Chapter 1: INTRODUCTION

Deep learning techniques may automatically extract high-level characteristics from low-level ones, allowing for robust representation and inference. We create a recurrent deep neural network to learn patterns from network traffic sequences and track network assault activities. The experimental findings show that our model performs better than other mechanisms.

One of the primary DDoS protection strategies is DDoS detection[1]. Unfortunately, it is difficult to identify DDoS attacks automatically since attack traffic is often quite similar to normal traffic and attackers attempt to resemble flash mobs. In the early phases, an attack activity with minimal traffic may even be considered lawful [7].

We train our deep learning models with a largescale dataset to solve complicated recognition problems. In the experiments, It leverages different neural network models: Recurrent Neural Network (RNN)[2], Long Short-Term Memory Neural Network (LSTM) [3], and Gated Recurrent Unit Neural Network (GRU) [4]. Bi-directional LSTM and Bi-Directional GRU. These methods are proved to greatly improve the performance in many domains when training large data sets. Deep learning approach is a natural fit for large scale of network traffic. LSTM and GRU can also help us gain context of network packets, especially the long- and short-term patterns in DDoS attack sequences.

The vulnerability to DDoS attacks is exploited in the creation of open, scalable, and autonomous Internet security [8]. DDoS attacks primarily target the host's resources and network capacity. The majority of attacks target protocol and application flaws: SYN flood, UDP flood, ICMP flood, SIP flood, and so on. Certain assaults, such as UDP flood and ICMP flood, drain network bandwidth. Others, such as SYN flood and SIP flood, deplete a victim's system resources (e.g., CPU and memory) as well [14]. By receiving packets over UDP, for example, a victim does not need to handshake. In a UDP flood attack, an attacker sends packets to random or designated ports with the intent of attacking these ports and overloading network resources.

Low-rate attacks are difficult to detect because they resemble actual network activity from the victim's end. Meanwhile, DDoS attacks on victim systems must be generated gradually. Otherwise, it will not be hazardous to network/system resources. This emphasizes the relevance of historical information in DDoS detection. Because of the missing historical pattern in the learning model, the single-packet detection technique is unable to enhance performance.

Our detection method employs a continuous network packet sequence that may learn the minor differences between attack and legal traffic. To detect DDoS attacks, historical data is loaded into an RNN model. It aids in locating recurring patterns of DDoS assaults in a long-term traffic sequence.

Our detection method employs a continuous network packet sequence and is capable of learning the tiny differences between attack and normal traffic. To identify DDoS attacks, historical data is loaded into an RNN model. It aids in identifying recurrent patterns that characterize DDoS assaults and locating them in a long-term traffic sequence.

Another advantage of RNN is its independence from the size of the input window. Previous machine learning algorithms employed task-dependent window sizes. This limits the ability of these approaches to identify various forms of assaults. Therefore, it becomes difficult to train a long-term sequence for traditional machine learning algorithms. Nevertheless, RNN (particularly gated RNN, such as LSTM and GRU) has demonstrated the capacity to tackle these challenges [30].

Chapter 2: LITERATURE SURVEY

In the cybersecurity domain, an Intrusion Detection System (IDS) serves as a clear defense line against cyber adversaries, which is critical for a system. We have gotten dependent on this parallel reality constituted by electronic gadgets as a result of mobile device adoption and the popularity of applications that swiftly complete numerous user activities. Users must be made aware of the consequences of failing to follow secure practices in order to safeguard network infrastructure against intrusion threats. A device is deemed safe if it accomplishes data protection, confidentiality, integrity, and availability.

A deep learning approach that combines the strengths of both convolutional neural networks (CNNs) and long short-term memory (LSTM) networks. The approach involves analyzing the traffic patterns of incoming data packets and using the CNN to extract features, followed by the LSTM to analyze the temporal relationships between the extracted features.

