iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.54497

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Packet Inspection to Identify Network Layer Attacks Using Machine Learning

N. Siva Nagamani[1] , U. Satya Narayana[2], D. Ramesh[3]
[1, 2, 3]*Assistant Professor, Department of CSE, Geethanjali Institute of Science & Technology, Nellore, A.P.*

Abstract: ***With the advent of technology, computer networks have become an integral part of our lives. However, with the increase in the use of computer networks, network attacks have also increased. Network attacks can cause serious harm to network infrastructure, resulting in loss of data, financial loss, and reputation damage. In this paper, we propose a machine learning algorithm to analyze network packets to detect malicious activities that are aimed at disrupting the normal functioning of a network. Network layer attacks typically target the underlying infrastructure of a network, which includes the IP layer, transport layer, and network access layer. These attacks can cause various problems such as denial of service, data theft, and network downtime.***

To detect network layer attacks, the proposed approach involves extracting features from network packets. Features refer to the attributes or characteristics of a packet, such as the source and destination IP addresses, protocol type, payload size, etc. These features are then used to train a machine learning model to identify various network layer attacks such as DDoS, ARP spoofing, and ICMP attacks. The machine learning model uses these features to learn the patterns and behaviours of these attacks and uses this knowledge to detect them in real-time. The proposed approach is evaluated using various metrics such as accuracy, precision, recall, and F1-score. The evaluation results demonstrate that the proposed approach is effective in detecting network layer attacks and outperforms existing approaches. The proposed approach can be used to enhance network security and prevent network attacks.

Keywords: Artificial Intelligance, Lung cancer, Neural Networks, SVM

I. INTRODUCTION

Here we are discussing about different attacks occurs on networks. Internet and computer networks are exposed to an increasing number of security threats. With new kind of attacks appearing continually, developing flexible and adaptive security-oriented approaches maybe a severe challenge. In this context anomaly-based network intrusion detection techniques are a valuable technology to protect target systems and networks against malicious activities. We analysis the traffic and make a dataset for types of attacks and that help to train dataset and predict the test dataset.

A key focus of IDS supported Machine Learning research is to detect patterns and build detection system supported the dataset. Multiple types of attacks on network occurs so identify that we going to do work in traffic packet identification to analysis the attacks. Packet inspection is a method used to analyse the contents of network traffic passing through a network interface, such as a router or firewall. This method is used to identify network layer attacks that can compromise the security and integrity of the network. Packet inspection is an important tool for protecting network security and ensuring the integrity of data transmitted over the network.

Packet inspection is a valuable tool for identifying network layer attacks, but it can be challenging to keep up with the constantly evolving threat landscape. Machine learning (ML) can help improve the effectiveness of packet inspection by enabling systems to learn from past data and adapt to new threats in real-time.Traditional packet inspection methods rely on pre-defined rules and signatures to detect known types of attacks, but these methods may not be effective against new or unknown threats. Machine learning algorithms can learn to detect patterns in network traffic and identify anomalies that may indicate an attack, without relying on pre-defined rules.By using machine learning to analyze network traffic, systems can adapt to changing threats and learn from new attack patterns. This can help improve the accuracy of packet inspection and reduce the number of false positives, while also enabling faster detection and response times. Furthermore, machine learning can help identify previously unknown or "zero-day" attacks that have not yet been identified or classified. These types of attacks can be especially dangerous, as they may not be detected by traditional signature-based methods.

Specifically, the objectives of using machine learning for packet inspection include:

1) Create a train dataset for identify attacks in network.
2) Understanding network traffic anomalies, Network data types for finding loopholes in networks.
3) Trying to develop systems which use Machine Learning techniques to identify the attacks.
4) Improving the prediction performance of the predictors when attacks is occurred.

Overall, the objective of using machine learning for packet inspection is to develop a system that can provide accurate and effective threat detection and response capabilities, enabling network administrators to protect the integrity and security of their networks.

