International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Network analysis of intrusion detection based on Machine Learning and Deep Learning

Anurag Busha, Vakeesh Kanna, Sagar Naidu, Sathya R

Abstract— The modern world is adopted to Machine learning and it shows superiority on almost all the conventional rule-based algorithms. These strategies are being combined in cyber security systems with the goal of supporting and even perhaps substituting the primary leve of security analysis. Although the entire automation detection and analysis is an an ideal goal, the effectiveness of machine learning in cyber security should be evaluated with due dilligence. We provide an analysis addressed to specialists of machine learning techniques applied to the detection of intrusion, malware and spam, The goal is twofold: to asses the present maturity of the solutions and to spot their main restrictions that stall a direct adoption of machine learning cyber detection schemes. Our conclusions are supported by an intensive review of the literature which include experiments performed on real enterprise systems and network traffic.

Keywords-- deep learning, machine learning, adversarial learning, cyber security

I.INTRODUCTION

The interest and certainty of machine learning (ML) is creating. Existing strategies are at the verge of being upgraded, and their ability to fathom and answer primary issues is exceedingly esteemed. These attainments have provoked the gathering of machine learning in a couple of territories, for instance, PC vision, remedial examination, gaming and electronic life exhibiting In a couple of circumstances, machine learning methods address the best option over regular standard based computations including human overseers. This example is moreover affecting the advanced security areas where some disclosure systems are being refreshed with Machine Learning parts. Despite the way that considering a completely electronic advanced shield structure is yet a far away target, first measurement chairmen in Network and Security Operation. Center (NOC) might benefit by acknowledgment and examination contraptions reliant on machine learning. This paper is expressly steered towards security chairmen along with plans that review the present improvement of the current game plans, to perceive their crucial constrainments and to include some chance to show signs of improvement. Our examination relies upon an expansive overview of the composition and on novel preliminaries are executed on real, broad endeavors and framework traffic.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
Anurag Busha*, Department of Computer Science and Engineering, SRM IST, Chennai
Vakeesh Kanna, Department of Computer Science and Engineering, SRM IST, Chennai
Sagar Naidu, Department of Computer Science and Engineering, SRM IST, Chennai
Sathya R, Department of Assistant Professor, Computer Science and Engineering, SRM IST, Chennai

Other academic journals consider Machine Learning answers for advanced security by pondering a single express application and are normally arranged to Artificial Intelligence (AI) authorities instead of security heads.
In the evaluation, we dismiss the business things reliant on ML (or on the misused Artificail Intelligence term) since dealers don't reveal their estimations and will all in all disregard issues and requirements. To begin with, we present a novel logical grouping of Machine Learning advanced cyber security approaches. By then, we map the perceived classes of estimations to three issues where machine learning is at present associated: interference ID, malware examination, spam and phishing area. Finally, we separate the principal controls of existing philosophies. Our examination highlights favorable circumstances and hindrances of various techniques, especially to the extent false positive or false negative alerts. Also, we raise a general underestimation of the multifaceted idea of regulating Machine Learning structures in advanced cyber security achieved by the nonattendance of transparently available and checked data for getting ready, and when required for adjusting exercises in a space depicted by steady change. We in like manner consider progressing results focusing on the feasibility of adversarial ambushes in avoiding Machine Learning locators. The affirm drawbacks make prepared to future redesigns that ML parts require before being totally gotten in advanced watchman stages. This paper is organized in pursues. Area 2 proposes our distinct scientific classification of Machine Learning calculations connected to digital security. Segment 3 plots the three classes of digital security issues considered in this paper and Section 4 looks at and assesses ML answers for digital security. Area 5 closes the paper with some last comments.

II.PROPOSED SYSTEM

This paper is worried about redesigning the current framework to beat difficulties with the assistance of informational indexes. Network security investigation is spoken to by the information. The right option alongside moderate utilization of data are the conditions for leading significant security examination. The measure of the dataset conjointly influences the preparation impacts of the Machine Learning and Deep Learning models. PC organize security information can as a rule be gotten in two different ways legitimately and utilizing a current open dataset. Direct access is that the utilization of changed methods for direct variety of the predetermined data, in a path through Win Dump or Wireshark programming apparatuses to catch organize bundles.