In another experiments, author has proposed method compares two deep learning models: an autoencoder (AE) and a multi-layer perceptron (MLP). The AE is used for unsupervised feature learning to extract meaningful features from network traffic data. The MLP is used as a classifier to distinguish between normal traffic and DDoS attacks based on the learned features. The authors evaluated the performance of the proposed method using the NSL-KDD dataset, and compared it with other state-of-the-art methods. The results showed that the proposed AE-MLP method outperformed other methods in terms of detection accuracy and classification accuracy.

We can also use Machine learning algorithm approach an evolutionary algorithm with a Support Vector Machine (SVM) model to enhance the accuracy of DDoS attack detection in SDNs. The evolutionary algorithm is used to optimize the SVM parameters to improve its performance in detecting DDoS attacks. The SVM model is trained using a set of features extracted from network traffic data, such as packet size, packet rate, and payload size.

A system on various metrics such as accuracy, precision, recall, and F1-score. The results show that the proposed system achieves high accuracy and outperforms existing IDS systems on both datasets. The proposed deep learning-based IDS can effectively detect DoS and DDoS attacks by leveraging protocol-based features from network traffic data.

It also highlights the importance of using publicly available datasets for training and evaluating IDS systems to promote transparency and reproducibility in the field of cybersecurity.

To address this problem, the authors propose[5] a deep learning approach that combines the strengths of both convolutional neural networks (CNNs) and long short-term memory (LSTM) networks. The approach involves analyzing the traffic patterns of incoming data packets and using the CNN to extract features, followed by the LSTM to analyze the temporal relationships between the extracted features.

In this paper[6], author proposed method compares two deep learning models: an autoencoder (AE) and a multi-layer perceptron (MLP). The AE is used for unsupervised feature learning to extract meaningful features from network traffic data. The MLP is used as a classifier to distinguish between normal traffic and DDoS attacks based on the learned features.

The proposed approach[7] an evolutionary algorithm with a Support Vector Machine (SVM) model to enhance the accuracy of DDoS attack detection in SDNs. The SVM model is trained using a set of features extracted from network traffic data. The authors evaluated the performance of the proposed approach using the KDD Cup 1999 dataset, which contains both normal and attack traffic. The results showed that the evolutionary SVM model outperformed methods.

The paper[8] evaluates the performance of the proposed system on various metrics such as accuracy, precision, recall, and F1-score. The results show that the proposed system achieves high accuracy and outperforms existing IDS systems on both datasets. The paper concludes that the proposed deep learning-based IDS can effectively detect DoS and DDoS attacks by leveraging protocol-based features from network traffic data. It also highlights the importance of using publicly available datasets for training and evaluating IDS systems to promote transparency and reproducibility in the field of cybersecurity.

This paper[9] proposes a deep learning-based approach for detecting DDoS attacks using convolutional neural networks (CNNs) with time-frequency representations. The proposed method achieved higher detection rates and lower false positives compared to traditional machine learning-based approaches. The proposed method can handle complex time-frequency patterns in network traffic data. The method may require large amounts of training data and computational resources.

This paper[10] proposes a deep learning framework for detecting DDoS attacks based on traffic behavioral analysis. The proposed method uses an autoencoder to reduce the dimensionality of the input data and a convolutional neural network (CNN) to classify the traffic data. The proposed method can detect new types of attacks that are not included in the training data. The method may require large amounts of training data and may not be effective in detecting low-intensity attacks.

This paper[11] proposes a deep learning-based approach for detecting DDoS attacks using a long short-term memory (LSTM) network. The proposed method achieved high accuracy in detecting various types of DDoS attacks. The proposed method can capture temporal patterns in network traffic data. The method may require large amounts of training data and may not be effective in detecting new types of attacks.

This paper[12] proposes a deep learning-based approach for detecting DDoS attacks based on time series analysis. The proposed method uses a long short-term memory (LSTM) network and achieved high accuracy in detecting different types of DDoS attacks. The proposed method can capture temporal patterns in network traffic data and can handle high-dimensional data. The method may require large amounts of training data and may not be effective in detecting new types of attacks.

This paper[13] proposes a deep learning-based approach for detecting DDoS attacks using SDN and a deep neural network. The proposed method achieved high accuracy in detecting various types of DDoS attacks. The proposed method can handle high-dimensional data and can learn complex patterns in the network traffic. The use of SDN can enhance the scalability of the method. The method may require large amounts of training data and computational resources.

