International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

An Improved Method in Recurrent CNN by using IDS

Sanjay Kumar[1], Jagpal Singh[2]

[1,2]*Department of Master of Computer Application, Compucom Institute of Information Technology and Mangement, Jaipur, India*

***Abstract*-- IDS is a hardware or software program that continuously scans the network of systems for malicious behaviour and policy violations. IDS looks for any potentially dangerous connections in the data. Technically speaking, IDS are designed to do three key security tasks: monitoring the data, identifying any transactions that might be dangerous, and ultimately, responding to illegal activity.Due to the Internet's enormous size, distributed nature, and lack of a centralised security system, assaults cannot be prevented, making detection and recovery from attacks essential. The IDS performs precisely what its name implies—it finds the potential incursion. To investigate the effects of applying wavelets to the classification model for network intrusion detection's detection coverage.**

***Keywords*—Intrusion Detection, Recurrent Neural Networks.**

I. INTRODUCTION

The term "intrusion" refers to a group of actions intended to get through a computer network or system's security measures. Finding intrusions is a necessary first step in implementing the appropriate measures. Intrusion Detection is the process of keeping an eye on a network connection to look for any potential intrusions, and IDS is the system in charge of looking for intrusions in network traffic. Intrusions are aimed at compromising one ormoreofthethreebasicsecuritygoalsofthenetworksystem:confidentiality,availabilityandintegrity[1]. The user from the outer world Internettogainaccesstothesystem,orthelegitimateandauthorizeduserwiththeintentionofgainingadditionalprivileges,andtheauthorizedusersmisusing the privileges given to them can initiateintrusions. classify attacks into seven broad groupsasgivenbelow:

- *Infection:* This attack is aimed at installing theharmful files or tampering the valid files therebyinfecting the files. These attacks can be further sub-categorizedasviruses,worms,andtrojansetc.
- *Exploding:* This attack is aimed at overflowingthe victim with bugs, the prominent attack of thistypeisbuffer-overflow[2].
- *Probe:*Thisattackisaimedatcollectingvitalinformation about the network so as to identify thepotentialentrypointsthatcanbecompromised.Some information of interest for an attacker can beto check which services are running, what InternetProtocols(IP)addressesareworkingcurrently.Some attacks falling in this class are Port Scan, IPscanandNmap.
- *Cheat:* These attacks are aimed at gaining accessthenetworkbyimpersonationi.e.,byprovidinga fake identity to access secured files of the system.Some oftheattacksfallingin this class are IP Spoofing, Session Hijack ingetc.
- *Traverse:* The attacks of this type attemptto break into the system by performing a passwordmatchingagainstallthepossiblepasswords.Dictionary attacks and brute force attacks are a fewexamplesofthistype.
- *Concurrency:* Attack soft his typecapitalize on one or more weaknesses of the systemto carry out some disastrous actions. A prominentattackofthissystemisDDoSwhereinsystemresources are exhausted, so as to deny it serving the legitimate users.

Various categories based on their carrier, and themostpopularcarrieroftheattackshasbeenmalwareAtypicalnetworkconfigurationisdepicted.Inthisnetworklayout, anetworkisconnected to an external network, there is a firewallto filter the disastrous connection originating fromthe outer world directed towards the network. Thefirewall is the first line of defense to block anyharmfulconnections. Ascanbeseenfromthefigure, gateways are positioned at the entry of then etwork, sotechnicallytheyareabletofilterout the connections that originate from / directed to ahostintheoutsideworld.IDS'sarepositionedinsidethenetwork, ratherthanblocking[3]thenetwork connections. Its goal is to examine network connections for any potential dangerous connections. IDS works to find potentially hazardous connections that have managed to get past the firewall.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

An IDS scans[4] for potential network attacks and launches the corrective action by notifying the system administrator.

