ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

ttps://doi.org/10.17559/TV-20230621000752
Original scientific paper

Hybrid Metaheuristics with Deep Learning Enabled Cyberattack Prevention in Software Defined Networks

P. B. ARUN PRASAD, V. MOHAN*, K. VINOTH KUMAR

Abstract: Software-Defined Networks (SDN) refers to a revolutionary pattern that separates the control plane from the data plane, converting the idea of a software-driven network. Cyber attackers had a target towards the SDN controllers to subdue the control planes that can be regarded as the SDN brain. It offers a plethora of functionalities like regulating flow control to routers or switches in the data plane below through southbound Application Programming Interfaces (APIs) and application logic and business in the application plane above through northbound APIs for implementing sophisticated networks. But the control plane is a tempting prospect for security attacks from adversaries due to its centralization features. The main concern is information safety in the network. To prevent the loss of extremely useful information, the Intrusion Detection System (IDS) has been formulated for recognizing the outbreak of a stream of attacks and notifying system administrators granting network security. With this motivation, this article develops a Hybrid Metaheuristics with Deep Learning Enabled Cyberattack Prevention (HMDL-CAP) model in SDN. The presented HMDL-CAP model initially carries out data preprocessing to scale the input data. Then,spiral dynamics optimization-based feature selection (SDOFS) algorithm is utilized for optimum selection of feature subsets. Next, hybrid convolutional neural network with recurrent neural network (HCRNN) model is applied to detect intrusions. As hyperparameter tuning is important, pelican optimization algorithm (POA) is used to tune the HRCNN parameters. To assess the experimental outcomes of the proposed model, a series of experiments were performed using benchmark dataset. The comparison study shows the promising performance of the HMDL-CAP model over recent models.

Keywords: cyberattack prevention; deep learning; feature selection; metaheuristics; security; software defined networks

1 INTRODUCTION

Recently, more than 25 billion gadgets have linked to the Internet globally. The Internet of Things (IoT) depends on interlinked smart gadgets, and various services were employed for integrating them into one network [1]. This lets the smart gadgets for collecting delicate information and important operations take place, and such gadgets communicate and connect with one another at maximum velocity and make choices in accordance with indicators data. The IoT network employs cloud service as a back-end to procede information and retain remote controls [2]. Users utilize web services or mobile applications to make data accessibility and adjusting their gadgets. The IoT structure employs many sensors to eliminate essential data, and it can be scrutinized by artificial intelligence (AI) methods [3]. An intrusion detection system (IDS) is administrative methodological, and regulatory means are employed to prevent unofficial use, misuse, and retrieval of electronic data and transmission mechanisms and the data they contain, focused on assuring the continuity and accessibility of works of the information method and fostering the privacy, protection, and secrecy of private data by some initiatives [4]. Cyber security means the practice of protecting electronic methods, computers, mobile devices, servers, networks, and data in malicious assaults. It is otherwise called information technology security [5]. Such intrusions include domain of research control mechanism by monitoring a change of the document mechanism, accessing sensitive records, making unapproved logins, using malware, and heightening advantages that can change the network conditions. Network intrusions happen because of approaching packets in the network for performing conducts, like denial of service (DoS) assaults or trials that separate as the mechanism [6]. DoS assaults were tried to make PC properties distant by its planned users, for instance, flood attacks, land assaults, and ping of death (POD). Intrusion indications includes abnormal results at executing various client charges were illustrated by moderate mechanism implementation, and sudden mechanism smashes and variations in fragments of data structure were bizarrely, moderate mechanism implementation (i.e., accessing sites or opening records). AI is a type of data-driven technique where the initial level was to comprehend the data [7]. Several kinds of data indicate particular attack conducts which include network activities and host behaviours. Network traffic indicates network behaviours and server logs reflect host behaviour. There were numerous kinds of assaults, each containing a specific paradigm [8]. Thus, it becomes significant for selecting appropriate data sources for detecting several assaults according to the threat features. One vital feature of a DoS assault, for instance, was to transmit numerous packets in a very limited period; therefore, flow data were ideal for DoS attack identification [9]. A hidden channel has a data leaking function amongst 2 distinct IP addresses and optimally suitable for session data recognition. Thus, the development of DL methods is helpful in detecting such network behaviours [10]. Several research works have devised the progression of network security systems, and AI serves the main part in cybersecurity areas related to IoT to design an intellectual mechanism for security in the IoT network. The conventional Internet architectures are very complex and almost failed in dynamic ecosystems because of its decentralized nature. It has too many devices, distributed nodes, and routers that were its main disadvantage [1]. The arrival of SDN with centralized control solved several issues. SDN is improvised for fog computing and it was programmable. It can be utilized as a structure for flow-related anomaly detection (AD) but it requires intelligence for ignoring assaults. The attack packet can be categorized by employing Machine Learning in SDN atmosphere [2, 3]. The authors devised ML approaches for detecting DDoS assaults in 3 different categories. An entropy-related solution for detecting DDoS assaults utilizing an SDN plane can be proposed. The rise in the number of IoT gadgets generates large amount of data. The authors estimated that more than 26 billion IoT gadgets are connected to the Internet [4]. And there is a rise in the commercial value of IoT gadgets and safeguarding the network in the future becomes mandatory as billions of devices would be connected [5]. Fig. 1 illustrates the overview of SDN.