II. LITERATURE SURVEY

Network information security is significantly aided by intrusion detection. In order to recognise malicious communications, machine learning techniques have been extensively employed in intrusion detection. These approaches, however, are part of shallow learning and frequently place an emphasis on feature engineering and selection. Low recognition accuracy and a high false alarm rate are the results of their inability to successfully address the enormous intrusion data classification problem and trouble choosing features. Deep learning-based intrusion detection techniques have been proposed repeatedly in recent years. To effectively capture the local aspects of traffic data, we use many convolutional layers. We refer to the BAT model as the BATMC since several convolutional layers are used to process data samples. Network traffic classification is done using the SoftMax classifier.

1) *Intrusion Detection Techniques for Internet of Things AUTHORS: Sarika Choudhary and Nishtha Kesswani*

The latest buzzword in internet technology now a days is the Internet of Things. The Internet of Things (IoT) is an ever-growing network which will transform real-world objects into smart or intelligent virtual objects. IoT is a heterogeneous network in which devices with different protocols can connect with each other in order to exchange information. These days, human life depends upon the smart things and their activities. Therefore, implementing protected communications in the IoT network is a challenge. Since the IoT network is secured with authentication and encryption, but not secured against cyber-attacks, an Intrusion Detection System is needed. This research article focuses on IoT introduction, architecture, technologies, attacks and IDS. The main objective of this article is to provide a general idea of the Internet of Things, various intrusion detection techniques, and security attacks associated with IoT.

2) *Network Intrusion Detection AUTHORS: B. Mukherjee, L.T. Heberlein and K.N. Levitt*

Intrusion detection is a new, retrofit approach for providing a sense of security in existing computers and data networks, while allowing them to operate in their current "open" mode. The goal of intrusion detection is to identify unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators. The intrusion detection problem is becoming a challenging task due to the proliferation of heterogeneous computer networks since the increased connectivity of computer systems gives greater access to outsiders and makes it easier for intruders to avoid identification. Intrusion detection systems (IDSs) are based on the beliefs that an intruder's behaviour will be noticeably different from that of a legitimate user and that many unauthorized actions are detectable. Typically, IDSs employ statistical anomaly and rule-based misuse models in order to detect intrusions. A number of prototypes IDSs have been developed at several institutions, and some of them have also been deployed on an experimental basis in operational systems. In the present paper, several host- based and network-based IDSs are surveyed, and the characteristics of the corresponding systems are identified. The host-based systems employ the host operating system's audit trails as the main source of input to detect intrusive activity, while most of the network-based IDSs build their detection mechanism on monitored network traffic, and some employ host audit trails as well. An outline of a statistical anomaly detection algorithm employed in a typical IDS is also included.

3) *Survey on SDN based network intrusion detection system using ML approaches AUTHORS: N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad*

