IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN INTRUSION DETECTION SYSTEM FOR NETWORK SECURITY USING RECURRENT NEURAL NETWORK

1)Age Yuvraj B. 2)Jadhav Kishor P.3)Dahe Abhay S. 4)Battise Yash R. 5)Game Pavan S.

1)DEVELOPER, 2)GUIDE, 3)DEVELOPER, 4)DEVELOPER, 5)DEVELOPER

Computer Technology.

SANJIVANI K.B.P.POLYTECHNIC,KOPARGAON,INDIA.

Abstract: To maintain the security of vulnerable network is the most essential thing in network system; for network protection or to eliminate unauthorized access of internal as well as external connections, various architectures have been suggested. Various existing approaches has develop different approaches to detect suspicious attacks on victimized machines; nevertheless, an external user develops malicious behaviour and gains unauthorized access to victim machines via such a behaviour framework, referred to as malicious activity or Intruder. A variety of supervised machine algorithms and soft computing algorithms have been developed to distinguish events in real-time as well as synthetic network log data. On the benchmark data set, the NLSKDD most commonly used data set to identify the Intruder. In this paper, we suggest using machine learning algorithms to identify intruders. A signature detection and anomaly detection are two related techniques that have been suggested. In the experimental study, the Recurrent Neural Network (RNN) algorithm is demonstrated with different data sets, and the system's output is demonstrated in a real-time network context.

Keywords: , Recurrent Neural Network, KDDCUP99, Intrusion Detection System, Network security.

I. INTRODUCTION

The IDS is responsible for detecting a connection form of attack, such as a fragment of unknown attack, a DoS attack, a U2R attack, or an R2L attack. It then deploys a series of such components one by one in a sequential fashion. This accomplishes two objectives: For starters, each sub-phase can only train a limited amount of characteristics that detect a specific form of attack. Second, the sub-size unit is still small enough to be helpful. A common disadvantage, similar to our system, is that it increases the amount of time it takes for modules to communicate. However, in our system, this can be easily prevented by making each sub-phase independent of the other layers. As a result, specific characteristics can be observed in more than one sub-phase. If an offense is committed without a centralized decision-maker, any thread will block it, depending on the channel's security policy. Numerous sub phases mainly function as filters blocking suspicious associations as long as they are formed during a specific layer, allowing for a quick response to the intrusion while also reducing analysis time in successive phases. It should be noted that in different sub-phases that rely on sight-trained attacks, completely different responses are often initiated. At the first layer and in subsequent stages, the amount of system-analysed auditing information decreases further as more and more attacks are detected and blocked. In the worst case, if no attacks are detected prior to the last sub-phase, all staggered sub-phases in phase 2 have the same load. However as attacks are detected and blocked in any subsequent method, the average load is expected to be significantly lower. On the other hand, when the sub-phases are arranged in parallel rather

than in a series, in a sequence configuration on a subsystem, the load is equal to the worst case. The initial step can be repeated in the sequential configuration to perform load balancing to improve performance.

Based on its position selection protocol, which operates on both HIDS and NIDS, the method describes generating RNN rules in this current research. A genetic algorithm is a solution-finding algorithm that uses genetics to find the best solution. The became too with various classifiers can provide the best identification of NIDS for all types of genius sub-attacks. The theoretical study aims to develop consistent guidelines and improve DOS, PROBE, U2R, and R2L malware detection for NIDS and HIDS.

II. LITERATURE SURVEY

This article uses the ANN (Artificial Neural) of an Operating System Sensor to monitor malicious activities in Android and ios devices, based on the Flow anomaly system [1], based on the flow anomaly Detection Platform for Android mobile devices. The detection rate of this approach is 85 percent and 81% accuracy, respectively. Impersonation is considered in terms of CPU, space and better view, which helps to characterize a small, scalable and effective IDS after an Integration node to combat public attacks by various services. By using powerful data mining algorithms, the data sources are analysed. Improving the accuracy and classification rate requires the future scope.

PRADEEP and Dr. Yogesh Kumar [2] Effectual Secured Approach for the Internet of Things with Fog Computing and Mobile Cloud Architecture Using Ifogsim, this work cloud computing performance is assessed Simulation model world using iFogSim, where artifacts and Cloud services provide a greater degree of consistency and Precise.