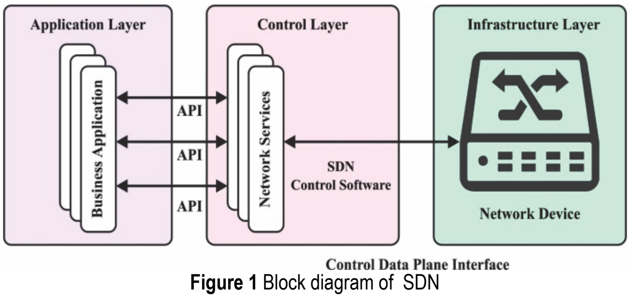


Figure 1 Block diagram of SDN

Cybersecurity refers to the collection of several technologies and security systems which are developed for the protection of network, data, or information. A program from various assaults acts like unauthorized access, data modification, destruction over the Internet or network, and stealing [6]. Cybersecurity element's main concern is network security system and host protection. Recently it can be utilized for protecting numerous areas namely IoT, cloud computing, and wireless sensor network. There exist more security measures to provide security to the networks or systems like IDS, antivirus, and firewall. But still, cyber threats continually harm and disturb Internet services on the daily basis [7]. This inspired several authors to provide their wide contributions to devising security mechanisms. The popular cyberattacks are as follows: adversarial attacks, denial of service attacks, remote local attacks, probing, phishing attack, distributed denial of service attacks, zero-day attacks, poisoning, and evasion attacks, spamming, user to root attacks, and botnet [8]. Several distinct approaches are used for attack detection, largely classified into 3 major categories like hybrid-based, anomaly, and misuse detection. Misuse-related detection is scanned by prestored assault signatures and is mainly utilized for detecting identified assaults [9]. It was helpful in detecting known attacks having minimal false alarms. It needs some alteration of the signature and attack rules on the database. By the viability and advent of Artificial Intelligence (AI) and the SDN programmable feature, AI-related security solutions are compiled into SDNs to improve security levels [10]. There were many AI-related approaches which were used as network traffic classifiers; several techniques like K-Nearest Neighbor (KNN), Decision Trees (DT), artificial neural networks (ANNs), Genetic Algorithms (GA), fuzzy logic (FL), support vector machine (SVM), and Naive Bayesian have shown ideal outcomes having some levels of precision. The demand to offer a flexible and powerful structure has motivated in developing a hybrid deep learning (DL) related threat detection solution. Utilising the capabilities of SDN to improve the safety of IoT devices and networks is an essential part of the attack detection strategy for the Internet of Things that uses SDN. Analysing the behaviour and communication patterns of IoT devices is one of the tasks that the fuzzy neural network (FNN) contributes to in the process of determining the various forms of assaults. The FNN model is able to describe complicated interactions and make reliable conclusions regarding attack detection thanks to the combination of fuzzy logic and neural network approaches. The method provides excellent defence mechanisms against cyber threats based on IoT by merging SDN and FNN.