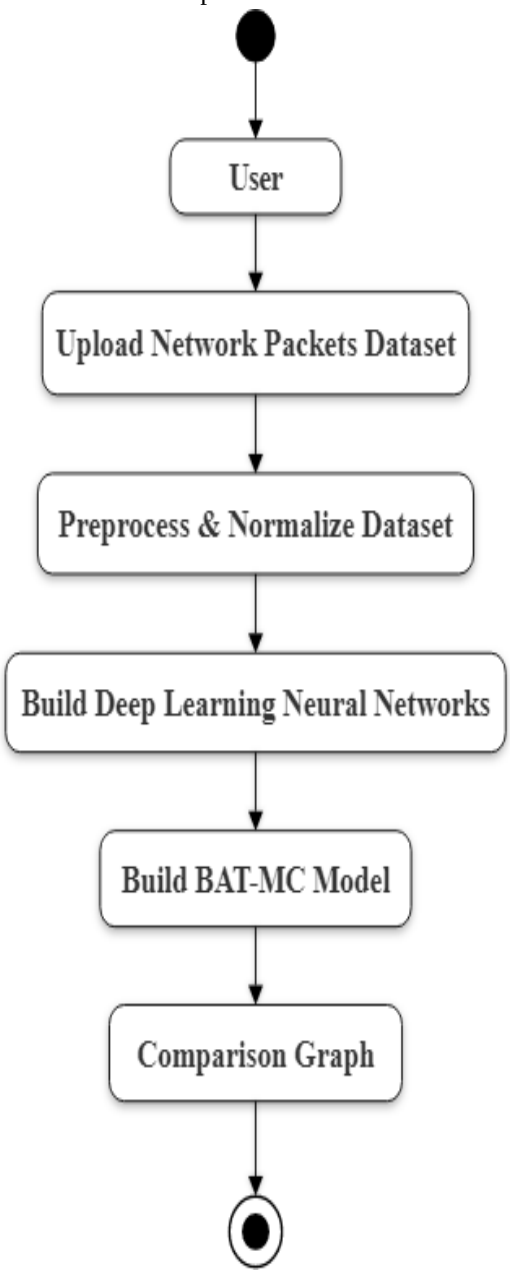
Software Defined Networking Technology (SDN) provides a prospect to effectively detect and monitor network security problems ascribing to the emergence of the programmable features. Recently, Machine Learning (ML) approaches have been implemented in the SDN- based Network Intrusion Detection Systems (NIDS) to protect computer networks and to overcome network security issues. A stream of advanced machine learning approaches –the deep learning technology (DL) commences to emerge in the SDN context. In this survey, we reviewed various recent works on machine learning (ML) methods that leverage SDN to implement NIDS. More specifically, we evaluated the techniques of deep learning in developing SDN-based NIDS.

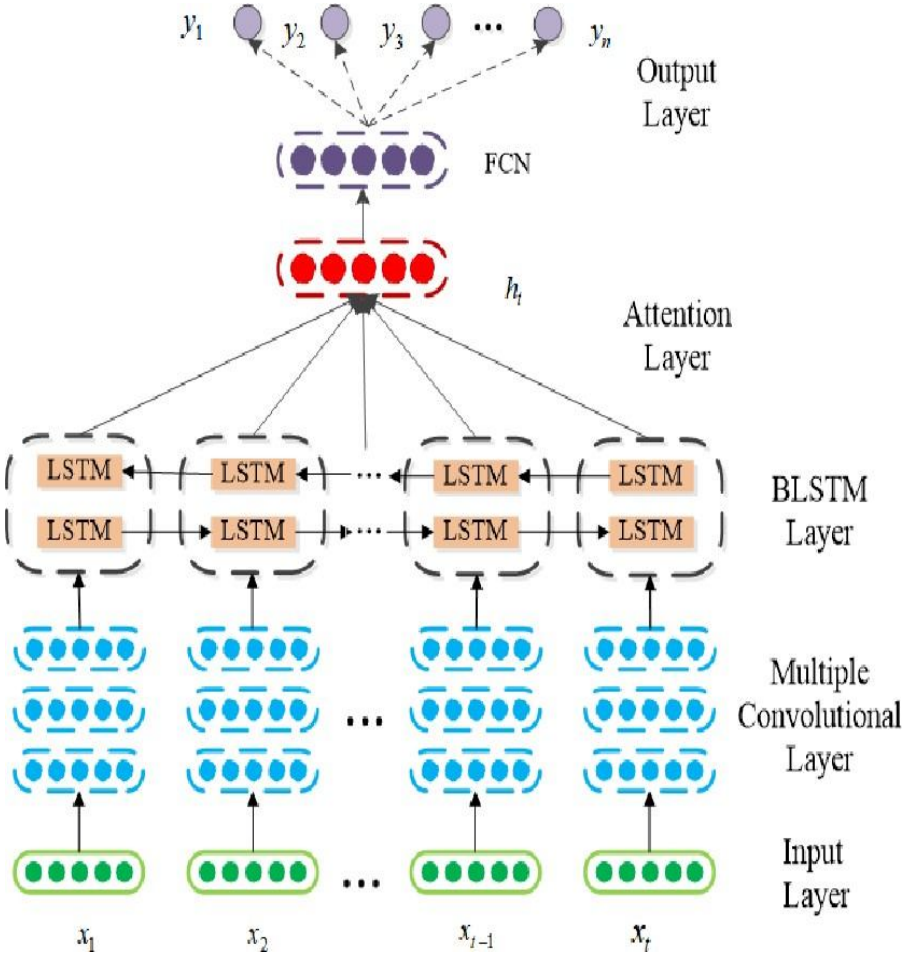
In the, meantime, in this survey, we covered tools that can be used to develop NIDS models in SDN environment. This survey is concluded with a discussion of ongoing challenges in implementing NIDS using ML/DL and future works.

