AI-Driven DDoS Mitigation at the Edge: Leveraging Machine Learning for Real-Time Threat Detection and Response

1st Sahil Arora
IT Department
Maharaja surajmal institute of Technology(MSIT), GGSIPU
New Delhi, India
Sahil9009@gmail.com

2nd Pranav Khare
SIRT (RGPV) Bhopal
Bhopal, MP, India
Khare.pranav@gmail.com

3rd Sandeep Gupta
Techieshubhdeep it Solutions Pvt. Ltd,
Gwalior, M.P. India
ceo.techies@gmail.com

2024 International Conference on Data Science and Network Security (ICDSNS) | 979-8-3503-7311-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICDSNS62112.2024.10690930

***Abstract*—As cyber threat actors develop increasingly sophisticated strategies, cutting-edge cyber security is necessary for industry organizations and government agencies. A security threat model must consider these developments since they might bring new cyber dangers. Many attacks have been cropping up on the Internet as it has grown. Today's most prevalent attacks are viruses, distributed denial of service (DDoS) attacks, service interruptions, code injection, and spoofing. Several new techniques for DDoS detection have been proposed, including AI-based machine learning and deep learning tactics. The most recent developments in cybersecurity's use of AI and ML are covered extensively in this article. Using the most current dataset, CICDDoS2019, this research compares and contrasts the performance of deep learning models that identify DDoS attacks, such as RNNs and GRUs. To measure how well the model detects DDoS assaults, use evaluation measures, including recall, accuracy, precision, and F1 score. Models exhibit comparable performance on the CICDDoS2019 dataset, as shown by the experimental findings, which show an accuracy score of 99.9%. The study highlights the effectiveness of AI-driven methods in improving cybersecurity resilience in network infrastructures to new and changing edge DDoS assaults.**

Keywords—threat detection, response, machine learning, distributed denial of service attacks, cybersecurity.

I. INTRODUCTION

The frequency and complexity of cybersecurity attacks have increased over time. More development and constant innovation in defensive methods are required to counteract this rising level of sophistication and complexity. Still widely used and recommended, traditional intrusion detection and deep packet inspection approaches are woefully unable to address the needs of evolving security threats. DoS (Denial of Service) It is a kind of electronic attack that may be used to isolate various services by the Internet. It is a highly potent technique developed to target network equipment and services. A more sophisticated form of DoS, dispersed DoS, employs several dispersed attack locations.[1]. Gligor first introduced DoS in the context of operating systems.[2][3], at which point it was extensively used. A DDoS assault is often called a DoS attack that attempts to coordinate attacks on several computers to target a victim. Several security holes are present in SDN architecture. This type of DDoS attack is extremely common. Some of the most destructive cyberattacks that can happen on the internet are DDoS assaults. Any hacking of a website is likely a DDoS attack. Fig. 1 shows the State of DDoS Mitigation Techniques.

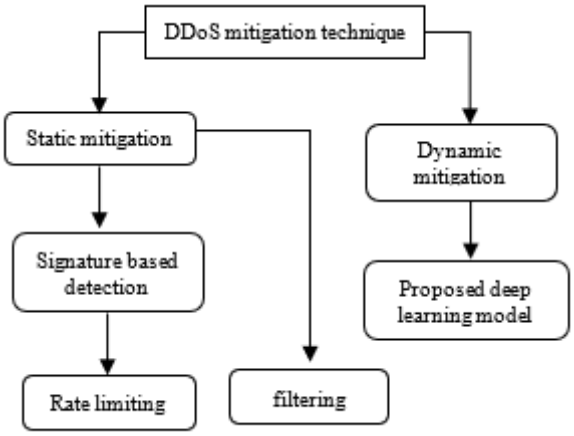

Fig. 1. Current State of DDoS Mitigation Techniques

Also, the point of DDoS assaults is to keep increasing their strength and frequency. Therefore, the newly developed systems must match modern data centres' needs for greater speed and scalability and provide maximum defence against DDoS assaults. Artificial intelligence (AI) is widely employed for predicting and detecting DDoS mitigation threats.[4][5]. AI is a part of machine learning. Machine learning is considered a supplementary defence mechanism against cyber threats like botnets and viruses as computer power decreases in price and availability. This article looks at ML and how it might identify fraudulent network traffic as a possible solution. An approach to DDoS attack detection is known as Deep Defense, which is based on deep learning. [6][7]. To boost the DDoS attack detection system's efficiency.