2 RELATED WORKS

Phan and Bauschert [11] presented an adaptive intrusion response system (IRS) dependent upon deep reinforcement learning (DRL) such as DeepAir, to efficiently support against cyberattacks from the SDN. In detail, it can be primary analysis of an IRS which drives at the SDN control plane. Afterward, it can model the IRS dependent upon Markov decision process (MDP) technique and express the compared optimized problem. Next, the author progresses to a Double Deep Q-Network (DQN) based IRS technique for supporting the IRS for rapidly accomplishing the optimal IRS. In [12], the authors initially progress a DQN based cyberattack reaction control technique for supporting the control agent from attaining the optimum policy rapidly. After that, the authors present a federated DQN based cyberattack reaction control method that removes the scalability problem and enhances the learning performance of the DQN technique from a distributed method. During this analysis of DoS attacks, the attained outcomes illustrate that the FEAR efficiently kept the victim from the malicious packets. Alanazi et al. [13] reported a DL-based ensemble solution to effective DDoS attack recognition from SDN. Four hybrid techniques were projected by implementing 3 ensemble systems and several DL infrastructures such as CNN, LSTM, and GRU, for improving the SDN traffic classifier. Althobiti et al. [14] examine network security improvement solutions purposing to enhance the level of performance. From the recognition of cyberattacks on SDN it prevents against DoS attacks. The authors are accepted for employing 2 solutions and relating to SDN attack recognition performances. The primary technique is the performance accuracy of SDN with IDS procedural, and the second technique was the combination of SDN with ML. Kurochkin and Volkov [15] assume the possibility of utilizing ML approaches from resolving the problem of intrusion detections from the SDN. The work is devoted to the investigation and improvement of network attack classifications that are basic for intrusion detection systems (IDSs). For evaluating the techniques, a present dataset is employed that contains network traffic records with many distinct network attack conditions. Farhin et al. [16] presented the attack detection approach for IoT utilizing SDN. The SDN controller analyses the traffic flow, distinguishes the anomaly, and blocks received traffic and source nodes. During the SDN, a Fuzzy neural network (FNN) based attack detection method was assumed that identifies attacks, namely malicious code, man-in-the-middle (MITM), distributed DoS, and side-channel. Detecting cyberattacks in the SDN environment is the goal of the HMDL-CAD algorithm that has been suggested. The term "Hybrid Metaheuristics with Deep Learning Enabled Cyberattack Detection" (HMDL-CAD) describes this method. To increase the accuracy and efficiency of cyberattack detection in SDNs, it blends metaheuristic optimisation approaches, such as the spiral dynamics optimization-based feature selection (SDOFS) algorithm, with deep learning algorithms. This article develops a Hybrid Metaheuristics with Deep Learning Enabled Cyberattack Prevention (HMDL-CAP) model in SDN. The presented HMDL-CAP model initially carries out data preprocessing to scale the input data. Then, spiral dynamics optimization-based feature selection (SDOFS) algorithm is utilized for optimum selection of feature subsets. Next, hybrid convolutional neural network with recurrent neural network (HCRNN) model is applied to detect intrusions. As hyperparameter tuning is important, pelican optimization algorithm (POA) is used to tune the HRCNN parameters. To assess the experimental outcomes of the proposed model, a series of experiments were performed using benchmark dataset. The primary objective of the Hybrid Metaheuristics with Deep Learning Enabled Cyberattack Prevention (HMDL-CAP) model that has been described is to improve the prevention of cyberattacks in SDNs via the combination of metaheuristic optimisation strategies with deep learning algorithms. It attempts to increase the accuracy and efficiency of intrusion detection systems as well as to lessen the impact that cyberattacks have on environments that use SDN.

3 THE PROPOSED MODEL

In this study, a new HMDL-CAD algorithm was formulated for cyberattack detection in the SDN environment. The presented HMDL-CAD model encompasses pre-processing, SDOFS based feature subset election, HCRNN classification, and POA hyperparameter optimizer. As hyperparameter tuning is important, POA is used to tune the HRCNN parameters and thereby boosts the classification performance to the next level. Fig. 2 demonstrates the overall block diagram of HMDL-CAD approach.

3.1 Data Pre-Processing

The presented HMDL-CAP model initially carries out data pre-processing to scale the input data. In the data given to DL methodologies to validation or trained drives, several preparation operations are carried out to refine the quality of data and forecast the performance. To be Specific, the outlier instances which were probably reasoned by unpleasant circumstances are eradicated in both datasets. Such values are interchanged with average value of its corresponding attributes. And then, all the feature variables were altered to particular range using the min-max normalized as given in Eq. (1).

$$X_{\text{normalized}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{1}$$

Here X represents the original data features, $X_{\min}$, and $X_{\max}$ denotes the maximal and minimal value of such features. In order to clarify the nature of information, correlation scrutiny has taken place to investigate the correlation between features.

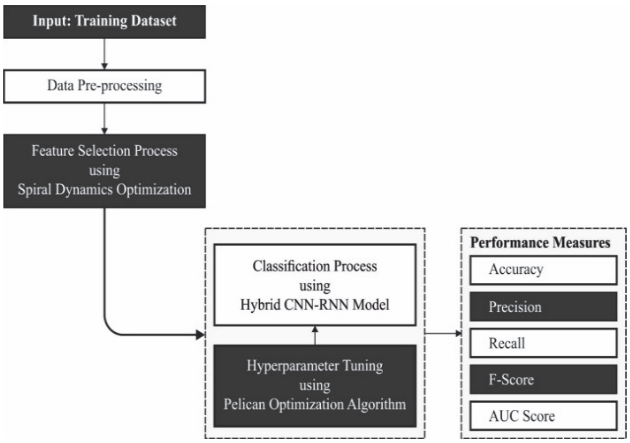

Input: Training Dataset
Data Pre-processing
Feature Selection Process using Spiral Dynamics Optimization
Classification Process using Hybrid CNN-RNN Model
Hyperparameter Tuning using Pelican Optimization Algorithm
Performance Measures
Accuracy
Precision
Recall
F-Score
AUC Score

