Indonesian Journal of Electrical Engineering and Computer Science
Vol. 38, No. 3, June 2025, pp. 1745~1754
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v38.i3.pp1745-1754

Chaotic crow search enhanced CRNN: a next-gen approach for IoT botnet attack detection

Veena Antony[1,2], Nainan Thangarasu[1]
[1]Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India
[2]Department of Cyber Security and Applied Computing, St. Teresa's College (Autonomous), Kerala, India

Article Info

Article history:

Received May 15, 2024
Revised Nov 15, 2024
Accepted Nov 30, 2024

Keywords:

Chaotic mapping
Crow search algorithm
Deep learning
IoT botnet attack
Machine learning

ABSTRACT

Internet of things (IoT) botnet attack detection is crucial for reducing and identifying hostile threats in networks. To create efficient threat detection systems, deep learning (DL) and machine learning (ML) are currently being used in many sectors, mostly in information security. The botnet attack categorization problem is difficult as data dimensionality increases. By combining convolutional and recurrent neural layers, our work effectively addressed the vanishing and expanding gradient difficulties, improving the ability to capture spatial and temporal connections. The problem of weight decaying and class imbalance affects the accuracy rate of the existing DL models. In convolutional neural network (CNN), fully connected layer optimizes the hyperparameters by utilizing its comprehension of the chaotic crow search method. The chaotic mapping maintains equilibrium between the global and local search spaces. The crow's strategy for hiding food is the main source of inspiration for optimizing the learning rate, weight, and bias components involved in the prediction process. When compared to other existing algorithms, the UNSW-NB15 dataset's results for IoT botnet attack detection in the presence of a high degree of class imbalance demonstrated the effectiveness of the proposed convolutional recurrent neural network (CRNN) boosted with chaotic crow searching algorithm, which produced the highest detection rate with the lowest false alarm rate.

Corresponding Author:

Veena Antony
Department of Computer Science, Karpagam Academy of Higher Education
Coimbatore, Tamil Nadu, India
Email: veenaantony22@gmail.com

1. INTRODUCTION

The number of internet of things (IoT) based attacks has been progressively increasing because of the widespread use of IoT devices. The IoT malware attack, that aims to carry out real, practical, and profitable cybercrimes, is one of the biggest IoT threats [1]. IoT- botnets are collections of malware-infected, remotely managed IoT devices linked to the internet. The rapid rise of hazards and different attack tactics pose significant issues for IoT platforms when it comes to providing methods to detect security flaws and assaults [2]. The detection methods and approaches based on machine learning (ML) algorithms or deep learning (DL) paradigms that employ full-time series data have been improving with each malware execution. Nevertheless, the utility of current efforts is significantly limited by the requirement to use full-time series data. However, earlier detection would allow for more effective IoT botnet reaction ideas. It lessens the harm that could be brought about by potential assaults [3]. The technique of dynamic analysis examines the ways in which ransomware interacts with the environment as it is running. For malware detection algorithms based on DL and ML, this data is crucial [4]. The representative approaches necessitated collecting data in a continuous series while the malware is operating. In this instance, the malware completely disrupted the information system and proved to be destructive in every way.

Since there are now methods for detecting these steps, it should not be too difficult to identify the malicious attack and the IoT botnet network itself if a botnet assault carried out by an IoT botnet occurred previously [5], [6]. A substantial hardware foundation for DL techniques has been made possible by the rapid advancement of parallel computing technology. The three most common problems with existing ML based models are as follows: with a wider range of fraudulent intrusions, they have a very high false alarm rate; most of the ID systems in use miss novel attacks due to outdated ID datasets, so they are not generalizable; and cutting-edge solutions are needed to maintain today's rapidly increasing rapid connectivity traffic on networks in an adversarial environment. Considering the assessment of ML and DL classifier's efficacy in the ID domain, this study investigates the impact of class imbalance in intrusion detection and the influence of hyperparameters over accuracy in detection of botnet attacks are the key issues behind the development of a convolutional recurrent neural network (CRNN) boosted with chaotic crow search based botnet attack detection employing in UNSW-NB15 dataset. This proposed model addresses the problem of optimizes the learning rate, weight decaying problem by fusing the chaotic crow search algorithm.

The following is how the paper is structured: the relevant literature is reviewed in section 2, and further background research and the purpose for this effort are covered in section 3. In section IV, various categories of algorithms used are analyzed and the proposed prediction model is detailed. The experiments, findings, and discussions are included in section 5. Section 6 is the paper's conclusion.

