International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 11 | November - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Network Attack Detection Using Long-Short Term Memory (LSTM)

Dhawal Tiwari[#1]
CSE
Chandigarh University
Punjab, India
20BCS7440@cuchd.in

Isha Paul[#2]
CSE
Chandigarh University
Punjab, India
20BCS7432@cuchd.in

Hemant Kashyap[#3]
CSE
Chandigarh University
Punjab, India
20BCS7412@cuchd.in

Vagesh Kumar[#4]
CSE
Chandigarh University
Punjab, India
20BCS7522@cuchd.in

Syad Abdul Safi[#5]
CSE
Chandigarh University
Punjab, India
20BCS2132@cuchd.in

Jyoti Chandel
Chandigarh University
Punjab, India
jyotichandel279@gmail.com

Abstract-

In an age of sophisticated cyber threats, the need for a good network intrusion detection system is crucial. This research aims to push the boundaries of cyber attack detection by leveraging the power of short term memory (LSTM) neural networks in the context of deep learning. The focus here is on different types of classification that solve the difficult task of classifying different types of cyber attacks . This approach goes beyond traditional binary classification and can be adapted to the nuances of cyberattacks. LSTM- based models that use realtime predictions on network traffic data show significant improvements in accuracy and adaptability. We conducted extensive testing to finetune the hyperparameters, adjust the data before the procedure, and improve the model design. The results demonstrate the effectiveness of this approach in classifying cyber attacks and minimizing the possibility of vulnerability.

This research contributes to the continuous improvement of network intrusion detection by combining the power of LSTM based deep learning models with integrated processing. It shows that different types of classification are possible using LSTM for cyber attack detection and paves the way for further developments in the field of cyber security.

Keywords:Multivariate classification, network attack detection, LSTM, deep learning, network penetration detection, network security, time dependency, accuracy, adaptability, data sheet preprocessing technology, model architecture, fake quality.

1.INTRODUCTION

In the rapidly evolving network, connectivity between devices and services is increasing in unprecedented ways. But this widespread connection is still subject to vulnerabilities, resulting in a constant stream of cyberattacks.These threats range from traditional attacks to extreme cyber attacks and challenge the security and integrity of today's data. Therefore, the development of strong power in network intrusion detection system (NIDS) has become an important concern in network security.

The NIDS approach has become an important part of the transition from rule-based methods to machine learning-based problem solving, with a particular emphasis on deep learning.In this paradigm, short-term memory (LSTM) neural networks have emerged as a unique approach. This change reflects the expansion seen in field of cybersecurity, where traditional signature-based technologies are being strengthened or even replaced with a flexible and data-driven approach.

This study is inspired by effective studies in cyber attack detection and aims to increase the effectiveness of NIDS.

Early research on deep learning demonstrates the potential of deep autoencoders and deep belief networks (DBNs) at NIDS , further facilitating the transition to machine learning techniques.

The current threat landscape reflects the need for a more resilient and flexible approach to cyber attack detection, as demonstrated by extensive research in the field. With the development of various types of attacks, the classification of various types of attacks has become an important method to adapt to the classification of various types of attacks.

To address this change, we present a new method to classify multiple classes of cyberattacks using the power of LSTMs in the context of general deep learning. Our approach goes beyond traditional binary classification to provide robust and flexible solutions based on dynamic environments.

In this research work, we aim to promote the integration of knowledge in the field to solve various problems caused by cyber attacks while using the capabilities of LSTM-based learning. vacuum example. We seek to validate our approach through rigorous testing and analysis and contribute to the ongoing debate on the evolution of NIDS.

This study reveals the potential of LSTM-based multi-class classification in network attack detection and proposes a more robust and adaptable network security solution.

2.RELATED WORK

Cyber attack In recent years, the cybersecurity community has noticed the inconsistency of deep learning models, especially those using short-term memory (LSTM) neural networks. These innovations not only expand the horizons of cyber attack detection, butal so redefine the ability to protect sensitive information.

The overview in this section illustrates the unusual history of network attack research, highlighting the important role played by deep learning and LSTM in improving network security. It is important to recognize the sea change in thinking that deep learning has brought about. Gone are the days of relying solely on rules- or signature-based systems, which often have difficulty adapting to the changing strategies of cyber adversaries.