This methodology is explicitly focused on and proper for accumulation of present moment or little measure of information, yet for longterm or a lot of information, securing time and capacity costs will heighten. The useage of system security datasets can spare information accumulation time and increment the strength of examination by rapidly getting the fluctuated information required for research.

The KDD data set is a standout among the most broadly utilized preparing sets; it depends on the DARPA 1998 data set. There is one kind of the ordinary sort with the character of typical and 22 assault sorts, which are partitioned into five noteworthy classifications: , R2L (Root to Local attack), DoS (Denial of Service attack), Probe (Probing attack) and U2R (User to Root attack). Every record found in the KDD Cup 99 preparing data set incorporates 41 fixed component properties and a class identifier. Of the forty-one fixed element characteristics, seven particular properties are the emblematic sort; the others are ceaseless. Also, the highlights incorporate essential highlights, content highlights, and traffic highlights. The testing data set has explicit attack types that don't show up in the preparation set, which enables it to give a significantly more reasonable hypothetical reason for recognizing interruption. The KDD Cup 99 dataset, to date remains the first totally reviewed and open dataset, with completely marked related records spreading over half a month of system traffic and an expansive number of dissimilar attacks[11]. Every affiliation record contains 41 input highlights arranged into essential highlights and more elevated amount highlights. The essential highlights are legitimately extricated or gotten from the header data of IP bundles and TCP/UDP fragments inside the tcp dump records of each session. The rundown documents for tcpdump from the DARPA preparing information were utilized to mark the association records. The flawed substance based more elevated amount highlights use space learning to appear to be explicitly for assaults inside the real information of the sections recorded inside the tcp dump documents. These location 'U2R' and 'R2L' attacks, which may either require just a solitary association or are with no noticeable consecutive examples.

The KDD Cup 99 contention gives the planning and testing datasets in an exceedingly full set and conjointly gives an indicated '20%' subset structure. The '20%' subset was made because of gigantic measure of affiliation records present in the full set; a couple of 'DoS' attacks have a large number records. Subsequently, not these affiliation records were choosen. Moreover, exclusively associations with a period window of 5 minutes when the total span of an assault were appended to the '20%' datasets[4]. To accomplish roughly the samilar dispersion of intrusions and ordinary traffic as the first DARPA dataset, a chose set of groupings with 'normal' associations were additionally left in the '20%' dataset. Preparing and test sets have distinctive likelihood conveyances. The whole preparing dataset contains upto 500,000 records. The whole preparing dataset and furthermore the relating '20%' contain twenty-two disparate assault types in the request that they were utilized. The full test set, with upto 300,000 records, is just open unlabelled; notwithstanding, a '20%' subset is given both as unlabeled and named test data. It is shown as the 'balanced' subset, with a substitute scattering and as an additional attack not being a bit of the readiness set. For the KDD Cup '99 competition, the '20%' subset was used for getting ready. The 'changed' subset can be used for execution testing; it has upto hunderd thousand records containing 35 totally novel assaults.

