{0i} = \frac{x'_{0i} - \min(x'_{0i})}{\max(x'_{0i}) - \min(x'_{0i})} \quad (1)$$

Where x''_{0i} is the normalised value and x'_{0i} = ln (x_{0i}+ 1). Through this normalisation, the characteristics of the data set have been condensed to a range between 0 and 1. The outcome of a descriptive study that divides harmless from malicious traffic, or groups all attacks into a single class, reveals that attacks often send more data packets than they receive, and this is to be predicted in attacks like a DoS attack. Additionally, the total number of packets transmitted reveals that there is higher variety in the attacks, tending towards values nearer to zero. For training the framework and communicating the findings, these factors are crucial.

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

7. Extraction of feature using Ant Colony Optimization

The main inspiration for this method came from how colonies of ants behave when foraging. Ants are extremely sociable insects which prioritize group survival over individual fulfilment for the species. In addition to pheromones, ants also interact with one another through touching and noises. Pheromones are organic substances that ants create that promote interaction between other ants from the same species. These substances function as hormones throughout the tissues of the ants that produce them and can influence how other ants behave. Since the majority of ants are underground, they utilize the top layer of the soil to lay down pheromone that other ants may detect and pursue. Ants begin to move aimlessly in the vicinity of their place of residence in looking for food. Numerous paths from the village to the supply of food become available as a result of such random search. As a result, ants deliver a tiny bit of food with the appropriate pheromone quantities, depending on the kind and amount of food. These signal releases would serve as a cue to food resources, with the chance that subsequent ants would follow them in a specific direction. Without a doubt, the rate and volume of pheromone dispersion affect this ability. Given that pheromones rate of evaporating is another important factor, it can also be observed that the duration of every route is properly compensated. Creating a solution, initializing the pheromone, and maintaining the pheromone are some of the steps that ACO algorithms commonly take. The process of creating solutions and upgrading pheromones continues till a terminal state (Fahad et al. 2020).

The nearest neighbors of the current location's grey levels are determined in order to establish the boundary. The neighbors are discovered from the current position by taking eight connection factors into account, much like the convolution mask techniques. Each ant visits a cell nearby and increases its pheromone concentration there. Eqn. (2) provides an illustration of the likelihood of being transferred from the state i to j.

$$N_{a,b} = \frac{(\sigma_{a,b}^{\gamma})(\rho_{a,b}^{\delta})}{\sum U \epsilon T (\sigma_{a,b}^{\gamma})(\rho_{a,b}^{\delta})} \quad (2)$$

Where $\rho_{a,b}^{\delta}$ is the degree of the heuristic functions that indicates the likelihood of selecting b,$(\sigma_{a,b}^{\gamma})$ is the density of pheromones along the route from a to b and regulate how heavily the pheromones and heuristic function are weighted. To divide the answer, each of the node' pheromones and heuristics levels that are connected to the a^{th} node are combined. The next node is selected based on the $N_{a,b}$ values of a node. After the ant completes its journey, the pheromone and path are adjusted, as stated in Eqn. (3).

$$\sigma_{a,b}^{'} = \sigma_{a,b} + \sigma_{a,b}.\left[\left(1 - \frac{1}{1+N_{a,b}}\right)\right] \quad (3)$$

Where the pheromone's previous level is$\sigma_{a,b}$. The quantity of ant movements along a route causes the concentration of pheromones to rise. In addition to changing the pheromone's concentration along every path, the ant approach also causes some of the pheromones to dissipate.

$$\sigma_{a,b} = (1 - \tau).\sigma_{a,b}^{'} + \Delta\sigma_{a,b} \quad (4)$$

Where $\Delta\sigma_{a,b}$ represents the ant's fitness along the path, and represents the percentage of pheromone that evaporates. The method ends when the convergence criteria is met after a certain number of cycles.

8. Classification and Detection based on Recurrent Neural Network

A directed loops in the RNN model (Merrill et al. 2020) analyses the error rate of current invisible layer with that of the preceding hiding layer and modifies the weights that are distributed among the hidden layers in a single-way transfer of data from the input of the units to the units that are hidden. A straightforward RNN design with two layers that are hidden is shown in Figure 2.

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

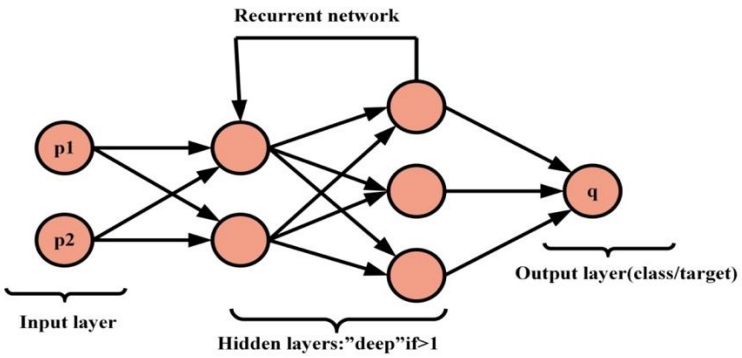

Figure 2: Recurrent Neural Network architecture

Conventional Feed-Forward Neural Networks (FFNNs) are expanded upon by RNN. There are no repetitions or loop in FFNNs; instead, data simply travels forward, from the inputs of the nodes via the nodes that are hidden to the resultant nodes. Conventional FFNNs do not require hidden layers. Assumed are a source vector order, an undetectable vector order, and a result vector sequence, each represented by the letters P, M, and R. The formula for an input vectors sequence is P = $(p_1, p_2, \dots, p_T)$. Using t = 1 to T, a typical RNN computes the undetectable vectors sequence M = $(m_1, m_2, \dots, m_T)$ and the resulting vectors sequence Q = $(q_1, q_2, \dots, q_T)$ as follows:

$$m_t = \sigma(W_{pm} p_t + W_{mm} m_{t-1} + b_m \quad (5)$$

$$q_t = W_{mq} m_t + b_q \quad (6)$$

Where W is a weighted matrix, b is a biased component, and function is a nonlinear activating function. In Equation (5), the terms m_t and m_{t-1} refer to the outputs of the prior and current hidden layers, respectively.

Back-propagating over time (BPTT) and real-time recurrent learning (RTRL) are two gradient-based techniques that RNN utilise for learning time sequences. When an order is processed in order to create an FFNN in BPTT, the network's structure is unfurled into a multi-layered FFNN. The resultant error gradients is retained for every run after the model has been trained using training data. Each FFNN is trained using the usual backpropagation algorithm utilising BPTT, and the weights are updated utilising the total of the gradient of every one of the networks layers' weights.

When the RNN design gets more complicated, the gradient established by the layer that is hidden from back propagation may vanish or explode. Gradient trimming can deal with gradient eruptions, but it has been unable to fix gradient disappearing. Consequently, RNN finds it difficult to precisely gather the relationship between text parts over the vast distances present in a text sequence. The use of a long short-term memory (LSTM) can solve these problems. The key component of an LSTM is the cell's state. Additionally, it contains three distinct gate architecture types: inputs, outputs, and forget (Talasila et al. 2020).

$$h_{0s} = \sigma(U_{h_0} . [f_{s-1}, a_s] + v_{h_0} \quad (7)$$

$$p_{0s} = \sigma(U_{p_0} . [f_{s-1}, a_s] + v_{p_0} \quad (8)$$

$$w_{0s} = \sigma(U_{w_0} . [f_{s-1}, a_s] + v_{w_0} \quad (9)$$

$$T_{0_s} = h_{0s} \times t_{s-1} + p_{0s} \times tanh\,(U_{t_0} . [f_{s-1}, a_s] + v_{t_0} \quad (10)$$

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

$$f_s = w_{0s} \times \tanh(T_{0_s}) \quad (11)$$

The forgotten gate, inputs gate, and outputs gate constitute three multiplicative gates that are denoted by equation (7), (8), and (9) respectively. While the variables differ, the value entered in equation (7), (8), and (9) remains $[f_{s-1}, a_s]$ refers for the sigmoid activating function. In Eq. (10), the data entered from the previous time stage and t_{s-1} together define the cell's configurationT_{0_s}. Only when the gate that forgets h_{0s} has been set to 0, that completely eliminates the previous state, will the entered data be taken into consideration with the current stage. The input gate makes the decision if it wants to receive inputs at this certain time Whether or not to outputs the cell state is a decision made by the final output gate. Since an outcome, overfitting is avoided by using RST in training data, and RNN efficiency is increased by selecting the key characteristics.

9. Results and Discussions

The receiver operating characteristic curve (ROC), which is a graphical representation of how a binary classifier system's diagnostic effectiveness fluctuates as its discriminatory limits are modified, and a confusion matrix, which in the field of machine learning for the effectiveness of a supervised algorithm for learning, specifically, the problem of statistical categorization, were used in the study to evaluate the effectiveness of the experimental results.

The percentage of events that the system accurately observes is predicted with accuracy. Eqn. (12) presents the formula.

$$Accuracy = \frac{T_P + T_N}{T_P + F_N + T_N + F_P} \quad (12)$$

The number of true positive projections that fall under the positive categorization is a precision-based metric. The formula is shown in Equation (13).

$$Precision = \frac{T_P}{T_P + F_P} \quad (13)$$

Recall measures the number of precise class projections produced from each successful occurrence in the dataset. Eqn. (14) presents the formula.

$$Recall = \frac{T_P}{T_P + F_N} \quad (14)$$

10. Training progress of the proposed approach

During the training process of threat detection, the model's accuracy and loss were monitored over a course of five epochs, consisting of a total of 125 iterations. Each epoch was divided into 25 iterations, indicating the frequency at which the model's parameters were updated. The training was performed using a learning rate of 0.001, ensuring gradual adjustments to the model's weights and biases. Throughout the training, the validation accuracy steadily improved, reaching an impressive rate of 98.62%. This indicates that the model performed exceptionally well in correctly classifying threats in the given dataset. The validation accuracy was consistently high across all five epochs, demonstrating the stability and robustness of the model's learned representations. The entire training process took approximately 9 minutes, during which the model underwent iterative optimization, refining its performance and enhancing its ability to detect threats accurately. Table 1 demonstrates the outcome of the training progress