A. Impact of DDoS Attacks

An attack renders the targeted service or website unavailable, causing a loss of prospective customers and revenue. Loss of customer confidence and harm to a company's image may also have far-reaching effects. Developing efficient mitigation strategies to protect services and avoid revenue loss is crucial in light of the rising frequency of these attacks. DDoS attacks have shown they may affect national security and international relations, in addition to causing harm to businesses. During the war between Russia and Ukraine, for instance, 128 government organisations from 42 countries that supported Ukraine were targeted by state-sponsored threat actors [4]. The goal of the threat actors in attacking these institutions is to sow disarray and uncertainty in the global political scene.

B. Contribution of this paper

The research makes key contributions to the fields of cybersecurity and DDoS mitigation in several important aspects, including the following:

- Analyse the CICIDS-2019 dataset and understand the preprocess to improve the reliability and quality of DDoS attack prevention models.
- To compare the models like RNN and GRU.
- To evaluate the performance of various DL models across precision, accuracy, recall, and f1-score.
- This comparative analysis of DDoS mitigation using AI techniques helps identify this system's performance for future analysis.

C. Organized of this paper

Here is the breakdown of the remaining sections of the paper: Some prior work on DoS attack detection is detailed in Section II. Section III delves into the methods, whereas Section IV presents and analyses the experimental outcomes. Section V concludes the whole process.

II. Literature Review

Attacks known as DDoS are on the rise and may compromise the security of any network. These attacks may severely disrupt online services and result in huge financial losses. The following Table II provides a comparison of existing related work between different models for DDoS mitigation. Here, you may find a few pieces of similar work.

Al-Shareeda, Manickam, and Saare (2023) contrast several machine-learning techniques for identifying DDoS attacks. From Google's research dataset comes the DDOS attack SDN dataset, Several methods are used when analysing network data for anomalies that could be signs of DDoS attacks, such as DT, SVM, NB, and RF. The outcomes display that when identifying DDoS assaults, the RF algorithm obtains the greatest accuracy rate of 99.4 per cent. Also, with 98.8% and 98.4% accuracy rates, respectively, DT and SVM algorithms work quite well.[8].

In this research, Sridevi et al. (2023) offer a thorough strategy for detecting insider threats using deep learning and ML algorithms. The purpose of this model would be to spot unusual insider behaviour. The model outperformed the current modern method with a detection accuracy of 96.3%. It used a dataset assembled from system logs and user activity records from many businesses.[9].

Fenil and Kumar (2022) use a mix of information about network traffic. One way to create a dictionary of parameters used in network traffic is using the KSVD technology. Additionally, two distinct data sets evaluate and contrast Wavelet-based DDoS detection systems with Matching Pursuit. The research found that the method had an 89% detection accuracy. They find that the two most common ways to detect DDoS attacks in SDN are cutoff point DDoS detection approaches and ML-based DDoS detection mechanisms.[10].

Wani et al., (2019) was completed on an own cloud environment employing Tor Hammer as an attack tool, and an IDS was used to create a new dataset. The study uses various ML techniques for classification, like NB, SVM, and RF. The total accuracy was NB: 98.0%, RF: 97.6%, and SVM: 99.7%[11].

Lima Filho et al. (2019) created a DoS detection system using ML. Four advanced benchmark datasets were used to conduct the tests. By sampling 20% of network traffic, the findings provide an online attack detection rate (DR) of over 96%, along with a low false alarm rate (FAR) and excellent precision (PREC)[12].

TABLE I. Ccomparative analysis of DDoS Mitigation for threat detection using various approaches