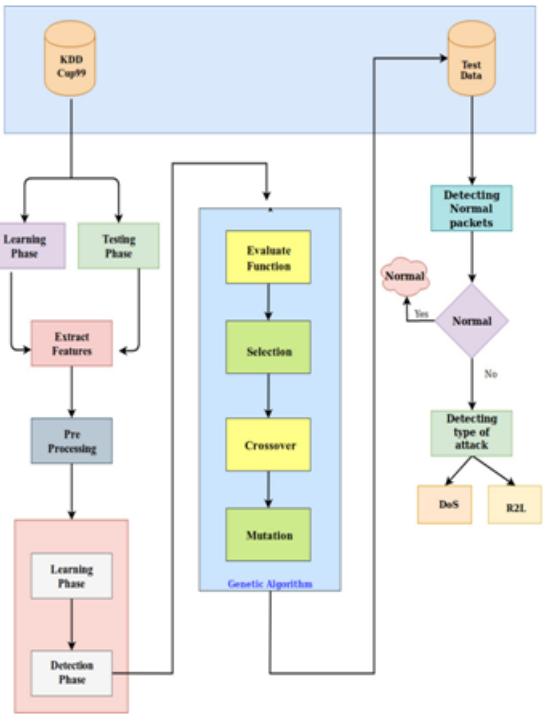

Figure 2.1: Work flow

III.PROPOSED METHOD

3.1 K-NEAREST NEIGHBOUR

The kNN classifier is relies upon a division work that evaluates the capability or comparability between two events. The regular Euclidean partition d(x, y) between two occasions x and y is characterized as :

n 2 kk k=1 d(x,y)= (x - y)

where, xk is the kth highlighted component of example x, yk is the kth included component of the case y and n is the absolute number of highlights in the dataset. Accept that the structure dataset for kNN classifier is Q. The all out number of tests in the plan dataset is P. Let D = {D1 ,D2 ,… DL} are the L different class names that are accessible in Q. Give x a chance to be the info vector for which the class mark ought to be determined. Let yk indicate the kth vector in the plan dataset Q. The kNN calculation is to discover the k nearest vectors in structure dataset P to enter vector x. At that point the information vector x is characterized to class Dj if most of the k nearest vectors have their class used Indexed Partial Distance search k Nearest Neighbor (IKPDS) to investigate diverse roads in regards to moved sorts of ambush and distinctive k esteems (i.e., 5, 8, and 20). They discretionarily picked 13,685 examples from the NSl-KDD dataset to test the arranged outcomes, bringing about 98.5% exactness and snappier characterization time. Test results uncover the IKPDS, which in a brief span Network Intrusion Detection Systems (NIDS), give improved grouping outcomes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Be that as it may, the investigation of the test pointers of the analysis isn't flawless; it neglected to consider the exactness and review rate[12] presents the K-Means and kNN blend interruption discovery framework.

To start with, the info intrusion information (NSL-KDD) is prepared by essential part examination to pick the main 5 imperative highlights. At that point, these preprocessed information are isolated into 3 sections and nourished into a k-implies calculation to get the grouping focuses and names. This procedure is finished multiple times to pick the best grouping plan. These group focuses alongside the marks are then used to arrange the info KDD information utilizing straightforward kNNs. In the investigation, two different ways were utilized to analyze the proposed technique and thusly the aftereffect of kNN. The measures depend upon the exactness of the genuine identification of threat and threat type or t mode. Actualize two or three projects to research these outcomes. In the underlying case, the test information is isolated from the train information, while in the second case, some test information isn't supplanted from the preparation information. Nonetheless, regardless, the deliberate exactness of the analysis is just roughly 89%, and it neglected to consider the precision and review rate.[11] contemplated some new systems to improve the grouping execution of KNN in interruption recognition and assess their execution on NSL-KDD datasets. The most remote neighbor (k-FN) and closest neighbor (KNN) are acquainted with partition the information. At the point when the most distant neighbor and furthermore the closest neighbor have indistinguishable class name, the second closest neighbor of the dataset is used for segregation. Exploratory outcomes uncover that this strategy has been improved as far as accuracy, recognition rate and decrease of disappointment caution rate. Grunt checks arrange bundles and produces alarms. From that point, all produced Snort cautions are going to sent to smart kNN-based alert channels for alert separating. Investigations utilize the exactness and F-score as pointers; the normal of results were 90.1% .