This paper[14] proposes a deep learning-based approach for detecting DDoS attacks using multiple features and a deep neural network. The proposed method achieved high accuracy in detecting various types of DDoS attacks. The proposed method can handle high-dimensional data and can learn complex patterns in the network traffic. The method may require large amounts of training data and computational resources.

This paper[15] proposes a deep learning-based approach for detecting DDoS attacks using adaptive traffic sampling and a convolutional neural network (CNN). The proposed method achieved high accuracy in detecting various types of DDoS attacks. The proposed method can handle high-dimensional data and can learn complex patterns in the network traffic. The use of adaptive traffic sampling can enhance the scalability of the method. The method may require large amounts of training data and computational resources.

This paper[16] proposes a deep learning-based approach for detecting DDoS attacks using feature fusion and attention mechanism and a deep neural network. The proposed method achieved high accuracy in detecting various types of DDoS attacks. The proposed method can handle high-dimensional data and can learn complex patterns in the network traffic. The use of attention mechanism can enhance the interpretability of the method. The method may require large amounts of training data and computational resources.

This paper[17] proposes a hybrid approach for detecting DDoS attacks using deep learning and machine learning techniques. The proposed method achieved high accuracy in detecting various types of DDoS attacks. The proposed method can handle high-dimensional data and can learn complex patterns in the network traffic. The use of machine learning techniques can enhance the efficiency of the method. The method may require large amounts of training data and computational resources. The hybrid approach may require more complex implementation and management compared to a single-model approach.

This paper[18] proposes a deep learning approach for DDoS attack detection using a recurrent neural network (RNN) and long short-term memory (LSTM) network. The proposed method achieved high accuracy in detecting DDoS attacks. The proposed method can handle sequential data and can learn complex patterns in the network traffic. The use of RNN and LSTM can improve the ability of the method to capture long-term

dependencies in the traffic. The method may require large amounts of training data and computational resources.

This paper[19] proposes a deep learning-based approach for detecting DDoS attacks using packet length distribution and a deep neural network. The proposed method achieved high accuracy in detecting various types of DDoS attacks. The proposed method can handle high-dimensional data and can learn complex patterns in the network traffic. The method may require large amounts of training data and computational resources.

This paper[20] proposes a hybrid approach for DDoS attack detection using deep learning and support vector machine (SVM) techniques. The proposed method achieved high accuracy in detecting various types of DDoS attacks. The proposed method combines the strengths of deep learning and SVM techniques for improved accuracy in DDoS attack detection. The method may require large amounts of training data and computational resources.

Chapter 3: METHODOLOGY

In this section, we discuss the proposed Protocol Based RNN model. The process involves features comparison to find similar features in the UNSW-NB15 and the Bot-IoT datasets, features selection, data pre-processing and selection and model training using un-supervised LSTM deep learning model.

A. RNN

Recurrent Neural Network is a type of neural network architecture that is designed to process sequential data, such as time series, speech, and natural language. The main advantage of RNN is that it can capture dependencies between elements in a sequence, which makes it well-suited for tasks that require modeling the temporal behavior of data. The basic architecture of an RNN consists of a set of hidden states, which are updated at each time step based on the input and the previous hidden state. The input at each time step is typically a vector representing the features of the current element in the sequence, and the output is typically a vector representing the predicted value or class.

RNN is well-suited for modeling the temporal behavior of data, and can capture dependencies between elements in a sequence. RNN can be used for a wide range of applications, including natural language processing, speech recognition, and time series prediction. RNN can be trained end-to-end, which means that the entire network can be trained simultaneously rather than in separate stages.

