International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 11, No.1 (Apr-2022)
https://dx.doi.org/10.12785/ijcds/1101107

ANN Based Multiclass Classification of P2P Botnet

Chirag Joshi[1], Ranjeet K Ranjan[2] and Vishal Bharti[3]

[1]*School of Computing, DIT University, Dehradun, India*
[2]*School of Computing, DIT University, Dehradun, India*
[3]*Department of Computer Science and Engineering, Chandigarh University, Chandigarh, India*

Received 4 Jun. 2021, Revised 9 Feb. 2022, Accepted 9 Mar. 20122, Published 15 Apr. 2022

Abstract: In the virtual world, most of the cyber-attacks are done by Botnet. The Botnet is one of the most versatile threats because it can be controlled from a remote place. Most of the existing Botnet detection approaches focused on binary classification based on traditional machine learning, and these have some limitations. In this paper, a Multiclass classification method has been proposed for Botnet detection based on Artificial Neural Networks with some variations. The proposed model is used to detect different types of Botnet from a large pool of Botnet families. This paper has used a dataset consisting of seven different classes to train and test the model. In this work, we got promising results in terms of accuracy, 99.04%, and other performance measures. The accuracy of the proposed is better when compared with other traditional machine learning models when evaluated using the same dataset.

Keywords: Artificial Neural Network (ANN), Botnet, Multi-Class Classification, MCPF (Malware Capture Facility Project), Cyber Security

1. Introduction and Overview

With the rapid growth of the Internet, the number of Internet users is also growing exponentially. This yields a large volume of data transfer in terms of uploading/downloading. The data contains malicious threats. There is different type of threat are roaming in the world of the Internet, e.g. malware, spyware, spam etc. Usually, we get rid of them using antivirus in our system. But still, when entered into the computer, many threats stay in the background and start infecting all the computer systems we get to be connected. Botnet are robotic machine which is controlled by a person who resides at remote location and known as a Botmaster. In general, Botnet have different types and variations. Every day a new kind of Botnet comes with more destructive power than its predecessors. Therefore, there is a need to find out the properties of every new Botnet which comes in this world of Internet. Some of the latest Botnet attacks are DDOS (Distributed Denial of Service) Attack, Web Injection, URL Spoofing, DNS Spoofing.

Exiting Botnet has three different architectures as shown in Figure 1, and each of them has advantages and disadvantages. In all these architectures person who starts the attack is called as the Botmaster. Existing Botnet architecture can be classified as follows

A. Centralized Architecture

In the centralized architecture, the Botmaster will start the attack by sending malicious packets through spamming or spoofing. If a person clicks on that email the computer system will get controlled by a Botmaster. In general, Botmaster uses the Command and Control (C&C) method to send commands in order to perform malicious activities in infected computers [1]. The Botmaster will send malicious packets through that computer system to all the other computer systems in a network. In this way, a chain will be made in which computer systems get infected through the malicious packets. In this architecture, all the control will be in the hands of Botmaster, who has started the attack.

B. Peer to Peer Architecture

In Peer-to-Peer (P2P) architecture, the first phase of infection will be similar to centralized architecture. Botmaster gives control to the first infected computer system after getting the control [2]. Next, packets will be sent by the Botmaster through the first infected system to another computer system. When a greater number of systems get infected, all of them will be controlled by their predecessor only but not by the Botmaster. In this architecture, every computer system which gets infected becomes Botmaster after infecting a computer system.

C. Hybrid Architecture

Hybrid architecture, as the name suggests, is a combination of centralized and P2P architecture at different layers. In this architecture, Botmaster has the independence to use P2P or centralized architecture. Here, the Botmaster implements P2P and Centralized architecture at each of the layers depending on the

E-mail address: erchiragjoshiji@gmail.com, ranjeetghitm@gmail.com, mevishalbharti@gmail.com

type of attack. Every packet works differently in this architecture [1]. In [3], authors have proposed a hybrid P2P botnet architecture that overcomes the problem of Centralized architecture.

