Detection Of Phishing Attacks Using Lstm In Deep Learning

Y Sujatha[1], L Sai Sravanthi[2], K Sai Kishen[3], K Vijay Kumar[4], K Venkata Lakshmi[5]

Assistant Professor, Department of Computer Science and Engineering[1]

U.G Scholars, Department of Computer Science and Engineering[2345]
Raghu Institute of Technology, Visakhapatnam, AP, India.

Abstract - Analytical detection can detect unknown attacks from network connections and is an effective method of network security. Today, existing methods for network anomaly detection are often based on traditional machine learning models, such as KNN, SVM, etc. While these methods can achieve great functionality, they achieve relatively low accuracy and rely heavily on manual traffic feature design. has become obsolete in the age of big data. To solve the low accuracy and feature engineering problems in intrusion detection, the BAT traffic anomaly detection model is proposed.

Additionally, we use multiple layers to capture the local characteristics of traffic data. Since multiple convolution layers are used to process the data samples, we call the BAT model BAT-MC. We test our model on a public benchmark dataset, and the test results prove that our model performs better than other comparison methods.

Index Terms - Intrusion detection, BLSTM, convolutional mechanism, malicious, network traffic.

I. INTRODUCTION

With the development and improvement of Internet technology, the Internet provides people with various convenient services. However, we also face various security threats. Fortunately, intrusion detection is a great solution to these problems. Intrusion detection plays an important role in ensuring the security of network information. However, with the explosive growth of Internet business, the traffic types within the network are increasing day by day, and the operating characteristics of the network are becoming more and more complex, which poses great challenges to intrusion detection. Identifying various types of malicious network traffic, especially unexpected malicious network traffic, is an important and unavoidable problem.

In fact, network traffic can be divided into two categories: normal traffic and malicious traffic. Furthermore, network traffic can generally be divided into five categories: DoS (denial of service attacks), R2L (root-to-local attacks), U2R (user-to-root attacks), and probes (probe attacks). Intrusion detection can therefore be viewed as a classification problem. Improving the performance of classifiers that effectively identify malicious traffic can greatly improve the accuracy of intrusion detection.

II. LITERATURE SURVEY

The intrusion detection era may be divided into 3 predominant categories: sample matching techniques, conventional system mastering techniques and deep mastering techniques. At the beginning, human beings especially use sample matching algorithms for intrusion detection. Pattern matching algo- rithm [14], [15] is the middle set of rules of intrusion detection device primarily based totally on characteristic matching. The site visitors anomaly detection techniques primarily based totally on system mastering have executed a number of achievement. In [18], the authors advocate a brand new approach of characteristic choice and classifica- tion primarily based totally on help vector system (SVM). The test end result at the KDD CUP 1999 dataset indicates that the technique plays higher than the conventional PNN, PCA-PNN and unoptimized DBN-PNN. The CNN version now no longer simplest reduces the fake alarm rate (FAR) however additionally improves the accuracy of the elegance with small numbers. In [32], an synthetic intelligence (AI) intrusion detection gadget the use of a deep neu- ral community (DNN) is investigated and examined with the KDD Cup ninety nine dataset in reaction to ever-evolving community attacks.