3.2 DECSION TREE

The decision teee has a structure like a tree inside which each internal node addresses to a test on one property and each branch addresses a test yield, with each leaf hub addressing an order. In ML, the decision tree is a prognostic structure; it demonstrates the mapping between article qualities and item esteems. Every node in the tree speaks to an item, every difference way speaks to a conceivable quality esteem, and each leaf node relates to the estimation of the article spoken to by the way from the root node to the leaf node. The decision tree incorporates just an unary yield; on the off chance that you need propelled yield, you can build up a free decision tree to deal with various yields. Regularly utilized choice tree models are AD3, F4.2 and CART. As showed up in Fig.2.1, the decsion tree arranges the models datasets through the conditions of setting up, and has improved discovery exactness for realized interruptions present in the strategies, yet it isn't reasonable for recognition of obscure interruptions. Ingre and Bhupendra [1] puprose a decision tree-based Intrusion Detection System for the NSL-KDDadataset. Feature decision utilizing an association incorporate decision (CFS) approach, picking fourteen frameworks where utilized on starters. The examinations are performed on a KDD99 dataset. From the test outcomes, the multi-target progression choice tree pruning (MO-DTP) method is most reasonable to compel the level of the whole tree. By and large, its tree measure is tripled separated and some other tree classifier utilized. Single Objective Optimization Decision Tree Trimming (SODTP) decreases overlift, understanding an unquestionably summed up tree. By utilizing these summed up trees to mastermind strikes, essential execution improvement can be seen. The fake caution rate, accuracy and precision of MO-DTP are 14.7%, 89.76 and 88.89, solely. The hoax ready rate, accuracy and precision of SO-DTP were 0.92%, 82.47% and 92.76%. The examination thinks about the parallel depiction and multiclassification and assorted parameters and is very expert. Rayn and Nella G.[4] propose two techniques for utilizing highlight confirmation, the D4.5 choice tree figuring and the D4.7 choice tree (with pruning). Train and test classifiers utilize the KDDCup99 and NSL-KDD datasets. Basically the discrete respect characteristics of is_host_login, class are considered, land, logged_in, protocol_type is_guest_login and Serviceflag in the solicitation strategy. D4.7 (with pruning) has higher accuracy and lower FAR of 76.27% and 2.01% than does the D4.5 choice tree. Another examination [17] utilized C4.5 for interruption identification on the NSL-KDD dataset. In our paper, feature assurance along with division regards is essential drawback in structure decison tree; the estimation is planned to clarify both of these the calculation is intended to take care of both of these issues. The data gain is utilized to choose the most applicable highlights, and the division esteems are picked to such an extent that the classifier has no inclination on the most successive qualities. Sixteen properties were chosen as highlights on the NSL-KDD dataset. The provided decision tree splitting (DTS) algorithm can be utilized for mark dependent interruption recognition. Be that as it may, the exactness of this strategy is just 79.52%.

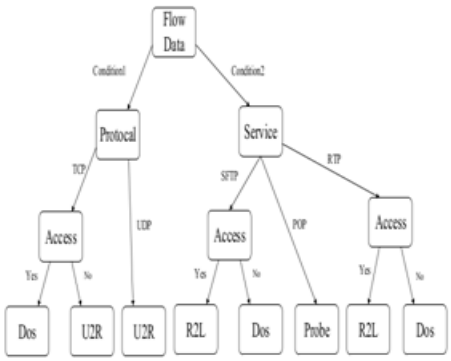

Figure 3.1: Decision tree

3.3 RECURRENT NEURAL NETWORKS

Recurrent Neural Networks (RNN) are utilized in strategy gathering information. In the standard neural structure appear, information from the data layer to the covered layer to the yield layer;