All these Botnet architectures are controlled by a Botmaster through Command and Control (C&C). The Command and Control (C&C) is the most crucial mechanism behind the working of all the architectures. In this method, when a computer system gets infected, it is controlled remotely by a Botmaster. Different commands will be sent by the Botmaster to the computer systems for further actions. Out of all these Botnet architectures, the most popular is the Peer to Peer (P2P) Botnet. This architecture is used by most of the attackers because in this architecture, all the Bots become Botmaster after they get infected by the previous Bot. P2P Botnets like Trojan, Peacomm [4], and Stormnet [5] have used the limitations of centralized architecture. In [6], authors have proposed a methodology that detects the P2P botnet in software defined networks. They have stated the amount of destruction done by P2P botmaster is huge in comparison to other botnet architecture.

Detection of P2P Botnet is always a difficult task because it has the ability to hide its identity. In centralized and hybrid architecture of Botnet vulnerability is more than the P2P Botnet. In recent years, Machine Learning and Deep Learning techniques have been prominent in the detection of Botnet. Authors in [7], [8], [9] used the different Machine Learning algorithms for the detection of P2P Botnet. Some authors have used the Deep Learning technique for the detection of Botnet [10], [11], [12]. However, there are not many literateurs on deploying Deep Learning to detect Multiclass P2P Botnets.

We present a Deep Learning approach for Multiclass P2P Botnet identification based on Artificial Neural Networks in this research. In this approach, we have selected the ANN architecture using an incremental method. In order to select our ANN architecture, we have started with one hidden layer and kept adding a new hidden layer. The architecture which has performed well is selected for detection of P2P Botnet. In order to evaluate our model, we have used MCPF (Malware Capture Facility Project) dataset [13]. The dataset is labelled with seven different classes and the proposed model is used to classify these multiple labels.

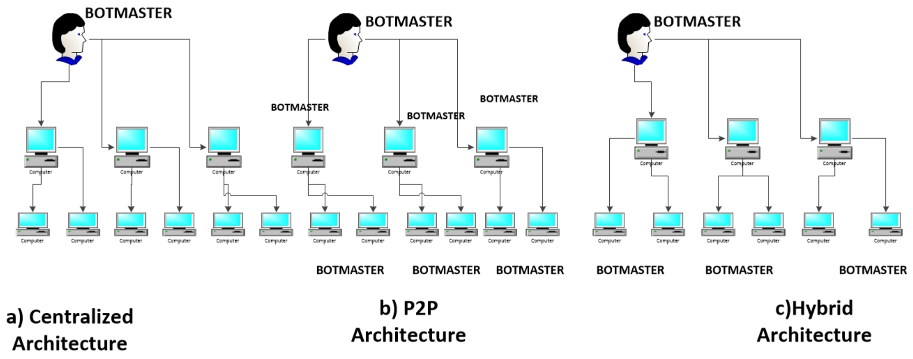
Section 2 covers related work in Botnet detection; Section 3 contains the detail about the dataset and its features, and presented the proposed method; Section 4covers the result and analysis. ; Section 5 presents the conclusion of this research.

2. Related Work

Many academics have been working on Botnet identification in recent years. The majority of the study focuses on Machine Learning and Deep Learning approaches. The raw data is also used for the detection and classification of malware traffic and generate different images of the flow for detection [14]. Some researchers also worked on the defence mechanisms against Command and Control (C&C) technique. They presented a survey on different attack mechanism like signature-based methods, DNS traffic analysis and malicious server detection [15]. PeerClean model is used to detect the real-time using only high-level features extracted from C&C network flow traffic. It works on the different clusters instead of an individual bot [16]. On the dataset, which comprises normal, background, and Botnet flow, different algorithms such as BotHunter, BClus and CAMNEP were compared. [13]. In [9], the authors examined and contrasted different machine learning algorithms for binary classification on the Botnet Dataset. A decision tree based structure is adopted in [17] for adaptive for successful detection of P2P Botnets. The MQTT protocol was deployed by the authors to detect the IOT-Botnet [18]. A review of malware is presented in [19]. Authors have reviews the different strategy and techniques for malware detection in HTTP traffic. The study shows that machine learning techniques are used widely for the detection of malware. Some authors also studied the different techniques for the detection android malware. The review comprises of signature and permission based methods [20].A framework is proposed to emulate diverse branch prediction behaviors and may be simply utilised by researchers to test the efficacy of more branch predictors. The experimental results presented in this paper compare the performance of several methodologies proposed for predicting conditional branching to that of using a machine learning technique [21].