Deep learning models highlight flexibility, sophistication and automation in cyber attack detection. Their innate ability to autonomously resolve complex patterns and anomalies in large data sets overcomes the limitations of traditional methods. Known especially for their ability to capture timely and complex data, LSTM networks have become a beacon of hope in the ongoing fight against threats for the first time today.

This review is an intellectual journey through the history of cybersecurity, where the combination of deep learning and LSTM has not only transformed our approach but also raised the bar in terms of analysis accuracy, scalability, and robustness. This is a testament to the dissatisfaction of cybersecurity experts and international researchers who recognizethat innovation is not just an option but a necessity in the face of powerful and changing threats.

2.1 Network Attack Detection

Traditional cyber attack detection methods have long reliedon formal protocols and signature procedures [1]. The detection process in these systems is based on defined rulesand patterns to detect known attacks. While effective against such threats, these methods often face significant limitations in the face of evolving cyber attacks.

Signature-based detection works by comparing network packets identifying signatures or known attack patterns. While this approach can detect plausible threats, it doesn't work well when attackers use new technologies or modifications to existing attacks. Such zero-day threats often do not have a prior signature, making signature-based

techniques unable to detect them effectively. Rules-based law, on the other hand, relies on predetermined criteria to identify certain patterns or behaviors that indicate terrorism. These policies are often developed by cybersecurity experts based on information about known attacks. While rule-based methods provide flexibility in creating custom search methods, they can produce negative or undetectable results due to their static nature.

Recent advances in cyber attack detection have shifted the focus to a more flexible and data-driven approach, particularly the detection of anomalies. Anomaly detection aims to identify differences in the structure of network behavior [1]. This approach recognizes that the online environment is dynamic, with traffic patterns, application usage, and user behavior changing over time.

Fault detection models, often using machine learning algorithms, learn to recognize underlying network behaviour and provide alerts when deviations from the threshold are detected. Unlike official or legal signatures, vulnerability detection has the ability to identify new and previously unseen attacks. By learning and adapting to changes in the network, these models provide flexibility and adaptability to access, making them crucial in modern network security.

2.2 Deep Learning In Network Security

The integration of deep learning models has changed the landscape of cybersecurity [1]. Deep learning is a branch of machine learning that has gained attention for its ability to extract complex features from data. Deep neural networks, in particular, show promise in many security applications, including network access.

The foundational work of [1] is an important foundation for realizing the potential of deep learning in network intrusion detection. Deep neural networks are capable of capturing complex and abstract patterns in large data sets, making them effective in analyzing existing and non-linear relationships in network traffic data.

One of the defining characteristics of deep learning models is their ability to process high-dimensional data (such as web data) without requiring manual effort [1]. Unlike traditional machine learning methods that rely heavily on experts to generate relevant features from raw data, deep learning models can uncover complex patterns and trends directly from raw data. This autonomous feature extraction speeds up model development and allows these models to discover subtle relationships and features that might otherwise escape manual feature engineering, making them particularly effective in the field of dynamic cyberattack detection.

Deep learning models, on the other hand, learn hierarchical representation directly from data. They adapt and evolve as they encounter new trends, so they can detect previously unknown threats. This change is especially important in network intrusion detection, as attackers continue to innovate and diversify their strategies.

Additionally, deep learning models show promise in solving problems posed by network access. As encryption becomes more widespread, the ability to inspect encrypted traffic for malicious purposes becomes more difficult. Deep learning models can learn patterns in encrypted data without needing to access decryption keys, providing a solution to this new challenge.

2.3 LSTM in Network Traffic Analysis

Short-term memory (LSTM) neural networks have become powerful tools for capturing time-dependent data sequences, making them meaningful in network traffic analysis [4]. In the context of deep learning, LSTMs belong to the family of neural networks (RNNs) designed to model and remember long-term data connections.

Researchers[4] have conducted research that has helped improve our understanding and use of LSTM architectures. LSTM has the unique ability to capture relationships and dependencies in data networks, making it suitable for analyzing network traffic data where events are frequently revealed.

The time dimension plays an important role when analyzing network access. Attacks can manifest as a series of events that evolve or exhibit non-linear behavior. LSTMs are good at capturing physical patterns, allowing them to describe complex situations that traditional models would ignore.The random nature of LSTMs allows them to preserve memories of past events, making them ideal for tasks where context and history are important. In network analysis, this means being able to identify behaviors that evolve over time, such as the detection and propagation of specific attacks.