Figure 2 Overall block diagram of HMDL-CAP approach

3.2 Feature Selection Using SDOFS Technique

Next to data pre-processing, the SDOFS algorithm is utilized for optimum selection of feature subsets. Tamura and Yoshida [17] established the SDO approach for stimulating the natural spiral phenomena. Various spirals are naturally available namely aurora, galaxies, hurricanes, blackbuck horns, seashells, tornadoes, ammonites, snails, Pieris brassicae, cabbage butterflies, seahorse, fish vortex, and chameleon tail. Also, the spirals are realized in earliest art produced by humankind from 5000 BC to 1600 AD. Recently, some research workers have made effort to comprehend the spiral sequence and complexity and developed algorithms and equations of the spiral. Furthermore, it is noteworthy that the regularly found spiral phenomenon naturally is a logarithmic spiral that is realized in tropical cyclones, nautilus shells, and galaxies. The distinct procedure of producing a logarithmic spiral was comprehended as efficient searching activities in metaheuristics that stimulated the spiral dynamics optimization technique. In this study, the multi-point searching function for n-dimension method is expressed as follows:

$$\chi_{k+1} = rR^{(n)}(\theta)\chi_k - \left(rR^{(n)}(\theta) - I_n\right)x^* \tag{2}$$

In Eq. (2), r denotes the spiral radius, $R^{(n)}(\theta)$ represents the rotation matrix of order $n \times n$, θ shows the spiral rotation direction, I_n indicates the identity matrix of order $n \times n$, x^* characterizes the spiral center, χ_k and χ_{k+1} denotes the searching point position at iteration k and k+1, correspondingly. The rotation matrix $R^{(n)}(\theta)$ for n-dimension on an arbitrary xx-plane is shown below:

$$R^{(n)}(\theta) = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \cos(\theta_{i,j}) & \dots & -\sin(\theta_{i,j}) & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \sin(\theta_{i,j}) & \dots & -\cos(\theta_{i,j}) & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{bmatrix} \tag{3}$$

In Eq. (3) $\theta_{i,j}$ shows the spiral rotation direction around the origin on $x_i x_j$ plane. The likelihood of rotation matrix $R^{(2)}(\theta)$ for 2D scheme on x_1x_2 plane is given as:

$$R^{(2)}(\theta)=\begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix} \tag{4}$$

Alternatively, the three probable groupings of rotational matrix $R^{(3)}(\theta)$ for a 3D scheme on x_1x_2, x_2x_3, and xx-planes are correspondingly shown below [18]:

$$R_{1,2}^{(3)}(\theta)=\begin{bmatrix}\cos(\theta_{1,2}) & -\sin(\theta_{1,2}) & 0\\ \sin(\theta_{1,2}) & \cos(\theta_{1,2}) & 0\\ 0 & 0 & 1\end{bmatrix} \tag{5}$$

$$R_{2,3}^{(3)}(\theta)=\begin{bmatrix}1 & 0 & 0\\ 0 & \cos(\theta_{2,3}) & -\sin(\theta_{2,3})\\ 0 & \sin(\theta_{2,3}) & \cos(\theta_{2,3})\end{bmatrix} \tag{6}$$

And.

$$R_{1,3}^{(3)}(\theta)=\begin{bmatrix}\cos(\theta_{1,3}) & 0 & -\sin(\theta_{1,3})\\ 0 & 1 & 0\\ \sin(\theta_{1,3}) & 0 & \cos(\theta_{1,3})\end{bmatrix} \tag{7}$$

Note that the algorithm produced the spiral trajectory around the center x^* and it is categorized as:

When $r > 1$ and $\in\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, the trajectory refers to conventional spiral;.

When $r < 1$ and $\in\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, the trajectory refers to hypotrochoid spiral.

As previously mentioned, the spiral direction of rotation depending on the θ value is categorized into.

When $\in\left(-\frac{\pi}{2}, 0\right)$, the trajectory rotation refers to clockwise.

When $\in\left(0, \frac{\pi}{2}\right)$, the trajectory rotation refers to anticlockwise.

The fitness function (FF) employed in the presented method can be formulated to have a balance among the quantity of selected features in every solution (lesser) and the classifier accuracy (greater) acquired through selected features, Eq. (8) indicates the FF for evaluating solutions.

$$Fitness=\alpha\gamma_R(D)+\beta\frac{|R|}{|C|} \tag{8}$$

where as $\gamma_R(D)$ indicates the classifier error rate of a presented classifier. $|R|$ denotes the cardinality of selected subset and $|C|$ signifies the total features in the datasets, α and β were 2 parameters respective to the significance of classifier subset length and quality.