Javier A. et al. proposed in [3] information security boosting using malware detection in a network environment. The platform designed would be an efficient algorithm for malware detectors for ghana limited application security due to extensive Framework. In the final research, the participants are already confident and pleased with their reliability and functionality. The research revealed this device met that experiment's goal. "High Quality" analyzed the processes and solution to the proposed method. The development of the malware detection system for Asia Technology Security to maintain its position was successful.

Bholanath Mukhopadhyay et al. [4], cloud-based task scheduling and Protection using SSL for IaaS Application, implemented a new approach wherein we built both protection and authorization access policies. We also implemented the functionality of an Endpoint Protection choice search. In our configuration, numerous profiles can be built, one with its own different access policy, for various network applications. For illustration, for dynamic access point connections, and internet connectivity authentication policy can be developed. Using our unorthodox technique, it is possible to quickly classify the user, customer location, existing network situation at the time of connection, and server status.

Self-Taught Learning (STL) with an inter RNN has used and according to [5] IDS to preserve the high highest accuracy of the IDS, except in unknown waters. The Neural Learning, a deep learning-based algorithm of vehicle routing modeling to promote the continued survival home, uses a self-healing approach in the IDS recovery phase. Simulation results indicate the efficacy of Precision, Precision, and accuracy of the proposed IDS against cyber security attacks on UAVs. This system able to prevent potential cyber-attacks such as GPS hacking and bumping, a drone's contact patterns lost, compromised, or hijacked etc.

According to study [6] describes the use of computer and machine learning technologies in Wireless Sensor Environments for IDS systems. It introduces Deep Boltzmann Computer Distributed DBCD-IDS. A possible need plenty of IDS technique for WSNs to track sensitive systems to execute that. RBC-IDS performance is studied and compared to the previously suggested efficient machine teaching IDS: the Adaptively Monitored and Grouped Hybrid IDS. This system experiments indicates that duplicate detection and accuracy rates are obtained by RBC-IDS and ASCH-IDS, while RBC-IDS provides better detection over the ASCH-IDS. Security vulnerabilities, including intrusions into network systems and sink nodes, may occur in either a cyber or digital portfolio. As an essential solution for computer security, Remote Monitoring has been implemented to deal with external aggression in communication systems and

immediately identify a different intrusion. The Restricted Boltzmann Machine (RBM) is a two-layer neural, energized network: visible (V) and hidden (V) (H).

A classifier is investigated in [7] Deep Naive Bayes to build a scalable and efficient IDS to detect and identify unexpected cyber-attacks. The constant change in network architecture and rapid attack development makes it essential to evaluate different datasets created by simple and complex strategies over the years. This form of research promotes discovering the best algorithm that can work effectively to identify potential cyber-attacks. On different publicly accessible benchmark minicom, a thorough assessment of observations on Datasets and other robust machine learning SVM classifiers seen. Using super configuration selection methods with the KDDCup 99 dataset, optimum system configurations and networking protocols for DNNs have been picked. All DNNs experiments have performed up to 1,000 iterations with a learning rate varying in the[0.01-0.5] range. The DNN template that worked well on KDDCup 99 added to the test's performance on specific datasets like NSL-KDD, UNSW-NB15, Kyoto, WSN-DS, and CICIDS 2017. Bypassing then into several hidden layers, this DNN model can learn about the complicated but high detailed image classification of the IDS data. It was verified by rigorous experimental research that DNNs performs well compared to classical classifiers. .A category for ANN is defined as a directed graph to transfer different display adapter along edges through one node to that without generating a cycle. Recurrent neural system

According to [8] the malicious activity identification using a structural steel part identifying formulation and construction provided by IDS-DLA framework. There is a massive volume of forms but found helpful, provided the composite materials. Using Mathematical and CNN triplet filters, IDS-DLA performs high precision and intrusion recognition from the Point cloud database. The IDS-DLA also tests the Hu moments ranking to pick its top 5 ranking forecasts as final results obtained. Undoubtedly, it was found from the experiments that high precision is achieved compared to the previous benchmarks. Using hybrid feature extraction approach and multi-filtering approach concludes that achieves greater efficiency. The main factors will be the coordination between humans, materials, and the corresponding machines with correct recipes to improve or increase the production lines' overall efficiency.