Author	Objectives	Data set	Algorithms	Limitations	Results
Khanday, Fatima and Rakesh [13]	The study proposes a new approach to data pre-processing that integrates ML and DL classifiers while maintaining a lightweight IDS.	TON-IOT, BOT-IOT	ANN, LSTM, LR, NB, linear SVM	Validation of the suggested model was not done using a state-of-the-art model.	The LSTM model achieved superior results compared to its competitors in BOT-IOT and TON-IOT, with 99% and 95% accuracy for binary and multiple classifications, respectively.
Zeeshan et al., [14]	While concurrently creating a dataset of packets from IoT traffic, this study offers a PB-DID architecture by comparing flow- and TCP-based features from the UNSW-NB-15 and BOT-IOT datasets.	UNSW-NB15, BOT-IOT	LSTM	The model is very heavy.	To achieve this 96.3% accuracy, the researchers used DL and LSTM.
Alimi et al.,[15]	This paper proposes an improved LSTM deep learning method-based IDS for identifying DoS assaults in IoT networks.	CICIDS-2017, NSL-KDS	Refined MLP and LSTM	The CICIDS-2017 dataset did not provide good results with MLP models.	For the CICIDS-2017 dataset, this model attained f-score rates of 99.22%, recall of 99.22%, and precision of 99.23%. For every performance indicator, the NSL-KDD dataset model reached 98.60%.
Ismail et al., [16]	This study focuses on applying machine learning to DDoS attack classification and prediction.	UNWS-NB-15	RF, XGBoost	The accuracy may be improved by using a more proper model.	The accuracy percentage for XGBoost is 90%, whereas the random forest is 89%.
Mihoub et al., [17]	This study proposes an architecture designed for the IoT to detect and mitigate DoS/DDoS attacks.	BOT-IOT	DT, RF, LSTM,	Every time the KNN model does a look-back, it shows a significant decrease.	Among the encouraging results of the assessment is the 99.81% accuracy achieved using looking-back-enabled RF.

Motylinski et al., [18]	This study aims to find ways to detect more quickly without sacrificing a reasonable detection level.	IoT-BoT	KNN, SVM, LR	GPU technology shortens the time it takes to train and make predictions.	According to the data, the recall and accuracy of the best-trained model are 99.7 and 99.9 per cent, respectively.
Amrish et al., [19]	This research aimed to distinguish DDoS attacks from other types of attacks.	CICDDoS2019	RF, KNN, DT, ANN	Due to its high false negative rate, the DT model had the weakest performance.	With an accuracy rating of 99.95%, the ANN model surpasses the other categorisation approaches.

A. Research gaps

Despite notable developments in DDoS attack detection resulting from a combination of DL and ML methodologies, many research drawbacks and limitations exist. It is difficult to compare and reproduce results due to the absence of consistent benchmarks and assessment frameworks across research. On top of that, many current methods only apply to certain DDoS attacks or datasets, which might not represent the complex nature of cyber threats nowadays. In addition, detection models' computational efficiency and scalability are still issues, especially in large-scale network settings and real-time monitoring situations. Additional research is needed to determine how well these models resist malicious attacks and whether they can be applied to various network designs and traffic patterns. Researchers, practitioners, and industry stakeholders must work together to fill these gaps in DDoS detection capabilities, making them robust enough to respond to new cyber threats while reducing the number of FP and FN.

III. METHODOLOGY

This section provides a methodology and dataset description for the comparative analysis of the proposed techniques. These methodological stages, such as data collection, preprocessing, feature selection, splitting, classification models, and model evaluation (Fig. 2), help the study endeavour to create a reliable and precise model for preventing DDoS attacks.

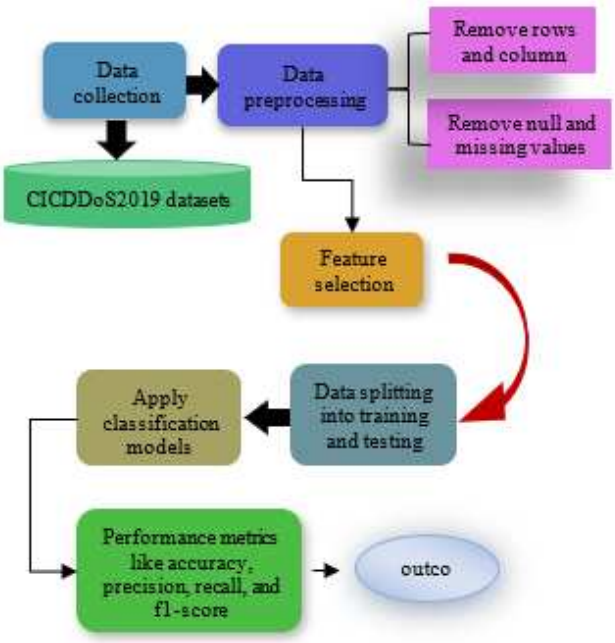

Fig. 2. Data flow architecture

A. Data collection

Computer security researchers have compiled the CICDDoS2019 datasets. The data, gathered and stored in CSV format, includes various traffic factors. This dataset includes many current reflected DDoS attacks, such as NetBIOS, PortMap, UDP-Lag, LDAP, UDP, MSSQL, NTP, SYN, DNS, and SNMP assaults. Attacks subsequently occurred throughout this period.