LSTM is good at processing continuous events present in network traffic data, providing time-varying transformations and the ability to extract important patterns [4]. Unlike temporal models, which would struggle with randomness, LSTMs can evolve over time and detect underlying patterns. This change is especially useful when events occur regularly and indicates significant changes for accurate analysis.

Additionally, LSTM is robust to noisy data; This makes it useful in real-world networks where data may be incomplete or contain errors. Their ability to model long-term expectations allows them to capture relationships between network events despite noise and uncertainty.

2.4 Multiclass Classification in Network Security

In order to classify different attack types, different attack types in the network need to be transformed into different classification classes [3]. The traditional binary classification of classifying network traffic as “normal” or “malicious” often fails to meet most of today's threat scenarios.

Multi-class classification extends the classification process to accommodate multiple classes of attacks, allowing Network Intrusion Detection Systems (NIDS) to analyze network traffic for a variety of threats. This approach is based on a changing threat landscape that includes a variety of attacks and countermeasures.

The combination of multiple classes allows NIDS to effectively distinguish between different attack types. For example, it can range from Distributed Denial of Service (DDoS) attacks, intrusion attempts, data deletion, and other specialized attacks. These features improve the accuracy and adaptability of intrusion detection tools, allowing them to respond more effectively to different threats.

Machine learning algorithms, especially deep learning models, have shown their promise in the field of various types of distributed network security [3]. These models learn complex patterns that indicate different types of attacks, allowing them to accurately classify attacks into different groups. The ability to distinguish between different types of attacks allows organizations to respond quickly and effectively to changing threats, increasing their overall security.

In summary, multiclassification represents a significant advance in the field of cybersecurity and provides the opportunity to improve the accuracy and adaptability of NIDS. Various classification types distinguish attack types, allowing NIDS to provide greater protection and effectiveness against a variety of network threats. This change is critical in today's cybersecurity environment, where attackers continue to innovate and diversify their strategies.

2.5 Recent Advances in Network Intrusion Detection

Recent network infiltration detection has made significant progress in using deep learning techniques to improve security [5]. These studies demonstrate the feasibility and effectiveness of deep learning models in identifying and mitigating cyber threats.

Researchers[5] proposed a deep learning-based intrusion detection system that combines autoencoders and deep neural networks to detect anomalies in network connections. Their approach focuses on capturing subtle changes in normal behavior, making it especially useful for new and unseen attacks. Integration of deep learning allows systems to adapt and evolve in response to emerging threats.

This research[6] solves certain problems of Software-Defined Networking (SDN) environment by introducing different types of access detection based on deep learning. SDN architecture brings a new change in network traffic management and special techniques are required to analyze it. Their research demonstrates the evolution of deep learning in adapting to specialized network infrastructures.

Researchers [7] studied the application of LSTM networks in industry 4.0 environments by addressing specific problems in the IoT environment. Their work demonstrates the effectiveness of LSTM models in capturing the real-time dynamics of different environments, including features of Internet of Things (IoT) technology. This change extends the usefulness of LSTM-based access detection beyond the network environment.

Recent advances demonstrate the amazing nature of network intrusion detection and demonstrate the potential of deep learning and LSTM models to improve security in various network environments. The flexibility and adaptability of these models make them useful in the ongoing fight against evolving cyber threats.

In summary, this literature review demonstrates the advancement of deep learning, and specifically short-term temporal (LSTM) neural networks, in intrusion detection and intrusion prevention. We have seen how these advanced techniques overcome the limitations of traditional techniques, automatically extract features, adapt to adaptive attack strategies, and have strong time adaptability. The connection between cognitive science and information studies demonstrates the important role that deep learning and LSTM play in improving cybersecurity. As we grapple with the changing cyber threat landscape, the insights gained here pave the way for the development of strategic intelligence that will help us protect the world's critical cyber infrastructure.

3.PROPOSED WORK

3.1 Data Collection and Preprocessing

3.1.1 Dataset Description

In this section, we will give general explanations about the data used in our study. These data form the basis for training and evaluating LSTM-based deep learning models for network attack detection. It is important to understand the origin of data sets, their characteristics, and their relevance to research purposes.

The data used in our study was taken from Kaggle. Contains samples of network traffic data collected during the data collection period for 2019. This data is particularly useful because it represents network performance quite well, including both normal and abnormal traffic patterns.

