Performance optimization for Intrusion Detection by Long Short Term Memory (LSTM)

Monika khatkar[1*], *Kaushal* Kumar[1], *Brijesh* Kumar[2], *Asha* Sohal[1], and *Kriti* Sharma[3], *Amita* Bisht[4], *B*. Sankara Babu[5], *Monica* Gulati[6], *M*. Manasa[7]

[1]School of Engineering and Technology, K R Mangalam University- Gurgaon 122103 Haryana, India
[2]Department of Computer Science and Engineering -Manav Rachna International University, Faridabad, 121004 Haryana, India
[3]Department of Engineering and Technology, Sushant University- Gurgaon 122003 Haryana, India
[4]Division of Research & Innovation, Uttaranchal University, Dehradun, India,
[5]Department of Civil Engineering, GRIET, Bachupally, Hyderabad, Telangana, India
[6]Lovely Professional University, Phagwara Punjab, 144001, India
[7]KG Reddy College of Engineering & Technology, Moinabad, Hyderabad, Telangana, India

Abstract. Concerns about cyber threats have emerged as the expansion of system connectivity and the proliferation of system applications intensified in the industry. This has underscored the necessity for a robust defense mechanism against various cyber threats, including potential intrusions from malicious actors within the network. A specially targeted system is the intrusion detection system (IDS), designed to safeguard the confidentiality, integrity, and availability of network traffic, especially in critical sectors like healthcare. Recent advancements in the area of IDS involve the utilization of artificial intelligence (AI) and deep learning (DL) based IDS to efficiently recognize network issues. Notably, the research at hand adopts a deep learning approach employing Long Short Term Memory (LSTM) models, applied to the CICIDS-2019 dataset that is sourced from New Brunswick University's website. The focal point of evaluation lies in the precision, recall, F1-score, and accuracy metrics, specifically analyzing its performance in identifying Denial-of-Service (DoS) cyber-attacks. The findings of this study lighten the superior performance of the Long Short Term Memory method in the realm of intrusion detection systems. The LSTM model showcases its proficiency, particularly in discerning Denial of Service attacks by giving a loss of less than 0.03%.

Keywords: Cyber Security, IDS, CICIDS-2019 dataset, Denial of Service, LSTM.

* Corresponding author : khatkarmonika@gmail.com

1 Introduction

With the recent surge in responsiveness as well as advancements in communication technologies within the past ten years, the safeguarding of network integrity has emerged as a crucial field of study [1]. This involves the utilization of tools like firewalls, antivirus software, and intrusion detection systems to ensure the protection of both the network and its assets in the virtual realm. Within this context, network intrusion detection systems play a pivotal role as mechanisms for identifying potential attacks. Their primary objective is to ensure the security of the network by constantly monitoring the flow of network traffic to detect any suspicious or malicious activities. However, the rapid progression of technology in the past decade has led to an outstanding expansion in network size and the complexity of applications managed by network nodes. Consequently, this has resulted in the generation and dissemination of a substantial volume of critical data, which is distributed across various areas of the network. In light of the rapid growth in internet awareness and technological progress over the past decade, assuring the security of networks and data nodes has become a complex problem. This also endorsed to the emergence of new attack methodologies, which can either be adaptations of previously generated attacks or entirely new approaches. In addition to this, the presence of latent intruders with nasty intent within networks cannot be overlooked. It can be said that virtually all network nodes are susceptible to security vulnerabilities. The concept of Intrusion Detection Systems (IDS) was initially introduced by Jim Anderson in 1980, and since then, a variety of IDS products have been developed and refined to address the evolving demands of network security.

2 Background and Related Work

Two overarching terms within the application security are intrusion detection and prevention systems, both serving to counteract intrusions and pre-empt emerging threats. Intrusion Detection Systems function as vigilant entities, akin to private investigators, responsible for identifying malicious activities. This is achieved through either active gating (as seen in Network Intrusion Prevention Systems) or passive monitoring of network traffic by using different machine-learning techniques [2]. To overcome the above-mentioned obstacles, security academics and researchers along with IDS developers are focused on the advanced ML methods for intrusion detection systems.

These systems generally utilize predefined rules and patterns to trigger alerts. IDS employs various features to discern normal activities from abnormal ones, effectively acting as predictive machine learning classifiers to distinguish between different attack types. Supervised classification methods, such as ANN and Long Short-Term Memory are applied in IDS [3]. These algorithms are evaluated based on accuracy and loss which results being particularly important, to classify and predict potential threats.

Machine learning (ML)-based IDS heavily relies on feature engineering to extract valuable insights from network traffic data. In contrast, deep learning (DL)-based intrusion detection systems dispense with extensive data pre-processing. They autonomously uncover intricate patterns from input data due to their inherent structural complexity. Deep learning finds practical application in cybersecurity, aiding in classifying threats and identifying anomalous behaviors. Several open-source deep learning libraries, including TensorFlow, support such endeavors.

The ongoing study delves into the classification and intrusion detection techniques employing machine learning and deep learning to detect cyber-attacks on the CICIDS-2019 dataset. In particular, the focus is on intrusion detection systems using Tensor Flow, an open-source software library from Google specially tailored for deep learning and deep neural networks.

Despite significant advancements by researchers, IDS still grapples with challenges in achieving higher accuracy in recognition while mitigating false positives and accurately identifying novel intrusions. The central aim of this research is to evaluate two i.e. ANN, and LSTM deep learning techniques for specific aspects of detecting Distributed Denia1-of-Service (DDoS) attacks and identifying the most effective approach. Building on previous work, the study broadens its scope to encompass various machine learning strategies for recognizing malicious activities, with DDoS attacks being a specific focus.

Intrusion Detection System (IDS) serves as a network security solution primarily designed to detect possible attacks directed at a particular application or computer. When properly configured, it can analyze inbound and outbound network data while consistently monitoring network behaviors. It promptly notifies users of any unforeseen or abnormal activities within the system.

Network IDS can be divided into two distinct types based on their operational methodology: active and passive.

Active IDS: Active IDS refers to systems that not only detect intrusions but also take preventative measures against attacks by promptly blocking suspicious traffic.

Passive IDS: Passive IDS, on the other hand, focuses on monitoring and analyzing network traffic. It alerts the administrator about ongoing attacks and vulnerabilities without actively intervening to block traffic.

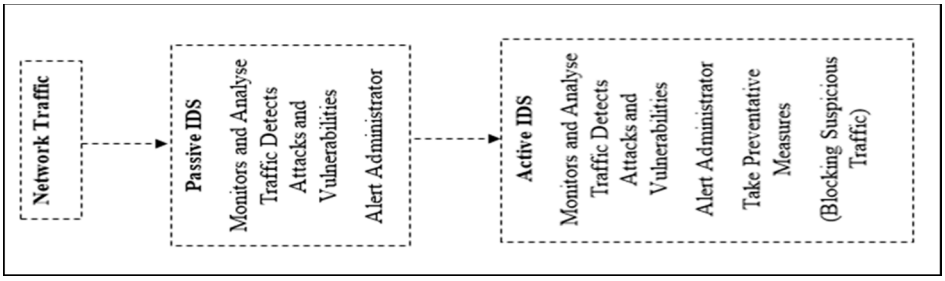

Fig. 1. Category of Intrusion Detection System [Author's Compilation]

Many other Intrusion detection systems are also categorized according to their function performance.

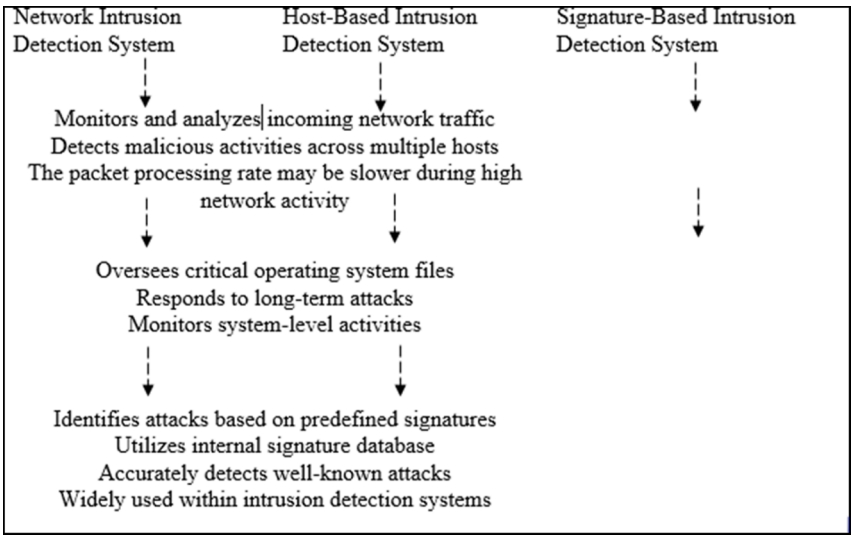

Fig. 2. Category of Intrusion Detection System [Author's compilation]