B. Data preprocessing

Data preprocessing is a critical preliminary step that must be completed before data analysis. Preprocessing of the data substantially and effectively enables this. This endeavour has implemented data purification as a preliminary data processing stage. The preprocessing steps are as below:

1) Remove rows: Certain entries in the dataset are eliminated due to the presence of infinity instead of a numerical value.

2) Missing and null values: For the present study, the data in the dataset containing missing or null values have been excluded. Eliminating these records decreases computational complexity and enhances the model's efficacy.

3) Feature selection: The process of choosing the required variables to improve accuracy is called "Feature Selection." Selecting features significantly complicates training a predictive learning algorithm.

C. Data splitting

After the data is preprocessed, it is split into two or more subsets. The CICDDoS2019 dataset contains training and testing sets. Data splitting is done using the Sklearn package. Thirty per cent is used for testing, while the remaining seventy per cent is used for training.

D. Classification techniques

Choose the best deep-learning neural network for model building for DDoS attack prevention. DL is the subset of an artificial neural network. In this research, some algorithms that provide below:

E. Recurrent neural network (RNN)

An expansion of the traditional FFNN, a recurrent neural network (RNN) can process sequence inputs of varying lengths. The RNN can handle sequences of varying lengths because it has a recurrent hidden state whose activation at every iteration depends on the activation at the preceding iteration. Formally, the recurrent neural network (RNN) modifies its recurrent hidden state ht in the given sequence x = (x1, x2, · · ·, xT) by (1).

$$h_t = \begin{cases} o, \\ \emptyset(h_t - 1, x_t), t = 0 \end{cases} \quad (1)$$

In the context of nonlinear functions, φ denotes a function composed of a logistic sigmoid and an affine transformation. An alternatively variable-length output y = (y1, y2,..., yT) may be generated by the RNN. (2) typically updates the recurrent hidden state as:

$$h_t = g(Wx_t + Uh_{t-1}) \quad (2)$$

Where g represents a bounded, smooth function, such as the hyperbolic tangent function or the logistic sigmoid function, to represent a distribution across sequences of varying lengths, generative RNNs employ a particular output symbol to indicate the series' termination. The model creates a probability distribution for the subsequent element in the sequence based on its present condition ht. One way to break down sequence probability is to consider it as (3).

$$p(x_t|, \dots x_T) = p(x_1)p(x_2|x_1)p\big(x_3\big|x_{1,}x_2\big) \dots . p(x_1, \dots . , x_T - 1) \quad (3)$$

Where a unique value denoting the conclusion of the sequence is the last member, with each conditional probability distribution, develop a model using (4):

$$p(x_t|x_1 \dots x_{t-1}) = g(h_t) \quad (4)$$

Where ht is from (4). Such generative RNNs are present in this research.

F. GRU

As proposed, using a GRU allows each recurrent unit to adaptively record relationships across several time scales.[20]. GRUs function similarly to LSTMs without dedicated memory cells because they have gating units that control the data flow inside the unit. At time t, the GRU's activation htj is calculated by linearly integrating the candidate activation h˜jt with the preceding activation on hjt−1, as (5):

$$h_t^j = \big(1 - z_t^j\big)h_{t-1}^j + z_{th_t^j}^j \quad (5)$$

An update gate z j t determines how much a unit changes its activation or content. This is a formula for the update gate as (6):

$$z_t^j = \sigma(W_z x_t + U_z h_{t-1})^2 \quad (6)$$

Consistent with the LSTM unit, this method linearly adds the current state to the freshly calculated state. Contrarily, the GRU reveals its whole state every time without any way to restrict the extent to which it is disclosed.

G. Model Evaluation

Model evaluation is the process of analysing a model's performance. Most existing DDoS attack detection techniques use common evaluation metrics, such as recall, precision, accuracy, and f1 score. These parameters evaluate a model and predict its outcome.

IV. Comparative Results & Discussions

This section offers a comparative analysis of different AI models for DDoS mitigations regarding performance measures. Evaluation metrics allow one to determine a model's performance. An important quality of assessment metrics is their capacity to distinguish between various model outputs. This study uses accuracy/loss score, recall, f1 score, and precision to evaluate algorithm performance.