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

The layers are completely related and there are no connections between its center points given between each layer. Different issues exist that the standard neural framework can't resolve. The reason that RNN is a discontinuous neural system is that its presenr yield of a course of action is also related to the yield before it. The strong appearance is framework can review the data of the past minute and apply it to the figuring of the present yield; that is, the inside focuses between the hidden layers become related, and the responsibility of the secured layer wires both the yield of the data layer and the last moment covered layer yield. Hypothetically, any length of accumulation information RNN can be taken care of. Regardless, practically speaking, to diminish the multifaceted nature, normally acknowledged that the present state is basically identified with the past states. Fig 1 displays the RNN timing properties, meandered into an entire system structure here in a multi-layer engineer. The improved model subject to RNN has Long Short Term Memory (LTSM) and a Gated Recurrent Unit (GRU). Yin and Long [9] obstruction affirmation (RNNIDS) in context on a cyclic neural structure. The NSL-KDD dataset was utilized to overview the execution of the model in twofold solicitation and multi-class strategy, and the impact of the measure of the neurons and contrasting learning rates in a execution of the model. The course of action exactness and the test accuracy gotten by the model in joined solicitation are solely 87.62% and 92.17%. The preparation accuracy and test precision of the multi-gathering model are 88.41% and 99.05%, solely. In a close work, Karan [5] additionally utilized RNN for impedance affirmation, at any rate the dataset utilized was the KDD 99 Cup. Preliminary precision, survey and exactness of Probe was 85.4%, 86.7% and 97.4%, exclusively; DoS was 89.6%, 88.97% and 88.7%, independently; U2R was 91.4%, 73.5% and 67.2%, separately; and R2L are 30.01%, 17.72% and 88.2%. Emeyersaud al et. [4] execute the LSTM discontinuous neural framework classifier for interruption unmistakable evidence information. The outcomes display that the LSTM classifier has certain central focuses over the other solid static classifiers in the 10% KDD cup99 dataset. These ideal conditions lie in the acknowledgment of DoS ambushes and Probe, the two of which produce exceptional time course of action events on the strike classes that make less events. The modelclassification precision rate accomplished 89.66%; the FAR was 2.01%. Jim and Yunjih [6] in like way use LTSM as their model and the 21% KDD Cup 99 as their dataset. They set 90 for the secured layer measure and 0.001 for the learning rate. The paper detailed the outcomes as 97.83% accuracy, the run of the mill precision as 98.8%, and the standard FAR as 10%. Separated and the primer deferred outcomes in [11], the technique got a higher false territory rate while acquiring a higher affirmation rate. To fix the issue of high false-prepared rates, Gyuwan et al. [2] propose a structure call language-appearing for organizing LSTM-based host interruption region frameworks. The framework incorporates two sections: the front end of LSTM appearing of structure secures assorted settings, and the backend is for abnormality want dependent on outfit of thresholding got from a end. Models were assessed utilizing the KDD cup99 adtaset and accomplish 4.4% FAR and 88.9% accuracy.

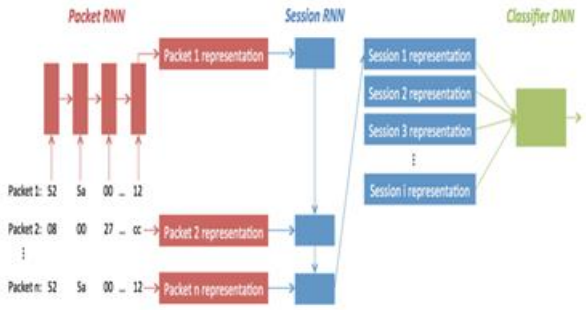

Figure 3.2: RNN Representation

3.4 CONVOLUTIONAL NEURAL NETWORKS

Convolutional Neural Networks (CNN) are a representation of fake neural system that have turned into a hotspot in the field of talk examination and picture affirmation. Its weight-sharing framework structure makes it logically like a characteristic neural framework, thusly reducing the multifaceted nature of the framework show and diminishing the amount of burdens. This good position is continuously obvious when the framework input is a multi-dimensional picture, and the picture can be immediate utilized as the dedication of the system to maintain a strategic distance from the convoluted segment extraction and information redoing in the standard attestation check. The CNN is a multi-networked sensor explicitly intended for see two-dimentional shapes that are varient to getting, scaling, tliting, or assorted sorts of bending. Convolutional Neural Networks is the primary truly productive learning figuring in planning multi-layer mastermind structures, the structure showed up in Fig 3.3. It lessens a amount in parameters which should be made sense of the most effective method to improve the arranging execution of the BP estimation through spatial affiliations. In a huge getting the hang of structuring, CNN is utilized to limit the information preprocessing necessities. There are three central techniques for it to diminish organize getting ready parameters:pooling, weight sharing and adjacent receptivity. The prevailing bit of CNN is the taking in feature movements from a ton of unlabeled information. Accordingly, CNN are enabling for application in the system interference disclosure field. To learn valuable element portrayals consequently and proficiently from a lot of unlabeled crude system traffic information by utilizing profound learning methodologies, a profoundlearning approach, called widened convolutional encoders, in the system interruption identification demonstrate, which consolidates the upsides of stacked autoencoders and CNNs. In a general sense, the model can consequently take in basic highlights from substantial scale and that's only the tip of the iceberg differed unlabeled crude system traffic information comprising of true trafficf rom online malware, botnets, misuses, ordinary traffic streams. sweeps and APTs (Advanced Persistent Threats). A comparable work, Santagio-CTU-UNB datasets and CTU-UNB datasets are made reliant on various malware traffic data. The game plan tasks are performed in the survey the execution of the proposed model. The precision, survey and F-score in course of action errands were 98.40%, 89.97% and 0.897 independently. Kolosnjaaji ett aal. Movements execution upgrades made in the zone of neural systems to demonstrating the execution succession of dismantled noxious parallel documents.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