Additionally, important characteristics of the data should also be addressed, such as what important features of the data are (e.g., network data packets, IP addresses, time records) and what unexpected problems might occur in the classroom. Addressing the issue of class ambiguity is a critical first step to ensure that our model can identify different attack types.

3.1.2 Data Preprocessing Techniques

The quality and completeness of the dataset plays an important role in the success of our cyber attack detection model. Therefore, pre-processing information is used to prepare the information for modeling.

Data preprocessing consists of several simple steps, including data cleaning, standardization, and handling of missing values. Data cleaning involves removing duplicates and outliers that may add noise to the sample. Normalization normalizes feature scales to ensure that no feature has an impact on the learning model.

Addressing missing expenses is another important part of the preliminary information. Missing data can affect the training model, and various strategies can be used to address this problem, such as imputation procedures or removal of missing cases.

Additionally, feature engineering can be used to extract relevant information from raw data to create input points for models. This may include techniques such as dimensionality reduction or the creation of features that capture specific aspects of network behavior.In general, preprocessing steps are important to ensure that the data input into the LSTM-based deep learning model is good, well-structured, and free of inconsistencies that may affect performance standards. The success of our network against attacks depends on the effectiveness of preprocessing, which forms the basis for training and evaluation of the next model.

3.2 LSTM-based Deep Learning Model

3.2.1 Architecture of the LSTM Mode

In this section, we examine the architecture of the Short-Term Memory (LSTM) model for cyber attack detection. The LSTM architecture is central to our research because it forms the basis of our deep learning method for capturing temporal and structural dependencies in network traffic data.

An LSTM model consists of several layers, each containing a network of LSTM units. The selection of the number of layers and the number of LSTM units in each layer is an important part of the design. This allows the model to capture both short-term and long-term dependency in traffic networks. The input to the LSTM model consists of a set of features of the network, where each time step represents a vector of data. The nature of the data fits perfectly with the power of LSTMs, which can remember data from previous steps and use it to estimate the current time.

Additionally, we describe specific modifications or enhancements made to adapt the standard LSTM architecture to the unique characteristics of network traffic data. For example, we may use techniques such as dropout or recursive processing to avoid overprocessing, or we may provide additional techniques (such as convolution techniques) to capture spatial patterns in the data.

The architecture section also includes performance optimizations, performance loss fixes for different deployment types, and optimizations used during training. These choices are important to ensure that the LSTM model effectively learns the difference between network behavior and different types of attacks.

3.2.2 Hyperparameter Tuning

The architecture section also includes performance optimizations, performance loss fixes for different deployment types, and optimizations used during training. These choices are important to ensure that the LSTM model effectively learns the difference between network behavior and different types of attacks.

We describe performance hyperparameters, which may include learning rate, batch size, number of sessions, and process orchestration. Selecting appropriate hyperparameters can affect the convergence, generalizability, and validity of the model.

The tuning process can be guided by grid search, random search, or Bayesian optimization, depending on the size of the hyperparameter space and the availability of computational resources. We explain the rationale behind choosing the hyperparameter transformation method and provide insight into the dimensions of the search space.

Additionally, we discuss how to use cross-validation methods to evaluate model performance under different hyperparameter configurations. Cross-validation helps ensure that our model performs well and does not depend on specific hyperparameter settings.

3.3 Multiclass Classification

3.3.1 Class Labels and Attack Types

In this section, we will examine the complexity of class lists and attack types in the context of multi-class classification for network discovery. Category articles play an important role in defining the sources and goals of our work.

The category label indicates categories that sample traffic on the network. It is necessary to give a general definition of these lists, explain how they are defined, their working criteria, the relationship between the lists and the types of cyber attacks.

Attack mode is an important part of our various classification systems. We list and describe the different types of attacks that our model is designed to detect. Each type of attack should be clearly defined, along with its characteristics and potential impact on network security. Deployment may involve attacks such as distributed denial of service (DDoS), intrusion attempts, malware, and other threats.

We also talk about all the difficulties or nuances associated with the distribution of traffic in the network to such attacks. This may include issues with class disparity, where certain types of attacks are not listed in the literature, or where obscure cases may have more than one class.

We also emphasize the importance of distributing network traffic in such attacks. Effective deployment increases network

security by allowing network administrators to quickly identify and respond to specific threats.