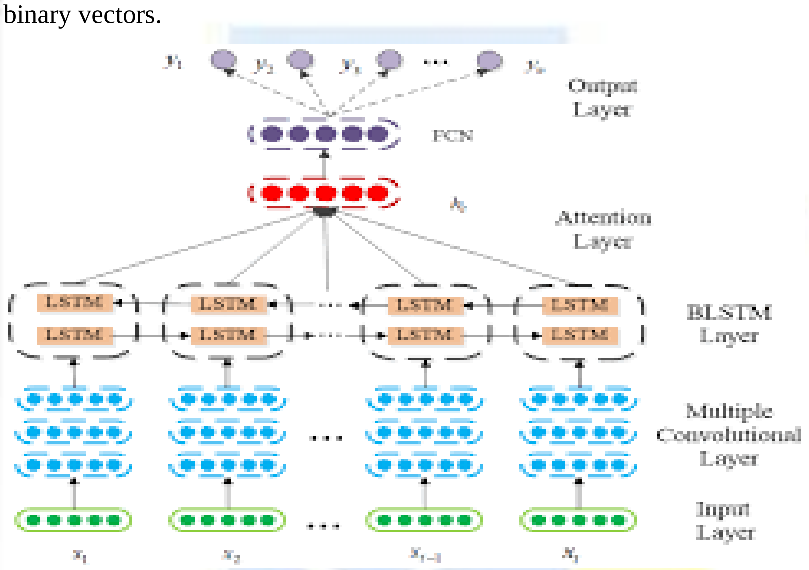
In this paper, drawing at the software techniques of deep mastering in NLP, we undertake phased processing. The BLSTM is used to research the sequential capabilities withinside the records packet to acquire a vector similar to every records packet. Hence, the BAT-MC version makes complete use of the shape statistics of community visitors.

III. PROPOSED WORK

As proven in Figure 1, the BAT-MC version includes 5 components, inclusive of the enter layer, more than one convolutional Layers, BSLTM layer, interest layer and output layer, from backside to top. At the enter layer, BAT-MC version converts every site visitors byte right into a one-warm facts format. Convolu- tional operation is used as a function extractor that takes an photograph illustration of facts packet. At the BLSTM layer, BLSTM version which connects the ahead LSTM and the backward LSTM is used to extract functions at the the site visitors bytes of every packet. BLSTM version can study the sequential traits inside the site visitors bytes due to the fact BLSTM is appropriate to the shape of community site visitors. At the output layer, the functions generated with the aid of using interest mechanism are then imported into a totally related layer for function fusion, which obtains the important thing functions that correctly symbolize community site visitors behavior. Finally, the fused functions are fed right into a classifier to get the very last popularity results.

A. DATA PREPROCESSING LAYER

There are 3 symbolic information kinds in NSL-KDD information fea- tures: protocol kind, flag and service. We use one-warm encoder mapping those functions into binary vectors.



One-Hot Processing: NSL-KDD dataset is processed through one-warm approach to convert symbolic functions into numerical functions. For example, the second one characteristic of the NSL-KDD information pattern is protocol kind. The protocol kind has 3 values: tcp, udp, and icmp. One-warm approach is processed right into a binary code that may be identified through a computer, wherein tcp is [1, 0, 0], udp is [0, 1, 0], and icmp is [0, 0, 1].

Normalization Processing: The cost of the authentic information can be too big, ensuing in troubles such as "big num- bers to consume decimals", information processing overflows, and incon- sistent weights so on. We use widespread scaler to normalize the non-stop information into the range [0, 1]. Normalization process- ing removes the have an impact on of the dimension unit at the version education, and makes the education end result extra depending on the traits of the information itself. The method is proven in equation (1) and equation (2).

$$r'c=r-rmin//rmax\text{-}rmin, \qquad (1)$$

$$rmax=max\{r\} \qquad (2)$$

where in r stands for numeric characteristic cost, rmin stands for the minimum cost of the characteristic, rmax stands for the max cost, r′ stands the value after the normalization.