A neural system comprising with convolutions and feedforwarding neural structure was executed. The engineering typifies a progressive element scraping technique which consolidates the highlights in the p-gram guidance with the straightforward vectorization of convolutions. In this work, highlights are extricated from header records in Portable Executable (PE) documents for assessment as it were. The outcomes demonstrate that the proposed strategy beats the benchmark techniques, for example, straightforwardfeedforward neural framework and support vector machine. The G1 score with 1.87 is come to nearby a precision and survey of 0.84. Saaxei ett all. Propose an eXpose neural framework that uses the significance learning technique we have made to take (vault keys) and figure out how to separate highlights and groupings all the while utilizing character-level installing and convolutional neural systems. Notwithstanding completely computerizing the component structure and extraction process, eXpose likewise outflanked the pattern dependent on manual component extraction for all interference disclosure issues attempted, the area rate was 89% and a reducing in false alarm rate was 0.01%. Chung wah ett aal.[12]propose a one-dimensional convolutional neural framework from beginning to endscrambled traffic characterization strategy. This strategy coordinates include scraping, highlight determination and classification into a brought together end-to-end system alongwith consequently learns the nonlinear connection between the first info and the normal yield. This technique utilizes an open ISCX VPN-non VPN traffic dataset for confirmation. 1D-CNN has givenn good results in two -class order with 99% and 100% accuracy for non-VPN and VPN traffic, separately. Review rates for VPN non-VPN traffic are 100% and 99%, separately. VPN traffic of ID-CNN in 12-class and 6-class frameworks likewise demonstrated execution of 94.9% and 92.0% accuracy and reviews of 97.3% and 95.2%, separately. Be that as it may, the 1D-CNN execution of non-VPN administrations isn't extremely great. The accuracy is just 85.8% and 85.5%; the review rate is just 85.9% and 85.8%. Chung Wah ett aal. proposed a malware traffic grouping strategy utilizing a convolutional neural system by taking traffic information as pictures. This technique required no hand-structured highlights yet straightforwardly accepting crude traffic as information of the classifier. In the investigation, the USTC-TRC2016 stream dataset was built up, and the information preprocessing pack USTCTK2016 were created. In light of the dataset and the toolbox, we found the best kind of traffic portrayal by breaking down the eight test results. Exploratory outcomes demonstrate the normal exactness of classifiers is 88.52%.

The strategy coordinates highlight extraction, include choice and classifier into a brought together endto-end system and consequently learns the nonlinear connection between the first info and the normal yield. This strategy utilizes an open ISCX VPN-non VPN traffic dataset for confirmation. 1D-CNN performed well in 2-class grouping with 99% and 100% exactness for vpn and non-VPN traffic, individually. Review rates for VPN and non-VPN traffic are 100% and 99%, separately. VPN traffic of ID-CNN in 12-class and 6-class systems.