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

Table 1: Description of Training progress

Components	Outcomes
Validation Accuracy	98.62%
Elapsed Time	9 mins
Iteration per Epoch	25
Maximum Iterations	125
Frequency	50 Iterations
Learning rate schedule	Constant
Learning rate	0.001

The training process involved a meticulous monitoring of the model's accuracy and loss at each iteration. By assessing the loss, the model's performance was evaluated in terms of the disparity between predicted and actual threat labels. Simultaneously, accuracy measurements gauged the proportion of correctly classified threats. The validation accuracy of 98.62% indicates that the model excelled in identifying threats within the dataset. Figure 3 depicts the graph of accuracy and loss of the training progress

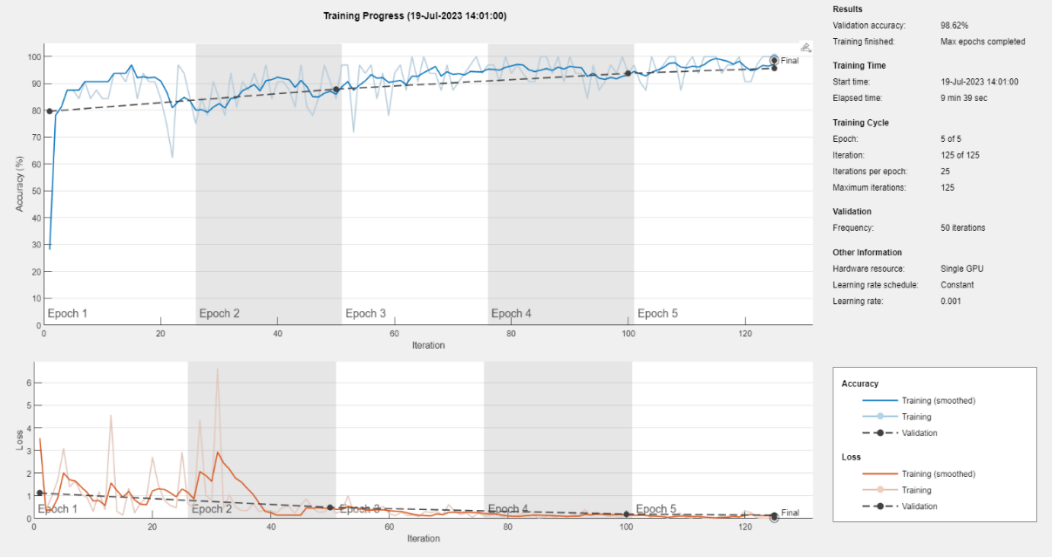

Figure 3: Accuracy and Loss of Training progress

The training process followed a structured approach, with 125 iterations meticulously executed over five epochs. Each epoch comprised 25 iterations, enabling the model to gradually learn and adjust its parameters based on the given training data. The learning rate of 0.001 facilitated a smooth optimization process, ensuring incremental updates to the model's weights and biases. With a consistent validation accuracy observed across all epochs, the model demonstrated its reliability and effectiveness in threat detection. The training duration of approximately 9 minutes showcased the model's efficiency in quickly learning and adapting to the given dataset, thereby enabling prompt and accurate threat detection.

11. Outcome of extraction process with TCP

When extracting data from the cloud, TCP (Transmission Control Protocol) offers several advantages over other protocols like UDP, ICMP, IPv6, IGMP, and GRE, particularly in terms of frame length and reliable data transmission. TCP, as a connection-oriented protocol, ensures reliable delivery of data by providing features such as error detection, acknowledgment of received packets, and retransmission of lost or corrupted packets. While the maximum frame length of TCP is typically determined by the underlying network technology, such as Ethernet with a standard maximum of 1500 bytes, TCP's reliability and flow control mechanisms make it suitable for handling larger data payloads. By ensuring data integrity and order, TCP enables efficient extraction of data from the cloud, minimizing the risk of packet loss or data corruption during transmission. Figure 4 shows the frame length of TCP.

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

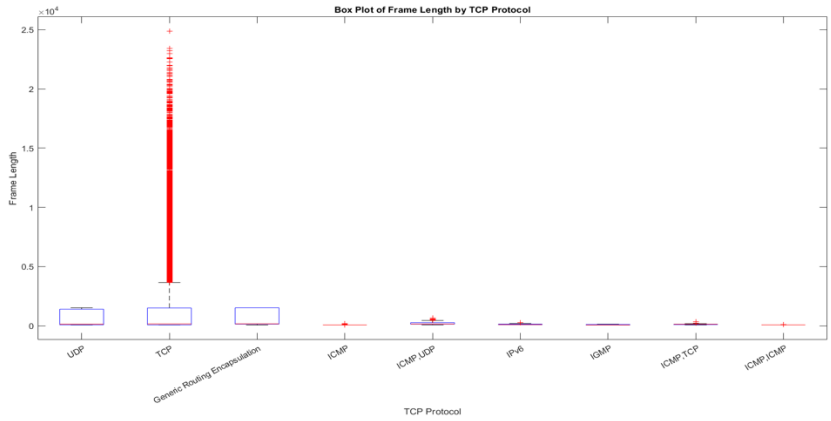

Figure 4: Frame Length of TCP

In threat detection, the source port and destination port in TCP (Transmission Control Protocol) are essential indicators for identifying potential security risks. The source port represents the port number from which the TCP packets originate, providing insights into the application or service initiating the communication. Table 2 shows the frame length in each time period.