B. MULTIPLE CONVOLUTIONAL LAYERS

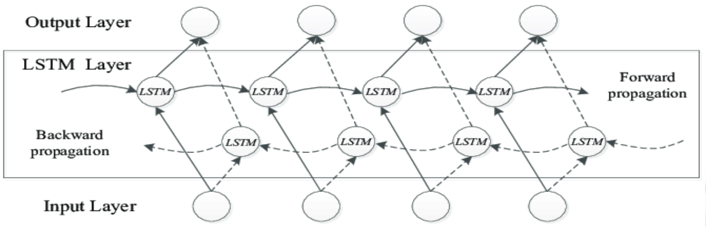
After the above processing operations, convolutional layer is used to seize the neighborhood functions of visitors statistics. Convolutional layer [33], [34] is the maximum essential a part of the CNN, which convolves the enter images (or characteristic maps) with a couple of convolutional kernels to create distinctive characteristic maps. Suppose we've a few N unites layer as enter that is observed through convolutional layer. If we use m width clear out out w, the convolu- tional output will be (N − m + 1) unites. The convolutional calculation procedure is as proven in equation (3).

$$x_{i,k}^{l,j} = \text{f (bj} + \sum_{a=1}^{m} w^{j} a, k^{r^{l-1,j}} i + (\mathrm{k}-1) \times \mathrm{s} + \mathrm{a} - 1) \qquad (3)$$

where $x_{i,k}^{l,j}$ is one of the ith unit of j feature map of the kth section in the lth layer, and s is the range of section. f is a non-linear mapping, it usually uses hyperbolic tangent function, tanh(·).

C. BLSTM LAYER

For the time collection facts composed of site visitors bytes, BLSTM can efficaciously use the context facts of facts for fea- ture learning. The BLSTM is used to examine the time collection function withinside the facts packet. The BLSTM version is used to extract coarse-grained capabilities with the aid of using connecting ahead LSTM and backward LSTM. LSTM is designed with the aid of using the enter gate i, the overlook gate f and the output gate o to manipulate a way to overwrite the facts with the aid of using evaluating the internal reminiscence mobileular C whilst new facts arrives [38]. When facts enters a LSTM network, we are able to decide whether or not it's miles beneficial consistent with applicable rules.



Only the facts that meets algorithms authentication may be remained, and inconsistent facts may be forgotten via overlook gate. Given an enter collection x = (x0,...,xt) at time t and the hidden states of a BLSTM layer, h = (h0,...,ht) may be derived as follows.

The overlook gate will take the output of hidden layer h_{t}-₁ the preceding second and the enter xt on the modern second as enter to selectively overlook withinside the mobileular kingdom Ct , which may be expressed as:

$$f_t = \text{sigmoid}(\omega_{xf} x_t + \omega_{hf} h_{t-1} + b_f), \qquad (4)$$

The enter gate cooperates with a tanh feature collectively to manipulate the addition of latest records. tanh generates a brand new candidate vector. The enter gate generates a cost for every object in Ct from zero to at least one to manipulate how a good deal new records could be added, which may be expressed as:

$$C_t = \text{sigmoid}(f_t . C_{t-1} + i_t . \tilde{C}_t), \qquad (5)$$

$$i_t = \text{sigmoid}(\omega_{xi} x_t + \omega_{hi} h_{t-1} + b_t), \qquad (6)$$

$$\tilde{C}_t = \tanh(\omega_c x_t + \omega_c h_{t-1} + b_c) \qquad (7)$$

The output gate is used to manipulate how a good deal of the modern unit kingdom could be filtered out, which may be expressed as:

$$o_t = \text{sigmoid}(\omega_{xo} x_t + \omega_{ho} h_{t-1} + b_o), \qquad (8)$$

D. ATTENTION LAYER

BLSTM ultimately generates a packet vector for every packet. These packet vectors are organized withinside the order of inter-movement among the 2 events withinside the community flow to shape a chain of packet vectors. Firstly, the packet vectors ht extracted with the aid of using the BLSTM version is used to reap its implicit represen- tation ut via a nonlinear transformation, which may be expressed as:

$$u_t = \tanh(\omega_w h_t + b_w), \qquad (9)$$

We subsequent degree the significance of packet vectors primarily based totally at the similarity illustration ut with a context vector uw and reap the normalized significance weight coefficient αt . uw is a random initialization matrix which can attention on crucial facts over ut. The weight coefficient for the above coarse-grained functions may be expressed as:

$$\alpha_t = \frac{\exp(U_t^T U_w)}{\sum \exp(U_t^T U_w)}, \qquad (10)$$

Finally, the satisfactory grained characteristic s may be computed thru the weighted sum of ht primarily based totally on αt . s may be expressed as:

$$s = \sum \alpha_t h_t , \qquad (11)$$

The satisfactory-grained characteristic vector s generated from the atten- tion mechanism is used for malicious site visitors popularity with a softmax classifier, which may be expressed as:

y=softmax(w_h s+b_h), (12)

wherein Wh represents the load matrix of the classifier, that may map s to a brand new vector with period h. h is the range of classes of community traffics.

E. MODEL TRAINING

Training the proposed community consists of a ahead byskip and a backward byskip.

Forward Propagation: The BAT-MC version is specifically com-posed of BLSTM layer and interest layer, every of which affords one of a kind systems and as a result performs one of a kind role withinside the entire version. Meanwhile, we set the mobileular nation vector length as S_{state}. In summary, the unusual visitors detection set of rules primarily based totally at the BAT-MC version is summarized as Algorithm 1. The goal characteristic of our version is the pass-entropy primarily based totally value characteristic [42]. The aim of schooling this version is to decrease the pass entropy of the anticipated and real outputs for all activities. The system is proven in (16):

$$c = -\sum_i \sum_j y_i^j \ln a_i^j + (1 - y_i^j) \ln(1 - a_i^j), \qquad (13)$$

wherein i is the index of community visitors. j is the visitors cate- gory. a is the real class of community visitors and y is the expected class.

Backward Propagation: The version is educated with adam [43]. Adam is calculated with the aid of using the back-propagation algorithm. Error differentials are back-propagated with the ahead-backward set of rules. Back-Propagation Through Time (BPTT) [44], [45] is carried out to calculate the mistake differentials. In this paper, we use the Back Propagation Through Time (BPTT) set of rules to acquire the derivatives of the objective characteristic with recognize to all of the weights, and decrease the goal characteristic with the aid of using stochastic gradient descent.

IV. EVALUATION

In this section, we first decide the parameters of BAT-MC to attain the gold standard version thru experiments which carry data.

Then, we examine the overall performance of the BAT-MC version. Finally, that allows you to confirm the development and practicability of the BAT-MC version, we examine the overall performance of this version with a few latest works.

A. BENCHMARK DATASETS

The very last end result of community site visitors anomaly detection is carefully associated with the dataset. The NSL-KDD dataset is an more advantageous model of KDD cup 1999 dataset [48], [49], that's extensively utilized in intrusion detection experi- ments.

The NSL-KDD dataset now no longer most effective efficaciously solves the inherent however additionally makes the range of facts rea- sonable withinside the education dataset and trying out dataset. redundant facts issues of the KDD Cup 1999 dataset

Table1:Different distributions in the NSL-KDD dataset.

	Total	Normal	Dos	Probe	R2L	U2L
KDDTrain+	125976	67342	49827	11654	994	53
KDDTest+	22455	9711	7528	2420	2753	210
KDDTest-21	11840	2412	4342	2419	2753	210

Network site visitors is usually gathered at constant time inter- vals. Essentially, community site visitors facts is a form of time collection facts. Network site visitors is a site visitors unit composed of more than one facts packets. Each facts packet is visible as an entire along with a series of site visitors bytes. According to its characteristics, there are 4 forms of assaults on this dataset: DoS (Denial of Service assaults), R2L (Root to Local assaults), U2R (User to Root attack), and Probe (Probing assaults).

B. EVALUATION METRIC

In this paper, Accuracy (A) is used to assess the BAT- MC version. Except for accuracy, fake nice rate (TPR) and fake nice rate (FPR) also are introduced. Where True Positive (TP) rep- resents the appropriate class of the Intruder. False Positive (FP) represents the wrong class of a ordinary consumer taken as an intruder. True Negative (NP) represents a ordinary consumer labeled efficaciously. False Negative (FN) represents an example in which the intruder is incorrectly labeled as a nor- mal consumer.