3.3.2 Evaluation Metrics

In the evaluation section, we discuss the criteria and metrics used to evaluate the performance of different classification models. The choice of metric is important to evaluate the effectiveness of the model in distinguishing between different attack types and network behaviors.

Common evaluation metrics for multiple classifications include accuracy, precision, recall, F1 score, and confusion matrix. It is necessary to explain the importance of each indicator and how it is calculated in the context of our study.

Accuracy measures the overall accuracy of our model's predictions across all categories. However, in the case of unequal class distribution, facts alone will not provide a complete picture. Precision, recall, and F1 scores provide further insight by identifying the strengths, weaknesses, and weaknesses of each category. These metrics help us evaluate the model's ability to accurately identify specific attack types while minimizing false positives.

We also discussed the importance of confusion matrices in visualizing model performance. These matrices provide insight into the model's ability to distinguish between different attack types and common links, revealing potential areas for improvement.

Additionally, we address any trade-offs or issues involved in optimizing multi model classification models. Balancing precision and recall is an important consideration, especially when the data is not balanced. We may also explore strategies such as class weighting or sampling to reduce class size and improve performance standards of small classes.

In summary, the class list and attack type, as well as the evaluation criteria, were chosen as the basis for evaluating the performance of our various classifications in the study. Clear definitions, meaningful measurements, and an understanding of real-world impact are critical in evaluating a model's ability to improve cybersecurity.

4.Experimental Setup

4.1 Dataset Selection

Selecting the right data is an important decision in any experimental research, especially in the context of DDoS attack detection using the LSTM model. In our research, we carefully select the CIC-DDoS2019 dataset for several reasons.

The CIC-DDoS2019 database is known for representing network traffic events and is suitable for our research purposes. It has many scenarios that cover a wide range of activities, from benign network traffic to various types of DDoS attacks. This distinction is useful because it allows us to test the model's ability to distinguish between good and bad traffic patterns.

Additionally, these data represent different types of DDoS attacks, such as UDP reflection, SYN flood, and HTTP flood, providing a realistic and challenging test for our LSTM DDoS detection model. These attacks represent different ideas and features, making them suitable for evaluating the model's ability to identify and classify different types of attacks.

This file is equipped with basic tools such as packet features, network analysis and time features, which are important in the training and testing phase. Special techniques are used to prepare the data to ensure that the LSTM model can capture typical patterns of DDoS attacks.

In summary, CIC-DDoS2019 data forms the basis of our research and provides different information that provides accurate and useful information for the LSTM-based DDoS detection models developed and evaluated. Selecting this information allows us to conduct successful experiments based on the complexity of competition in the cybersecurity world, ultimately increasing the value of our research.

4.2 Feature Extraction

Feature extraction is an important step in our research and plays an important role in planning LSTM-based DDoS attack detection data. Given the complexity of traffic data in the network, video extraction involves the selection and generation of relevant features that best represent the characteristics of the data and enables pattern analysis of DDoS attack patterns.

The CIC-DDoS2019 file provides useful information including packet-level features, traffic analysis, and time details. From this raw data, we extract features that capture the essence of network behavior. These features may include text counts, bytes, data protocols, and real-time measurements.

Feature engineering is done to obtain details of raw data. This may include calculating totals across time windows, generating time statistics, and identifying trends or differences in network connectivity. Special selection procedures were also used to remove irrelevant or redundant features and thus improve the performance of the model.

The purpose of feature extraction is twofold: to reduce the remaining data so that it can be used to check the LSTM model and to highlight relevant patterns in the data. By transforming raw traffic data into detailed traffic data, we enable LSTM models to identify and distinguish between good and bad traffic patterns. Feature extraction ensures that the training and testing phases of the model are performed with relevant data and optimized for accurate DDoS attack detection.

In this section we describe the specific features selected and developed, giving insight into the decisions and processes used to prepare training material, instruction and subsequent assessment.

4.3 Training and Testing Split

Distribution of training and testing data is an important step in our testing setup. It involves splitting the data into two different parts: one for training the LSTM DDoS detection model and the other for evaluating its performance.

To ensure the validity and reliability of the model, we adopt a general approach such as 70%-30% or 80%-20% classification according to the size of the data set. This classification allows us to use most of the data for training models while keeping data separate for demanding testing.