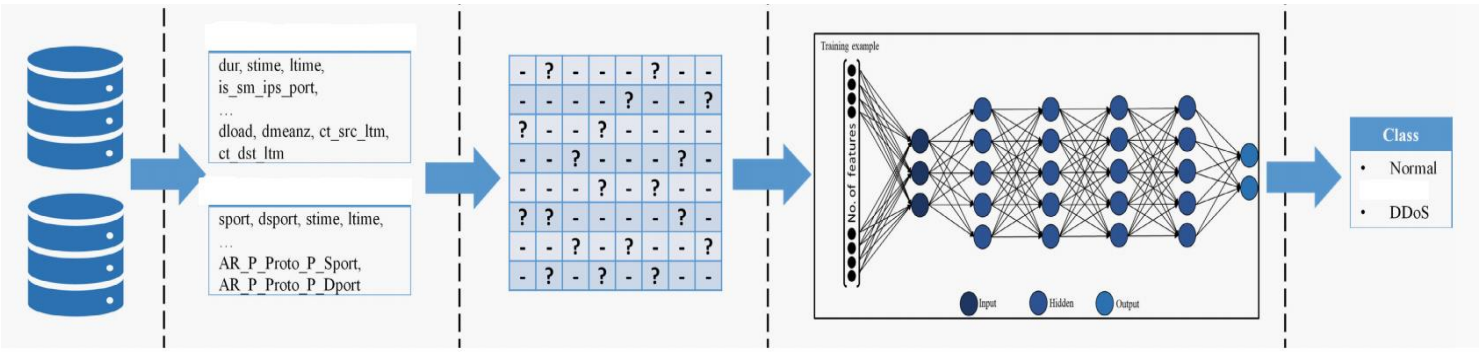


Fig 1: Architecture of Deep Learning model

In this study, we use both LSTM and GRU to overcome scalability concerns in deep RNN networks. LSTM, in particular, seeks to avoid RNN's vanishing gradient issue by presenting the prior timestamp via a memory cell [12]. GRU is a simplified variation of the conventional LSTM that may be learned more quickly due to fewer parameters. Each cell of a modified LSTM typically contains three gates: input, forget, and output.

B. Long Short-Term Memory

LSTM is a type of recurrent neural network (RNN) that is designed to overcome the problem of vanishing gradients, which can occur when training standard RNNs on long sequences of data. The key innovation of LSTM is the use of memory cells, which can store information over long periods of time and selectively forget or remember this information as needed. The LSTM is trained using backpropagation through time, which involves calculating the gradients of the loss function with respect to the weights and biases of the LSTM at each time step and propagating these gradients back through the network.

LSTMs are able to store information over long periods of time, making them well-suited for tasks that require processing of long sequences of data. LSTMs are able to selectively forget or remember information based on the input, allowing them to adapt to changing contexts and avoid interference from irrelevant information.

C. Bi-Directional LSTM

Bidirectional LSTM is a type of neural network architecture that combines the benefits of LSTM and bidirectional processing. BLSTM is designed to capture both forward and backward dependencies in a sequence, making it well-suited for tasks such as speech recognition, where the context both before and after a given phoneme can be important. The basic architecture of a BLSTM consists of two LSTM layers: one that processes the input sequence in a forward direction and another that processes it in a backward direction. The outputs of both these LSTM layers are then concatenated to produce the final output.

BLSTM is able to capture dependencies in both directions, which can be useful in tasks such as speech recognition, where the context both before and after a given phoneme can be important. BLSTM has been shown to outperform standard LSTMs and other types of neural networks in a wide range of applications, including natural language processing, speech recognition, and time series prediction.