Accuracy represents the share of efficaciously labeled samples to the entire range of samples. The assessment metric are described as follows:

accuracy,A=(TP+TN)/(TP+FP+FN+TN) (14)

True Positive Rate (TPR): because the equal of the Detec- tion Rate (DR), it represents the share of the range of facts efficaciously diagnosed over the entire range of anomaly facts.

DR = TPR = (TP)/(TP+FN) (15)

False Positive Rate (FPR) represents the share of the range of facts rejected incorrectly is split with the aid of using the entire range of ordinary facts. The assessment metric are described as follows:

FPR = (FP)/(FP+TN) (16)

C. EXPERIMENTAL SETTINGS

In order to check the overall performance of BAT-MC version proposed on this paper, NSL-KDD dataset is used for verification. The facts samples of the NSL-KDD dataset are divided into parts: one is used to construct a classifier, this is known as the schooling dataset. The different is used to assess the classifier, this is known as the trying out dataset. There are 125,973 statistics withinside the schooling set and 22,543 statistics withinside the trying out set. Table 2 suggests the distribution of schooling and trying out statistics for the (everyday/assault) sort of community traffic.

Table2:provide training materials and tests

	Normal	Dos	Pbobe	U2R	R2L	Total
Train	6,343	46,927	11,656	53	994	1,75,973
Test	9,811	7,558	2,421	900	2,865	21,564

The working surroundings of all experiments is Keras with tensorflow because the backend; Operating machine is 64-bit CtOS7; Processor is E5-2620 v4; Main frequency is 2.10GHz; Mem- ory is 32.0G; Python model is three.6. In view of many hyper parameters current withinside the BAT-MC version, we achieved one hundred iterations of schooling at the NSL-KDD set. The hyper parameters with the very best accuracy is chosen because the version parameter. The BAT-MC version is likewise confirmed at the check- ing dataset. After masses of experiments, 3 one-dimensional convolution layers are followed while constructing the BAT-MC version for intrusion detection challenge. The parameter listing of BAT- MC community is ready as proven in Table three.

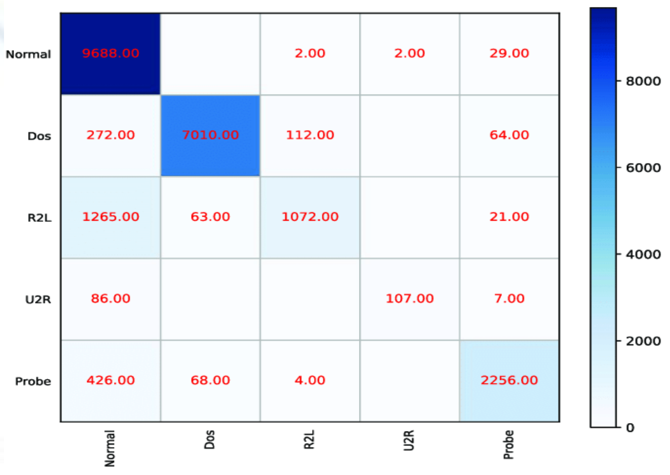
D. PERFORMANCE ANALYSIS OF BAT-MC

Experiments had been designed to examine the overall performance of the BAT-MC version for 2-class and 5-class clas- sification, which include Normal, DoS, R2L, U2R and Probe.