Table 2: Frame length in each time period

Time	Frame length
0	68
0.000218	900
0.000233	171
0.000235	1500
0.000466	126

Meanwhile, the destination port signifies the intended recipient's port number, helping to identify the target application or service. Monitoring these ports allows security analysts to detect anomalies, such as port scanning activities or connections to unauthorized or unusual ports, which may indicate unauthorized access attempts or the presence of malicious activity. Analyzing the source and destination ports within TCP connections, along with other network attributes, enables the detection of suspicious patterns, unauthorized communication, and potentially harmful network traffic associated with various threats and attacks. Figure 5 shows the source and Destination port of TCP.

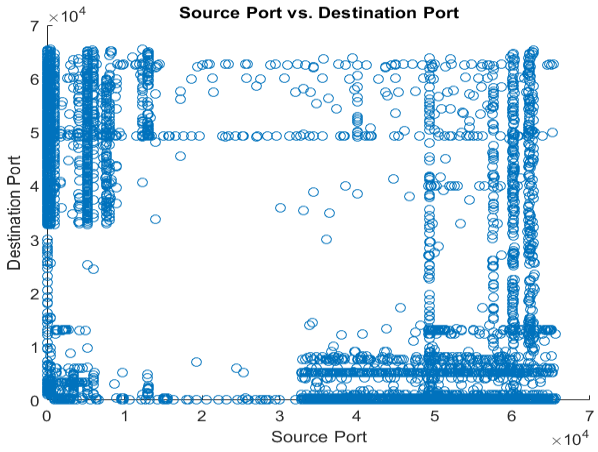

Figure 5: Source and Destination port of TCP

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

While extracting data from cloud with TCP, two histograms are used in threat detection such as frame length histograms and TTL (Time to Live) histograms. A frame length histogram represents the distribution of packet sizes in a network capture, which provides valuable insights into the size characteristics of TCP packets, allowing security analysts to identify anomalies such as unusually large or small packets that may indicate malicious activities like data exfiltration or evasion techniques. By examining the histogram's frequency distribution, patterns and outliers can be detected, aiding in the identification of potential threats. TTL histogram represents the distribution of TTL values within TCP packets. Analyzation of TTL values helped in understanding the network topology and identifying abnormal TTL values that may indicate suspicious or malicious behavior. By utilizing frame length histograms and TTL histograms in threat detection with TCP, security analysts can gain deeper insights into network traffic characteristics, identify deviations from normal patterns, and effectively detect potential threats or security breaches. These histograms serve as valuable tools for visualizing and analyzing TCP packet attributes, enabling proactive monitoring and the timely identification of suspicious activities within a network environment. Figure 6 depicts the histogram of both TTL and Frame length of TCP.

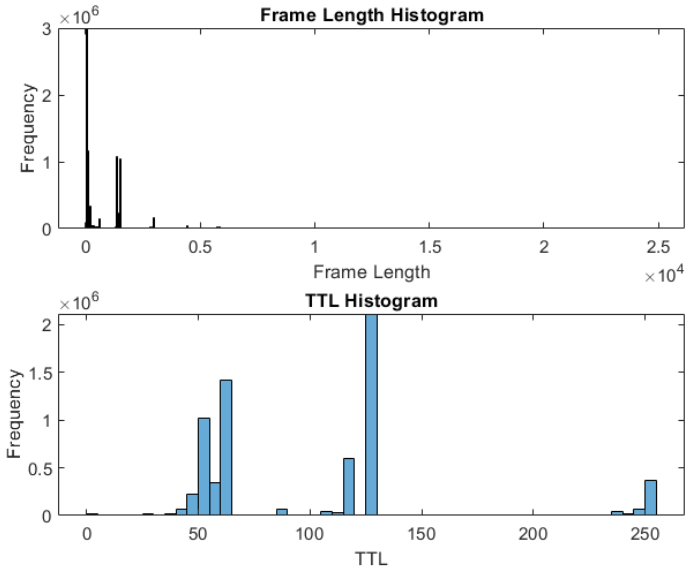

Figure 6: TTL and Frame length histogram of TCP

12. Performance Evaluation of the proposed approach

The area under the curve (AUC) provides another method for evaluating the median effectiveness of the classification approach; an efficient classifying method should be as close to the top left corner of the ROC curve as possible (TPR = 1, FPR = 0). The area under the curve (AUC) of the ROC curve is another approach to estimating the average performance of the algorithm for classification. An AUC value close to one implies that the classifier is effective. The model's AUC was 0.98. Figure 7 compares the suggested approach's ROC curve of attack and non- attack.