In combination with [9], the durability of IDS focused on computer vision against intrusion detection. This refers to the min-max method in the UNSW-NB 15 dataset to train intrusion detection systems against crown prosecution samples. On the other hand, this uses the current min strategy as a security strategy to optimize the detection mechanism that minimizes the loss during training data of the integrated adversarial samples. This research tests and calculates the efficacy of the techniques of malicious attacks and the resistance of the training images against such attacks. This system used a methods of remote attack that have been built in binary environments should be used in trustworthy environment and generate network attacks. Finally, this shows that removing the primary component analysis function will improve the robustness of the sensor network using a learning algorithm. Each column has 49 characteristics, including the class name, in the dataset. You pick the best 28 features known as feature ranking (or score). Regularization is also used to select several features with a broader composition to enhance the classifier's effectiveness and reliability.

Anomaly dependent on Flow. [10] This paper on Android Mobile Devices' flow-anomaly intrusion detection framework uses ANN in the Android OS to detect Android behavior. This technique has a detection rate of 85% and 81%, respectively. Imitation of the CPU, memory and battery power are taken into consideration. This work seeks to classify lightweight, scalable, successful IDS in a variety of public attack services in an Android environment. Using powerful machine learning algorithms, the data streams are analysed. The rate of detection and precision will be increased in the future.

A Secret Markow IDS software-defined network is created, as suggested [11] (SDN). By examining the Webs in a hole and deciding to protect the network based on data from the entire system, including the use of ANN IDS, the SDN network can track the overall safety of a system. The paper has benefits such as improved behavior and increased safety. To further extend the HMM vector to evaluate the maliciousness of a collection of data, it represented the potential for an app to access the networking risk.

Loganathan, Gobinath et al. according to [12] Present a new multi-attribute method to estimate a network packet sequence based on past packets using the Sequence-to-Sequence (Seq2Seq) encoder-decoder algorithm. This The model is used to learn the standard sequence of packets in TCP communications in an attack-free dataset, and is then used to classify anomalous packets in TCP traffic. We demonstrate that the experimental multi-attribute model Seq2Seq identifies anomalous raw TCP packets in the DARPA 1999 dataset which are part of 97 percent intrusions through precision. It can also detect selected

intrusions with 100% real-time precision and surpass existing algorithms based on replicated neural network models, like LSTM. The Detecting Irregularities in raw TCP packets via a Seq2Seq algorithm designed specifically for sequences with different attributes. Packets in connections apart from regular network traffic are used to train the model system. Anomalies are known to science as actual packets which deviate significantly from the packets planned. Training the model on normal traffic rather than intrusion traffic gives access to extensive training data and enables the model to detect even new unknown threats which deviate from regular traffic pattern.

According to [13], This paper describes a system for intrusion detection of PS-Poll DOS infiltration in 802.11 networks, using a distinct case structure in real time. This methodology utilizes RTDES to track DOS attack on a single Event System in real-time. High detection rate and accuracy rate are one of the significant advantages, but shortage of frames is one of the major drawbacks. This system also able to detect software as well as hardware attacks simultaneously.

A PS-Poll DOS attack intrusion detection system for 802.11 networks using a single real-time event system, depending on[14], is defined in this paper. This method utilizes RTDES on a discrete event system to detect DOS attacks in real time. One of the key benefits is the high detection rate and precision, but the main downside is the lack of frames. Detection of PS-DOS attacks includes protocol or proprietary hardware installation changes.

[15] Serious problems in cyberspace have been identified as cyber security. By means of a deep learning methodology, the paper demonstrates a cognitive neuromorphic computing technology for the cyber safety network ID method. This approach uses differential factorization of vectors. The NSL-KDD dataset improves precision and scoring by up to 90.12% and 81.31% respectively. Deep learning, a comprehensive learning approach that incorporates classification characteristics, is especially successful in recognition tasks. The task for the future is to decide the interpretation for use in the spiking format of the actual northern data structure.

III. PROPOSED SYSTEM

Machine learning methods were used to identify and avoid intrusions in the current research methods. The runtime packets data block will conduct training, including packet selection for remote data monitoring. The role collection for a particular packet operation will then be submitted. Send it forward as a group if all is well. Misconduct samples will be examined for feature selection for different attributes in order to identify individual attacks. Figure 1 illustrates the system's entire execution using specified algorithms. To produce train modules and conduct research, various machine learning techniques were employed. The goal of proposed anomaly network intrusion detection system is to maximize the detection accuracy, to minimize false positive rate and detector generation time. Basically there are two phase in the proposed system, system have taken NSLKDD dataset for system training as well testing purpose.