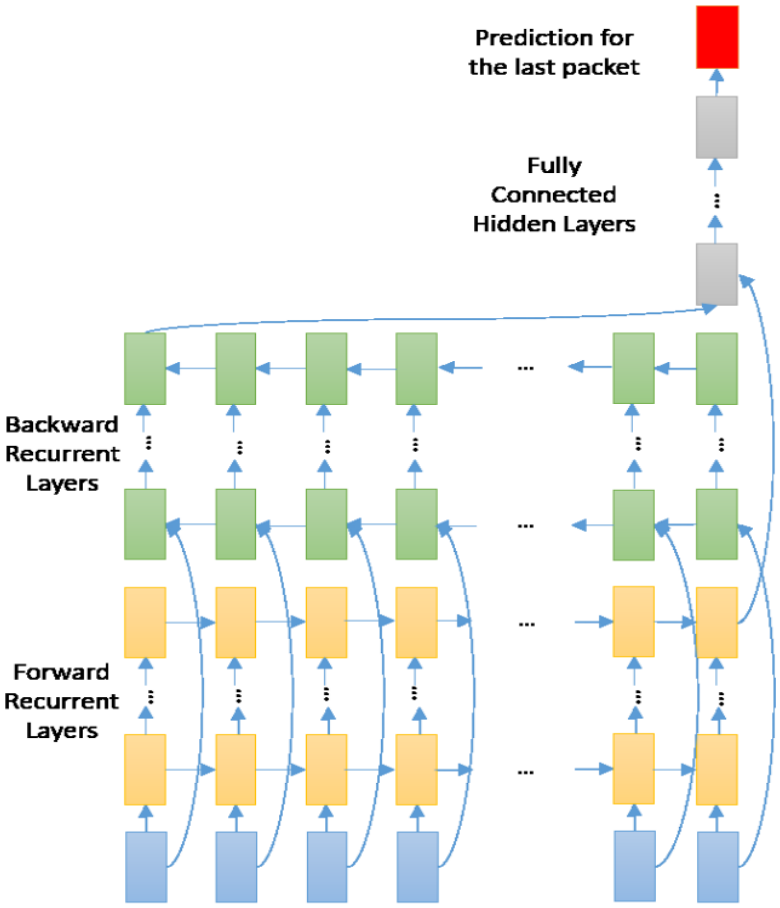


Fig 2: architecture of Bidirectional LSTM

D. GRU

GRU is a type of recurrent neural network (RNN) that is similar to LSTM in that it is designed to overcome the problem of vanishing gradients that can occur when training standard RNNs on long sequences of data. GRU is simpler than LSTM and has fewer parameters, which makes it easier to train and faster to run.

GRU is simpler than LSTM and has fewer parameters, which makes it easier to train and faster to run. GRU requires less memory than LSTM, which makes it well-suited for applications with limited computational resources. GRU addresses the problem of vanishing gradients that can occur in standard RNNs by using gating mechanisms, which help to ensure that gradients can flow through the network without becoming too small to be useful.

Chapter 4: Experimental Results and Analysis

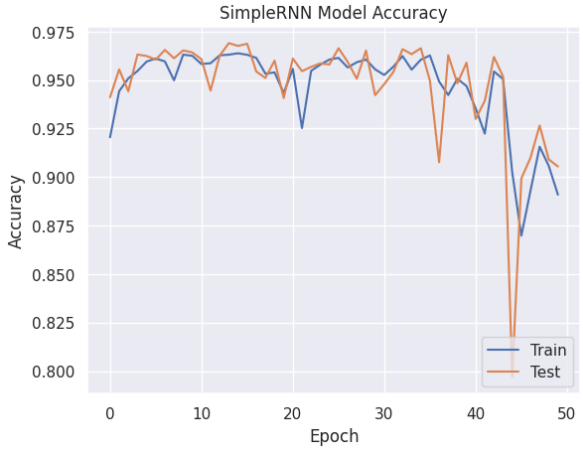
Dataset Detail:

We have used dataset CoAP-DDoS. It consists network traffic with around 10,00,000 attack traffic and normal traffic. Attribute for traffic single is taken from Wireshark consists attributes like frame length, header length, source IP, port etc. We have taken 25 attributes from the dataset.

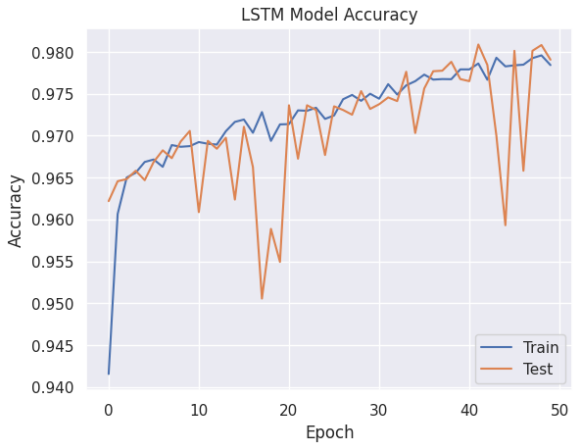
Results:

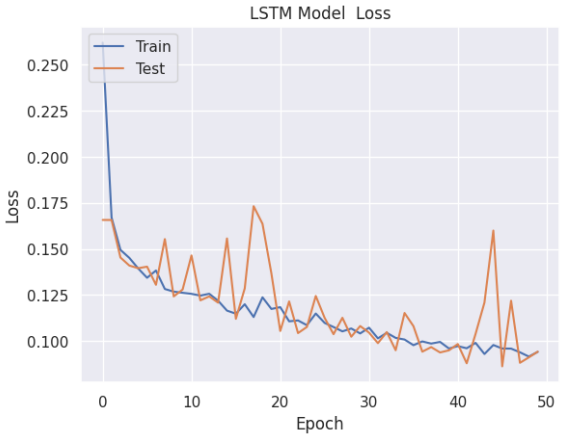
We have trained all deep learning model mentioned in the methodology and came up with few parameters to compare, for finding better performing model. Let's see accuracy of these models' epoch wise and their training loss.

1) RNN

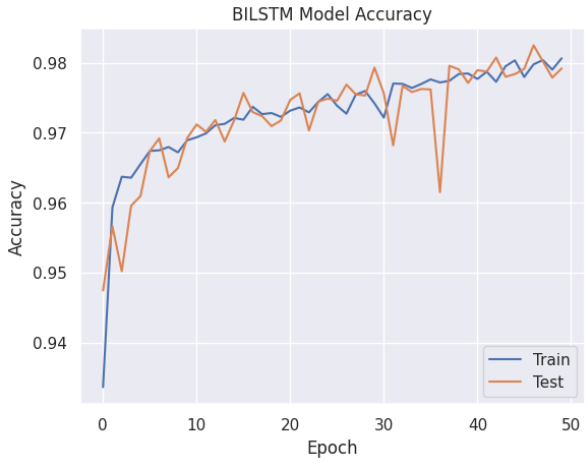


2) LSTM

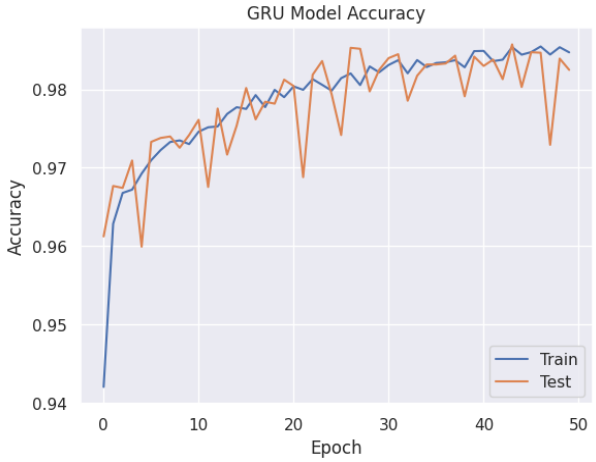




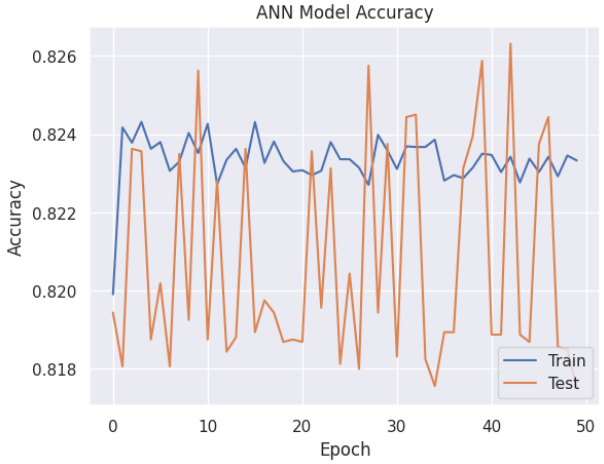
3) Bi-directional LSTM

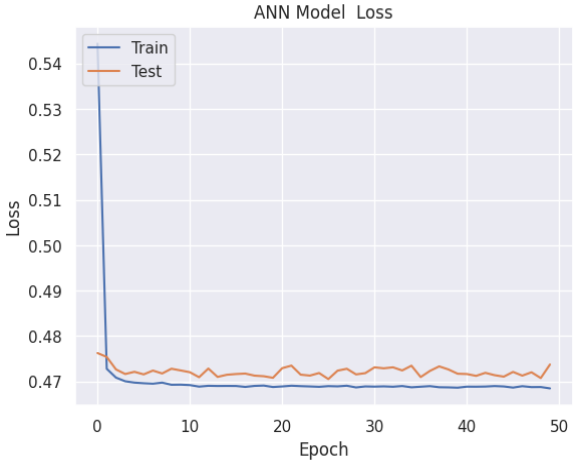


4) GRU



5) ANN





Based on confusion matrix we have derived some masseurs for comparing each model such as accuracy, precision, recall.

Precision is the number of correctly classified positive examples divided by the total number of examples that are classified.

Recall is the number of correctly classified positive examples divided by total number of actual positive examples in the test set.

Accuracy is nothing but ratio of correctly predicted examples to total number of examples.

Here is the table of all accuracy measurements with respect to the model and number of epochs the model is trained.

TABLE II: Comparison between models with 40 epochs

	RNN	LSTM	BLSTM	GRU	ANN
Accuracy	94.87%	97.08%	95.65%	**98.07%**	82.38%
Precision	91.22%	94.47%	92.07%	**96.49%**	75.65%
Recall	99.19%	**99.95%**	99.91%	99.74%	95.74%

TABLE III: Comparison between models with 50 epochs

	RNN	LSTM	BLSTM	GRU	ANN
Accuracy	90.67%	97.87%	97.95%	**98.27%**	82.19%
Precision	86.61%	96.36%	97.99%	**98.33%**	75.52%
Recall	96.21%	**99.50%**	97.92%	98.21%	95.03%

TABLE IV: Comparison between models with 100 epochs

	RNN	LSTM	BLSTM	GRU	ANN
Accuracy	91.57%	98.71%	96.51%	**98.18%**	82.77%
Precision	87.48%	97.91%	94.14%	**98.50%**	76.35%