III. METHODOLOGY

The methodology for using machine learning in packet inspection to identify network layer attacks involves several key steps:

1) *Data Collection:* Collecting a large volume of labelled network traffic data, which includes both benign and malicious traffic.
2) *Feature Extraction:* Extracting relevant features from the collected network traffic data that can be used to identify patterns and anomalies indicative of an attack.
3) *Model Training:* Training machine learning algorithms using the extracted features and labelled data.
4) *Model Evaluation:* Evaluating the performance of the trained model using test data that was not used in training.
5) *Model Deployment:* Deploying the trained machine learning model in a real-time packet inspection system.
6) *Monitoring and Updating:* Monitoring the performance of the deployed machine learning model and updating it regularly to keep up with new threats and changes in network traffic patterns.





The BAT-MC Model consists of five components, including the input layer, multiple convolutional layers, BLSTM layer, attention layer and output layer, from bottom to top.

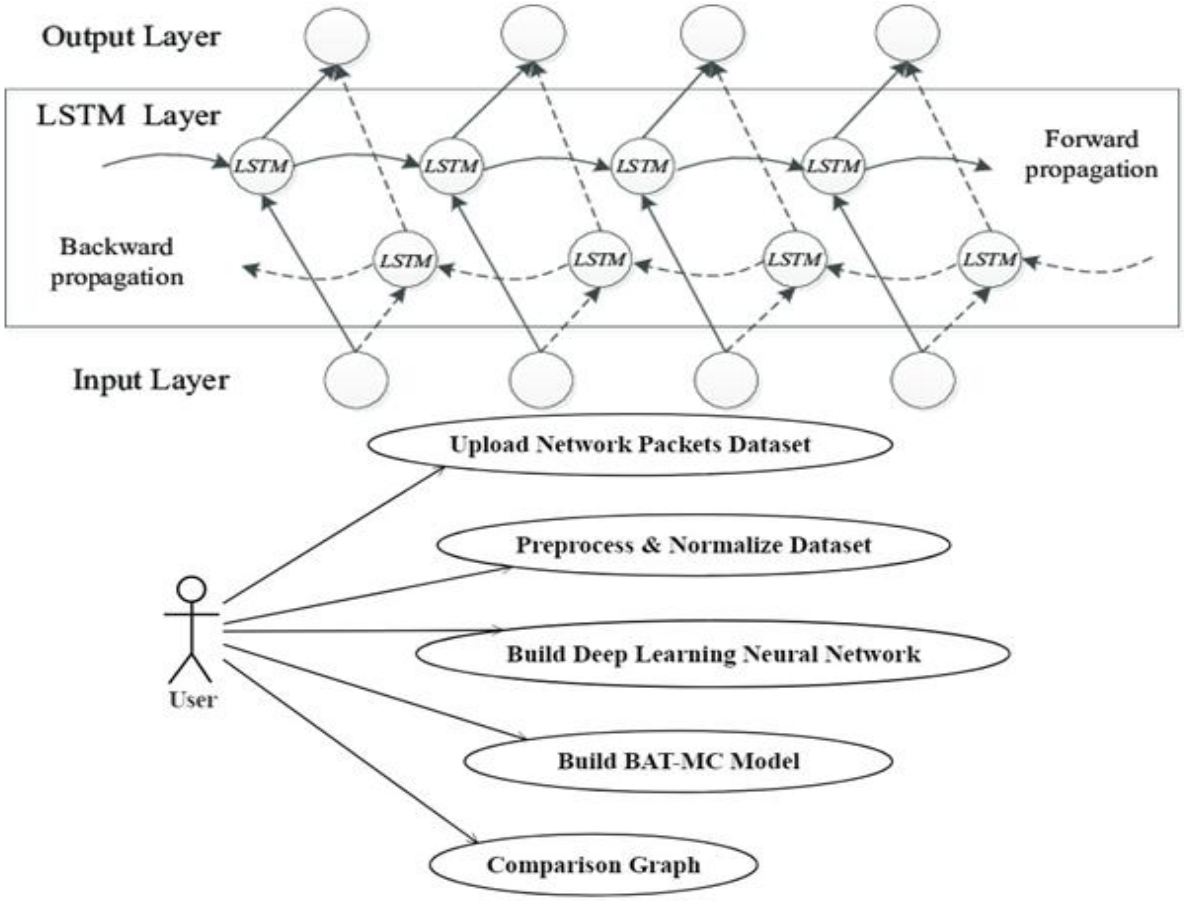
a) *Input Layer:* The input layer is the first layer in the BAT-MC model and receives input data in the form of network traffic packets. Each packet is represented as a sequence of numerical features, such as packet size, packet direction, and protocol type.