The proposed System worked with an ensemble configuration. When two or more combinations form a new model commonly called an ensemble model. This ensemble model incorporates input from multiple classifiers and has produced a single composite classification. Our conceptual structure consists of numbers for the classifiers. First, the software receives data from various outlets, both online and offline. Once the data is collected by software, other data mining strategies will be applied in different classifications approaches.

Training Phase:

1. Upload training data for feature extraction.

2. Apply PSO for rule creation

3. Create rules set as normal pool as well as intrusion pools set.

Testing Phase:

1. Upload Testing data or any packet which is collected from network environment.

2. Extract all features using attribute selection.

3. Apply Normalization approach on dataset.

4. Apply ensemble approach on all train as test features.

5. Show results with classification accuracy.

6. Classify all attacks.

7. Show detection results.

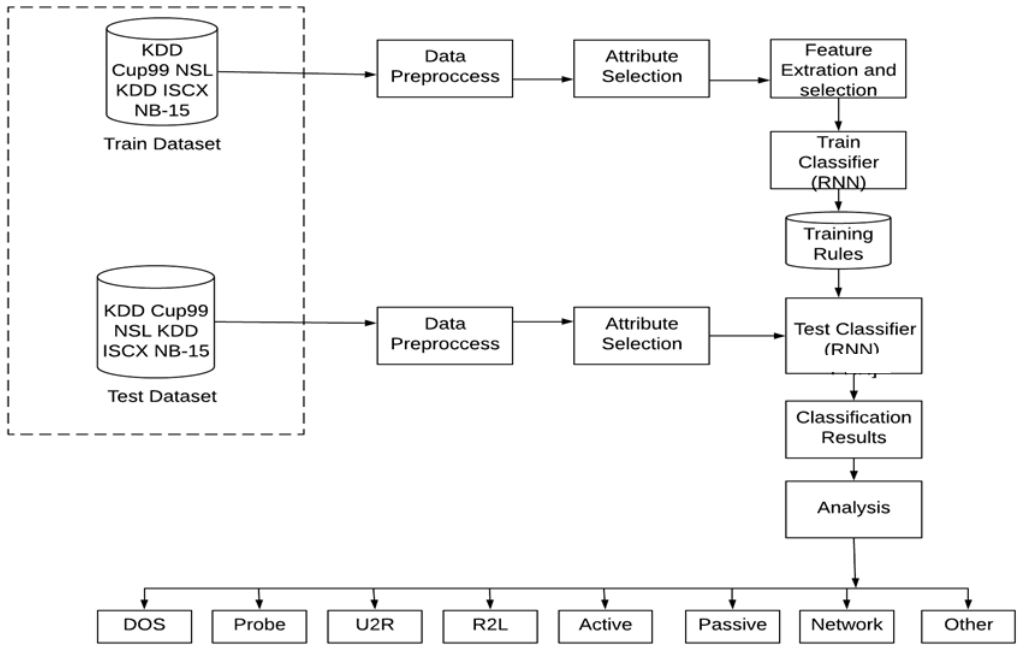

Figure 1 : Proposed system architecture

System initially collects the input packet from various sources like KDD CUP, NSL KDD, ISCX and real time network packets. The entire execution holds three different phases which are listed as below.

Module 1: Intrusion Detection System (IDS) this Step implements the first Genetic Algorithm and Fuzzy Algorithm for task extraction and context development rules.

Module 2: Intrusion Prevention System (IPS) This work to prevent known attacks which have already been generated from remote sources. For device avoidance any classification algorithm is used. Naïve Bayes, ANN, weight calculation algorithms J48 method to find the same network movement and packet signature.

Module 3: Intrusion Response System called as (IRS), It carried out the security from various kind of unknown attacks as well as malicious behaviours. The system executes the ensemble modules with the help multiple machine learning classifiers for detecting malicious activity.