Recall	96.92%	**99.53%**	99.18%	98.17%	94.92%

As we can see clearly see, GRU model is predicting DDoS attack with high accuracy. We have trained these models with number of epoch of 40, 50 and 100. After 50 epochs there is no significant improvement in the accuracy may be possibly due to overfitting of the model. Hence, we are considering 50 as ideal number of epochs for the training.

Chapter 5: Conclusion and Future Work

In this study, we investigated various deep learning-based DDoS detection approaches. It aids in the performance of detecting DDoS attack traffic. We frame DDoS identification as a sequential classification issue and shift from packet-based to window-based detection. Among simple RNN, LSTM, GRU, BLSTM and ANN we compared their accuracy and recall. As compared with each other we found GRU is outperforming with accuracy of 98.27% followed by LSTM model with accuracy 98.71%.

In the future, we intend to broaden the variety of DDoS vectors and system parameters to evaluate the robustness of our model in a variety of situations. We can implement hybrid Deep Learning model which can overcome with each other's disadvantages.

Chapter 6: References

[1] Kamboj, Priyanka, Munesh Chandra Trivedi, Virendra Kumar Yadav, and Vikash Kumar Singh. "Detection techniques of DDoS attacks: A survey." In *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)*, pp. 675-679. IEEE, 2017.

[2] Polat, Hüseyin, Muammer Türkoğlu, Onur Polat, and Abdülkadir Şengür. "A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks." *Expert Systems with Applications* 197 (2022): 116748.

[3] Hochreiter, Sepp, and Jürgen Schmidhuber. "Long short-term memory." *Neural computation* 9, no. 8 (1997): 1735-1780.