b) *Multiple Convolutional Layer:* The second component of the BAT-MC model consists of multiple convolutional layers. These layers apply convolutional filters to the input data to extract spatial and temporal features from the network traffic. The output of each convolutional layer is a set of feature maps, which represent the activation of each filter at different locations in the input data.

c) *BLSTM Layer:* The third component of the BAT-MC model is a Bidirectional Self- Attention Long Short-Term Memory (BSLTM) layer. This layer processes the feature maps produced by the convolutional layers and applies bidirectional self-attention mechanisms to learn long-term dependencies between different parts of the input data. The BSLTM layer uses a combination of convolutional and recurrent neural network (RNN) techniques to capture both spatial and temporal features in the input data.

d) *Attention Layer:* The fourth component of the BAT-MC model is an attention layer. This layer uses the outputs of the BSLTM layer to learn a set of attention weights, which represent the relative importance of each feature map for detecting intrusions in the network traffic. The attention weights are used to weigh the contributions of each feature map when making predictions.

e) *Output Layer:* The final component of the BAT-MC model is the output layer. This layer receives the weighted feature maps from the attention layer and applies a fully connected layer to predict the probability of each network traffic packet being malicious or benign. The output layer produces a binary output for each packet, indicating whether it is classified as malicious or not.



IV. RESULTS AND SCREENSHOTS

The steps followed in the execution process are shown in the attached screenshot pictures:

1) Open the command prompt
2) Enter the command to view the display to perform algorithms
3) Open the dataset
4) In the display click on load dataset to load the dataset
5) Once the data gets loaded click on pre-process data for performing data pre- processing
6) Click on the SVM
7) Click on the CNN to get the accuracy
8) Click on Accuracy comparison to get the graph that compares the accuracies of all the algorithms