MATHEMATICAL MODEL

System_Execution = {Train_Module, Test_Module, Analysis_Module }

Train = { RNN, Fuzzy_Logic, ANN_Module, J48_Algo, NB_Module }

RNN = { Input Layer → Convolutional → Activation function→ pooling → Selection_Function }

Fuzzy = { Probability, {0,1}}

{ GA → Fuzzy → ARM → } {0,1}

Test = {Pattern_Match, Threshold, Weight, Attackclass, Subclass }

Class = { Input → Bk_Rule → Calc_Weight } → { Normal, Attack } → { subattacks }

Analysis = { dos,probe,U2R,R2L,Normal,unknown }

IV. RESULTS AND DISCUSSION

We measure the confusion matrix for the system after it has been successfully implemented. The classification output of data collection by KDDCUP using the density-based method of the machine learning algorithm software is shown in Table Figure 2. Figure 3 shows how various methods, such as the RNN algorithm, were used to identify and predict the precision of the proposed system.

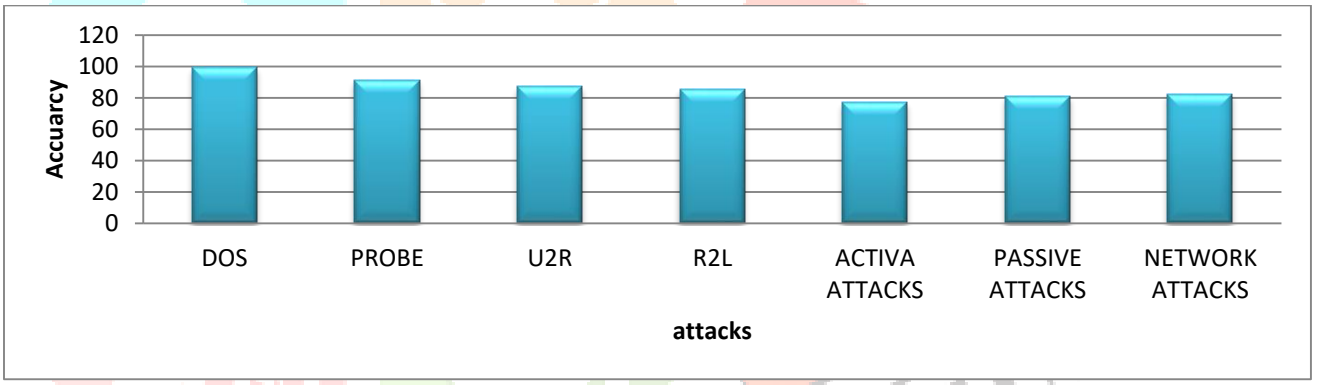

Figure 2 : detection accuracy with various attacks using RNN classification

According to the results of the second experiment, RNN with sigmoid has a higher classification accuracy than the other two activation functions, ReLU and TanH (see Figure 3). Based on the results of the above experiment, we may infer that the proposed framework improves the accuracy of trust computation in the IoT in-service environment. The entire study is driven by a collection of simulation environmental conditions and a mix of machine learning techniques. With regards to machine learning algorithms, a variety of computation specifications have been used clusters distinction and id.mi.com.