In [22], Deep learning has been used to detect malware on Android. Fully connected layers and recurrent neural networks are used in the technique. Along with deep learning, the Feed Forward back propogation technique is employed for Botnet monitoring [11]. Botnet's diagnosis is also carried out using the Botshark framework. It is based on deep neural networks for network transaction inspections, as well as the Convolutional Neural Network (CNNs) [23]. In [24], for feature extraction, the researchers employed a Convolutional Neural Network (CNN), which will be valuable in predictive analysis. In [25], the model was evaluated on a real-world dataset, and the accuracy was determined to be satisfactory. On a Botnet dataset, various feature selection approaches are used to identify the greatest possible set of characteristics for binary classification [26]. Authors in [27] have given a study about different feature selection algorithms based on behavior analysis. After this the dataset has been classified into ransomware or non ransomware using supervised ML techniques.

Deep learning is also usually utilized in the health industry. Many scientists have also deployed deep learning approaches in tandem with autoencoders to diagnose a child's premature delivery [28]. A survey of deep learning methods in the field of agriculture is also presented in .[29]. The IoT Botnet dataset is also detected using LSTM. IoT devices are subject to a variety of



a) Centralized Architecture

b) P2P Architecture

c)Hybrid Architecture

Figure 1. Botnet Architecture

attacks, including botnets. Over time, researchers have shown that the bidirectional approach provides a better model [30]. In [31], researchers developed a method for detecting Botnet using graph nodes. On the features, it employs a self-organizing map clustering approach. On a blend of Botnet samples, researchers have also applied Transfer Learning techniques [32]. Some researchers have employed an approach that employs Multiclass classification algorithms. For handling multiclass imbalance, they used an LSTM-based system. [33]. In [34], authors employed a network flow detection method to detect Botnet. The dataset was subjected to a multiclass categorization. Deep learning or machine learning have been intensively researched for binary class categorization of Botnet in most of the existing literateurs. There are only a few litterateurs that have been proposed for Multiclass Botnet detection. This prompted us to use ANN to detect Multiclass Botnets.

3. Proposed Methodology

In this study, we propose an efficient deep learning methodology for the detection of Botnet. The approach is based on Artificial Neural Networks (ANN) for Multiclass classification. A Botnet dataset containing samples from several Botnet families is used to train and test (validate) the proposed ANN-based model. We compared the proposed model's results to those of various other machine learning-based methods. Figure 2 depicts the architecture of the proposed Botnet Detection technique:

The proposed methodology for identification of multiple types of Botnet are divided into the following steps:-

- Dataset Collection.
- Dataset Cleaning.
- Feature Selection.
- ANN Model Evaluation.

A. Dataset Collection

The dataset, which is used in this paper, contains both the Botnet and normal traffic. We have taken great care in selecting the dataset because we needed the maximum number of Botnet families in a dataset. The selected dataset is taken from MCPF (Malware Capture Facility Project) [13] dataset, which contains different families of Botnet. First, we have extracted the data from the pcap files from Wireshark. Wireshark helped us to view all those pcap file and we are able to extract the complete dataset from Wireshark.

The data used for training and testing of the proposed model consists of 8 features such as Protocol, Source Address, Source Port, Destination Address, Destination Port, Total Packet, Total Bytes, Source Bytes. The samples of the dataset belong to seven different Botnet families with their packet count in the dataset is listed in TABLE I.