Most importantly, there is no overlap between training and test data to prevent data outliers and ensure that the model can be generalized to unknowns. This configuration also reflects a real-life situation where the model must be accurate on data that has not been encountered before.

Training data is used to train an LSTM model to identify patterns in network traffic data that indicate DDoS attacks. The test data then serves as an independent standard to evaluate the model's performance in distinguishing between normal and negative traffic. By separating the training and testing data, we can make a good evaluation of the performance of the model to ensure that it can be trusted in the real situation as a DDoS attack.

4.4 Software Requirement

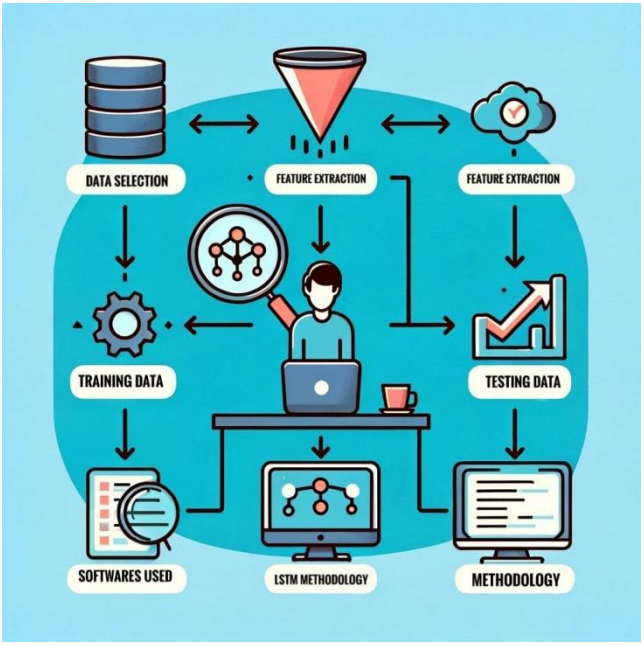
Software Tool Used	Description
Jupyter Noebook	Jupyter Notebook is a web based open-source application that is used for editing, creating, running, and sharing documents that contain live codes, visualisations, text, and equations. There are over 100 kernels other than IPython available for use.
Atom Text Editor	Atom is a text and source code editor which works across all operating systems. It speeds up find and-replace operations by an order of magnitude and improves performance of files .
Visual Studio Code	Visual Studio Code is an open source code editor for the Windows, Mac and Linux operating systems which can be used to write in many programming languages such as Java, JScript, Python, C++, Node.js.

4.5 Evaluation Methodology

The evaluation method aims to evaluate the effectiveness of the LSTM DDoS detection model. Considering the distribution of current attack types in the literature, we use a number of measures suitable for classifying different types. Evaluate model performance using metrics such as accuracy, precision, recall, F1 score, and confusion matrix.

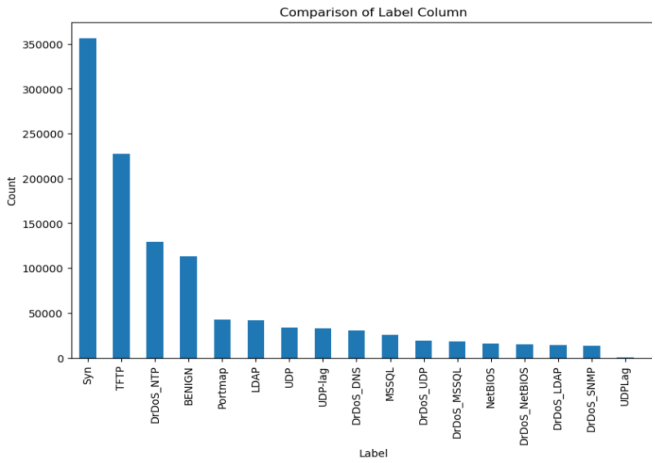
Also, to address possible class biases in the data, we use class weights or weighted scales to ensure equal measurement. We also include all hyperparameter tuning procedures performed to improve model performance.