A. Accuracy

It represents the proportion of accurate forecasts to all input sample numbers. It is given as (7)-

$$Accuracy = \frac{TP+TN}{TP+Fp+TN+FN} \quad (7)$$

B. Precision

It is calculated by dividing the number of correctly predicted positive outcomes by the number of positive results the classifier anticipated. It is expressed as (8)-

$$Precision = \frac{TP}{TP+FP} \quad (8)$$

C. Recall

To get it, divide the sum of all relevant samples by the sum of all correct positive results. In mathematical notation, it is expressed as (9):

$$Recall = \frac{TP}{TP+FN} \quad (9)$$

D. F1 score

The accuracy of a test is measured using it. Precision and recall are the harmonic means that make up the F1 Score. An F1 Score might fall between 0 and 1. It indicates both the robustness and the precision of the classifier. It is stated mathematically as (10):

$$F1 - Score = \frac{2(Precision*Recall)}{Precision+Recall} \quad (10)$$

E. Experimental Results

The analysis presented in the following section pertains to the outcomes derived from the conducted experiments for DDoS detection. The following experiment results are as follows:

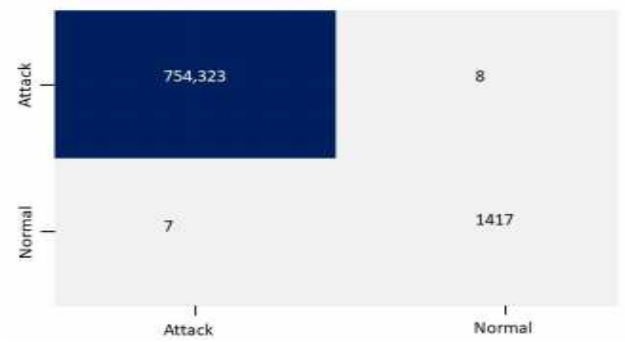

Fig. 3. Confusion matrices for recurrent neural network

Fig. 3 displays the Confusion matrices for RNN on the CICDDoS2019 dataset, which contains two classes: attack and Normal. In this Fig. 3, the attack class false positive value is 8, and the true positive is 754,323. The normal class false negative value is 7, and the true negative is 1417.

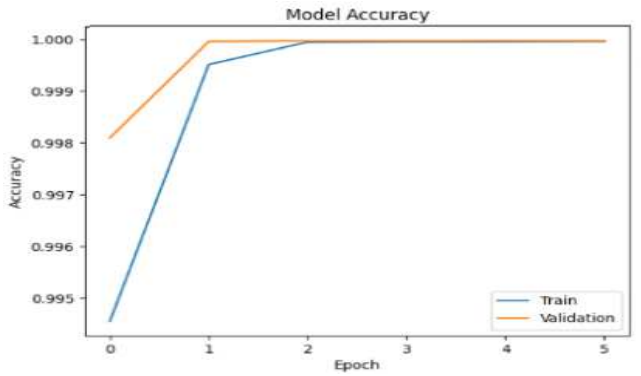

Fig. 4. Accuracy graph of recurrent neural network

Fig. 4 represents the Accuracy graph of the recurrent neural networks. The training accuracy of RNN models begins at 99.45% and goes up to 99.99%.

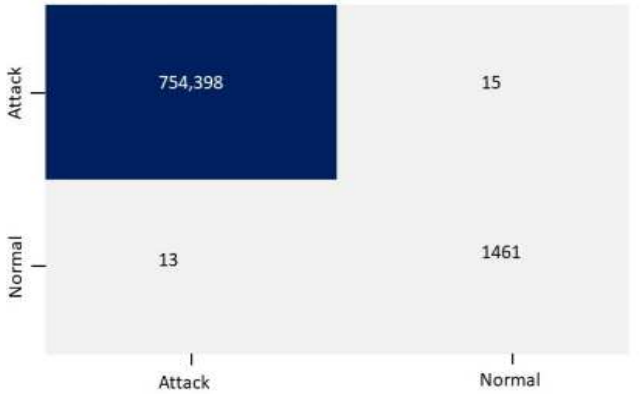

Fig. 5. Confusion matrices for gated recurrent unit

Confusion matrices for gated recurrent units are exhibited in Fig. 5. The false positive is 15 identified, and the true positive is 754,398 as an attack. In the normal class false negative value is 13, and the true negative is 1461.