B. Dataset Cleaning

Dataset Cleaning is needed to be done before applying any machine learning or deep learning model on the dataset. Data cleaning involves removing or correcting missing data. It is also done when data has some outliers or redundant values. The dataset we have selected for our experiments have some missing value for some features. We removed those missing data because we cannot apply any method for features like Destination Port, Source Port. We also convert the hexadecimal values of some features into decimals for our prediction. All the Botnet family's data were in different files so, we also need to merge them into a complete dataset that we have used in the proposed model. Dataset also consists of different kinds of data types and for deep learning algorithms the values in the dataset should not be in the form of string. We have used different encoders like label encoder, one hot encoder and column transfer for changing the string type data into the int or float.

C. Feature Selection

Feature selection is an essential task before the starting any type of classification. We have used different feature selection methods and also find out the accuracies based on extracted features which is shown in TABLE II. Based on the accuracy we got after using different feature selection methods, We chose to keep all of the features for our experiment because the proposed model's accuracy is higher when all of the dataset's features are used.

D. ANN Model Evaluation

In the proposed architecture, we have used Artificial Neural Network. We have used four hidden layers

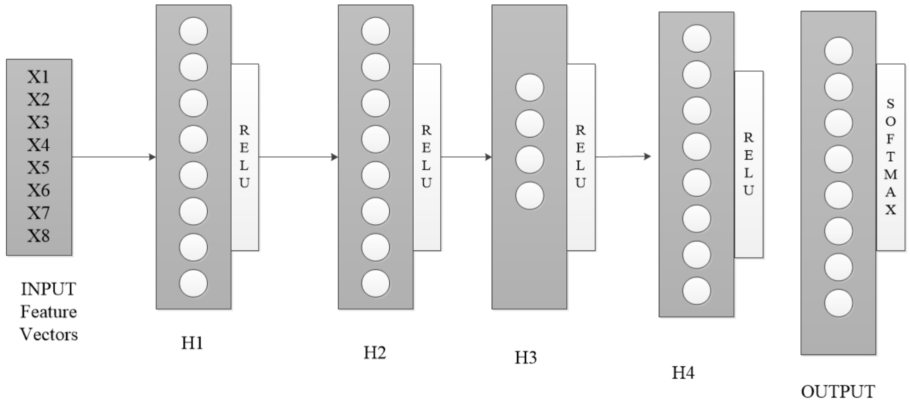


Figure 2. ANN Based Model

TABLE I. Botnet Families

S.NO	NAME	COUNT
1	Menti	4630
2	Murlo	1520
3	Neris	2693
4	NSIS	2168
5	RBOT	836
6	Sogou	63
7	Virut	901

TABLE II. Feature Selection Methods and Accuracy on the basis of Extracted Features

S.NO	Feature Selection Methods	Accuracy
1	PCA	91.25%
2	Univariate Selection	92%
3	Recursive Feature Selection	94.5%
4	Correlation Matrix	88.78%
5	Feature Importance	94.54%

H1, H2, H3 and H4. The input layer has eight units which take eight input features and the output layer has eight units which result an output vector to classify seven different malware families and benign packets. As described earlier, we have used an incremental approach for finding the number of hidden layers for the proposed ANN model. We have started with one hidden layer then added a second hidden layer, and similarly continued till the four hidden layers. The accuracy of the proposed model on the different hidden layers is shown in TABLE III.

We have opted to employ four hidden layers in the suggested model, according to TABLE III. Figure 2 depicts the proposed four-layered model.

Let a^i_j be an activation function for j^{th} unit of H^{th}_i layer and it is defined as

$$a_j = r[w^i_j * a^{i-1} + b] \tag{1}$$

where r(m)=max(0,∞) known as Relu Function.

The output layer of model has 8 feature vector. The output at this layer is defined as

$$y = S(\sum_{k=1}^{8}(w^i_j * x_i + b)) \tag{2}$$

where S(m) known as Softmax Function.

4. Implementation and Result Analysis

A. *Experimental Setup*

There are numerous platforms available for the implementation of Deep Learning and Machine Learning algorithms. We have used the online platform provided by Google known as Google Collab for our experiment. Google Collab is an online platform which provides a large size of RAM and Disk Space from different cloud server. Our dataset is is large in size and thus we have selected this platform for our experiment. Initially, we have given 102GB of Disk Space and 12 GB of RAM, which is sufficient for the proposed model execution. Different libraries are also used in this model, like Keras, NumPy, Pandas and TensorFlow. We have also used

TABLE III. Hidden Layer and their Accuracy

S.NO	Feature Selection Methods	Accuracy
1	One	93.45%
2	Two	94%
3	Three	96.78%
4	Four	99.04%

Wireshark for the extraction of the dataset from the flow packets.