Figure: GUI Window

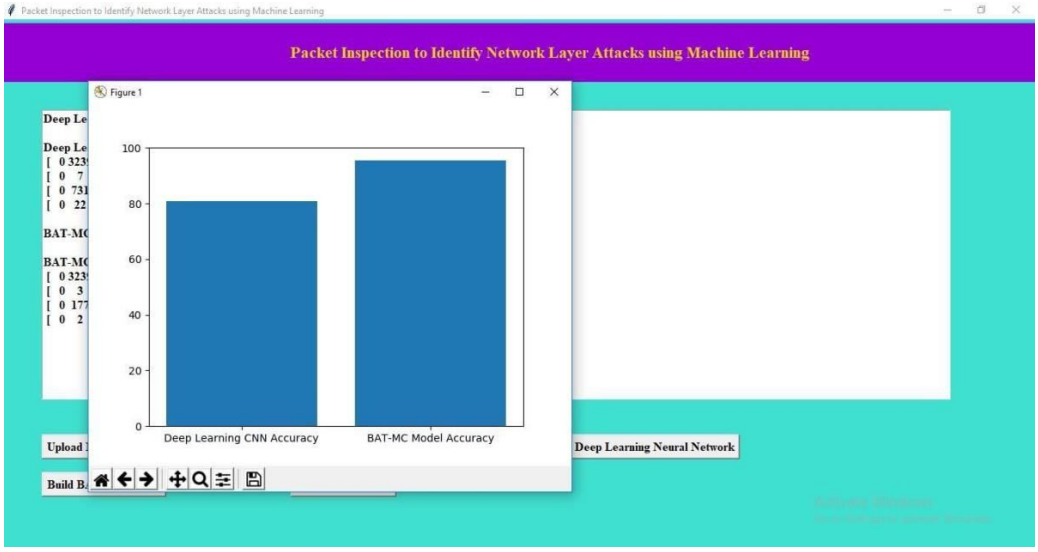


Figure: Output Window

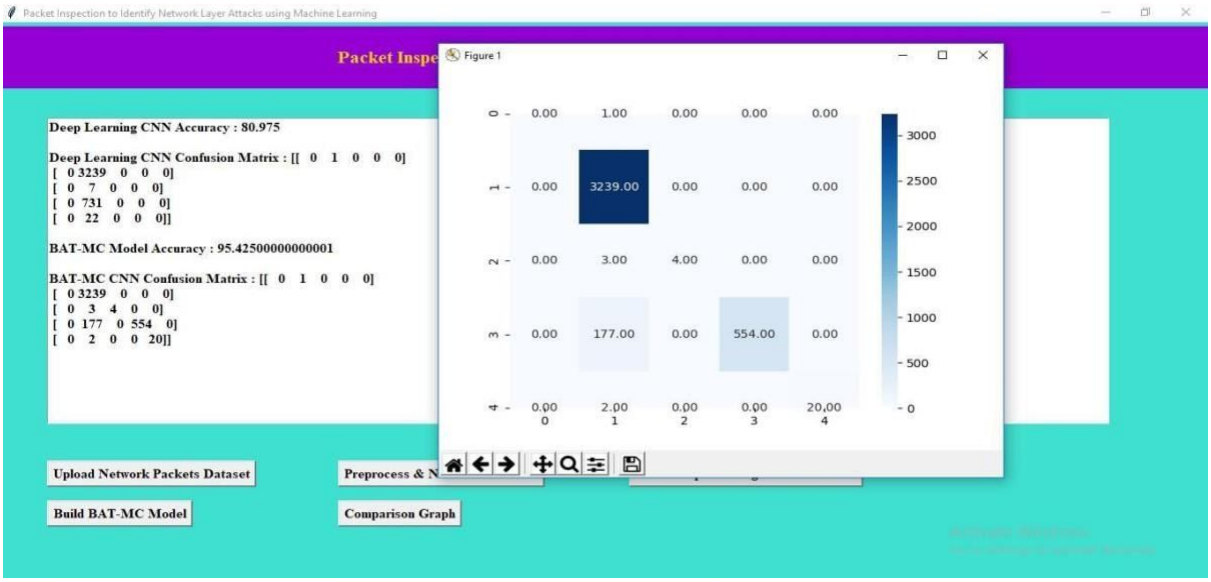


Figure: Comparison Results of all models

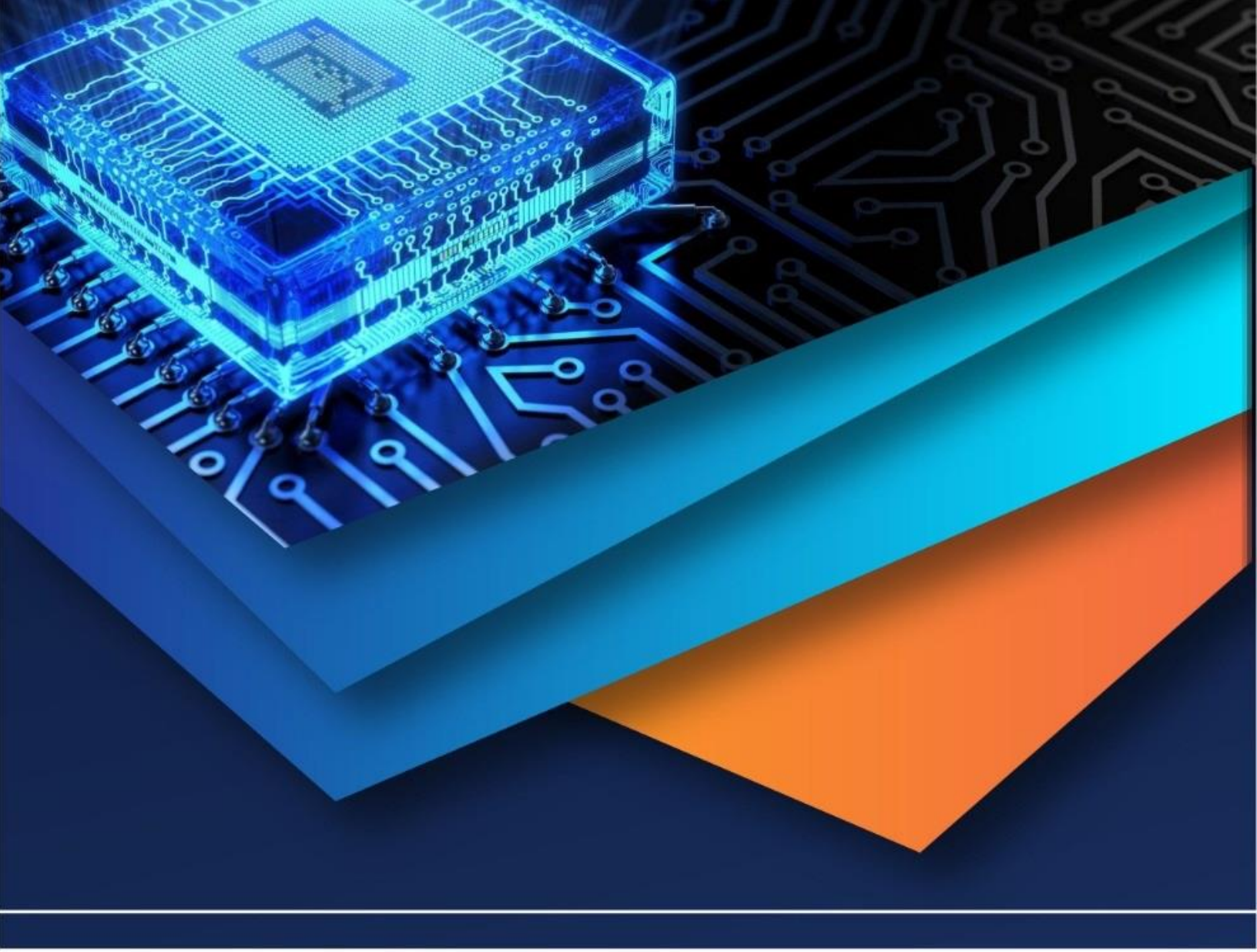
V. CONCLUSION

The current deep learning methods in the network traffic classification research don't make full use of the network traffic structured information. Drawing on the application methods of deep learning in the field of natural language processing, we propose a novel model BAT- MC via the two phase's learning of BLSTM and attention on the time series features for intrusion detection using NSL-KDD dataset. BLSTM layer which connects the forward LSTM and the backward LSTM is used to extract features on the traffic bytes of each packet. Each data packet can produce a packet vector. These packet vectors are arranged to form a network flow vector. Attention layer is used to perform feature learning on the network flow vector composed of packet vectors. The above feature learning process is automatically completed by deep neural network without any feature engineering technology. This model effectively avoids the problem of manual design features. Performance of the BAT-MC method is tested by KDDTest+ and KDDTest-21 dataset. Experimental results on the NSL-KDD dataset indicate that the BAT-MC model achieves pretty high accuracy. By comparing with some standard classifier, these comparisons show that BAT-MC models results are very promising when compared to other current deep learning-based methods. Hence, we believe that the proposed method is a powerful tool for the intrusion detection problem.