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

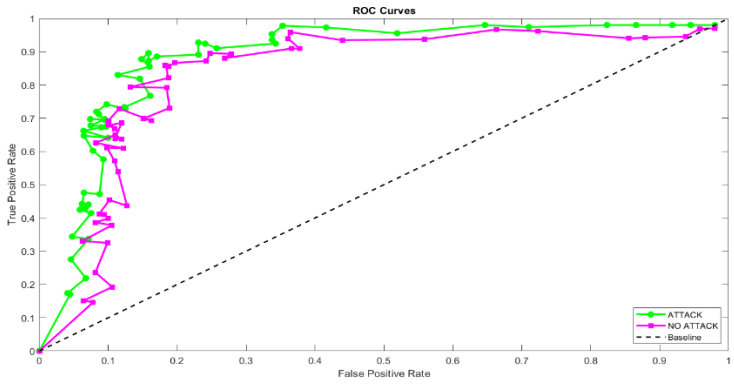

Figure 7: ROC of attack and No attack

To achieve better fitness improvement over iterations with the ACO algorithm for threat detection, several key factors come into play. It is important to define an appropriate fitness evaluation metric that aligns with the specific objectives of threat detection, such as accuracy, precision, recall, or F1-score. This metric serves as a guide for optimizing the algorithm's performance. Tuning of ACO parameters, including ant population size, and exploration-exploitation balance, can significantly impact the algorithm's convergence towards optimal solutions. Balancing exploration to discover new threat patterns and exploitation to reinforce successful detection strategies is crucial. Incorporating domain knowledge and expertise into the ACO algorithm, such as incorporating known threat indicators or behavior patterns, can enhance fitness improvement by leveraging prior understanding of threats. Finally, continuous evaluation, analysis, and adaptation of the algorithm's representation and parameters based on the evolving threat landscape and feedback from real-world threat data can further improve fitness over iterations. By considering these aspects, ACO can iteratively refine the threat detection system, leading to better fitness improvement and more accurate identification and mitigation of potential threats. Figure 8 shows the fitness improvement of ACO.

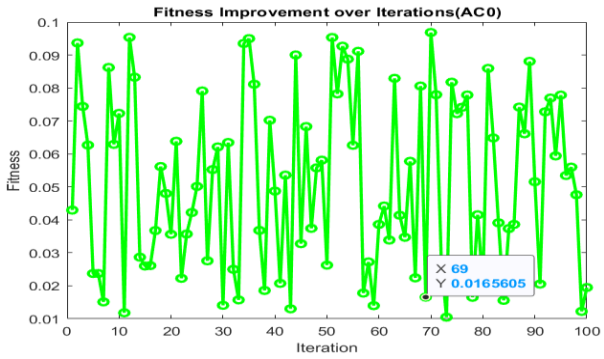

Figure 8: Fitness Improvement of ACO

The convergence curve represents the trend of fitness accuracy over successive iterations, indicating how quickly the algorithm converges towards optimal solutions. To improve the convergence curve with ACO, several factors need to be considered. Additionally, continuously analysing and adapting the representation, parameters, and knowledge based on real-world threat data and feedback helps refine the convergence curve over time. By considering these factors, ACO can improve the fitness accuracy over iteration convergence curve, leading to a more effective and reliable threat detection system. Figure 9 depicts the convergence curve of ACO.

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

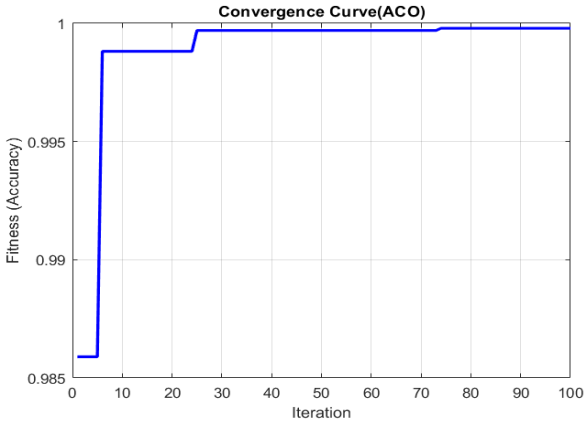

Figure 9: Convergence Curve of ACO

In threat detection, the task involves classifying data instances as either representing an attack or no attack. An attack refers to any malicious or unauthorized activity that poses a security threat to the system or network. It encompasses various types of malicious behaviors, including malware infections, intrusion attempts, data breaches, and denial of service attacks. No attack instances are considered normal and do not exhibit any signs of malicious or unauthorized activities. The goal of threat detection is to accurately distinguish between these two classes by analyzing various attributes and patterns within the data.

Table 3: Recall, F-measure and precision of Evaluation generalization

Type of traffic	**Precision**	**F-measure**	**Recall**	**Accuracy**
Attack	97.1%	98.0%	98.3%	98.6%
No Attack	98%	98.2%	96.6%	98%

Table 3 shows the performance metrics with attack and No attack in the data. The current test set has a detection accuracy of 98.62%. Figure 10 shows the graph of Generalization evaluation. According to the findings of the evaluation, Suggested model might acquire certain useful and generic properties from botnet data in order to identify anonymous attacks.

