



Wayanamac Education Trust ®
DON BOSCO INSTITUTE OF TECHNOLOGY
Kumbalagodu, Mysore Road, Bengaluru – 560074
www.dbit.co.in Ph: +91-80-28437028/29/30 Fax:
+91-80-28437031



Department of CSE (Artificial Intelligence and Machine Learning)

DDoS Attack Intrusion Detection System Based on Hybridization of CNN and LSTM



2023-24

8th Semester

BE in CSE(AI & ML)

UNDER THE GUIDENCE:

Mr. Sanjay Kumar

Associate Professor

Department of CSE(AI & ML)

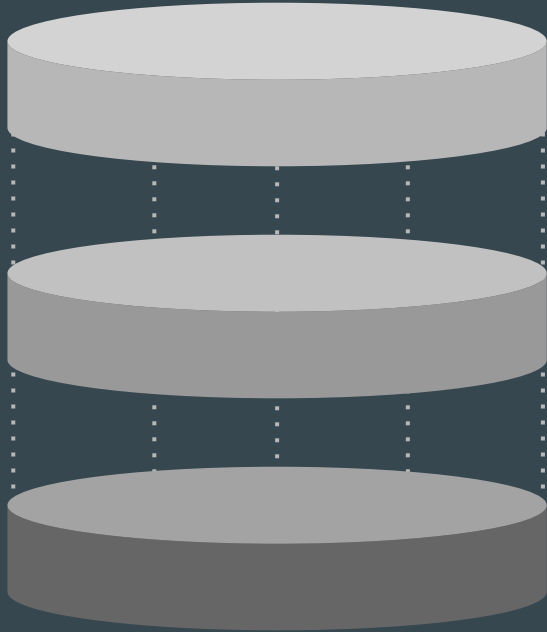
PRESENTED BY:

NIDHI SINHA

1DB20CI029

DDoS Attack Intrusion Detection System

Finding a solution to the rising threat of DDoS attacks.



Problem Statement

The threat of DDoS attacks is on the rise, and current intrusion detection systems are not sufficient. Distributed Denial-of-Service (DDoS) attacks pose a significant cyber threat by inundating servers or networks with excessive traffic, rendering them inaccessible to legitimate users. These attacks result in substantial disruptions and financial harm to businesses and organizations. Their sophistication is on the rise, making detection a formidable challenge. Conventional intrusion detection systems (IDS) often struggle to identify intricate DDoS attacks, particularly those that disperse attack traffic across numerous sources.

Literature Survey

- 2017: A. S. Ahmed Issa et al. proposed a feature selection approach combining DDoS Characteristic Features (DCF) and Consistency Subset Evaluation (CSE) for IDS enhancement using machine learning.
- 2018: Kushwah and Ali introduced an ANN and black hole optimization approach for DDoS attack detection in cloud computing.
- 2019: Anjum and Shreedhara presented a Semi-Supervised Machine Learning technique to improve DDoS attack detection performance.
- 2020: Bagyalakshmi and Samundeeswari proposed filter and dimensionality reduction methods combined with various classification algorithms for effective DDoS attack detection.
- 2023: A study by A. S. Ahmed Issa et al. introduced a DDoS Attack Intrusion Detection System based on hybridization of CNN and LSTM.
- 2024: Azizi and Hosseini suggested a hybrid framework for DDoS detection, incorporating process classification to improve organizational efficiency.
- Prathyusha and Kannayaram highlighted the efficacy of artificial immune systems (AIS) for DDoS detection in cloud computing environments.

The Literature Survey

distributed denial-of-service (DDoS) attack

1

Signature-based

methods: These methods rely on pre-defined signatures of known DDoS attacks. However, they are ineffective in detecting new or zero-day attacks.