4 RESULTS AND DISCUSSION

The experimental results of the HMDL-CAP model that was proposed were tested with the use of a benchmark dataset. The particular dataset that is utilised for assessment may change based on the study being conducted, but in most cases, it is a collection of network traffic data that includes both usual occurrences and instances of attacks. The performance of the model was evaluated based on a number of different criteria, including accuracy, precision, recall, and F1 score. The study sheds light on how successful and efficient the suggested methodology is in terms of the prevention of cyberattacks. The experimental results of the HMDL-CAP model are tested using the Coburg Intrusion Detection Data Set (CIDDS-001) flow-based dataset. The dataset holds 180386 samples under four distinct class labels as depicted in Tab. 1.

Table 1 Dataset details

Classes	No. of Records
Benign	147073
DDoS	18542
Port-Scan	2168
Brute-Force	12603
Total number of Records	180386

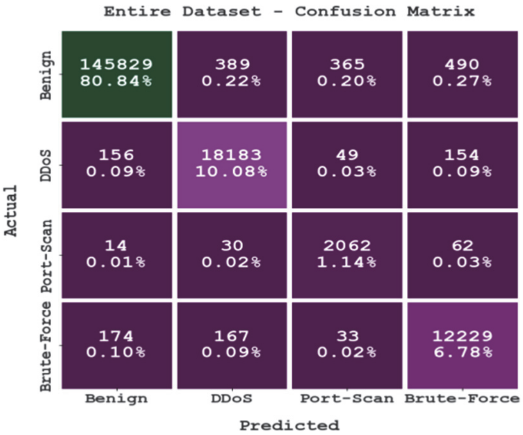


Figure 3 Confusion matrix of HMDL-CAP approach under entire dataset

Fig. 3 demonstrates the confusion matrix generated by the HMDL-CAP model on the entire dataset. The figure represents that the HMDL-CAP model has properly recognized 145829 samples under benign class, 18183 samples under DDoS class, 2062 samples under Port-Scan class, and 12229 samples under Brute-Force class. Tab. 2 and fig. 4 depict the overall results accomplished by the HMDL-CAP model on entire dataset. The obtained values inferred that the HMDL-CAP model has shown enhanced results under distinct class labels.

Fig. 5 depicts the overall results rendered by the HMDL-CAP approach on entire dataset. The results denote the HMDL-CAP algorithm has obtained enhanced results with maximum average.

Table 2 Result analysis of HMDL-CAP approach with distinct class labels under entire dataset

Entire Dataset					
Labels	Accuracy	Precision	Recall	*F*-Score	AUC Score
Benign	99.12	99.76	99.15	99.46	99.06
DDoS	99.48	96.88	98.06	97.47	98.85
Port-Scan	99.69	82.18	95.11	88.18	97.43
Brute-Force	99.40	94.54	97.03	95.77	98.31
Average	99.42	93.34	97.34	95.22	98.41

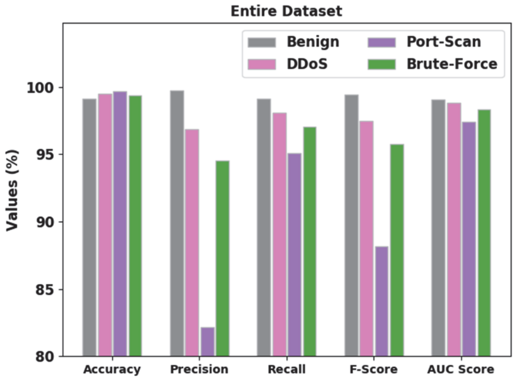


Figure 4 Result analysis of HMDL-CAP approach under entire dataset

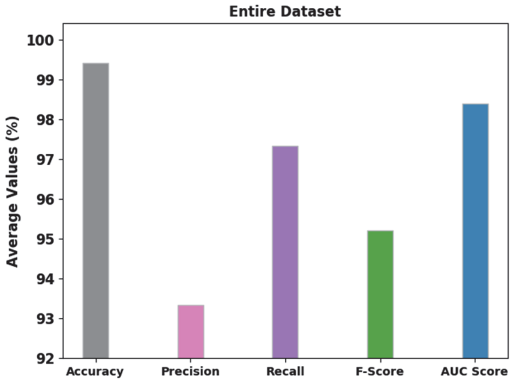


Figure 5 Average analysis of HMDL-CAP approach under entire dataset

Fig. 6 establishes the confusion matrix generated by the HMDL-CAP approach on 70% of training (TR) data. The figure implicates the HMDL-CAP method has properly recognized 102079 samples under benign class, 12698 samples under DDoS class, 1450 samples under Port-Scan class, and 8605 samples under Brute-Force class.