B. Evaluation Metrics

For the evaluation of the suggested model, we used a variety of evaluation metrics.

Accuracy Accuracy of a model shows how accurately model is predicting the correct values.

Precision Precision tells the number of correct predictions of different Botnet families in this model. This metric's value ranges from 0 to 1. Nearer to 1, the model is more accurate. It can be calculated as

$$Precision = \frac{TP}{TP+FP}$$

Where TP stands for True Positive and FP stands for False Positive, as determined by the confusion matrix.

Above formula will works well in case of binary classification but in this paper we did multi class classification and for that above formula will be modified as below

$$Precision = \sum_{i=1}^{n} (\frac{TP_i}{TP_i+FP_i})$$

where n will be the number of classes , here in this model n=8.

Recall Recall tells the number of correct prediction of actual positive. It is also known as the sensitivity.Its value lies between 0 and 1.It can be calculated as

$$Recall = \frac{TP}{TP+FN}$$

Where TP=True Positive and FN=False Negative ,which will be derived from confusion matrix.

This formula will be for the binary classification and for multi class classification we will change the formula as

$$Recall = \sum_{i=1}^{n} (\frac{TP_i}{TP_i+FN_i})$$

where n will be the number of classes , here in this model n=8.

False Alarm Rate The number of incorrect predictions made by a model is known as the False Alarm Rate. It can be calculated as [8]

$$FalseAlarmRate = \frac{FP}{TN+FP}$$

Where,FP=False Positive and TN=True Negative.

C. Result Analysis

We applied the model, shown in Fig. 1, on the dataset and got the following result. We have also applied the other machine learning algorithms. TABLE IV contains the accuracy of all the algorithms we have applied on this dataset.

From TABLE IV, we can see that the accuracy of the proposed model is higher than the traditional machine learning algorithms. Even the Random Forest algorithm cannot perform accurately and produce an overfitted model. TABLE V shows the results of the various performance metrics calculated for the proposed work. The proposed model gives high Precision, Recall and F-Score value and low False Alarm rate.

We also compared the proposed model's accuracy to that of some existing models. TABLE VI shows a comparison of all current models with the proposed model in terms of accuracy. The comparison showing that the proposed model giving higher accuracy then existing model.

5. Conclusion

In this paper, we have evaluated Multiclass classification using an Artificial Neural Network (ANN). The proposed classification model is evaluated using the MCPF dataset. The dataset has seven different Botnet families on which we have trained and tested the proposed model and also some of the traditional Machine Learning Algorithms. Before using the dataset to evaluate the proposed model and other machine learning algorithms, we also performed some data cleaning and normalization operations on the dataset. The proposed model has given the highest accuracy of 99.04% with precision equals to 99.34% and recall value is 99.35% on the dataset. The outcomes of the proposed ANN based Botnet detection model has also been compared with some of the existing Multiclass Botnet detection models. The comparison result has established that the proposed model performs well on the MCPF dataset. However, there is a scope of

TABLE IV. Accuracy Comparison with Machine Learning Models

S.NO	Name	Accuracy
1	Proposed Model	99.04%
2	SVM	95%
3	Decision Tree	93%
4	Random Forest	1.0(Overfitted)

TABLE V. Different Measures of Classification

Model	Precision	Recall	F-Score	False Alarm Rate
Proposed Model	99.35%	99.35%	99.29%	0.484%

TABLE VI. Comparison with Existing Models

Model	Accuracy
WANG ET AL. [14]	98.52%
WEN-HWA ET AL. [35]	98 %
FEDYNYSHYN ET AL. [36]	92%
ANCHIT ET AL. [37]	94.78%
HECTOR ALAIZ-MORETON ET AL. [18]	96%
Proposed Model	99.04%

applying this model on some other dataset and test the performance.