2. LITERATURE REVIEW

Okur and Dener [7], the intent of this research is to apply ML methods to accurately distinguish between attack and regular network traffic. There were two methods used to conduct the study: under supervision and without. Alissa *et al.* [8] suggested ML techniques for binary class classification. This is accomplished by using the publicly available UNSW-NB15 dataset. A comprehensive pipeline for ML was suggested, comprising pre-processing and analysis of exploratory data. Alshamkhany *et al.* [9] created a cutting-edge ML method to identify botnet attacks. Four artificial intelligence models based on four classifiers are constructed for prediction of intrusion detection. A ML-based sequential detection architecture for botnet attack detection was designed by Soe *et al.* [10]. The implementation of a high-performing, lightweight detection system makes use of an effective feature selection strategy. According to their findings, the suggested architecture is capable of both efficiently identifying botnet-based attacks and expanding to accommodate appropriate sub-engines for novel types of attacks.

Munoz and Valiente [11] carried out a comprehensive review with the goal of determining the best ML and DL methods for identifying IoT botnets by carefully examining benchmark datasets, evaluation criteria, and data pre-processing methods. Kim *et al.* [12] presented a framework for ML and DL algorithms in IoT botnet attack detection based on an amalgamation of the results and offered suggestions for further study in this field. The architecture presented by Nazir *et al.* [13] comprises a software-defined network application layer abnormality detection system for IoT edge devices. IoT-edge devices ask the software-defined network controller for details regarding how they are acting within the network. Natarajan *et al*. [14] employed the N-BaIoT dataset, which consists of nine malicious IoT devices with the benign and dangerous viruses, each of which has 10 sub attacks. To classify the malicious and sub-attacks of an IoT device infected, the authors conducted a comparative study using the N-BaIoT dataset.

Sakhnini *et al.* [15] utilized the concept of dung beetle optimizer for selecting the centroid while clustering the instances to detect the IoT botnet attacks. Almuqren *et al*. [16] developed a hybrid model with modified firefly optimization for botnet detection in cloud IoT environment. Bojarajulu *et al.* [17] devised an improved mode of information gain for selecting the feasible attributes to detect the IoT botnet attacks and the integrated bidirectional with recurrent deep neural network is used for predicting the presence of botnet attacks. Arshad *et al.* [18] proposed an ensemble learning model to detect the suspicious behavior of botnet attacks by analyzing the network traffic in IoT devices using three different classifiers that were used for performance analysis.

From the above literature's it is observed that both ML and DL models contributes high in detection of botnet attacks in IoT environment. But the issues in hyperparameter fine tuning during the training phase is not well focus by most of the research articles, hence in this proposed work the overfitting problem arise commonly due to improper assignment of learning rate, weight and bias parameters are majorly focused by devising a nature inspired algorithm for assigning best parameter values to improve the detection rate.

3. PRELIMINARIES

3.1. Min-max normalization

In general, the dataset used for IoT botnet detection, comprised of different range of values for each attribute. The values of the attributes highly influence the prediction model, so treat all the attributes equally, the process of normalization will be conducted as a pre-processing step, in which all attributes value will be transformed to the range of 0 to 1. For this, process min-max normalization is applied, and its mathematical formulation (1) is as:

$$M - M\,(X(ATT)) \;=\; (X(ATT) \;-\; Min\,(ATT))\,/\,(Max\,(ATT) \;-Min\,(ATT)) \qquad (1)$$

3.2. Recurrent neural network

An algorithm with a sequential approach that is focused on DL is called an recurrent neural network (RNN). Because RNNs have connections between their hidden levels, they are unique. It replicates the hidden layer repeatedly, giving the inputs the same weights and biases to the inputs at each time step. The process will be carried out repeatedly by the network, which will store the information in its internal memory and update and alter its hidden state. Through training on appropriate data, the RNN will build its mode [19], [20]. Every time a set of data passes through the RNN chain, the model is reconstructed and revised.

RNN performs well with huge datasets and is very easy to interpret the data throughout the training process. It is capable of handling either quantitative and categorical data, requires minimum data preparation, and can be used to evaluate a model employing statistical tests. RNN is a statistical algorithm that employs data cluster points in functional groups. Due to a variety of factors, categorization and clustering will be more difficult and complex with larger data sets.

In addition, RNNs have the ability to store information in their neuron units via capturing changes. This is a benefit in handling time series data, giving RNN a special characteristic in DL models [21]. An RNN can gather information from any length of sequence. When creating predictions, RNN considers features dependencies and sequential information found in the input data. RNNs are constructed from neurons, also referred to as data-processing nodes. The arrangement of neuron’s input, output, and hidden layers is depicted in Figure 1. The result is provided by the output layer, while input layer receives the data to process. The hidden layer is where the data processing, analysis and predictions happen.