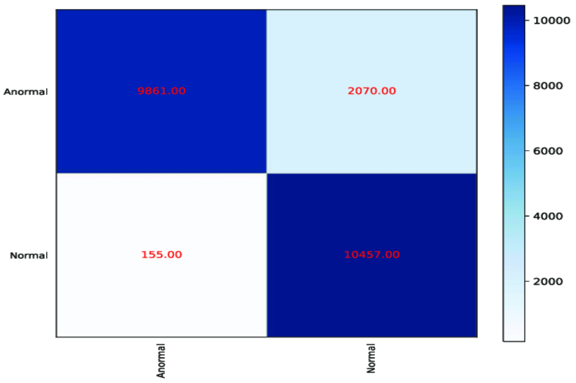
Parameters	Neurons/Filters
conv+tanh	20
conv+tanh	40
conv+tanh	60
BLSTM hidden nodes	80
BLSTM Activation nodes	relu
Dense	320
Dropout	0.1
Softmax	10
Cost function	Cross entropy
optimizer	adam
Batch size	128
Learning rate	0.001

Table 3: Hyperparameters for end-to-end learning models.

In the test of figuring out malicious traffics, while there are eighty hidden nodes withinside the BAT-MC version, the accuracy of BAT-MC at the KDDTest+ dataset is better. Meanwhile, the getting to know charge is ready to 0.01 and the range of schooling is one hundred epoches. The confusion matrix generated with the aid of using the BAT-MC version at the KDDTest+ dataset is proven in Figure three and Figure four. Figure three and Figure four constitute the experimental consequences of the BAT-MC version for the 2-elegance and 5-elegance category, respectively.



The experimental consequences display that maximum samples is targeting the diagonal of the confusion matrix, indicating that the general category overall performance could be very high. However, it could be intuitively visible from the confusion matrix in Figure three display that the BAT-MC community achieves correct detection overall performance in distinguish- ing everyday traffics from assault traffics (handiest fifty one samples are fake positives), however there's nonetheless similarly development in distinguishing exclusive assault traffics. The detection impact of Dos and Probe assault traffics are notably correct, at the same time as R2L and U2R assault traffics are invalid.



After cautious fine-tuning, the accuracy evaluation of the BAT-MC version at the KDDTest+ and KDDTest-21 set is proven in Figure 5. As the range of iterations increases, the accuracy of the BAT-MC version on each the schooling set and the check set suggests an standard upward trend. Experiments at the KDDTest+ dataset display that once epoch = one hundred, the BAT-MC version has a great accuracy (84.25%). At the identical time, the accuracy of the BAT-MC version at the KDDTest-21 facts set is 69.42% and the accuracy at the KDDTrain+ facts set is 99.21%. Table four suggests detection charge (DR) and fake wonderful charge (FPR) for exclusive assault types, the incentive of intrusion detection is to gain a better accuracy and detection charge with a decrease fake wonderful charge. It may be visible that U2R elegance has the bottom detection charge and fake wonderful charge. The U2R elegance with fewer samples are much more likely to be misclassified than people with greater samples.

Table 4 DR and FPR of BAT-MC model **in** NSL-KDD dataset

	FPR	DR
Normal	25.60%	96.50%
Dos	1.53%	86.45%
R2L	0.81%	43.35%
U2R	0.09%	20.94%
Probe	1.14%	85.97%

Table 5 Convolutional layer **diversity.**

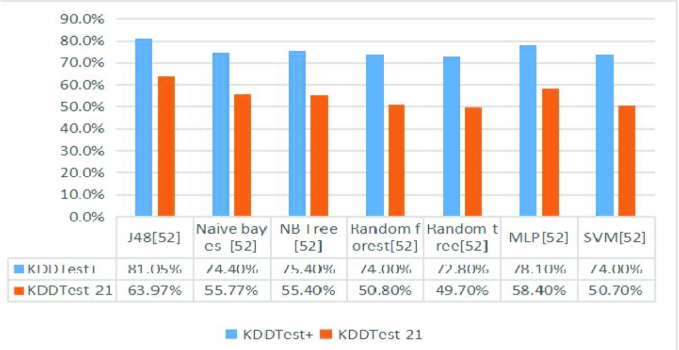
layer	1	2	3	4
Accuracy	82.87%	83.81%	85.25%	84.14%