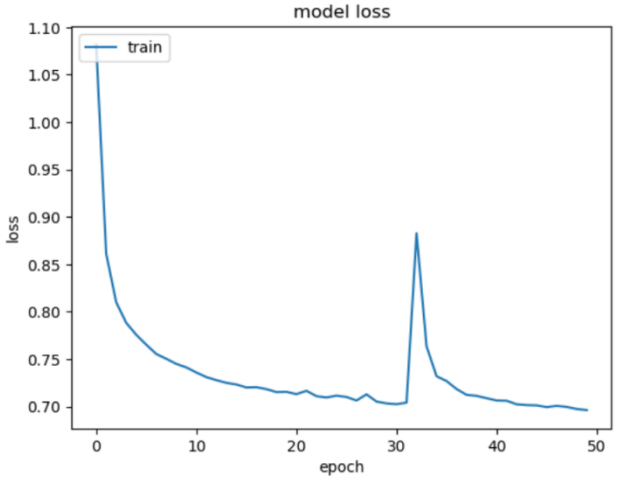
This experimental setup forms the basis of our research to train, test and evaluate LSTM-based DDoS detection models. and a clear framework that allows for an accurate assessment of its potential and effectiveness.



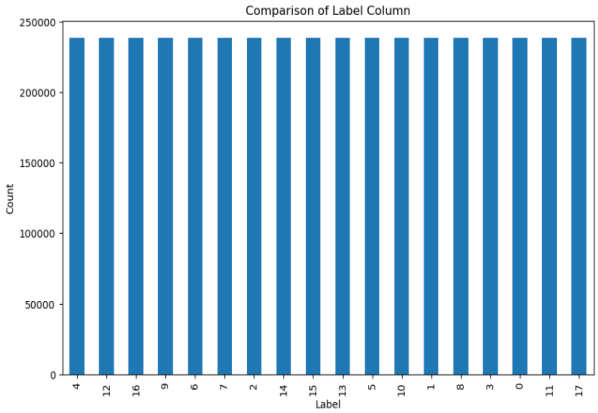
5.Results

5.1Plot of Sample data after loading and labelling the dataset



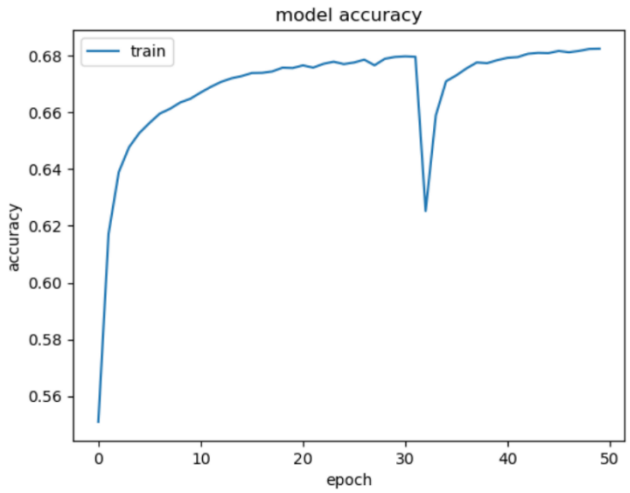


5.2Plot after resampling



5.3Plot after training the dataset

5.3.1 Model Accuracy



5.3.2 Model Loss

5.4 Accuracy and Prediction

```
from sklearn.metrics import accuracy_score
accuracy_score(y_test_label, y_pred_label)
```

```
0.8268255095613953
```

5.5 Classification Report

```
#                precision    recall  f1-score   support

#             0       0.47      0.99      0.64     37272
#             1       0.70      0.34      0.45     10007
#             2       0.00      0.00      0.00      4819
#             3       0.43      0.45      0.44      5937
#             4       0.99      0.97      0.98     42689
#             5       0.59      0.31      0.40      5087
#             6       0.41      0.76      0.53      4498
#             7       0.53      0.27      0.36      6316
#             8       0.00      0.00      0.00     13571
#             9       0.60      0.14      0.22      8315
#            10       0.64      0.11      0.19      5311
#            11       0.74      0.53      0.62     14089
#            12       1.00      0.99      0.99    118000
#            13       0.99      0.99      0.99     75196
#            14       0.67      0.66      0.66     11050
#            15       0.84      0.87      0.86     10910
#            16       0.07      0.84      0.12        25
#            17       0.11      0.96      0.20        23

#     accuracy                           0.83    373115
#    macro avg       0.54      0.57      0.48    373115
# weighted avg       0.82      0.83      0.80    373115
# '
```

6.Conclusion

6.1 Summary Of Research

In this research, we embarked on a journey to improve cyber attack detection using long-term memory (LSTM) models. Our research focuses on using deep learning techniques to combat evolving cyber threats. Thanks to the

preparation of good information, development of prototypes and training of models, we have made significant progress in solving important problems in network security.