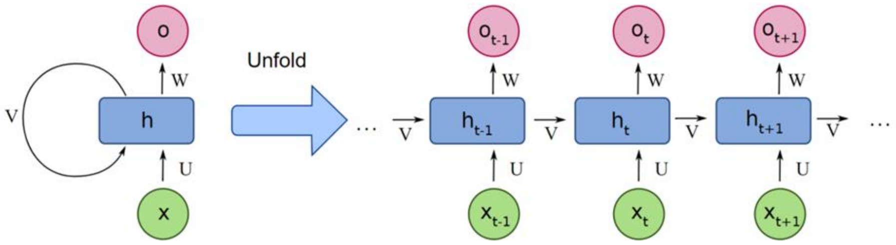


Figure 1. Recurrent neural network [22]

3.3. Crow search algorithm

The most intellectual bird is thought to be the crow. When needed, they retrieve food that has been hidden. They stalk and observe the food storage locations of other crows, follow each other, and after the owner departs, steal food. Crows will relocate their hiding spot to prevent theft if they notice that they are being followed. The four fundamental ideas of the program are derived from the crows' behavioral patterns.

- Crows are sociable species.
- Crows can recall where food is hidden.
- Crows prowl around to scavenge food together.
- Crows are capable of perception. They will relocate their food hiding spot to avoid theft if they feel like they are being followed.

There are thought to be numerous crows in a d-dimensional environment. The precise position of the crow at every iteration in the area of search and the total amount of crows, or flock size, are specified by a vector. The location of each crow's hiding place is stored in a memory. The exact location of the crow’s hiding spot is indicated at each iteration. A crow could never have found a better spot than this. Yes, every crow does recall the exact place of its most memorable experience. Crows search for improved food sources by moving throughout the area. Suppose that a different crow wants to visit the hiding place that the preceding crow indicated in the following iteration. This time, the first crow chooses to follow the other crow to where they are hidden. There are two conceivable outcomes in this scenario. The second crow is unaware that the first one is trailing behind. The first crow will therefore go closer to the other crow's hiding spot. In this instance, a uniformly distributed random number is used to determine the new location of the first crow.

While adopting conventional crow search algorithm it leads to local optimization and the global search is not well balance due to its searching strategy. Hence early convergence affects the optimal searching of best solution. Hence in this proposed work chaos is used for initial population selection and to balance both global and local optimization while searching best set of values to be assigned in hyperparameters.

4. METHOD

4.1. Overview

To enhance the botnet attack detection in IoT with system's learning capacity and performance by incorporating modern DL techniques like CNN and RNN with metaheuristic model upon to upgrade botnet detection on IoT. Our study has made significant contributions that can be summed up as follows:

- This work created CRNN-CCRSA to minimize overheads and optimize advantages by combining DL variants convolutional and recurrent network to handle both temporal and spatial features.
- Attacks can be categorized into the appropriate intrusion class in IoT botnet, the proposed method focuses on determining whether network traffic behavior is benign or malevolent.
- The proposed model tackles the prevalent issue of class imbalance in UNSW-NB15 dataset.
- We compare the suggested strategy with existing ML techniques. With ten-fold cross-validation, the empirical results demonstrate that the system is very suitable for the detection of attack and can correctly detect misuses in 99.3% of cases.

4.2. Dataset description

The UNSW-NB15 [23] is the dataset that was used to do feature reduction and was retrieved from the Kaggle repository. With the reduced feature subset obtained from our previous work, eight potential attributes of UNSW-NB15 dataset with 2,57,673 records is used for detecting the botnet attacks in IoT. In previous work, the curse of dimensionality is handled by our reliable fuzzy chaotic cuckoo search relief choice of features technique that enhances the classification accuracy in uncertain settings during botnet attack detection in the IoT.

4.3. Proposed methodology: CRNN with chaotic crow search algorithm

In Figure 2 demonstrates the working principle of the proposed CRNN boosted with chaotic crow search algorithm for prediction of the normal and attack traffics in IoT botnet dataset. Initially, the UNSW-NB15 dataset [23] is pre-processed using min max normalizer, to convert all features falls under the interval of 0 and 1. To accomplish this, subtract the feature’s minimum value from each value, then divide the result by the feature’s range values. The normalized data is fed as input to the convolutional layer which performs the feature extraction using filter vectors within convolutional layers to transform data to the reduced dimension with two layers of convolutional and pooling layers, the temporal features are obtained by recurrent neural network integrated with the output of convolutional layers and the final processed output is passed to the fully connected layer to classify the instances as normal or abnormal traffic. The chaotic mapping-based crow searching strategy is deployed to fine tune the hyperparameters of fully connected layer more precisely and achieves the accuracy rate of the malicious attack prediction in IoT botnet attack detection.

Process of convolutional recurrent neural network with chaotic crow search algorithm is described. CRNN is made up of two main parts: a classifier and a feature extractor. The two layers that make up the feature extractor are the pooling and convolution layers. The feature map, or extracted output, serves as the input for the second classification component. In this way, CNN picks up on the local characteristics quite well. The flaw, though, is that it fails to recognize the time dependence of key characteristics. Thus, this proposed work added recurrent layers following the CRNN layers to more robustly capture both spatial and temporal variables. By doing so, we were able to properly handle the vanishing and inflating gradient difficulties, which enhances our capacity to identify temporal and spatial connections and extract useful information from variable aspect patterns.