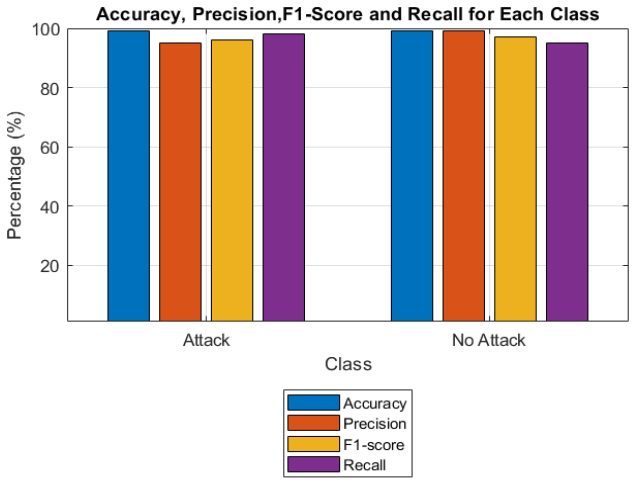

Figure 10: Efficiency of Attack and No attack

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

13. Comparison of Threat Detection with existing approaches

The study compares the outcomes to different approaches of data classification that detect threats. In comparison to the other computations, the CNN, DT, EM, and ACO-RNN algorithms are often better at detecting assaults. The ACO-RNN algorithms outperform the unsupervised ones across all algorithms. When training and testing times are taken into account and when they are neglected, respectively, ACO-RNN and CNN are found to be the best-supervised learning algorithms. While this is happening, EM emerges as the top unsupervised learning algorithm, both when training and evaluation time have been taken into account. Table 4 shows the performance metrics of the existing and proposed approach

Table 4: Performance of existing and proposed algorithm

Methods	Recall	Precision	Accuracy
Convolutional Neural Network (CNN)	0.98%	0.96%	0.96%
Decision Tree (DT)	098%	0.97%	0.97%
Naïve Bayes (NB)	0.97%	0.98%	0.97%
Expectation Maximization (EM)	0.60%	0.85%	0.62%
Proposed ACO-RNN	0.99%	0.99%	0.98%

These findings provide the standard deviation (SD) of accuracy for each tested mathematical representation of a certain algorithm. In addition, a few benchmark algorithms from this work outperform the outcomes of existing studies. The accuracy, for the algorithms is displayed in Figure11. This graph confirms the conclusion that the best fundamental algorithms for detecting attacks are DT, CNN, EM, and ACO-RNN

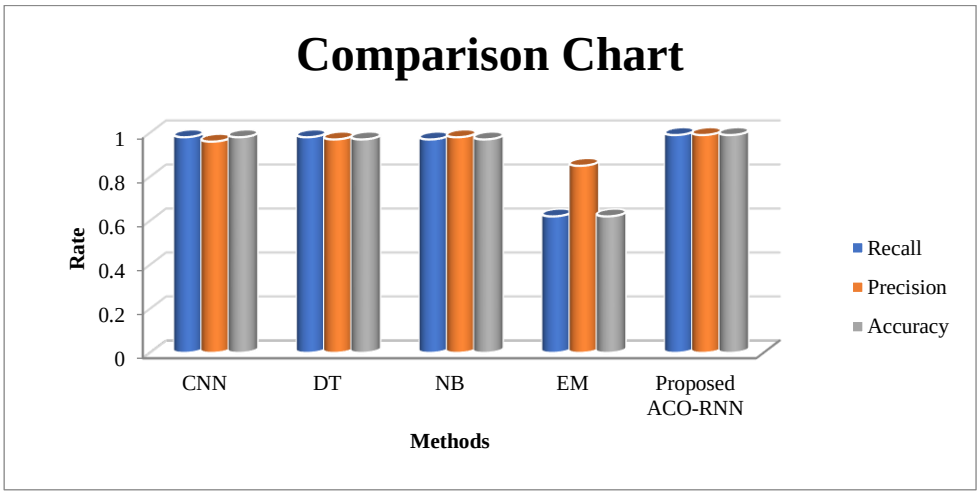

Figure 11: Comparison chart of proposed and existing methods

In the age of the fourth industrial revolution, artificial intelligence is among the mostly utilized systems because it enables networks to learn from experience and get better without needing to be explicitly programmed. In NIDS, machine learning techniques are frequently employed. Numerous NTF records are combined with publicly accessible datasets to categorize incursions.

14. Conclusion:

Cybersecurity worries and cyberattacks have increased in relation to emerging technologies including edge computing, cloud computing, fog computing, and the Internet of Things (IoT). The current global increase in scamming and computer network threats has raised the demand for stronger threat detection and prevention technologies. Threat detection is crucial in order to recognize network anomalies and attacks, which have grown in size and frequency. However, because of the rise in network traffic, the growth of new attack and computing techniques, and the need to provide security measures, the community is compelled to develop novel threat detection algorithms that are capable of identifying threats using anomalies. In a deep learning-based picture categorization system, a novel approach is used to spot risks. Main aim of this study is to use a Deep Learning-

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

based picture classification framework. As a result, Ant Colony Optimisation (ACO) is used to do feature extraction. The classification and detection of attacks in data are performed using recurrent neural networks (RNN). The BOUN DDoS current dataset, which includes a variety of assault types and enables the effectiveness of the framework to be determined and compared to earlier efforts, has also been used to evaluate and train the suggested approach. The outcomes demonstrate that the suggested strategy outperformed traditional deep learning algorithms in terms of DDoS attack identification accuracy. The proposed methodology achieves 98.62% accuracy in both the identification of the DDoS assault with the detection of common threats, while the existing method identifies the general attack with less efficiency.