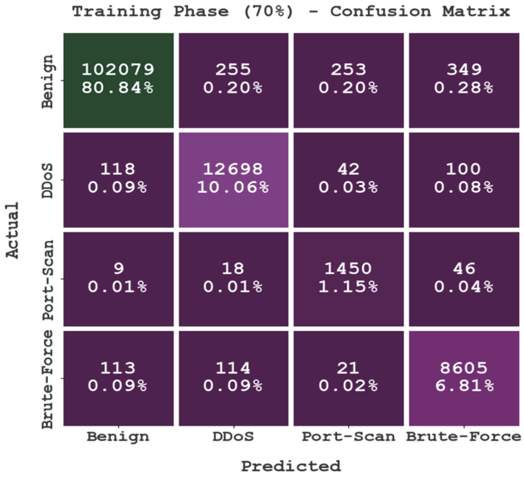


Figure 6 Confusion matrix of HMDL-CAP approach under 70% of TR data

Tab. 3 and Fig. 7 showcase the overall results accomplished by the HMDL-CAP method on 70% of TR data. The obtained values denoted the HMDL-CAP approach has shown enhanced results under distinct class labels

Table 3 Result analysis of HMDL-CAP approach with distinct class labels under 70% of TR data

Training Phase (70%)					
Labels	Accuracy	Precision	Recall	*F*-Score	AUC Score
Benign	99.13	99.77	99.17	99.47	99.07
DDoS	99.49	97.04	97.99	97.52	98.83
Port-Scan	99.69	82.11	95.21	88.17	97.48
Brute-Force	99.41	94.56	97.20	95.86	98.39
Average	99.43	93.37	97.39	95.25	98.44

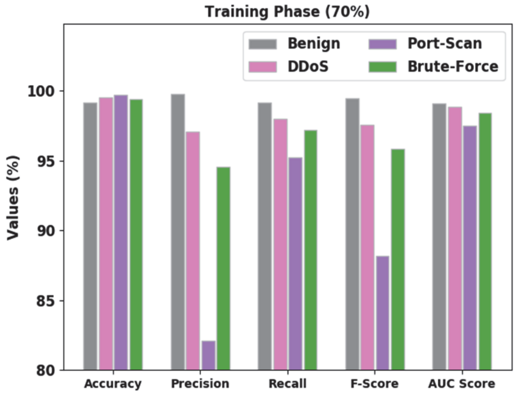


Figure 7 Result analysis of HMDL-CAP approach under 70% of TR data

Fig. 8 illustrates the overall results offered by the HMDL-CAP method on 70% of TR data. The results show the HMDL-CAP model has attained enhanced results with maximal average.

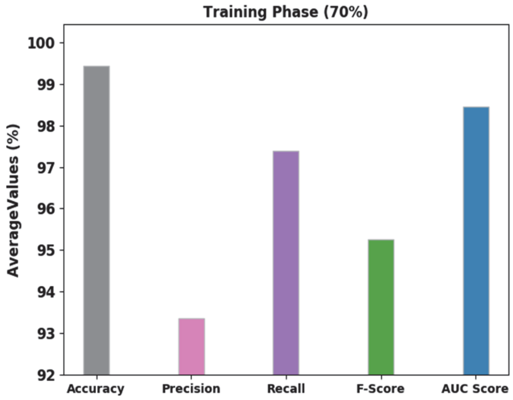
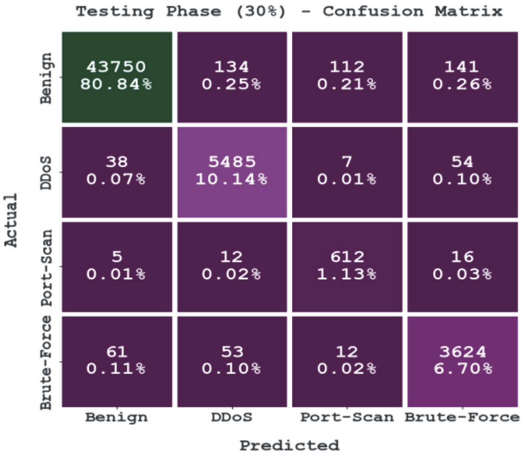


Figure 8 Average analysis of HMDL-CAP approach under 70% of TR data

Fig. 9 validates the confusion matrix generated by the HMDL-CAP model on 30% of testing (TR) data. The figure signifies that the HMDL-CAP model has properly recognized 43750 samples under benign class, 5485 samples under DDoS class, 612 samples under Port-Scan class, and 3624 samples under Brute-Force class.

Tab. 4 and Fig. 10 portray the overall results accomplished by the HMDL-CAP model on 30% of TS data. The obtained values infer that the HMDL-CAP method has shown enhanced results under distinct class labels.