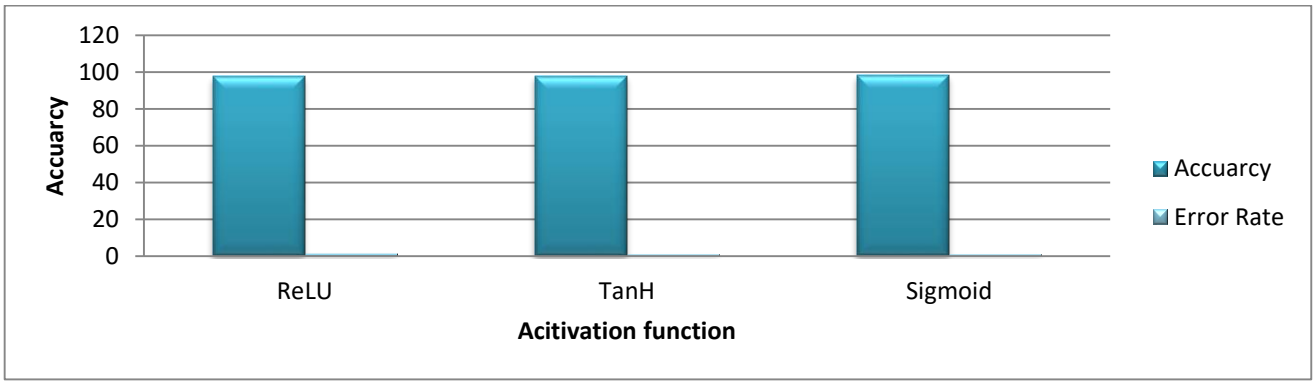

Figure 3: Experimental analysis of RNN with three activation function

5. CONCLUSION

In this research we proposed an efficient IDS scheme, this research proposes an RNN-IDS approach focused on deep learning. We used the numerous real time networks as well as some synthetic dataset to evaluate anomaly detection and classification accuracy. We also use deep learning to apply IDS in the cloud environment in the future. In addition, we examine and compare different deep learning approaches, such as. During the data search, the software basically functions as an RNN classification and soft computing algorithms to evaluate the unknown type of connection and attacks. To improved classification and high-class identification are possible important to the powerful rule structure. Several studies have been used for experimental investigation for evaluate the algorithm's effectiveness using a variety of methods, and we came to the conclusion that we were getting satisfactory results..

REFERENCES

[1] Panagiotis I. Radogloa-Grammatikis; Panagiotis G. Sarigannidis, "Flow anamoly based Intrusion Detection System for Android Mobile Devices", 2017 6th International Conference on MOCAST, May 4-6, 2017, Kazani, Greece.

[2] PRADEEP, S.; SHARMA, Dr Yogesh Kumar. Effectual Secured approach for Internet of Things with Fog Computing and Mobile Cloud Architecture Using IFogSim. WE C-2019-London, UK, DOI, 2019, 978-988.

[3] Jaevier A. Villanueva, Luisito L. Lacatan, Albert A. Vinluan, Information Technology Security Infrastructure Malware Detector System, International Journal of Advanced Trends in Computer Science and Engineering, pp. 1583-1587 ,Volume 9, No.2, 2020.

[4] Bholanath Mukhopadhyay , Dr. Rajesh Bose, Dr. Sandip Roy, A Novel Approach to Load Balancing and Cloud Computing Security using SSL in IaaS Environment, International Journal of Advanced Trends in Computer Science and Engineering, pp. 2130-2137,Volume 9, No.2, 2020.

[5] Arthur, Menaka Pushpa. "Detecting Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS." 2019 International Conference on Computer, Information, and Telecommunication Systems (CITS). IEEE, 2019.

[6] Otomo, Safa, Burak Kantarci, and Hussein T. Mouftah. "On the feasibility of deep learning in sensor network intrusion detection." IEEE Networking Letters 1.2 (2019): 68-71.

[7] Vinayakumar, R., et al. "Deep learning approach for the intelligent intrusion detection system." IEEE Access 7 (2019): 41525-41550.

[8] Sheu, Ruey-Kai, et al. "IDS-DLA: Sheet Metal Part Identification System for Process Automation Using Deep Learning Algorithms." IEEE Access 8 (2020): 127329-127342.

[9] Abou Khamis, Rana, M. Omair Shafiq, and Ashraf Matrawy. "Investigating Resistance of Deep Learning-based IDS against Adversaries using min-max Optimization." ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020.

[10] Panagiotis I. Radogloa-Grammatikis; Panagiotis G. Sarigannidis, "Flow anamoly based Intrusion Detection System for Android Mobile Devices", 2017 6th International Conference on MOCAST, May 4-6, 2017, Kazani, Greece.

[11] Trae Hurley, Jorge E. Perdomo, Alexander Perez-pons, "HMMBased Intrusion Detection System for software-defined networking", 2016 15th IEEE Conference on Machine Learning and Application, Dec 18-20, 2016, Miami, Florida.

[12] Loganathan, Gobinath, JagathSamarabandu, and Xianbin Wang. "Sequence to sequence pattern learning algorithm for real-time anomaly detection in network traffic." 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE). IEEE, 2018.

[13] Mayank Agarwal, SankethPurwar, Santosh Biswas, Sukumar Nandi, "Internal Detection System for PS-Poll DOS attack in 802.11 networks using real-time discrete event system",IEEE,vol.4,issue4,2017.

[14] Mayank Agarwal, Sanketh Purwar, Santosh Biswas, Sukumar Nandi, "Internal Detection System for PS-Poll DOS attack in 802.11 networks using real-time discrete event system",IEEE,vol.4,issue4,2017.

[15] Md Zahangir Alom, Tarek m. Taha, "Network Intrusion Detection for cybersecurity on neuromorphic computing system", 2017 International Joint Conference on Neural Networks (IJCNN), May 14-15,2017, USA.