The future enhancements for packet inspection to identify network layer attacks using machine learning could be in several areas. Firstly, the accuracy and efficiency of the approach could be improved further. This could be achieved through the use of more advanced machine learning techniques or by exploring ensemble methods. Additionally, the proposed approach could be tested on larger datasets to determine its scalability and effectiveness in detecting attacks. Secondly, the proposed approach could be implemented in real-time to enable immediate detection of network layer attacks. This would enable a prompt response to mitigate the impact of the attack. Thirdly, the approach could be made more adaptable to new attack patterns. This could be achieved through the use of incremental learning techniques to update the machine learning model in real-time as new attack patterns emerge. Fourthly, the proposed approach currently focuses on detecting network layer attacks, but attacks can also occur at other layers such as the application and presentation layer. Future research could explore the extension of the proposed approach to detect attacks at these layers as well. Finally, the proposed approach could be integrated with existing network security frameworks to provide an additional layer of security. This would enable prompt response to detected network layer attacks, enhancing overall network security. Overall, future enhancements for the proposed approach could strengthen network security and improve the accuracy and efficiency of attack detection and mitigation.

REFERENCES

[1] B. B. Zarpelo, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ‘‘A survey of intrusion detection in Internet of Things,’’ J. Netw. Comput. Appl., vol. 84, pp. 25-37, Apr. 2017.