References

[1] Alwasel, Bader, Abdulaziz Aldribi, Mohammed Alreshoodi, Ibrahim S. Alsukayti, and Mohammed Alsuhaibani. 2023. "Leveraging Graph-Based Representations to Enhance Machine Learning Performance in IIoT Network Security and Attack Detection." *Applied Sciences* 13 (13): 7774. https://doi.org/10.3390/app13137774.

[2] Arul, Easwaramoorthy, and A Punidha. 2021. "Supervised Deep Learning Vector Quantization to Detect MemCached DDOS Malware Attack on Cloud." *SN Computer Science* 2 (2): 85.

[3] Ambeth Kumar, V.D. Ramakrishnan,M. Ashok Kumar, V.D. Malathi,S. (2015). Performance Improvement using an Automation System for Recognition of Multiple Parametric Features based on Human Footprint. kuwait journal of science .42(1), 109-132.

[4] De Neira, Anderson Bergamini, Burak Kantarci, and Michele Nogueira. 2023. "Distributed Denial of Service Attack Prediction: Challenges, Open Issues and Opportunities." *Computer Networks* 222 (February): 109553. https://doi.org/10.1016/j.comnet.2022.109553.

[5] Fahad, Labiba Gillani, Syed Fahad Tahir, Waseem Shahzad, Mehdi Hassan, Hani Alquhayz, and Rabia Hassan. 2020. "Ant Colony Optimization-Based Streaming Feature Selection: An Application to the Medical Data Diagnosis." *Scientific Programming* 2020: 1–10. https://doi.org/10.1155/2020/1064934.

[6] Fatani, Abdulaziz, Mohamed Abd Elaziz, Abdelghani Dahou, Mohammed A. A. Al-Qaness, and Songfeng Lu. 2021. "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization." *IEEE Access* 9: 123448–64. https://doi.org/10.1109/ACCESS.2021.3109081.

[7] Gaurav, Akshat, Brij B. Gupta, Wadee Alhalabi, Anna Visvizi, and Yousef Asiri. 2022. "A Comprehensive Survey on DDoS Attacks on Various Intelligent Systems and It's Defense Techniques." *International Journal of Intelligent Systems* 37 (12): 11407–31. https://doi.org/10.1002/int.23048.

[8] Abhishek Kumar, Rini Dey, G. Madhukar Rao, Saravanan Pitchai, K. Vengatesan, V. D Ambeth Kumar, " 3D Animation and Virtual Reality Integrated Cognitive Computing for Teaching and Learning in Higher Education", Advances in Parallel Computing, 2021, 39, pp. 615 - 620.

[9] Kumar, A., Singh, K.U., Hsieh, SY., Kumar, V.D.A., Kumar, A. (2021). Distribution Key Scheme for Secure Group Management in VANET Using Polynomial Interpolation. In: Lin, L., Liu, Y., Lee, CW. (eds) Security and Privacy in Social Networks and Big Data. SocialSec 2021. Communications in Computer and Information Science, vol 1495. Springer, Singapore. https://doi.org/10.1007/978-981-16-7913-1_1

[10] Lee, Jonghoon, Jonghyun Kim, Ikkyun Kim, and Kijun Han. 2019. "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles." *IEEE Access* 7: 165607–26. https://doi.org/10.1109/ACCESS.2019.2953095.

[11] Liu, Hongyu, and Bo Lang. 2019. "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey." *Applied Sciences* 9 (20): 4396.

[12] Merrill, William, Gail Weiss, Yoav Goldberg, Roy Schwartz, Noah A. Smith, and Eran Yahav. 2020. "A Formal Hierarchy of RNN Architectures." arXiv. https://doi.org/10.48550/arXiv.2004.08500.

[13] Mittal, Meenakshi, Krishan Kumar, and Sunny Behal. 2022. "Deep Learning Approaches for Detecting DDoS Attacks: A Systematic Review." *Soft Computing*, January. https://doi.org/10.1007/s00500-021-06608-1.

[14] Najafimehr, Mohammad, Sajjad Zarifzadeh, and Seyedakbar Mostafavi. 2023. "DDoS Attacks and Machine-learning-based Detection Methods: A Survey and Taxonomy." *Engineering Reports*, May, e12697. https://doi.org/10.1002/eng2.12697.

[15] Nishant, Rohit, Mike Kennedy, and Jacqueline Corbett. 2020. "Artificial Intelligence for Sustainability: Challenges, Opportunities, and a Research Agenda." *International Journal of Information Management* 53 (August): 102104. https://doi.org/10.1016/j.ijinfomgt.2020.102104.