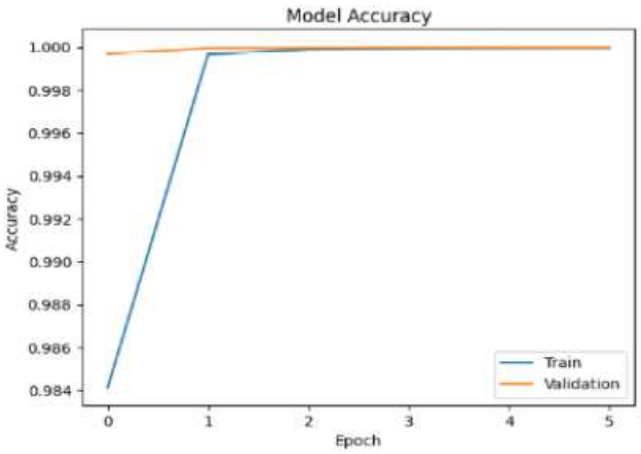

Fig. 6. Accuracy graph of gated recurrent unit

Fig. 6 displays the GRU training and validation losses. On the one hand, the accuracy of the GRU model training ranges from 98.4% to 99.99%

Table II compares different machine learning models for DDoS mitigation regarding accuracy, precision, recall and f1-score measures.

TABLE II. COMPARISON OF VARIOUS MODELS ON THE PERFORMANCE PARAMETER

Models	Accuracy	Precision	Recall	F1 score
LR[21]	97.7%	99.6%	96.1%	97%
LSTM[22]	0.98%	0.97%	0.97%	0.98%
KNN[23]	0.8686%	0.9494%	0.8636	0.8600
RF[24]	0.99%	0.99%	0.99%	0.99%
RNN	99.99%	99.99%	99.99%	99.99%
GRU	99.99%	99.0%	100%	100%

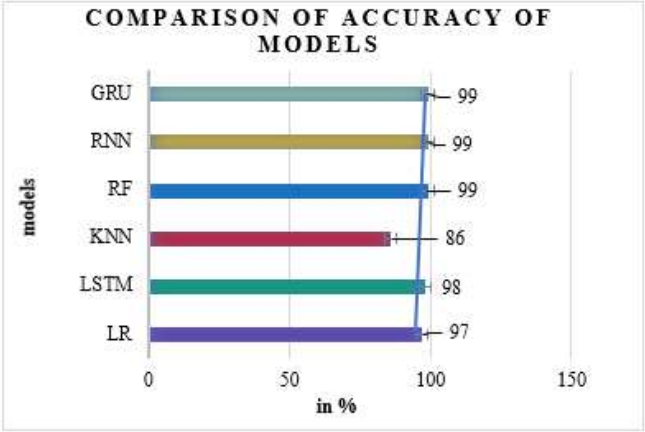

Fig. 7. Comparison of accuracy of different models

The accuracy of many models is compared in Fig. 7, which is located above. In this Fig. 7 RNN and GRU models outperform compared to other models' accuracy. RNN and GRU achieve 99% accuracy.

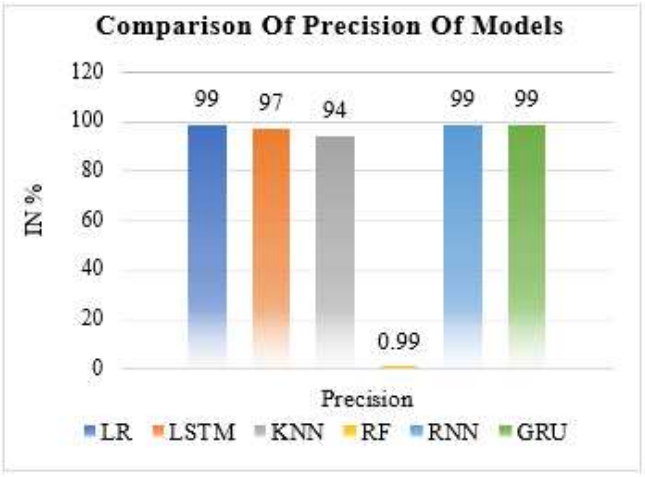

Fig. 8. Comparison of Precision of different models

Fig. 8 displays a comparison of the models' corresponding levels of precision. The RNN and GRU achieved the highest precision scores of 99.99% and 99.0% compared to other models.