II. Related Work

- *Anomaly Detection for IDS*

Methods for anomaly-based detection are based on the evaluation of profiles that represent typical traffic patterns. These techniques were introduced with the intention of automatically identifying zero-day attacks. These models start by continuously tracking network activity before building a baseline profile of the expected traffic. Any new action that departs from the typical profile is hence regarded as abnormal. Too many false alarms could be a problem with this approach because it can't handle idea drift. Any deviation from the typical profile, no matter how little, will be reported as an anomaly. While many different methods have been used to create anomaly-based systems, we solely record the models based on statistical and machine learning techniques in this review.

III. Statistical Methods

The statistical models are built on the premise that two system profiles should be kept active throughout the anomaly identification process. The two statistical profiles are made up of the most recent statistical profile, which is based on the system's variables across time, and the statistical profile that is now being observed.

The observed network behaviour is compared to the most recent behaviour using statistical models to create a profile of the normal traffic activity. If there is a significant difference between the observed behaviour and the most recent behaviour, the current behaviour is treated as anomalous; otherwise, the behaviour is considered to be normal. The statistical method's methodology entails fitting the training data into a statistical model and running a statistical deduction test on each unknown piece of information to determine its class.

[5] The instances which score very low probabilityinthedeductiontestbythelearnedmodelaredeclare dasanomalies.Statisticalmodelincludesparametric and non-parametric techniques to buildthelearningmodel. While non-parametric techniques do not assume knowledge from the distribution of the data, parametric techniques attempt to learn things by examining the distribution of the input data [6].

[7] created a learning model based on the differences between the attributes by utilising three expectation-maximization algorithms and statistical anomaly detection techniques. In order to increase the probability that a user would correctly identify which qualities reflect an abnormality, they divided data attributes into indicator attributes and environmental attributes. The indicator property was created to read successive data instances, learn the environment, and classify whether or not an anomaly has occurred. If the environmental attributes were not conditional over the indicator attributes in the statistical technique, the indicator attributes were ignored. Despite having high recall and precision values, the model was nonetheless adaptable to any learning environment.

To remove the abnormalities from the network flow, [8] used statistical hypothesis testing and an unconditional - stable first order model. The Generalized Likelihood ratio test was used to classify the marginal distribution of the initial traffic and to model and function it. The suggested research located anomalies like flash floods and crowding. A non-parametric adaptive cumulative sum approach was additionally used as an extension of this work[9] for the statistical calculation and identification of anomalies in network traffic.

The Flow-based Statistical Aggregation Scheme (FSAS), a flow-based statistical IDS, was created by combining two components: a feature generator and a flow-based detector. The feature generator was created with network traffic collection in mind.

And reports were produced by event handlers and given to the flow management module, which made the decision on whether the packet was already a part of the flow or whether a new flow key needed to be formed [10]. The flow keys were examined, collected, and dynamic updating was carried out in accordance with the flow keys. The flows were transformed by the event time module into a format that the statistical model could use. The neural network classifier graded the score vectors based on how harmful the data was. If the flow had more hostile data, it was rated as having a higher possibility of being an attack.

IV. Proposed Methodolgy

TheRNN architecture [9] is the addition of sequentialin formation to the feed forward neural network. The RNN performs the same task for each part. This is why it is called are current network; the output is dependent upon the previous computation.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

The hidden computation of RNN [11][12] is computed as given below: where denotesthehiddenstatevectorattimet; σ is the activationfunction,alsoknownasthenonlinearity function[13];isthehiddenweightmatrix[14][15]; is the hidden to hidden weight matrix; is the input vector attime t; and isthe biasterm.

$$H_t = \sigma\left(Wx_t + VH_{t-1} + b_H\right), t = T, \ldots, 1,$$

Workingofproposedapproach [16] Let us assume thatthereisarandomvariable *X*takingon*N* differentvalues.Letusassumethatoutofthe*N* values there are into tal*n*uniquevalues[16]afeature *X* can take. One of the working hypothesisforthisworkisthat if,Basis[26] function is used to develop the model.The reason for choosing RNN is that it has a rich setof kernel functions that can be used effectively withthe different data. The RNN model[27] is trainedwith a series of gamma