[16] Rahman, Md Arafatur, A. Taufiq Asyhari, Ong Wei Wen, Husnul Ajra, Yussuf Ahmed, and Farhat Anwar. 2021. "Effective Combining of Feature Selection Techniques for Machine Learning-Enabled

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024

IoT Intrusion Detection." *Multimedia Tools and Applications* 80 (20): 31381–99. https://doi.org/10.1007/s11042-021-10567-y.

[17] Rao, Sunil, Gowtham Muniraju, Cihan Tepedelenlioglu, Devarajan Srinivasan, Govindasamy Tamizhmani, and Andreas Spanias. 2021. "Dropout and Pruned Neural Networks for Fault Classification in Photovoltaic Arrays." *IEEE Access* 9: 120034–42. https://doi.org/10.1109/ACCESS.2021.3108684.

[18] Shieh, Chin-Shiuh, Thanh-Tuan Nguyen, and Mong-Fong Horng. 2023. "Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric." *Mathematics* 11 (9): 2145. https://doi.org/10.3390/math11092145.

[19] Sommese, Raffaele, Kc Claffy, Roland Van Rijswijk-Deij, Arnab Chattopadhyay, Alberto Dainotti, Anna Sperotto, and Mattijs Jonker. 2022. "Investigating the Impact of DDoS Attacks on DNS Infrastructure." In *Proceedings of the 22nd ACM Internet Measurement Conference*, 51–64. Nice France: ACM. https://doi.org/10.1145/3517745.3561458.

[20] Sousa, Bruno, Miguel Arieiro, Vasco Pereira, Joao Correia, Nuno Lourenco, and Tiago Cruz. 2021. "ELEGANT: Security of Critical Infrastructures With Digital Twins." *IEEE Access* 9: 107574–88. https://doi.org/10.1109/ACCESS.2021.3100708.

[21] Talasila, Vamsidhar, Kotakonda Madhubabu, K Madhubabu, M Mahadasyam, N Atchala, and L Kande. 2020. "The Prediction of Diseases Using Rough Set Theory with Recurrent Neural Network in Big Data Analytics." Al-Saedi, W., S. Lachowicz, D. Habibi, and O. Bass. 2013. Power flow control in grid-connected microgrid operation using particle swarm optimization under variable load conditions. International Journal Of Electrical Power & Energy Systems 49:76–85. doi:10.1016/j.ijepes.2012.12.017.

[22] Toldinas, Jevgenijus, Algimantas Venčkauskas, Agnius Liutkevičius, and Nerijus Morkevičius. 2022. "Framing Network Flow for Anomaly Detection Using Data Recognition and Federated Learning." *Electronics* 11 (19): 3138.

[23] Ullah, Farhan, Shamsher Ullah, Muhammad Rashid Naeem, Leonardo Mostarda, Seungmin Rho, and Xiaochun Cheng. 2022. "Cyber-Threat Detection System Using a Hybrid Approach of Transfer Learning and Multi-Model Data Representation." *Sensors* 22 (15): 5883. https://doi.org/10.3390/s22155883.

[24] Wang, Zhendong, Yong Zeng, Yaodi Liu, and Dahai Li. 2021. "Deep Belief Network Integrating Improved Kernel-Based Extreme Learning Machine for Network Intrusion Detection." *IEEE Access* 9: 16062–91. https://doi.org/10.1109/ACCESS.2021.3051074.

[25] Wu, Jiashu, Yang Wang, Binhui Xie, Shuang Li, Hao Dai, Kejiang Ye, and Chengzhong Xu. 2022. "Joint Semantic Transfer Network for IoT Intrusion Detection." arXiv. http://arxiv.org/abs/2210.15911.

[26] Yang, Jiwon, and Hyuk Lim. 2021. "Deep Learning Approach for Detecting Malicious Activities over Encrypted Secure Channels." *IEEE Access* 9: 39229–44.

[27] Balakrishnan, Chitra, and V. D. Ambeth Kumar. (2023). IoT-Enabled Classification of Echocardiogram Images for Cardiovascular Disease Risk Prediction with Pre-Trained Recurrent Convolutional Neural Networks. Diagnostics 13(4), 775

[28] Hemamalini, Selvamani, and Visvam Devadoss Ambeth Kumar. (2022). Outlier Based Skimpy Regularization Fuzzy Clustering Algorithm for Diabetic Retinopathy Image Segmentation. Symmetry, 14(12), 2512

[29] S. Hemamalini ,V. D. Ambeth Kumar ,R. Venkatesan,S. Malathi. (2023). Relevance Mapping based CNN model with OSR-FCA Technique for Multi-label DR Classification. Journal of Fusion: Practice and Applications, 11 (2), 90-110.

[30] C. S. Manigandaa,V. D. Ambeth Kumar,G. Ragunath,R. Venkatesan,N. Senthil Kumar. (2023). De-Noising and Segmentation of Medical Images using Neutrophilic Sets. Journal of Fusion: Practice and Applications, 11 (2), 111-123.

Doi : https://doi.org/10.54216/JCIM.140209
Received: January 07, 2024 Revised: March 13, 2024 Accepted: June 25, 2024