Network Intrusion Detection Systems (NIDS): These systems are crafted to oversee and evaluate incoming network traffic. Their functionality encompasses the detection of malicious activities across numerous hosts. [4], [9].
Host-Based Intrusion Detection Systems (HIDS): HIDS is oriented towards the monitoring of critical operating system files. It exhibits the capability to effectively counter extended attacks by maintaining a vigilant watch over activities occurring at the system level [4], [9].
Signature-Based Intrusion Detection Systems (SIDS): A signature-based system typically monitors incoming network traffic for sequences and patterns that correspond to a particular attack signature [4], [9-10].
Limitations of Signature and Anomaly-based Intrusion Detection: Signature-based intrusion detection systems have a significant drawback, primarily in their inability to identify unknown attacks. Malicious actors can evade detection by altering attack sequences within malware and other attack types. Encryption of traffic can render signature-based tools ineffective. Behavior-based IDS solutions offer a robust defense against network breaches by leveraging AI and machine learning for intelligent data analysis [4-6]. These solutions provide comprehensive insights into intricate, expansive networks that span offices, data centers, and the cloud. However, they have a downside in the form of a high false-positive rate, detecting malicious and unusual traffic across the entire network attack surface.
Machine learning involves the development of systems that can learn from data and uncover concealed patterns [7-9]. The main challenge lies in efficiently sifting through the abundant data to unearth valuable and relevant information. This is why machine learning models have permeated numerous domains. Deep learning models learn by examples means they classify the data directly from the images, text, sound, etc. These models are trained by using a big set of labeled data. These models perform tasks that humans do naturally, and their performance sometimes exceeds expectations this is the reason that deep learning models such as LSTM and RNN are attaining good attention [7], [9]. In this research, a deep learning-based LSTM algorithm is applied to the CICIDS -2019 dataset to check whether it is an attack or not.

3 Experimental Analysis

The experimental work is done using LSTM for CICICDS 2019 dataset, executed with the help of a graphic card processor system and tensor flow. The confusion metric is used to evaluate the performance of the model by calculating different metrics like Sensitivity, Recall, etc. The whole experiment was performed for 100 epochs. As discussed in the different studies confusion matrix is a four-sided shape/square shape shown in Fig. 4, in which the column signifies the actual values and the row represents the model's predicted value and vice versa.

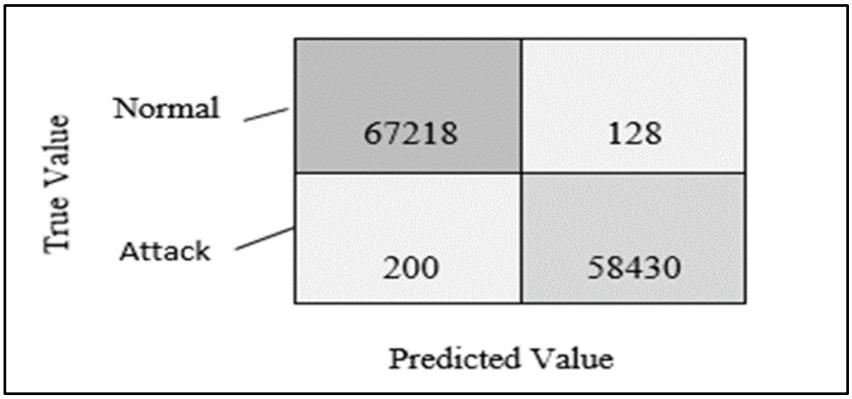

Fig. 3. Confusion Metric [System Generated]

As derived from the confusion metrics the score achieved by the state-of-the-art system is a precision value of 0.998 whereas the Recall, F1 Score, Accuracy, and validation accuracy are 0.997, 0.998, and 0.997, 0.997 respectively.