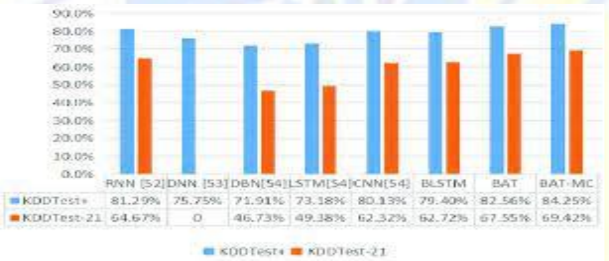
Here, we compare the overall performance of our version to convolutional layer diversity. We carry out the category challenge on exclusive range of convolutional layer. As proven in Table 5, the accuracy has a notably boom while the convolutional layer increases. When the BAT-MC version does now no longer finish convolutional layers, the accuracy of BAT-MC reaches to 84.25%. Overall, our BAT-MC version suggests a higher category accuracy (84.25%) for various convolutional layer.

E. COMPARISON TO THE STATE OF THE ART

In order to objectively examine the accuracy and differen- tiation of the BAT-MC community, we examine our community with a few associated works proposed through [52]–[54]. In [52], the authors advise a deep mastering technique for intrusion detection the use of recurrent neural networks (RNN). Compared with conventional class techniques, which includes J48, naive bayesian, and random forest, the overall performance obtains a better accuracy charge and detection charge with a low fake tremendous charge, particularly below the assignment of multiclass clas- sification at the NSL-KDD dataset. In [53], the authors construct a Deep Neural Network (DNN) version for an intrusion detection device and educate the version with the NSL-KDD Dataset. Experimental effects affirm that the deep mastering technique suggests robust capacity for use for flow-primarily based totally anomaly detection in SDN environments. In [54], the authors advise to apply an average deep mastering approach Convolution Neural Networks (CNN) for detecting cyber intrusions. The experimental effects display that the overall performance of this IDS version is advanced to the overall performance of fashions primarily based totally on conventional system mastering techniques and novel deep mastering techniques in multi-elegance class. These works use the equal dataset NSL-KDD for community visitors class. They aren't best latest distinctly relative and consultant works on intrusion detection, however can also attain terrific accuracy. The evaluation effects amongst those works at the NSL-KDD dataset are proven in Figure 6 and Figure 7, respectively.

Compared with the version of the authors undertake the conventional system mastering techniques to hit upon atypical traffics. That is to say, it wishes to manually layout visitors functions and entire the extraction and choice of community traffics earlier than version training. In contrast, the BAT-MC version without delay takes the gathered visitors as unique input. Experimental effects display that the BAT-MC version can mechanically extract functions through stop- to-stop mastering, which achieves higher class effects than guide layout techniques. Meanwhile, we compares the latest works of the use of deep mastering version for atypical visitors The BAT-MC version can seize functions of community traffics extra comprehensively, that could extract the data of every records packet after which put it to use on a body-through-body way. These effects show that the BAT-MC community can provide a sizable gain throughout very special scenarios.





As the quantity of iterations increases, the accuracy of every version suggests an general upward trend. It may be visible from Figure eight that the accuracy charge of checking out dataset primarily based totally at the BAT-MC version isn't best the fastest, however the accuracy is much less fluctuating after the new release of 20 times. The accuracy of the BAT-MC version stays nearly unchanged. The CNN version begins offevolved to enhance at a slower charge and has the worst perfor- mance in every version. In summary, the BAT-MC community can as it should be pick out the time collection records through 84.25% accuracy, that's an powerful intrusion detection approach**.**

V. CONCLUSION

The cutting-edge deep gaining knowledge of techniques withinside the community visitors clas- sification studies do not make complete use of the community visitors dependent information. Drawing at the software techniques of deep gaining knowledge of withinside the area of herbal language processing, we suggest a unique version BAT-MC thru the 2 phase's learn- ing of BLSTM and interest at the time collection functions for intrusion detection the usage of NSL-KDD dataset. BLSTM layer which connects the ahead LSTM and the backward LSTM is used to extract functions at the the visitors bytes of every packet. Each information packet can produce a packet vector. The above function gaining knowledge of system is mechanically finished through deep neural community with none function engineering technology.