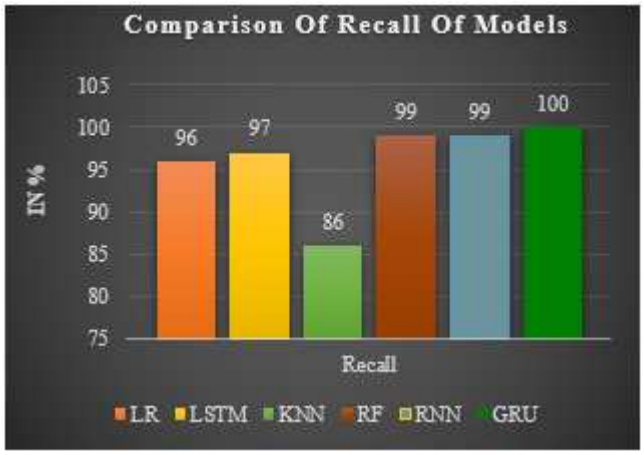

Fig. 9. Comparison of Recall of different models

Fig. 9 displays the results of comparing the recall of several models. When comparing recall rates, the RNN and GRU models come out on top with impressive 99.99% and 100% rates, respectively. The KNN achieve the lowest performance.

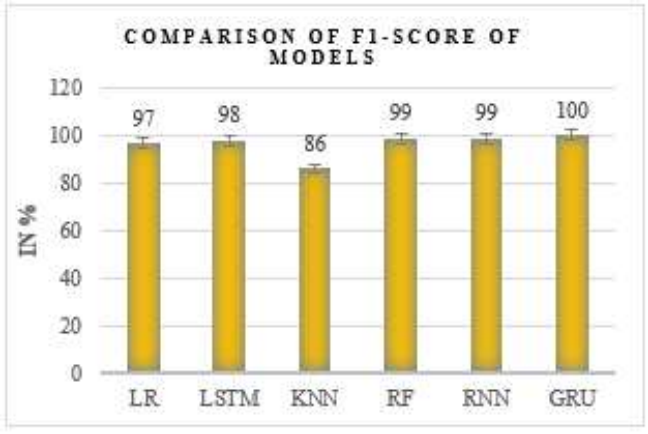

Fig. 10. Comparison of F1-score of different models

As shown in Fig. 10, the F1 scores of several models are compared. With an F1 score of 99.99%, the RNN and GRU perform very well. RNN and GRU models have the highest F1 scores compared to other methods.

V. Conclusion And Future Work

The research concluded with a comparative analysis that used deep learning approaches to build a model that effectively prevents DDoS attacks. The study analysed several deep learning models, including RNN and GRU, for edge threat identification and response using the CICDDoS2019 dataset and preprocessing methods, such as feature selection and dividing a dataset into training and testing sets. The findings demonstrate the value of using advanced DL methods to detect and react to attacks in real time when conducting DDoS mitigation operations. In this research, the RNN and GRU models outperform each other with remarkable scores of 99.99% on several performance parameters. According to the findings, there is much room for growth in cybersecurity systems that use AI and ML. Improving cybersecurity resilience in network infrastructures through integrating AI-driven techniques at the edge shows great potential for the future, as it will allow for the prompt and effective mitigation of changing security threats. Improving deep learning models' resistance to adversarial assaults and creating adaptive algorithms for continuous learning to address changing DDoS techniques might be areas of future research. Incorporates progressive learning for future work by recording network traffic. Thus, a new kind of attack may be added to the machine. Beyond the technological details, future research should investigate the moral questions raised by AI and ML applications to develop policies that promote responsible use and open decision-making. There are a lot of untapped potential uses for AI and ML in cybersecurity, particularly in areas such as proactive threat hunting, incident response, and catastrophe recovery.

References

[1] M. Iqbal, F. Iqbal, F. Mohsin, M. Rizwan, and F. Ahmad, "Security issues in software-defined networking (SDN): Risks, challenges and potential solutions," Int. J. Adv. Comput. Sci. Appl., 2019, doi: 10.14569/ijacsa.2019.0101042.

[2] K. Lakshminarayanan, D. Adkins, A. Perrig, and I. Stoica, "Taming IP packet flooding attacks," in Computer Communication Review, 2004. doi: 10.1145/972374.972383.

[3] A. Sayed, "Face mask detection model based on deep CNN technique using AWS," Int. J. Eng. Res. Appl., vol. 13, no. 5, pp. 12–19, 2023.