[2] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, ‘‘Network intrusion detection,’’ IEEE Netw., vol. 8, no. 3, pp. 26-41, May 1994.
[3] S. Kishorwagh, V. K. Pachghare, and S. R. Kolhe, ‘‘Survey on intrusion detection system using machine learning techniques,’’ Int. J. Control Automat., vol. 78, no. 16, pp. 30-37, Sep. 2013.
[4] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, ‘‘Survey on SDN based network intrusion detection system using machine learning approaches,’’ Peer-to-Peer Netw. Appl., vol. 12, no. 2, pp. 493-501, Mar. 2019.
[5] M. Panda, A. Abraham, S. Das, and M. R. Patra, ‘‘Network intrusion detection system: A machine learning approach,’’ Intell. Decis. Technol., vol. 5, no. 4, pp. 347–356, 2011.
[6] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, ‘‘A new intrusion detection system based on KNN classification algorithm in wireless sensor network,’’ J. Electr. Comput. Eng., vol. 2014, pp. 1-8, Jun. 2014.
[7] S. Garg and S. Batra, ‘‘A novel ensembled technique for anomaly detection,’’ Int. J. Commun. Syst., vol. 30, no. 11, p. e3248, Jul. 2017.
[8] F. Kuang, W. Xu, and S. Zhang, ‘‘A novel hybrid KPCA and SVM with GA model for intrusion detection,’’ Appl. Soft Comput., vol. 18, pp. 178-184, May 2014.
[9] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, ‘‘Malware traffic classification using convolutional neural network for representation learning,’’ in Proc. Int. Conf. Inf. Netw. (ICOIN), 2017, pp. 712-717.
[10] P. Torres, C. Catania, S. Garcia, and C. G. Garino, ‘‘An analysis of Recurrent Neural Networks for Botnet detection behaviour,’’ in Proc. IEEE Biennial Congr. Argentina (ARGENCON), Jun. 2016, pp. 1–6.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY