**Detecting Anomalous Network Behaviors using Deep Learning based LSTM Model**

*Sahil Sehrawat*

*Department of Computer Science Engineering*

*Hindu College of Engineering*

*Sonipat, Haryana, India*

*sahilsehrawat934@gmail.com*

**Abstract**：

In today's digital landscape, the protection of networks, resources, and sensitive data from cyber threats is of utmost importance. Intrusion Detection Systems (IDS) play a vital role in ensuring the safety of companies. Numerous methods have been developed and implemented to counter these threats. This research focuses on evaluating the performance of machine learning models, specifically Bi-LSTM models, in creating a reliable intrusion detection system using the UNSW-NB15 dataset. The UNSW-NB15 dataset provides a more up-to-date and accurate representation of modern attacks compared to the NSL-KDD dataset. It includes standardized and preprocessed versions of various network traffic properties, facilitating model training and evaluation. The Bi-LSTM model leverages sequential data and incorporates both forward and backward dependencies to detect and classify intrusions. To assess the model's effectiveness, data scientists utilize a portion of the dataset for training and evaluate its performance on a separate test set. Experimental findings reveal promising results, with the IDS model achieving an accuracy of 96.7%. The proposed method demonstrates accurate intrusion detection through evaluation criteria such as accuracy, recall, and F1-score. These results establish a strong foundation for future research and advancements in network security, aiming to enhance overall network protection and safeguard sensitive information. Moreover, this study contributes to the field of intrusion detection by showcasing the potential of deep learning techniques, particularly Bi-LSTM models, in achieving exceptional accuracy and reliability.

**Keywords:** ML, deep learning, intrusion detection system, Bi-LSTM model, accuracy, reliability

**1. Introduction**

With the rapid development of computer and communication networks, the internet has revolutionized the way people access services worldwide. However, this increased connectivity has also led to a surge in cyberattacks, posing significant threats to information security and property safety. While firewalls serve as a basic security measure, they are insufficient for high-security environments such as government and military sectors.To address these challenges, researchers have proposed the adoption of IDS as a proactive approach to swiftly identify and respond to anomalous network activities[1,2]. IDS monitors and analyzes traffic data within computer systems, detecting known threats and malicious activities and generating alerts when suspicious behavior is detected.

Two essential techniques for observing pernicious exercises are mark based discovery and irregularity based location. Signature-based discovery thinks about network traffic against known attack marks, while inconsistency put together identification depends with respect to laying out examples of typical way of behaving and hailing deviations from these examples as expected dangers.

Lately, the blend of IDS and AI (ML) strategies has shown promising outcomes in really distinguishing network attacks. Analysts have investigated different ML algorithms, including credulous Bayes, choice trees, support vector machines (SVM), hereditary algorithms, random forest models, and k-closest neighbor (KNN) classifiers, to improve the exactness of network attack ID.

In any case, conventional ML approaches frequently require broad component designing and may have restrictions in catching complex examples and profound level conditions in network traffic data[3]. To conquer these constraints, there is a developing interest in utilizing profound learning methods. Profound learning models, for example, profound conviction networks (DBNs), convolutional brain networks (CNNs), and repetitive brain networks (RNNs), have shown guarantee in straightforwardly handling network traffic information and consequently learning many-sided features, bypassing the requirement for manual component designing.

By embracing the capability of profound learning and its capacity to deal with complex network information, specialists expect to work on the precision and effectiveness of IDS, at last fortifying data security and safeguarding against developing digital dangers.

**2. Literature Review**

ML algorithms have exhibited promising abilities in distinguishing strange and pernicious way of behaving in IoT networks. Different examinations have investigated abnormality location and interruption recognition in IoT conditions.

**Pahl et al.** [4] fostered a finder and firewall for IoT microservices irregularities in an IoT site. Liu et al. [5] proposed a finder for On and Off-attacks by malevolent network hubs in modern IoT destinations. [6] presented an interruption discovery framework for IoT, using ML classifiers to recognize network investigation overviews and Disavowal of Administration (DoS) attacks.

**Ukil et al**. [7] zeroed in on peculiarity recognition in IoT-based medical care examination, including heart anomaly discovery through cell phones. Pajouh et al. [8] introduced an interruption discovery model in light of aspect decrease and classification modules, focusing on Client to Root (U2R) and Remote to Neighborhood (R2L) attacks.

**Alrashdi et al.** [9] planned a peculiarity recognition IDS for Brilliant urban communities, accomplishing a high exactness rate utilizing the Random Forest (RF) classifier. Bakhtiar et al. [10] applied the J48 algorithm for interruption location, explicitly distinguishing disavowal of administration attacks.

A few examinations have used CNN, LSTM, and half breed strategies for peculiarity recognition in IoT networks [11, 12]. **Monika et al.** [13] joined CNN and LSTM for digital attack identification in IoT foundation. **Diro et al.** [14] directed a similar report among profound and shallow brain networks, accomplishing high exactness in distinguishing four classes of attacks. [15] presented the Thick Random Brain Network (DRNN) technique for recognizing security weaknesses in a savvy home framework, zeroing in on disavowal of-administration and refusal of rest attacks in a straightforward IoT site.

 **Jiadong et al.** [16] proposed a staggered random forest model to distinguish unusual network conduct, utilizing the force of AI.

**Torres et al.** [17] presented the utilization of intermittent brain networks (RNN) for Botnet oddity identification, zeroing in on the examination of timing features to work on the precision of classification.

**Wang et al**. [19] used convolutional brain networks (CNN) to recognize network traffic information. They handled the information into the type of pictures, bridling the capacities of profound learning in catching complex examples.

**Zhao et al.** [18] introduced a model construction in view of profound conviction networks (DBN) and probabilistic brain networks (PNN) to decrease the dimensionality of the information utilizing DBN and classify the information utilizing CNN. This approach intended to improve the effectiveness and precision of the location cycle.

**Su et al.** [20] proposed a model in view of the blend of CNN and LSTM networks. This mixture model expected to distinguish each attack type in the network by utilizing the qualities of both profound learning structures.

These examinations feature the different utilizations of AI and profound learning algorithms, like random forest, RNN, CNN, DBN, and PNN, in identifying oddities and interruptions in various network conditions. These methodologies add to upgrading the precision and adequacy of interruption identification frameworks by utilizing the force of cutting edge information investigation and example acknowledgment strategies.

**3.Methodology and Dataset used**

**3.1 Dataset**

The UNSW-NB15 dataset is an exhaustive assortment of organization traffic information that incorporates different classifications of typical exercises and engineered attack ways of behaving. This dataset was created utilizing the IXIA Powerful coincidence apparatus in the Digital Reach Lab of the Australian Place for Network safety (ACCS). It joins genuine present day typical exercises with manufactured contemporary attack ways of behaving to give a sensible portrayal of organization traffic.

Here are a few vital insights regarding the UNSW-NB15 dataset:

- Absolute number of records: 2,540,044

- Number of records in the training set: 175,341

- Number of records in the testing set: 82,332

- Number of features: 49

- Reaction features: The dataset incorporates two principal reaction features, specifically "attack\_class" and "label"

 - Attack class: The dataset comprises of nine sorts of attacks, including Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms.

 - Label: The label demonstrates whether a particular organization movement is sorted as an attack or typical way of behaving.

 **Fig 1:** Representation of distribution of Attack class **Fig 2:** Representation of Label

The UNSW-NB15 dataset contains a total of 49 features that provide detailed information about the network traffic data. These features capture various aspects of network communication and can be used to analyze and classify different types of activities.

**3.2 Result and discussion :-**

**Algorithm :-**

*1. Import the necessary libraries: pandas, numpy, sklearn, keras, imblearn, and matplotlib.*

*2. Load the dataset from the "ids.csv" file into a pandas DataFrame.*

*3. Drop unnecessary columns from the dataset.*

*4. Encode the categorical labels into numerical labels using LabelEncoder.*

*5. Normalize the input features using StandardScaler.*

*6. Part the dataset into preparing and testing sets utilizing train\_test\_split.*

*7. Apply SMOTE to adjust the classes in the preparation set.*

*8. Reshape the preparation and testing information to fit the LSTM model.*

*9. Define the LSTM model using the Sequential API in Keras.*

*10. Compile the model with binary\_crossentropy loss and adam optimizer.*

*11. Fit the model on the balanced training data.*

*12. Assess the model on the testing information and print the exactness.*

*13. Predict the labels for the testing data and convert them to binary values.*

*14. Calculate and print the confusion matrix, classification report, precision, and F1-score.*

*15. Plot the training and val. accuracy curves.*

*16. Plot the training and val. loss curves.*

The algorithm utilizes the LSTM model to train and predict on the network traffic dataset, with SMOTE applied to address class imbalance. It also includes evaluation metrics and visualizations to assess the model's performance.

In this review, we proposed a profound learning-based approach utilizing Bidirectional LSTM networks for the recognition of unusual organization exercises in an online protection setting. The goal was to accurately classify network traffic data into normal and attack categories.

LSTM networks are a kind of recurrent neural organization (RNN) that can really catch successive data and conditions in time series information. Bidirectional LSTM expands the LSTM engineering by handling the information in both forward and in reverse bearings, permitting the model to catch past and future setting all the while.

**3.3 Methodology:**

The experimental setup involved preprocessing the dataset by dropping unnecessary columns and converting categorical labels into numerical representations. The input features were then standardized using the StandardScaler, ensuring the compatibility of the data for training the LSTM model. The dataset was parted into preparing and testing sets, with the preparation set additionally adjusted SMOTE to address class irregularity issues.The LSTM model was developed utilizing the Keras library, involving different Bidirectional LSTM layers with changing quantities of units. Dropout layers were consolidated to forestall overfitting. The model was ordered with double cross-entropy misfortune and streamlined utilizing the Adam enhancer. Preparing was performed for 30 epoch with a cluster size of 32, and the model's presentation was assessed on the approval set.

**4 Results and Findings :\_**

The proposed approach achieved an impressive accuracy of 96.7% on the testing set, indicating its ability to effectively distinguish between normal and abnormal network activities. Furthermore, the recall and precision values obtained were 0.97, highlighting the model's capability to correctly identify true positive instances while minimizing false positives.fig3 and 4 shows model loss and accuracy.



 **Fig 3** Shows Model accuracy **Fig 4** Shows loss in Model

**4.1 Evaluation Metrics:-**

To gain deeper insights into the model's performance, several evaluation metrics were computed. The confusion matrix provided a comprehensive overview of the classification results, demonstrating the quantity of genuine positive, genuine negative, misleading positive, and bogus negative forecasts. The order report additionally summed up the accuracy, review, F1-score, and backing for each class. The accuracy worth of 0.97 demonstrates a high extent of accurately ordered positive examples, while the review worth of 0.97 shows the model's capacity to recognize a huge extent of genuine positive occurrences precisely. These outcomes show the viability of the proposed approach in precisely distinguishing unusual organization activities, making it a valuable tool for cybersecurity applications. Table1 shows classification report and fig 4 shows confusion matrix.



**Table1.** shows report of classification



**Fig4** shows confusion matric

**5 Conclusion**

This study focused on using deep learning techniques to detect anomalous behaviors in IoT networks, specifically using the UNSW-NB15 dataset. By employing LSTM and Bidirectional LSTM models, we achieved impressive results with an accuracy rate of 96.7%, indicating the effectiveness of our approach. The recall and precision values of 0.97 further highlighted the model's ability to correctly classify instances and minimize false positives. The utilization of the diverse UNSW-NB15 dataset provided a realistic representation of IoT network traffic. These findings contribute to the field of IoT security by showcasing the efficacy of deep learning models in detecting anomalies and highlighting their potential for developing robust intrusion detection systems in IoT environments.