V. RESULTS

Afterreducingthe data- set then extstepistocheckouthow good o rbad the RNN [21]has reducedthedata-set.As the purpose of this research work is to enhance the detection rate forRNN[22] model by applying RNN[23]. It is alreadywell established that the main aimof the work is notactually to reduce the dimension but to enhance thedetection rate. DR is simply used as a tool[24] toenhancethedetectionrate. Then extlogicalstep is to test the classifiermodelforIDS. In this work RNN[25] with non-linear kernel, i.e., Radial ndwidths and the bestresult of the bestone is retained[28]. For testing themodel, a 10-fold cross-validation is applied.Theresults ofthemodelareevaluatedintermsofPrecision, Recall, ROC[28] etc. Moreover, Johns Quality[29] Assignment Curve[30] is used to check the effectiveness soft he proposed model.

VI. CONCLUSION

Attack detection comes next in the process after the capturing unit has captured and pre-processed the traffic. A suggested can now have a signature matching approach or anomaly detection because the core of an IDS is a detection methodology that can be based on anomaly detection or misuse detection.

If signature matching methods are to be used, a signature database must be accessible, and if anomaly detection methods are to be used, a normal data model must be in place. The detection module categorises each connection as either an attack or a legitimate network connection.

REFERENCES

[1] V.K.Kukkala,S.V.ThirulogaandS.Pasricha,"INDRA:IntrusionDetectionUsingRecurrentAutoencodersinAutomotiveEmbeddedSystems,"inIEEETransactions on Computer-Aided Designof IntegratedCircuitsandSystems,vol.39,no.11,pp.3698-3710,Nov.2020,doi: 10.1109/TCAD.2020.3012749.

[2] N.MboulaandE.Nogues,"IDrISS:IntrusionDetectionforITSystemsSecurity : Toward a semantic modelling ofside-channel signals," 2020 28th EuropeanSignal Processing Conference(EUSIPCO),2021,pp.735-739,doi:10.23919/Eusipco47968.2020.9287662.

[3] A.Prabhu,H.N.ChampaandD.Kalasapura, "Network Intrusion DetectionUsingSequenceModels,"2019GraceHopper Celebration India (GHCI), 2019,pp. 1-5, doi:10.1109/GHCI47972.2019.9071806.

[4] R.Vinayakumar,K.P.SomanandP.Poornachandran, "Applying convolutionalneuralnetworkfornetworkintrusiondetection," 2017 International ConferenceonAdvancesinComputing,CommunicationsandInformatics(ICACCI),2017,pp.1222-1228,doi:10.1109/ICACCI.2017.8126009.

[5] S. Althubiti, W. Nick, J. Mason, X. Yuanand A. Esterline, "Applying Long Short-Term Memory Recurrent Neural NetworkforIntrusionDetection,"Southeaston2018,2018,pp.1-5, doi: 10.1109/SECON.2018.8478898.

[6] P. Singh, J. J. P, A. Pankaj and R. Mitra,"Edge-Detect:Edge-CentricNetworkIntrusionDetectionusingDeepNeuralNetwork,"2021IEEE18thAnnualConsumer Communications & NetworkingConference (CCNC),2021,pp. 1-6, doi:10.1109/CCNC49032.2021.9369469.

[7] S.Nayyar,S.AroraandM.Singh,"RecurrentNeuralNetworkBasedIntrusionDetectionSystem,"2020InternationalConference on Communication and SignalProcessing(ICCSP),2020, pp.0136-0140, doi:10.1109/ICCSP48568.2020.9182099.

[8] A. Kotian, S. Patil, N. Prajapati and Y.Mane,"RealtimeDetectionOfNetworkAnomalies Using Neural Network," 2020InternationalConferenceonSmartTechnologies in Computing, Electrical andElectronics(ICSTCEE),2020, pp.240-245.