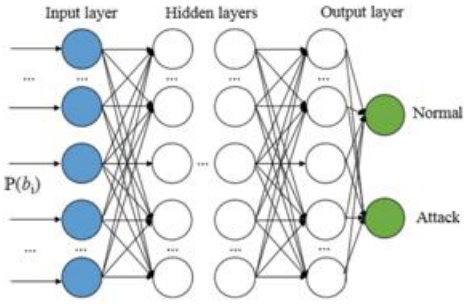

Figure 3.3: CNN representation

IV.EXPERIMENTAL RESULTS

Our work inspects an extensive number of scholarly interruption discovery examines dependent on AI and profound learning as appeared. In these examinations, numerous awkward nature show up and uncover a portion of the issues around there of research, to a great extent in the accompanying territories: (I) the benchmark datasets are few, in spite of the fact that the equivalent dataset is utilized, and the strategies for test extraction utilized by each establishment fluctuate. (ii) The assessment measurements are not uniform, numerous investigations just evaluate the exactness of the test, and the outcome is uneven. In any case, examines utilizing multi-criteria assessment regularly embrace diverse metric mixes to such an extent that the exploration results can't be contrasted and each other. (iii) Less thought is given to organization productivity, and the majority of the exploration remains in the lab regardless of the time multifaceted nature of the calculation and the proficiency of recognition in the genuine system. Notwithstanding the issue, drifts in interruption discovery are likewise reflected. (I) The investigation of cross breed models has been getting to be hot lately, and better information measurements are acquired by sensibly joining distinctive calculations. (ii) The appearance of profound learning has made start to finish learning conceivable, including taking care of a lot of information without human association. Be that as it may, the tweaking requires numerous preliminaries and experience; interpretability is poor. (iii) Papers contrasting the execution of various calculations after some time are expanding step by step, and expanding quantities of scientists are starting to esteem the reasonable noteworthiness of calculations and models. (iv) variousnew datasets are in the school's charge, improving the ebb and flow look into on cybersecurity issues, and the best of them is presumably going to be the benchmark dataset here.The technique coordinates highlight extraction, include choice and classifier into a bound together start to finish system and consequently learns the nonlinear connection between the first information and the normal yield. This technique utilizes an open ISCX VPN-non VPNtraffic dataset for affirmation. 1D-CNN performed well in two-class portrayal with 99% and 100% precision for VPN, non-VPN traffic, independently. Survey rates for VPN, non-VPN traffic are 100% and 99%, independently.. VPN traffic of 1D-CNN in 12-class and 6-class systems

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

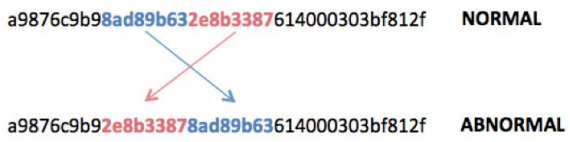

Figure 4.1: IP and Port switch

Figure 4.2: Destination IP swap out

V.CONCLUSION

Our work exhibits a writing audit of Machine Learning and Deep Learning strategies for system security. This paper, which has for the most part centered around the most recent three years, presents the most recent utilizations of Machine Learning and Deep Learning in the field of interruption recognition. Tragically, the best strategy for interruption discovery has not yet been set up. Each way to deal with actualizing an interruption location framework has its own favorable circumstances and impediments, a point obvious from the dialog of correlations among the different strategies. Therefore, it is hard to pick a specific technique to execute an interruption discovery framework over the others. Datasets for system interruption recognition are critical for preparing and testing frameworks,Datasets for system interruption discovery are crutial for preparing and testing frameworks. Machine Learning and Deep Learning strategies don't work without agent information, and getting such a dataset is troublesome and tedious. Be that as it may, there are numerous issues with the current open dataset, for example, uneven information, obsolete substance and so forth. These issues have generally constrained the improvement of research around there. System data refresh exceptionally quick, which conveys to the ML and DL show getting ready and use with inconvenience, show ought to be retrained whole deal and quickly. So relentless learning and profound established learning will be the focus in the examination of this field later on.