References

[1] M. Stevanovic and J. M. Pedersen, "Machine learning for identifying botnet network traffic," 2013.

[2] A. Pektaş and T. Acarman, "Effective feature selection for botnet detection based on network flow analysis," in *International Conference Automatics and Informatics*, 2017, pp. 1–4.

[3] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 2, pp. 113–127, 2008.

[4] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study." *HotBots*, vol. 7, no. 2007, 2007.

[5] T. Holz, M. Steiner, F. Dahl, E. W. Biersack, F. C. Freiling *et al.*, "Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm." *Leet*, vol. 8, no. 1, pp. 1–9, 2008.

[6] S.-C. Su, Y.-R. Chen, S.-C. Tsai, and Y.-B. Lin, "Detecting p2p botnet in software defined networks," *Security and Communication Networks*, vol. 2018, 2018.

[7] L. F. Maimó, Á. L. P. Gómez, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, "A self-adaptive deep learning-based system for anomaly detection in 5g networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018.

[8] X. Dong, J. Hu, and Y. Cui, "Overview of botnet detection based on machine learning," in *2018 3rd International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*. IEEE, 2018, pp. 476–479.

[9] C. Joshi, V. Bharti, and R. K. Ranjan, "Botnet detection using machine learning algorithms," in *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences*. Springer, 2021, pp. 717–727.

[10] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, "Hybrid deep learning for botnet attack detection in the internet-of-things networks," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4944–4956, 2020.

[11] A. A. Ahmed, W. A. Jabbar, A. S. Sadiq, and H. Patel, "Deep learning-based classification model for botnet attack detection," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–10, 2020.

[12] C. Joshi, R. K. Ranjan, and V. Bharti, "A fuzzy logic based feature engineering approach for botnet detection using ann," *Journal of King Saud University-Computer and Information Sciences*, 2021.

[13] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," *computers & security*, vol. 45, pp. 100–123, 2014.

[14] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in *2017 International Conference on Information Networking (ICOIN)*. IEEE, 2017, pp. 712–717.

[15] J. Gardiner and S. Nagaraja, "On the security of machine learning in malware c&c detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 49, no. 3, pp. 1–39, 2016.

[16] Q. Yan, Y. Zheng, T. Jiang, W. Lou, and Y. T. Hou, "Peerclean: Unveiling peer-to-peer botnets through dynamic group behavior analysis," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 316–324.

[17] R. U. Khan, X. Zhang, R. Kumar, A. Sharif, N. A. Golilarz, and M. Alazab, "An adaptive multi-layer botnet detection technique using machine learning classifiers," *Applied Sciences*, vol. 9, no. 11, p. 2375, 2019.

[18] H. Alaiz-Moreton, J. Aveleira-Mata, J. Ondicol-Garcia, A. L. Muñoz-Castañeda, I. García, and C. Benavides, "Multiclass classification procedure for detecting attacks on mqtt-iot protocol," *Complexity*, vol. 2019, 2019.

[19] A. P. Singh and M. Singh, "A comparative review of malware

analysis and detection in https traffic," *International Journal of Computing and Digital Systems*, vol. 10, no. 1, pp. 111–123, 2021.

[20] A. A. Ali and A. S. H Abdul-Qawy, "Static analysis of malware in android-based platforms: A progress study," *International Journal of Computing and Digital Systems*, vol. 10, no. 1, pp. 321–331, 2021.

[21] S. Abudalfa, M. Al-Mouhamed, and M. Ahmed, "Comparative study on behavior-based dynamic branch prediction using machine learning," *International Journal of Computing and Digital Systems*, vol. 8, no. 01, pp. 33–41, 2019.

[22] X. Pei, L. Yu, and S. Tian, "Amalnet: A deep learning framework based on graph convolutional networks for malware detection," *Computers & Security*, vol. 93, p. 101792, 2020.

[23] S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, "Botshark: A deep learning approach for botnet traffic detection," in *Cyber Threat Intelligence*. Springer, 2018, pp. 137–153.