**REFERENCES：**

1. Patel, A.; Qassim, Q.; Wills, C. A survey of intrusion detection and prevention systems. Inf. Manag. Comput. Secur. 2010, 18, 277–290. [[CrossRef](http://doi.org/10.1108/09685221011079199)]
2. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges.Cybersecurity 2019, 2, 20. [[CrossRef](http://doi.org/10.1186/s42400-019-0038-7)]
3. Yuan, L.; Chen, H.; Mai, J.; Chuah, C.N.; Su, Z.; Mohapatra, P. Fireman: A toolkit for firewall modeling and analysis. In Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P’06), Berkeley/Oakland, CA, USA, 21–24 May 2006; IEEE: Manhattan, NY, USA, 2006; pp. 15–213.
4. M.-O. Pahl , F.-X. Aubet , All eyes on you: distributed multi-dimensional IoT microservice anomalydetection, in: Proceedings of the 2018 Fourteenth International Conference on Network and Service Management (CNSM)(CNSM 2018), 2018 . Rome, Italy
5. X. Liu , Y. Liu , A. Liu , L.T. Yang , Defending on– offattacks using light probing messages in smart sensors for industrial communication systems, IEEE Trans. Ind. Inf. 14 (9) (2018) 3801–3811 .
6. E. Anthi, L. Williams, P. Burnap, Pulse: an adaptive intrusion detection for the internet of things (2018).
7. Ukil , S. Bandyoapdhyay , C. Puri , A. Pal , Iot healthcare analytics: The importance of anomaly detection, in: Proceedings of the 2016 IEEE 30th
8. H.H. Pajouh , R. Javidan , R. Khayami , D. Ali , K.-K.R. Choo , A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks, IEEE Trans. Emerg. Top. Comput. (2016) .
9. Alrashdi, I., Alqa zzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming , H. (2019 , January). AD-loT: anomaly detect ion of loT cyberattacks in smart city using machine learning. In 2019 IEEE 9th Annual Computing and Communication Work shop and Conference (CCWC) (pp. 0305-0310). IEEE.
10. Bakhtiar, F. A., Pramukantoro, E. S., & Nihri , H. (2019, March). A Lightweight IDS Based on J48 Algorithm for Detecting DoS Attacks on loT Middleware. In 2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech) (pp. 41-42). IEEE .
11. A .A . Diro , N. Chilamkurti , Distributed attack detection scheme using deep learning approach for internet of things, Future Gen. Comput. Syst. 82 (2018) 761–768 .
12. O. Brun , Y. Yin , E. Gelenbe , Y.M. Kadioglu , J. Augusto-Gonzalez , M. Ramos , Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments, in: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Recent Cybersecurity Re- search in Europe. Lecture Notes CCIS, in: 821, 2018 .
13. Yanmiao Li, Yingying Xu, Zhi Liu, Haixia Hou, Yushuo Zheng, Yang Xin, Yuefeng Zhao, Lizhen Cui, Robust detection for network intrusion of industrial IoT based on multi-CNN fusion, Measurement, Volume 154, 2020, 107450, ISSN 0263-2241,
14. D. Wu, Z. Jiang, X. Xie, X. Wei, W. Yu and R. Li, " LSTM Learning With Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5244-5253, Aug. 2020, doi: 10.1109/TII.2019.2952917
15. M. Roopak, G. Yun Tian and J. Chambers, " Deep Learning Models for Cyber Security in IoT Networks," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0452- 0457, doi: 10.1109/CCWC.2019.8666588.
16. Jiadong, R.; Xinqian, L.; Qian, W.; Haitao, H.; Xiaolin, Z. A multi-level intrusion detection method based on KNN outlier detection and random forests. J. Comput. Res. Dev. 2019, 56, 566.
17. Torres, P.; Catania, C.; Garcia, S.; Garino, C.G. An analysis of recurrent neural networks for botnet detection behavior. In Proceedings of the 2016 IEEE Biennial Congress of Argentina (ARGENCON), Buenos Aires, Argentina, 15–17 June 2016; IEEE: Manhattan, NY, USA, 2016; pp. 1–6.
18. Zhao, G.; Zhang, C.; Zheng, L. Intrusion detection using deep belief network and probabilistic neural network. In Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 21–24 July 2017; IEEE: Manhattan, NY, USA, 2017; Volume 1, pp. 639–642.
19. Wang, W.; Zhu, M.; Zeng, X.; Ye, X.; Sheng, Y. Malware traffic classification using convolutional neural network for representation learning. In Proceedings of the 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 11–13 January 2017; IEEE: Manhattan, NY, USA, 2017; pp. 712–717.
20. Su, T.; Sun, H.; Zhu, J.; Wang, S.; Li, Y. BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset.IEEE Access 2020, 8, 29575–29585. [[CrossRef](http://doi.org/10.1109/ACCESS.2020.2972627)]