This version correctly avoids the trouble of guide layout functions. Performance of the BAT-MC approach is examined through KDDTest+ and KDDTest-21 dataset. Experimental effects at the NSL-KDD dataset imply that the BAT-MC version achieves quite excessive accuracy. By evaluating with a few stan- dard classifier, those comparisons display that BAT-MC fashions effects are very promising while in comparison to different cutting-edge deep gaining knowledge of-primarily based totally techniques. Hence, we consider that the proposed approach is a effective device for the intrusion detection trouble.

REFERENCES

[1] Da Silva CMR, Feitosa EL, Garcia VC (2020) HeuristicBased Phishing Prediction Strategies: A Survey of URLBased Method Comput Secur 88:101613

[2] Emamgholizadeh S, Mohammadi B (2021).A collection of new nativebased hybrid algorithms support vector machines for the esti mation of soil cation exchange capacity. Soft Comput 25(21): 13451–13464

[3] Gardner MW, Dorling SR (1998) Artificial neural networks (multilayer sensors) A review of applications to atmospheric science. Atmospheric Environment 32(14–15): 2627–2636.

[4]Hochreiter S, Schmidhuber J (1997) Short-term memory. Neural Comput 9(8): 1735–1780

[5] Kiruthiga R, Akila D (2019) Detecting Phishing Websites Using Machine Learning. Int J State of the Art Eng 8(2): 111–114

[6] Mohamed AR, Dahl G, Hinton G (2009) Deep trust for Telecognition. In: Nips Symposium on Deep Learning for Speech Recogni tion and Related Applications, Vol. 1, no. 9, p. 39

[7] Singh C, Meenu (2020) Machine learningbased phishing website detection: a survey. In: 2020 6th International Conference on Ad vanced Computing and Communication Systems (ICACCS).IEEE, pp 398–404

[8] Sumathi K, Sujatha V (2019) Deep learnigbased phishing attack detection. Int J State of the Art Eng (IJRTE) 8(3): 8428–8432

[9] Vrbančič G, Fister I Jr, Podgorelec V (2020) Phishing web search dataset. Short Data 33: 106438

[10] Zhang Y, Wang J, Chen B (2020) Detecting Fraudulent Data Injection Attacks in Smart Grids: Semisupervised Deep Learning A pproach. IEEE Trans Smart Grid 12: 623–634

[11]Zhang Qing; To buy. ; Chen, B. (1999).Zhang, S. Lu, X. Research on a phishing web page detection system based on the CNN-BiLSTM algorithm. J. Physics.Phone number 2021, 1738, 012131.

[12]C. Yin, "An Advanced UN Model Matching Algorithm in Intrusion Detection Systems", Appl. Mecha Alma Mater, Vol. 148-149: I. 1145-1148, Three. 2012.

[13]S. Garg ve S. Batra, "A Novel Ensemble Technique for Anomaly Detection", Int.J. Community. System, Vol. 30, no.Page 11 e32 48, July 2017.

[14]F. Kuang, W.Xu and S. Zhang, "A New Hybrid KPCA and SVM with a GA Model for Research", Appl. Flexible Computing.., V ol.18 sayfa, S. Cornegruta, R. Bakewell, S. Withey ve G.1-11. 178–184, Peb 2014.

[15] S. Garg ve S. Batra, "A Novel Ensemble Technique for Anomaly Detection", Int.J. Community. System, Vol. 30, no. Page 11 e3248, July 2017.