[24] C. Chen, P. Zhang, Y. Liu, and J. Liu, "Financial quantitative investment using convolutional neural network and deep learning technology," *Neurocomputing*, vol. 390, pp. 384–390, 2020.

[25] M. Alauthman, N. Aslam, M. Al-Kasassbeh, S. Khan, A. Al-Qerem, and K.-K. R. Choo, "An efficient reinforcement learning-based botnet detection approach," *Journal of Network and Computer Applications*, vol. 150, p. 102479, 2020.

[26] C. Joshi, V. Bharti, and R. K. Ranjan, "Analysis of feature selection methods for p2p botnet detection," in *International Conference on Advances in Computing and Data Sciences*. Springer, 2020, pp. 272–282.

[27] S. Malik, B. Shanmugam, K. Kannorpatti, and S. Azam, "Critical feature selection for machine learning approaches to detect ransomware," *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. XXXX–XXXX, 2022.

[28] L. Chen and H. Xu, "Deep neural network for semi-automatic classification of term and preterm uterine recordings," *Artificial Intelligence in Medicine*, vol. 105, p. 101861, 2020.

[29] A. AlKameli and M. Hammad, "Automatic learning in agriculture: A survey," *International Journal Of Computing and Digital System*, 2021.

[30] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the internet of things using deep learning approaches," in *2018 international joint conference on neural networks (IJCNN)*. IEEE, 2018, pp. 1–8.

[31] S. Chowdhury, M. Khanzadeh, R. Akula, F. Zhang, S. Zhang, H. Medal, M. Marufuzzaman, and L. Bian, "Botnet detection using graph-based feature clustering," *Journal of Big Data*, vol. 4, no. 1, pp. 1–23, 2017.

[32] B. Alothman and P. Rattadilok, "Towards using transfer learning for botnet detection," in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2017, pp. 281–282.

[33] D. Tran, H. Mac, V. Tong, H. A. Tran, and L. G. Nguyen, "A lstm based framework for handling multiclass imbalance in dga botnet detection," *Neurocomputing*, vol. 275, pp. 2401–2413, 2018.

[34] L. Mathur, M. Raheja, and P. Ahlawat, "Botnet detection via mining of network traffic flow," *Procedia computer science*, vol. 132, pp. 1668–1677, 2018.

[35] W.-H. Liao and C.-C. Chang, "Peer to peer botnet detection using data mining scheme," in *2010 international conference on internet technology and applications*. IEEE, 2010, pp. 1–4.

[36] G. Fedynyshyn, M. C. Chuah, and G. Tan, "Detection and classification of different botnet c&c channels," in *International Conference on Autonomic and Trusted Computing*. Springer, 2011, pp. 228–242.

[37] A. Bijalwan, N. Chand, E. S. Pilli, and C. R. Krishna, "Botnet analysis using ensemble classifier," *Perspectives in Science*, vol. 8, pp. 502–504, 2016.

Mr.Chirag Joshi Mr.Chirag Joshi is a PhD Research scholar at DIT University, Dehradun. He has complted his M.Tech (CSE) in 2012 from SCSIT, DAVV, Indore (M.P). His research area is Machine Learning, Deep Learning and Cyber Security.ORCID ID:- https://orcid.org/0000-0002-5392-6590

Dr.Ranjeet K Ranjan Dr.Ranjeet Kumar Ranjan currently working as an Assistant Professor at DIT University, Dehradun, India. He has completed his Ph.D. degree from School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India. His research interests include Data Warehousing, Machine Learning, Deep Learning and Cyber Security.ORCID: https://orcid.org/0000-0002-8796-4579

Dr.Vishal Bharti Dr. Vishal Bharti is working as Professor and Additional Director at Chandigarh University, Mohali, Punjab. Previously he worked as Professor & Head in Department CSE at DIT University, Dehradun. He completed his Ph.D. in 2016 in the area of Information Security. He did his M.Tech.and B.E. from Birla Institute of Technology, Mesra. Ranchi. His area of specialization is Cyber Security, Network Security and Distributed Computing. ORCID ID:- https://orcid.org/0000-0002-7806-9169