Our work began by exploring the CIC-DDoS2019 dataset, a rich source of network traffic data. We performed data preprocessing and feature extraction to transform the raw data into features that could inform our models. By doing this, we lay the foundation for LSTM-based methods for network intrusion detection.

6.2 Contributions

This research contributes to the field of cybersecurity by introducing new forms of LSTM modeling. With an accuracy of approximately 0.8268, our model shows great promise in identifying various types of cyberattacks. This result is an important step to improve network security as it shows that the LSTM model can distinguish between normal and malicious network.

Our work demonstrates the value of deep learning in cybersecurity. LSTM models provide a data-driven approach to threat detection by automating the feature extraction process and using the physical characteristics of data traffic in the network. The model's ability to adapt to different time periods and identify relevant patterns is a useful feature for the field.

6.3 Limitations

Although our study has promising results, we are aware of some limitations. The truth, although important, still leaves room for improvement. Class mismatch in the dataset is problematic and further research is needed to resolve this issue. Additionally, the difference between real-world traffic and the change pattern for emerging threats can be further investigated.

6.4 Future Works

The future has interest in researching cyber attacks. Building from this work as a foundation, future work should focus on improving the LSTM model, exploring data diversity, and solving class-based inequality issues. Additionally, research should continue to evaluate the real-life performance of the model and evaluate the effectiveness of the deployment in network security.

The journey to strengthen cybersecurity continues, and our research is a step towards creating stronger, more effective investigative tools. As cyber threats evolve, so too must our defenses. Our work contributes to this ongoing effort and lays the foundation for further advances in cybersecurity.

REFERENCES

[1] X. Zhang, J. Zhao, X. Le, and Y. Song (2016). A Deep Learning Approach to Network Intrusion Detection

[2] Y. Zhang, M. Zhang, and J. Ding (2018). Deep Learning-Based Network Intrusion Detection: A Comprehensive Review

[3] T. S. Dillon, J. Singh, and M. L. Chiang (2011). Intrusion Detection System: A Comprehensive Review.IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans

[4]A. Graves, S. Fernández, et al.(2013). Long Short-Term Memory Recurrent Neural Network Architectures for Large Scale Acoustic Modeling.IEEE Transactions on Audio, Speech, and Language Processing.

[5] R. Islam, D. Huang, et al. (2017). A Deep Learning Approach for Network Intrusion Detection System.IEEE Transactions on Network Science and Engineering

[6] M. Rehman, I.Yaqoob, et al.(2018). Deep Learning-Based Multiclass Intrusion Detection System in Software Defined Networking.IEEE Transactions on Network Science and Engineering.

[7] M. R. Mukhtar, F. Hu, et al. (2019). LSTM Networks for Intrusion Detection in IoT-Enabled Industry 4.0.IEEE Transactions on Industrial Informatics

[8] Y. Zhang, X. Zhao, and Y. Zheng(2019). A Review on Deep Learning Approaches for Network Intrusion Detection Systems

[9] J. Ren, Y. Zhang, et al. (2020). Deep Learning for Network Intrusion Detection: A Survey.

[10] M. R. Gupta and R. K. Gupta (2015). Network Anomaly Detection Using Recurrent Neural Networks.

[11] Doshi, R., Apthorpe, N., & Feamster, N. (2018). “Machine Learning DDoS Detection for Consumer Internet of Things Devices”. IEEE Security and Privacy Workshops (SPW).

[12] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi and Y. Gulzar (2021), ‘‘Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight’’ Symmetry, vol. 13, no. 2, p. 227.

[13] Saini, P. S., Behal, S., & Bhatia, S (2020). “Detection of DDoS Attacks using Machine Learning Algorithms”. 7th International Conference on Computing for Sustainable Global Development (INDIA.Com).pp;16-21,.

[14] Sharma, M.; Pant, S.; Kumar Sharma, D.; Datta Gupta, K.; Vashishth, V.; Chhabra, A (2020). "Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions." In Transactions on Emerging Telecommunications Technologies; Wiley: Hoboken, NJ, USA; Volume 32, p. e4137.