REFERENCES

1. Y. Zhou and A. Kumar , Palm -vein images Human identification, IEEE Trans. Inf. Forensics Security, vol. 6, no. 4, pp. 1259-1274, Dec. 2011.
2. Masmoudi, A.D., Trabelsi, R.B., Masmoudi, D.S.: 'Hand vein image enhancement with radon like features descriptor', Int. J. Comput., Electr., Autom., Control Inf. Eng., 2013, 7, (6), pp. 797–800
3. Masmoudi, A.D., Trabelsi, R.B., Masmoudi, D.S.: 'A novel finger vein recognition system based on monogenic local binary pattern features', Int. J. Eng. Technol. (IJET), 2014, 5, (6), pp. 4528–4535
4. Trabelsi, R.B., Masmoudi, A.D., Masmoudi, D.S.: 'A novel biometric system based hand vein recognition', J. Test. Eval., 2013, 42, (4), pp. 1–10
5. Masmoudi, A.D., Trabelsi, R.B., Krid, M., et al.: 'Implementation of a fingervein recognition system based on improved Gaussian matched filter', J. Magnt. Res. Rep., 2014, 2, (4), pp. 251–260
6. Trabelsi, R.B., Masmoudi, A.D., Masmoudi, D.S.: 'A new multimodal biometric system based on finger vein and hand vein recognition', Int. J. Eng. Technol., 2013, 5, (4), pp. 3175–3183
7. Yakno, M., Mohamad-Saleh, J., Rosdi, B.A.: 'New technique for larger ROI extraction of hand vein images'. Int. Conf. on BioSignal Analysis, Processing and Systems (ICBAPS), 2015
8. M.V., Kavati, Prasad, I., Ravindra, K.: 'Hand vein authentication system using dynamic ROI'. Int. Symp. on Security in Computing and Communication, 2013
9. M.V., Kavati, Prasad, I.: 'Hand vein authentication system using connected minutiae neighbours', Int. J. Trust Manage. Comput. Commun., 2014, 2, (3), pp. 296–308
10. Trabelsi, R.B., Masmoudi, A.D., Masmoudi, D.S.: 'Hand vein recognition system with circular difference and statistical directional patterns based on an artificial neural network', Multimedia Tools Appl., 2016, 75, (2), pp. 687–707
11. Trabelsi, R.B A.D., Masmoudi, Masmoudi, D.S.,.: 'A novel biometric system based hand vein recognition', J. Test. Eval., 2013
12. Fan, K.C Lin, C.L.,.: 'Biometric verification using thermal images of palmdorsa vein patterns', IEEE Trans. Circuits Syst. Video Technol., 2004
13. Leedham, G., Wang, L., D.S.Y. Cho,: 'Minutiae feature analysis for infrared hand vein pattern biometrics', Pattern Recognit., 2008
14. Tang, D Wang, M.,.: 'Region of interest extraction for finger vein images with less information losses'. Multimedia Tools and Applications, 2017, pp. 1–13
15. D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, ''A survey of deep learning-based network anomaly detection,'' Clust. Comput., vol. 4,
16. no. 3, pp. 1–13, Sep. 2017.
17. B. B. Rao and K. Swathi, ''Fast kNN classifiers for network intrusion detection system,'' Indian J. Sci. Technol., vol. 10, no. 14, pp. 1–10,
18. 2017.
19. C. Azad and V. K. Jha, ''Genetic algorithm to solve the problem of small disjunct in the decision tree based intrusion detection system,'' Int.
20. J. Comput. Netw. Inf. Secur., vol. 7, no. 8, pp. 56–71, 2015.
21. T.-T.-H. Le, J. Kim, and H. Kim, ''An effective intrusion detection classifier
22. using long short-term memory with gradient descent optimization,'' in Proc. Int. Conf. Platform Technol. Service, 2017, pp. 1–6.
23. I. M. Coelho, V. N. Coelho, E. J. da S. Luz, L. S. Ochi, F. G. Guimarães, and E. Rios, ''A GPU deep learning metaheuristic based model for time series forecasting,'' Appl. Energy, vol. 201, no. 1, pp. 412–418, 2017.
24. J. N. Goetz, A. Brenning, H. Petschko, and P. Leopold, ''Evaluat-ing machine learning and statistical prediction techniques for landslide susceptibility modeling,'' Comput. Geosci., vol. 81, no. 3, pp. 1–11, 2015.