[4] S. Mathur., "Supervised Machine Learning-Based Classification and Prediction of Breast Cancer," Int. J. Intell. Syst. Appl. Eng., vol. 12(3), 2024.

[5] S. Mathur and S. Gupta, "Classification and Detection of Automated Facial Mask to COVID-19 based on Deep CNN Model," in 2023 IEEE 7th Conference on Information and Communication Technology, CICT 2023, 2023. doi: 10.1109/CICT59886.2023.10455699.

[6] V. Rohilla, S. Chakraborty, and R. Kumar, "Deep learning based feature extraction and a bidirectional hybrid optimised model for location based advertising," Multimed. Tools Appl., vol. 81, no. 11, pp. 16067–16095, May 2022, doi: 10.1007/s11042-022-12457-3.

[7] V. Rohilla, M. Kaur, and S. Chakraborty, "An Empirical Framework for Recommendation-based Location Services Using Deep Learning," Eng. Technol. Appl. Sci. Res., 2022, doi: 10.48084/etasr.5126.

[8] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," Bull. Electr. Eng. Informatics, vol. 12, no. 2, pp. 930–939, 2023, doi: 10.11591/eei.v12i2.4466.

[9] D. Sridevi, L. Kannagi, V. G, and S. Revathi, "Detecting Insider Threats in Cybersecurity Using Machine Learning and Deep Learning Techniques," in 2023 International Conference on Communication,

Security and Artificial Intelligence (ICCSAI), 2023, pp. 871–875. doi: 10.1109/ICCSAI59793.2023.10421133.

[10] E. Fenil and P. M. Kumar, “Towards a secure Software Defined Network with Adaptive Mitigation of DDoS attacks by Machine Learning Approaches,” in Proceedings - IEEE International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2022, 2022. doi: 10.1109/ACCAI53970.2022.9752607.

[11] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, “Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques,” in Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019, 2019. doi: 10.1109/AICAI.2019.8701238.

[12] F. S. De Lima Filho, F. A. F. Silveira, A. De Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, “Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning,” Secur. Commun. Networks, 2019, doi: 10.1155/2019/1574749.

[13] S. A. Khanday, H. Fatima, and N. Rakesh, “Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks,” Expert Syst. Appl., 2023, doi: 10.1016/j.eswa.2022.119330.

[14] M. Zeeshan et al., “Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets,” IEEE Access, 2022, doi: 10.1109/ACCESS.2021.3137201.

[15] K. O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, S. Rimer, and O. A. Alimi, “Refined LSTM Based Intrusion Detection for Denial-of-Service Attack in Internet of Things,” J. Sens. Actuator Networks, 2022, doi: 10.3390/jsan11030032.

[16] Ismail et al., “A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks,” IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3152577.

[17] A. Mihoub, O. Ben Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, “Denial of service attack detection and mitigation for the internet of things using looking-back-enabled machine learning techniques,” Comput. Electr. Eng., 2022, doi: 10.1016/j.compeleceng.2022.107716.

[18] M. Motylinski, Á. MacDermott, F. Iqbal, and B. Shah, “A GPU-based machine learning approach for detection of botnet attacks,” Comput. Secur., 2022, doi: 10.1016/j.cose.2022.102918.

[19] R. Amrish, K. Bavapriyan, V. Gopinath, A. Jawahar, and C. Vinoth Kumar, “DDoS Detection using Machine Learning Techniques,” J. ISMAC, 2022, doi: 10.36548/jismac.2022.1.003.

[20] C. Gulcehre, K. Cho, R. Pascanu, and Y. Bengio, “Learned-norm pooling for deep feedforward and recurrent neural networks,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014. doi: 10.1007/978-3-662-44848-9_34.

[21] Z. He, T. Zhang, and R. B. Lee, “Machine Learning Based DDoS Attack Detection from Source Side in Cloud,” in Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017, 2017. doi: 10.1109/CSCloud.2017.58.

[22] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, “DDoS Detection using Deep Learning,” Procedia Comput. Sci., vol. 218, pp. 2420–2429, 2023, doi: https://doi.org/10.1016/j.procs.2023.01.217.

[23] L. Xinlong and C. Zhibin, “DDoS Attack Detection by Hybrid Deep Learning Methodologies,” Secur. Commun. Networks, 2022, doi: 10.1155/2022/7866096.

[24] Stefanos Kiourkoulis, “DDoS Dataset - Use of machine learning to analyse intrusion detection performance,” Lulea Univ. Technol., p. 81, 2020.