	Benign	DDoS	Port-Scan	Brute-Force
Benign	43750 80.84%	134 0.25%	112 0.21%	141 0.26%
DDoS	38 0.07%	5485 10.14%	7 0.01%	54 0.10%
Port-Scan	5 0.01%	12 0.02%	612 1.13%	16 0.03%
Brute-Force	61 0.11%	53 0.10%	12 0.02%	3624 6.70%

Figure 9 Confusion matrix of HMDL-CAP approach under 30% of TS data

Table 4 Result analysis of HMDL-CAP approach with distinct class labels under 30% of TS data

Testing Phase (30%)					
Labels	Accuracy	Precision	Recall	*F*-Score	AUC Score
Benign	99.09	99.76	99.12	99.44	99.04
DDoS	99.45	96.50	98.23	97.36	98.91
Port-Scan	99.70	82.37	94.88	88.18	97.32
Brute-Force	99.38	94.50	96.64	95.56	98.11
Average	99.40	93.28	97.22	95.13	98.34

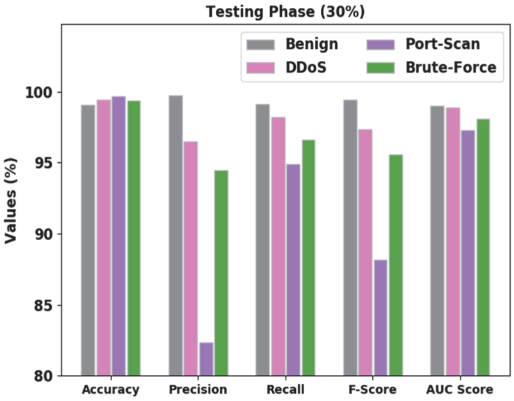


Figure 10 Result analysis of HMDL-CAP approach under 30% of TS data

Fig. 11 displays the overall results provided by the HMDL-CAP method on 30% of TS data. The results indicated that the HMDL-CAP approach has acquired enhanced results with maximum average.

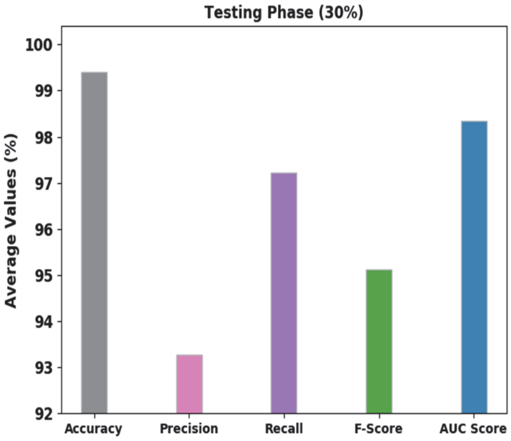


Figure 11 Average analysis of HMDL-CAP approach under 30% of TS data

5 CONCLUSIONS

In this research, a new HMDL-CAD algorithm was modelled for cyberattack detection in the SDN environment. The presented HMDL-CAD model encompasses pre-processing, SDOFS based feature subset election, HCRNN classification, and POA hyperparameter optimizer. As hyperparameter tuning is important, POA is used to tune the HRCNN parameters and thereby boosts the classification performance to the next level. To assess the experimental outcomes of the proposed model, a series of experiments were performed using benchmark dataset. The comparison study shows the promising performance of the HMDL-CAP model over recent models. Therefore, the HMDL-CAP model can be employed as an effectual tool for improved cyberattack detection performance. In future, the performance of the HMDL-CAP algorithm can be boosted by outlier reduction approaches.

6 REFERENCES

[1] Premkumar, M., Sundararajan, T. V. P., & Mohanbabu, G. (2022). Dynamic Defense Mechanism for DoS Attacks in Wireless Environments Using Hybrid Intrusion Detection System and Statistical Approaches. *Tehnički vjesnik*, *29*(3), 965-970. https://doi.org/10.17559/TV-20210604113859

[2] Radoglou-Grammatikis, P., Rompolos, K., Sarigiannidis, P., Argyriou, V., Lagkas, T., Sarigiannidis, A., Goudos, S., & Wan, S. (2021). Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach. *IEEE Transactions on Industrial Informatics*, *18*(3), 2041-2052. https://doi.org/10.1109/TII.2021.3093905

[3] Al Eroud, A. & Karabatis, G. (2019). SDN-GAN: generative adversarial deep nns for synthesizing cyber attacks on software defined networks. *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, 211-220. https: //doi.org/10.1007/978-3-030-40907-4_23

[4] Hossain, M. B. & Wei, J. (2019). Reinforcement learning-driven QoS-aware intelligent routing for software-defined networks. *2019 IEEE global conference on signal and information processing (GlobalSIP)*,1-5. https://doi.org/10.1109/GlobalSIP45357.2019.8969320

[5] Tawfik, M., Al-Zidi, N. M., Alsellami, B., Al-Hejri, A. M., & Nimbhore, S. (2021). Internet of Things-Based Middleware Against Cyber-Attacks on Smart Homes using Software-Defined Networking and Deep Learning. *2nd International Conference on Computational Methods in Science & Technology (ICCMST)*, 7-13 https://doi.org/10.1109/ICCMST54943.2021.00014