In the Figure 3, the CRNN network, we can simulate both temporal and spatial aspects by first processing the input through the CNN and then passing the CNN's output via the recurrent layers to construct patterns at each time step. Subsequently, the sequence vector is supplied into a SoftMax layer for the probability dispersion across the classes after passing through a fully connected layer. In the information pre-processing section, the network traffic was initially arranged and pre-processed.

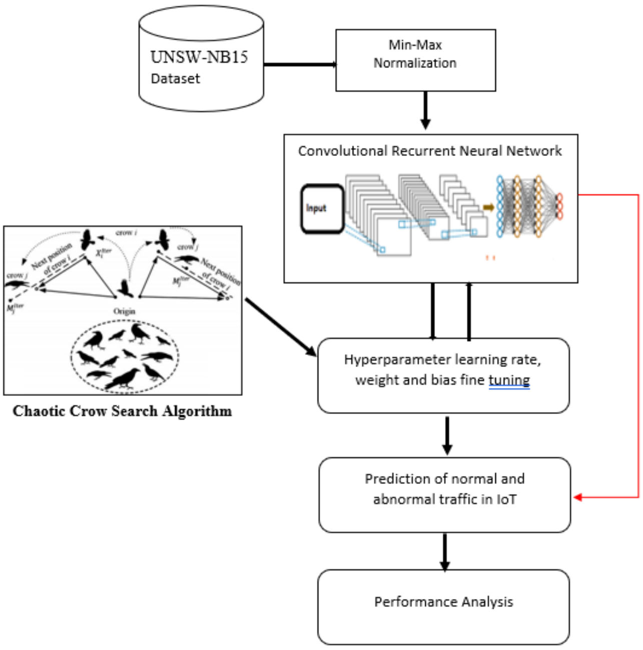

UNSW-NB15 Dataset
Min-Max Normalization
Convolutional Recurrent Neural Network
Input
Chaotic Crow Search Algorithm
Hyperparameter learning rate, weight and bias fine tuning
Prediction of normal and abnormal traffic in IoT
Performance Analysis

Figure 2. Working principle of the proposed CRNN

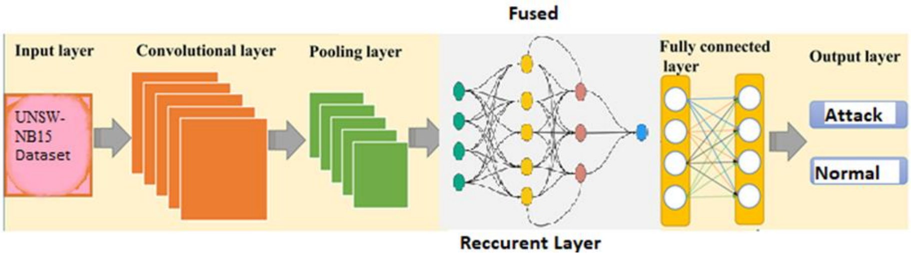


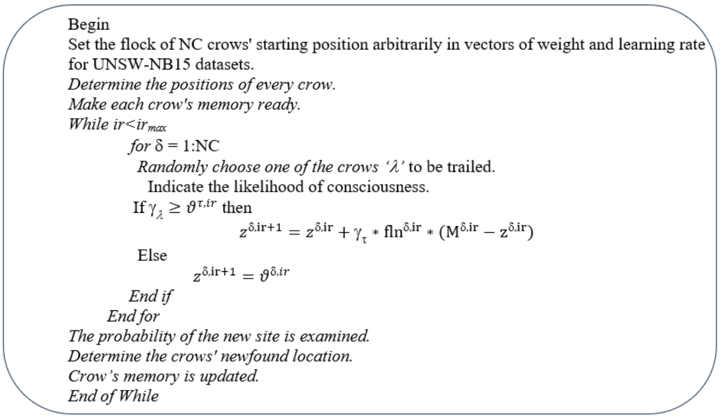
Figure 3. Process of CRNN for IoT botnet attack detection

4.4. Chaos map-based crow search algorithm

To prevent local optima and early convergence to the IoT botnet detection solution, the usual crow search algorithm is upgraded in this study work. By modifying chaotic mapping, which creates well-scattered characteristics to develop optimized solutions, global optima in the search for the optimal hyperparameters applied in the fully connected layer of the CRNN are achieved. Diversification and intensification are the two components that make up the tactics employed to accomplish local and global search, respectively [24]. For exploration and exploitation, the probability parameters are appropriately managed.