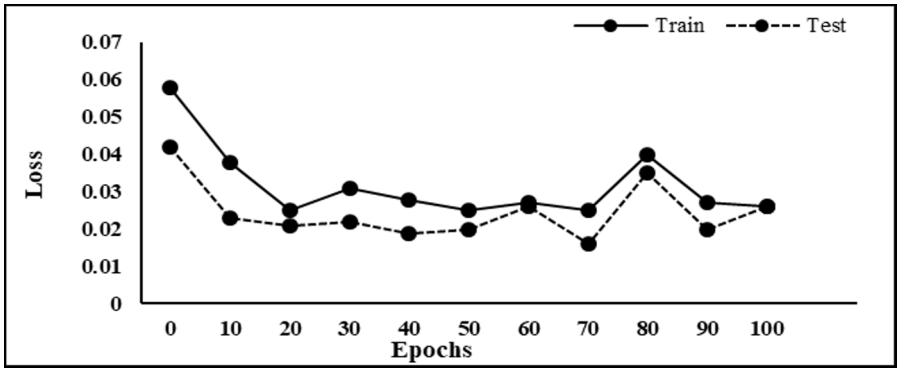

Fig. 4. Epochs Versus Loss Graph

Fig. 4. depicts that the LSTM model exhibited strong performance on the validation set. Over the course of 100 epochs, the loss was found to be notably lower compared to the loss observed in the training set during the execution of the model. Furthermore, the architecture achieved very impressive results, like precision, F1 Score, recall, and validation accuracy around 99.6% mark, as demonstrated in Figure 4. As it can be seen the loss during training and testing dataset is minimum during the execution of the model for 100 no of epochs.

4 Conclusion

A new area of research is emerging in the realm of artificial intelligence and machine learning, focusing on classifier methodologies within intrusion detection systems. This matter has been a focal point of investigation for an extended period. Anomaly and signature detection systems play a critical role in identifying and categorizing malicious activities [10-16]. In this study, the deep neural network technique is applied for detecting malicious instances, accompanied by a comprehensive range of evaluation metrics that assess the performance of the intrusion detection algorithm. Further, in the future, the focus will be on the system's user-friendliness and reliability. This objective can be chased through the application of different ensemble techniques and the exploration of different architectures, using explainable AI and high-performance systems. The ultimate aim is to streamline the model's time complexity.

Furthermore, the scope offers numerous feature selection algorithms as applying these algorithms under the umbrella of classification can significantly enhance the efficiency of intrusion detection systems. This also underscores the feature selection stage's growing importance within the broader intrusion detection framework.

References

1. A. Alotaibi, M. A. Rassam, F.I., ***15*(2)**, 62 (2023).
2. M. A Talukder, K. F Hasan, Islam, M. M., Uddin, M. A., Akhter, M. A. Yousuf, & M. A. Moni, J.I.S.A., **72,** 103405 (2023).
3. M.Kalinin, V. Krundyshev, J.C.V.H.T., **19,** 125–136 (2023).
4. Fuat, T. Ü. R. K, B.E.Ü.F.B.D., **12(2)**, 465-4779(2023).
5. N. Mishra, & S. Mishra, I.J.S.A.E., **11(5s)**, 247-260(2023).
6. Y. S. Almutairi, B. Alhazmi, & A. A. Munshi, A.S.T.R.J., **16(3)**, 193-206(2022).
7. I.Hidayat, Ali, M. Z., & A. Arshad, J.C.C.E., **2(2)**, 88-97(2023).
8. M. Maabreh, I. Obeidat, E. A. Elsoud, A. Alnajjar, R. Alzyoud, & Darwish, I.J.I.M.T., **17(14)** (2022).
9. S. Latif, F. F. Dola, M. D. Afsar, I. J.Esha, & D. Nandi, I.J.I.E.E.B., **14(2)**(2022).
10. Q. V. Dang, C & I, **41(1)**, 12-33(2022).
11. F. Louati, F. B. Ktata, & I. A. B. Amor, I.J.S. NS pp. 152-157 (2022).
12. S. Sheikh, B. Suthar, and M. Uddin, in 2017 International Conference on Innovations in Control, Communication and Information Systems (ICICCI) (IEEE, 2017), pp. 1–6
13. S. Singh, S. Dixit, S. Sahai, A. Sao, Y. Kalonia, and R. Subramanya Kumar, in MATEC Web of Conferences (2018)
14. A. Sao, S. Singh, S. Dixit, A. K. Pandey, and S. Singh, International Journal of Mechanical Engineering and Technology 8, 579 (2017)
15. M. S. Malik, R. I. Alsantali, R. S. Jassas, A. A. Alsimaree, R. Syed, M. A. Alsharif, K. Kalpana, M. Morad, I. I. Althagafi, and S. A. Ahmed, RSC Adv 11, 35806 (2021)
16. S. P. Arunkumar, C. Prabha, R. Saminathan, J. A. Khamaj, M. Viswanath, C. K. Paul Ivan, R. Subbiah, and P. M. Kumar, Mater Today Proc 1411 (2022)