[6] Makuvaza, A., Jat, D. S., & Gamundani, A. M. (2021). Deep neural network (DNN) solution for real-time detection of distributed denial of service (DDoS) attacks in software defined networks (SDNs). *SN Computer Science*, *2*(2), 1-10. https://doi.org/10.1007/s42979-021-00467-1

[7] Guha Roy, D. & Srirama, S. N. (2021). A blockchain-based cyber attack detection scheme for decentralized Internet of Things using software-defined network. *Software: practice and experience*, *51* (7), 1540-1556. https://doi.org/10.1002/spe.2972

[8] Alonso, R. S., Sittón-Candanedo, I., Casado-Vara, R., Prieto, J., & Corchado, J. M. (2020). Deep reinforcement learning for the management of software-defined networks and network function virtualization in an edge-IoT architecture. *Sustainability*, *12*(14), 5706 https://doi.org/10.3390/su12145706

[9] Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. *Journal of Network and Computer Applications*, *136*, 71-85. https://doi.org/10.1016/j.jnca.2019.03.005

[10] Shinan, K., Alsubhi, K., Alzahrani, A., & Ashraf, M. U. (2021). Machine learning-based botnet detection in software-defined network: a systematic review. *Symmetry*, *13*(5), 866. https://doi.org/10.3390/sym13050866

[11] Phan, T. V. & Bauschert, T. (2022). Deepair: Deep reinforcement learning for adaptive intrusion response in software-defined networks. *IEEE Transactions on Network and Service Management*. https://doi.org/10.1109/TNSM.2022.3158468

[12] Phan, T. V. & Nguyen, T. G. (2022). FEAR: Federated Cyber-Attack Reaction in Distributed Software-Defined Networks with Deep Q-Network. *Wireless Telecommunications Symposium (WTS)*, 1-7. https://doi.org/10.1109/WTS53620.2022.9768169

[13] Alanazi, F., Jambi, K., Eassa, F., Khemakhem, M., Basuhail, A., & Alsubhi, K. (2022). Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network. *Intelligent Automation and Soft Computing*, *32*(2), 923-938. https://doi.org/10.32604/iasc.2022.024668

[14] Althobiti, A., Almohayawi, R., & Bamsag, O. (2020). Machine Learning approach to Secure Software Defined Network: Machine Learning and Artificial Intelligence. *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, 1-8. https://doi.org/10.1145/3440749.3442597

[15] Kurochkin, I. I. & Volkov, S. S. (2020). Using GRU based deep neural network for intrusion detection in software-defined networks. *IOP Conference Series: Materials Science and Engineering*, *927*(1), 012035. https://doi.org/10.1088/1757-899X/927/1/012035

[16] Farhin, F., Sultana, I., Islam, N., Kaiser, M.S., Rahman, M. S. & Mahmud, M. (2020). Attack detection in internet of things using software defined network and fuzzy neural network. *2020 Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (icIVPR)*, 1-6. https://doi.org/10.1109/ICIEVicIVPR48672.2020.9306666

[17] Derhab, A., Aldweesh, A., Emam, A. Z., & Khan, F. A. (2020). Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering. *Wireless Communications and Mobile Computing.* 2020. https://doi.org/10.1155/2020/6689134

[18] Omar, M. B., Bingi, K., Prusty, B. R., & Ibrahim, R. (2022). Recent advances and applications of spiral dynamics optimization algorithm: A review. *Fractal and Fractional*, *6*(1), 27. https://doi.org/10.3390/fractalfract6010027

[19] Agarwal, A., Yadav, A., & Vishwakarma, D. K. (2019). Multimodal sentiment analysis via RNN variants. *2019 IEEE International Conference on Big Data, Cloud Computing, Data Science & Engineering (BCD)*, 19-23 https://doi.org/10.1109/BCD.2019.8885108

[20] Tuerxun, W., Xu, C., Haderbieke, M., Guo, L., & Cheng, Z. (2022). A Wind Turbine Fault Classification Model Using Broad Learning System Optimized by Improved Pelican Optimization Algorithm. *Machines*, *10*(5), 407. https://doi.org/10.3390/machines10050407

Contact information:

P. B. ARUN PRASAD, Assistant Professor
Department of Computer Science and Engineering,
Saranathan College of Engineering
Thiruchirappalli, Tamilnadu, 620 012, India

V. MOHAN, Professor
(Corresponding Author)
Department of Electronics and Communication Engineering Saranathan
College of Engineering,
Thiruchirappalli, Tamilnadu, 620 012, India
E-mail: mohansec@outlook.com

K. VINOTH KUMAR, Professor
Department of Electronics and Communication Engineering,
SSM Institute of Engineering & Technology,
Dindigul, Tamilnadu, India, 624002