In this proposed work, chaotic maps were created using non-invertible maps. Intensification and diversification are two essential metaheuristic system mechanisms. To make the crow search process work effectively in the search space, intensification focuses on local search while diversification concentrates on global search [25]. Exploration and exploitation in crow search are heavily influenced by the consciousness probability parameter in this work. Therefore, using low levels encourages amplification and vice versa. The chaotic maps are switched by possibilities and random variables when points from samples or chances are used in a metaheuristic, leading to irregularities for the crow pursuit approach. Crows travel from place to place in a typical crow searching algorithm, looking for the ideal place to hide food. The crow improves its memory of where its food is stored and rearranges its group to safeguard it. The likelihood of the crow spotting the hidden food giving is determined. The crow search algorithm uses a chaotic map to find random locations and increase awareness.

In Figure 4, where chaotic map is denoted by ϑ. The awareness probability of a crow, with a value of 0.1, is employed in the traditional crow search algorithm to find the optimal solution. In this suggested work, chaotic sequences are utilized in place of the awareness probability of the crow, and chaotic maps are used in place of random values, as in the usual crow search algorithm, to determine the optimal location of the crow.



```
Begin
Set the flock of NC crows' starting position arbitrarily in vectors of weight and learning rate
for UNSW-NB15 datasets.
Determine the positions of every crow.
Make each crow's memory ready.
While $ir<ir_{max}$
        for $\delta = 1$:NC
          Randomly choose one of the crows '$\lambda$' to be trailed.
            Indicate the likelihood of consciousness.
         If $\gamma_{\lambda} \geq \vartheta^{\tau,ir}$ then
                          $z^{\delta,ir+1} = z^{\delta,ir} + \gamma_{\tau} * fln^{\delta,ir} * (M^{\delta,ir} - z^{\delta,ir})$
          Else
                    $z^{\delta,ir+1} = \vartheta^{\delta,ir}$
        End if
     End for
The probability of the new site is examined.
Determine the crows' newfound location.
Crow's memory is updated.
End of While
```

Figure 4. Step by step process of chaotic crow search algorithm

5. RESULTS AND DISCUSSION

5.1. Performance analysis

The section discusses the performance of the proposed model convolutional recurrent network with chaotic crow search algorithm (CRNN+CCRSA) deployed using Python software. The metrics used for performance analysis are accuracy, precision, recall, and F-measure. The dataset used for IoT botnet attack detection is acquired from UNSW-NB15 dataset. The parameter values of the proposed RNN model are shown in Table 1.

Table 1. Parameter values of the proposed model

Hyper-parameters	Values
Number of layers	10
CNN hyper-parameters	Number of filters used 64, filter -size is 3
RNN- parameters	Cells: GRU, number of states are 64
Drop-out rate	[0.2, 0.3, 0.5]
Learning rate	0.001
Number of epochs	5
Batch size	256

Table 2 explores the outcome of the four different IoT botnet detection approaches based on the measure accuracy, precision, recall, and F-measure. Based on the outcomes, it is observed that the proposed RNN-CCRSA achieves the highest rate of accuracy with 99.3% while precision, recall, and F-measure as 99%, 99.1%, and 99.05% respectively. From the performance evaluation it is observed that without optimizing the hyperparameters and assigning the values in imbalanced dataset and early convergence due to gradient descent algorithm used in deep neural network great affects the detection of IoT botnet. Hence, the fusion of chaotic crow searches based optimization in fine tuning the parameters of RNN improve the learning rate of determining the vague attack patterns and classify them more accurately compared with the other three DL models.

Table 2. Performance evaluation

Methodologies	Accuracy	Precision	Recall	F-measure
Artificial neural network (ANN)	82	84	86	84.99
Deep neural network (DNN)	87	89	90	89.50
DNN-support vector machines (SVM)	98	97	98	97.50
RNN-CCRSA	99.3	99	99.1	99.05

5.2. Comparative analysis of the CRNN-CCRSA with ANN, DNN, and DNN-SVM

This section discusses in detail about the comparative analysis of the proposed algorithm CRNN-CCRSA with three existing algorithms ANN [26], DNN [27], and DNN-SVM in prediction of IoT botnet intrusion detection. The proposed model CRNN-CCRSA was deployed using python software and the dataset used for botnet attack detection is collected from UNSW-NB15 dataset with 2,57,673 records. The metrics used for evaluating the performance is done using accuracy, precision, recall, and F-measure. The detailed explanation about the results obtained are shown in Figures 5 to 8.

The result shown in Figure 5, proves that RNN-CCRSA attains highest rate of accuracy compared to ANN, DNN, and DNN-SVM. The RNN-CCRSA with the ability of recurrently updating its parameters with the knowledge of crow searching behavior predicted the presence of abnormal traffic pattern in IoT with appropriate assigned of values to the hyperparameters. While ANN, DNN, and DNN-SVM works based on the sigmoid and activation function. The existing algorithms face the issue of overfitting due to class imbalance in the IoT botnet attack dataset which causes inconsistency during the training phase and thus they produce less accuracy compared to RNN-CCRSA.

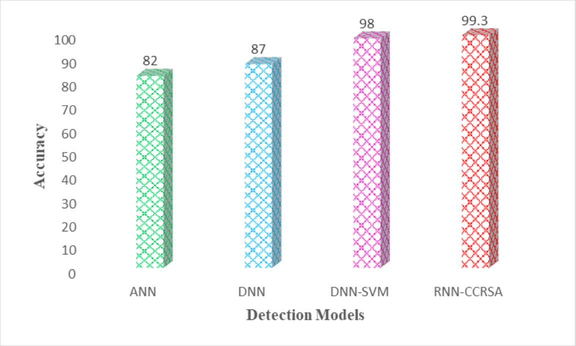


Figure 5. Accuracy on IoT botnet attack detection

The results based on precision rate of RNN-CCRSA, DNN-SVM, DNN, and ANN for IoT botnet attack detection is displayed in the Figure 6. The worst performance in attack prediction is obtained while using ANN because of inconsistent nature of dataset. The DNN with raw IoT botnet dataset the parameters are assigned using arbitrary nature of greedy search strategy. By integrating RNN with CCRSA it well handles the vagueness in classification of instances with high imbalance among attacks and normal traffic patterns. The chaotic mapping of crow searching algorithm emphasis the process of proposed RNN-CCRSA balance both local and global searching in optimizing the hyperparameter values.

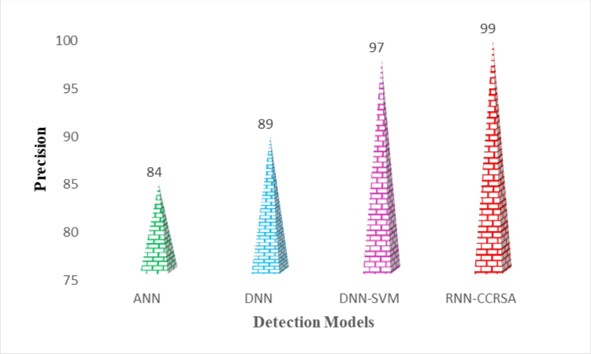


Figure 6. Precision on IoT botnet attack detection

Figure 7 displays the performance of the three different neural network models based on recall rate to predict the botnet attacks in IoT environment. It is proved from the result that RNN-CCRSA with the concept of hyperparameter fine tuning of RNN with chaotic crow search algorithm examines the incoming data more relevantly and evaluate the contribution of each feature in distinguish the presence or absence of botnet attacks. Hence, its performance is predominant compared with ANN, DNN, and DNN-SVM. With the knowledge of exploration and exploitation, the chaotic mapping-based crow searching behavior improves the performance of RNN in detection of normal packets and anomaly attacks in IoT.

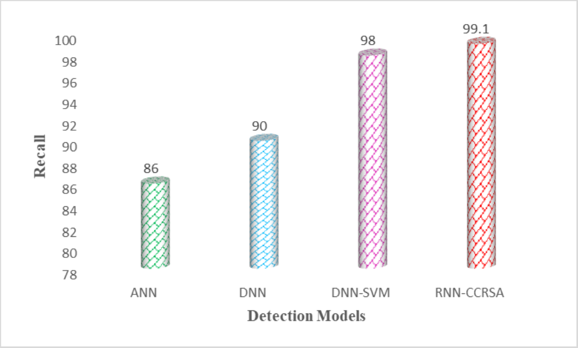


Figure 7. Recall rate on IoT botnet attack detection

In Figure 8, it is proved that the impact of both precision and recall reflected in the F-measure metric for prediction of IoT botnet attacks by four different variants of neural network models. The proposed RNN-CCRSA obtains highest F-measure rate, as it improves the learning rate and the parameters value assignment of the RNN in an optimized manner by the nature of crow's food hiding location searching strategy is implied in this work. Thus, RNN-CCRSA produced the best F-measure of 99.05% compared to other DL paradigms.

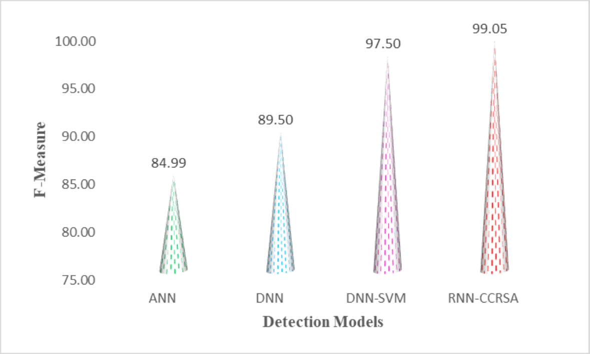


Figure 8. F-measure rate on IoT botnet attack detection

5.3. Findings and discussions

From the existing literature, the major drawback considered in this proposed work is handling the uncertainty when the input cases are vague and inconsistent. The class imbalance during the training phase is also another main factor which are not properly focus and treated in the existing and conventional models. The use of nature inspired algorithms can be able to achieve optimal solutions with their searching strategy. But initialization of parameters is often random in the conventional or traditional algorithms which leads to early convergence of results. To overcome the butterfly effect, the chaos theory-based nature inspired searching strategy is used.

6. CONCLUSION

The class imbalance problem in the IoT botnet attack detection dataset is frequently caused by an inadequate distribution of data, with most of the occurrences falling into one class and the rest falling into another. Due to limitless data values and imbalanced classes, the botnet attack predictions problem grows increasingly challenging as data dimensionality rises. While using the conventional DL models the back propagation and gradient descent based hyperparameter initialization takes place, this affects the performance of the classification model when the degree of class imbalance is high during training phase. Thus, the proposed work concentrates on handling the aforementioned challenge in IoT botnet attack detection by devising a fused model of CRNN which extracts the spatial and temporal features of the attack dataset. While using DL models vanishing and exploding gradient method to assign the hyperparameter values results in overfitting, to overcome this issue, crow searching algorithm with chaotic mapping optimizes parameters of the RNN more reliably. In future, various other nature inspired algorithms can be used for balance global and local searches. DL algorithms can be developed to handle small amounts of dataset while testing with the real case scenarios.

ACKNOWLEDGEMENTS

The authors express their gratitude to Karpagam Academy of Higher Education for their recommendations and unwavering support during the experimental work.

FUNDING INFORMATION

Authors state there is no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Veena Antony	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
Nainan Thangarasu		✓				✓		✓	✓	✓	✓	✓		

C	: **C**onceptualization	I	: **I**nvestigation	Vi	: **Vi**sualization
M	: **M**ethodology	R	: **R**esources	Su	: **Su**pervision
So	: **So**ftware	D	: **D**ata Curation	P	: **P**roject administration
Va	: **Va**lidation	O	: Writing - **O**riginal Draft	Fu	: **Fu**nding acquisition
Fo	: **Fo**rmal analysis	E	: Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

ETHICAL APPROVAL

Authors state no conflict of interest.

DATA AVAILABILITY

The authors declare that all data supporting the findings of this study are available within the article. Additionally, the dataset used in this research is openly accessible on Kaggle at https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15.

REFERENCES

[1] S. Haider *et al.*, "A deep CNN ensemble framework for efficient ddos attack detection in software defined networks," in *IEEE Access*, vol. 8, pp. 53972-53983, 2020, doi: 10.1109/ACCESS.2020.2976908.

[2] M. A. Ferrag, L. Shu, H. Djallel, and K.-K. R. Choo, "Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0," *Electronics*, vol. 10, no. 11, 2021, doi: 10.3390/electronics10111257.

[3] L. Chettri and R. Bera, "A Comprehensive survey on internet of things (IoT) toward 5G wireless systems," in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16-32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

[4] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, and L. Cheng, "Internet of things botnet detection approaches: analysis and recommendations for future research," *Applied Sciences*, vol. 11, no. 12, 2021, doi: 10.3390/app11125713.

[5] F. Abbasi, M. Naderan, and S. E. Alavi, "Anomaly detection in internet of things using feature selection and classification based on logistic regression and artificial neural network on N-BaIoT dataset," *2021 5th International Conference on Internet of Things and Applications (IoT)*, Isfahan, Iran, 2021, pp. 1-7, doi: 10.1109/IoT52625.2021.9469605.

[6] C. Yang, W. Guan, and Z. Fang, "IoT botnet attack detection model based on DBO-catboost," *Applied Science*, vol. 13, no. 12, 2023, doi: 10.3390/app13127169.

[7] C. Okur and M. Dener, "Detecting IoT botnet attacks using machine learning methods," *2020 International Conference on Information Security and Cryptology (ISCTURKEY)*, Ankara, Turkey, 2020, pp. 31-37, doi: 10.1109/ISCTURKEY51113.2020.9307994.

[8] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet attack detection in iot using machine learning," *Computational Intelligence and Neuroscience*, 2022, doi: 10.1155/2022/4515642.

[9] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, and F. Aloul, "Botnet attack detection using machine learning," *2020 14th International Conference on Innovations in Information Technology (IIT)*, Al Ain, United Arab Emirates, 2020, pp. 203-208, doi: 10.1109/IIT50501.2020.9299061.

[10] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based iot-botnet attack detection with sequential architecture," *Sensors*, vol. 20, no. 16, 2020, doi: 10.3390/s20164372.

[11] D. C. Muñoz and A. d-C. Valiente, "A novel botnet attack detection for IoT networks based on communication graphs," *Cybersecurity*, vol. 33, 2023, doi: 10.1186/s42400-023-00169-6.

[12] J. Kim, M. Shim, S. Hong, Y. Shin, and E. Choi, "Intelligent detection of IoT botnets using machine learning and deep learning," *Applied Science*, vol. 10, no. 19, 2020, doi: 10.3390/app10197009.

[13] A. Nazir *et al.*, "Advancing IoT security: a systematic review of machine learning approaches for the detection of IoT botnets," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 10, 2023, doi: 110.1016/j.jksuci.2023.101820.

[14] D. Natarajan, S. P. Shakthi, and S. S. Shruthi, "Botnet attack detection in IoT-based security camera device using principal component analysis with various machine learning algorithms," *International Research Journal of Multidisciplinary Technovation*, 2023, doi: 10.1007/978-981-99-2746-3_65.

[15] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Security aspects of internet of things aided smart grids: a bibliometric survey," *Internet of Things*, vol. 14, p. 100111, 2021, doi: 10.1016/j.iot.2019.100111.

[16] L. Almuqren, H. Alqahtani, S. S. Aljameel, A. S. Salama, I. Yaseen, and A. A. Alneil, "Hybrid metaheuristics with machine learning based botnet detection in cloud assisted internet of things environment," in *IEEE Access*, vol. 11, pp. 115668-115676, 2023, doi: 10.1109/ACCESS.2023.3322369.

[17] B. Bojarajulu, S. Tanwar, and T. P. Singh, "Intelligent IoT-BOTNET attack detection model with optimized hybrid classification model," *Computers & Security*, vol. 126, no. c, 2023, doi: 10.1016/j.cose.2022.103064.

[18] A. Arshad, M. Jabeen, S. Ubaid, A. Raza, L. Abualigah, K. Aldiabat, and H. Jia, "A novel ensemble method for enhancing internet of things device security against botnet attacks," *Decision Analytics Journal*, vol. 8, p. 100307, 2023, doi: 10.1016/j.dajour.2023.100307.

[19] G. T. Taye, H.-J. Hwang, and K. M. Lim, "Application of a convolutional neural network for predicting the occurrence of ventricular tachyarrhythmia using heart rate variability features," *Scientific Reports*, vol. 10, no. 6769, 2020, doi: 10.1038/s41598-020-63566-8.

[20] H. Hewamalage, C. Bergmeir, and K. Bandara, "Recurrent neural networks for time series forecasting: current status and future directions," *International Journal of Forecasting*, vol. 37, no. 1, pp. 388-427, 2021, doi: 10.1016/j.ijforecast.2020.06.008.

[21] S. I. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, and A. A. Atayero, "Memory-efficient deep learning for botnet attack detection in IoT networks," *Electronics*, vol. 10, no. 9, p. 1104, 2021, doi: 10.3390/electronics10091104.

[22] AILEPHANT Artificial Intelligence Lab, "Recurrent neural network," [Online]. Available: https://ailephant.com/glossary/recurrent-neural-network/ (accessed: July 11, 2018)

[23] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," *2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, ACT, Australia, 2015, pp. 1-6, doi: 10.1109/MilCIS.2015.7348942.

[24] Y. Fan, H. Yang, Y. Wang, Z. Xu, and D. Lu, "A variable step crow search algorithm and its application in function problems," *Biomimetics*, vol. 8, no. 5, p. 395, 2023, doi: 10.3390/biomimetics8050395.

[25] A. Askarzadeh, "A novel metaheuristic method for solving constrained engineering optimization problems: crow search algorithm," *Computers & Structures*, vol. 169, pp. 1-12, 2016, doi: 10.1016/j.compstruc.2016.03.001.

[26] S. Sohail, Z. Fan, X. Gu, and F. Sabrina, "Multi-tiered artificial neural networks model for intrusion detection in smart homes," *Intelligent Systems with Applications*, vol. 16, p. 200152, 2022, doi: 10.1016/j.iswa.2022.200152.

[27] R. Anne W., Kirubavathi G, Sridevi UK, "Detection of IoT botnet using machine learning and deep learning techniques," *Research Square*, 2023, doi: 10.21203/rs.3.rs-2630988/v1.

BIOGRAPHIES OF AUTHORS

Veena Antony is research scholar at Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu. She holds a master’s in technology with information systems security in computer science. Her research areas are cloud computing, internet of things, machine learning, deep learning, optimization, pattern recognition, and cryptography. She has published different research articles in various journals. She has reviewer of many international conferences. She presented papers at various national and international conferences. She is currently employed as assistant professor from St. Teresa's College (Autonomous), Kerala, India. She can be contacted at email: veenaantony22@gmail.com or veenaantony@teresas.ac.in.

Nainan Thangarasu is currently working as an assistant professor in the Department of Computer Science, at Karpagam Academy of Higher Education, Coimbatore. He is greatly fascinated with the advanced computing technology and research programs is cluster computing, cryptography and network security, cloud computing, artificial intelligent system, information security in large database and data mining as well as the strong teaching experience. His doctoral dissertation also focuses on advanced security systems with cloud computing, and he has published more than 20 publications in reputed journals, which he find would be a great addition to the success of your teaching and research department. He can be contacted at email: thangamrasu14@gmail.com or drthangarasu.n@kahedu.edu.in.