[4] Chung, Junyoung, Caglar Gulcehre, KyungHyun Cho, and Yoshua Bengio. "Empirical evaluation of gated recurrent neural networks on sequence modeling." *arXiv preprint arXiv:1412.3555* (2014).

[5] Elsaeidy, Asmaa A., Abbas Jamalipour, and Kumudu S. Munasinghe. "A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City." *IEEE Access* 9 (2021): 154864-154875.

[6] Wei, Yuanyuan, Julian Jang-Jaccard, Fariza Sabrina, Amardeep Singh, Wen Xu, and Seyit Camtepe. "Ae-mlp: A hybrid deep learning approach for ddos detection and classification." *IEEE Access* 9 (2021): 146810-146821.

[7] Sahoo, Kshira Sagar, Bata Krishna Tripathy, Kshirasagar Naik, Somula Ramasubbareddy, Balamurugan Balusamy, Manju Khari, and Daniel Burgos. "An evolutionary SVM model for DDOS attack detection in software defined networks." *IEEE Access* 8 (2020): 132502-132513.

[8] Zeeshan, Muhammad, Qaiser Riaz, Muhammad Ahmad Bilal, Muhammad K. Shahzad, Hajira Jabeen, Syed Ali Haider, and Azizur Rahim. "Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets." *IEEE Access* 10 (2021): 2269-2283.

[9] Xu, Congyuan, Jizhong Shen, and Xin Du. "Low-rate DoS attack detection method based on hybrid deep neural networks." *Journal of Information Security and Applications* 60 (2021): 102879.

[10] Zhao, David, Issa Traore, Bassam Sayed, Wei Lu, Sherif Saad, Ali Ghorbani, and Dan Garant. "Botnet detection based on traffic behavior analysis and flow intervals." *computers & security* 39 (2013): 2-16.

[11] Agarwal, Ankit, Manju Khari, and Rajiv Singh. "Detection of DDOS attack using deep learning model in cloud storage application." *Wireless Personal Communications* (2021): 1-21.

[12] Fouladi, Ramin Fadaei, Orhan Ermiş, and Emin Anarim. "A DDoS attack detection and defense scheme using time-series analysis for SDN." *Journal of Information Security and Applications* 54 (2020): 102587.

[13] Niyaz, Quamar, Weiqing Sun, and Ahmad Y. Javaid. "A deep learning based DDoS detection system in software-defined networking (SDN)." *arXiv preprint arXiv:1611.07400* (2016).

[14] Li, Chuanhuang, Yan Wu, Xiaoyong Yuan, Zhengjun Sun, Weiming Wang, Xiaolin Li, and Liang Gong. "Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN." *International Journal of Communication Systems* 31, no. 5 (2018): e3497.

[15] Ujjan, Raja Majid Ali, Zeeshan Pervez, Keshav Dahal, Ali Kashif Bashir, Rao Mumtaz, and Jonathan González. "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN." *Future Generation Computer Systems* 111 (2020): 763-779.

[16] Ma, Li, Ying Chai, Lei Cui, Dongchao Ma, Yingxun Fu, and Ailing Xiao. "A deep learning-based DDoS detection framework for Internet of Things." In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2020.

[17] Shurman, Mohammad M., Rami M. Khrais, and Abdulrahman A. Yateem. "DoS and DDoS attack detection using deep learning and IDS." *Int. Arab J. Inf. Technol.* 17, no. 4A (2020): 655-661.

[18] Zekri, Marwane, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi. "DDoS attack detection using machine learning techniques in cloud computing environments." In *2017 3rd international conference of cloud computing technologies and applications (CloudTech)*, pp. 1-7. IEEE, 2017.

[19] Nugraha, Beny, and Rathan Narasimha Murthy. "Deep learning-based slow DDoS attack detection in SDN-based networks." In *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 51-56. IEEE, 2020.

[20] Zhang, Hao, Yongdan Li, Zhihan Lv, Arun Kumar Sangaiah, and Tao Huang. "A real-time and ubiquitous network attack detection based on deep belief network and support vector machine." *IEEE/CAA Journal of Automatica Sinica* 7, no. 3 (2020): 790-799.