2

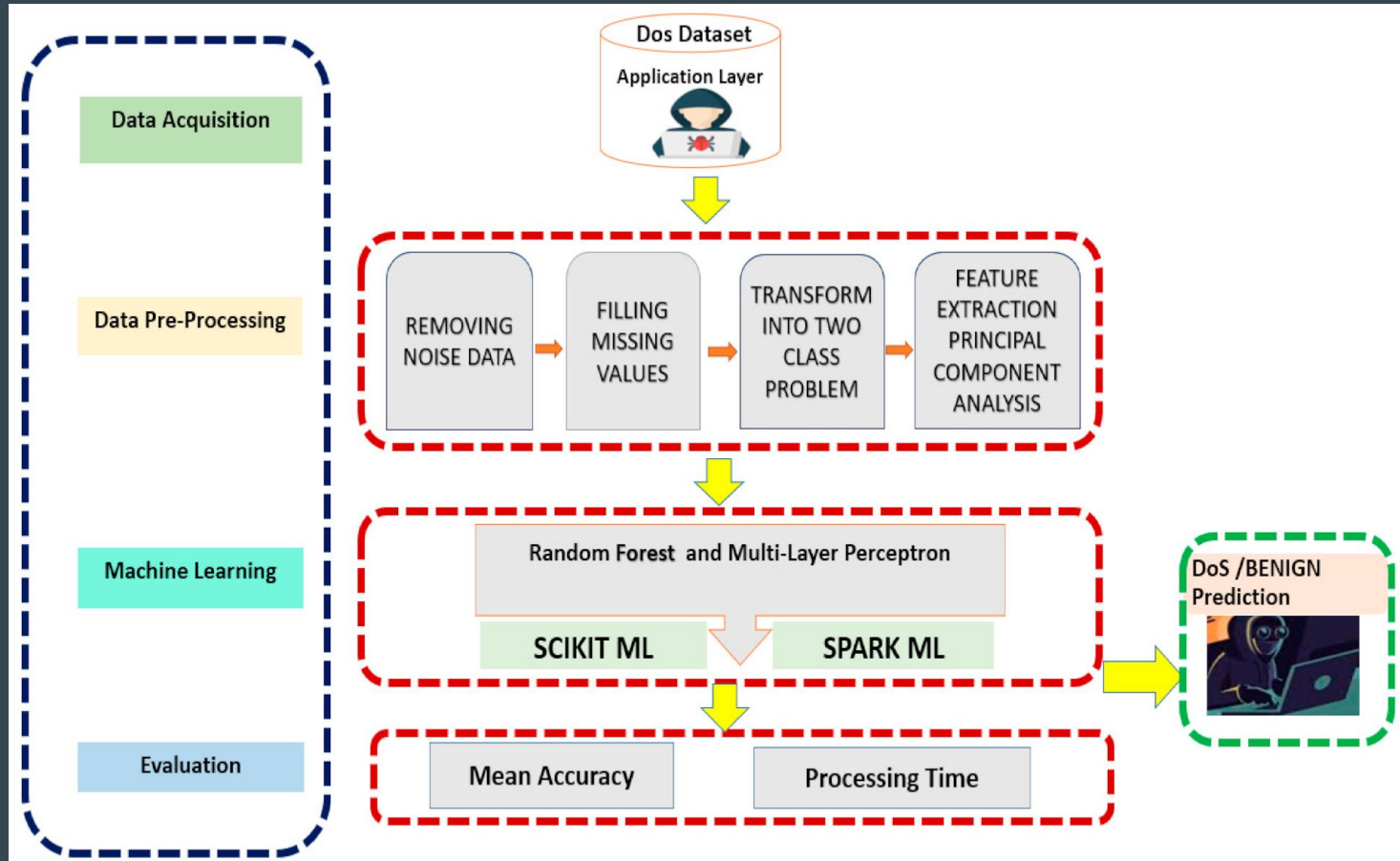
Anomaly-based

methods: These methods identify traffic patterns that deviate from normal baseline behavior. However, they can suffer from high false positive rates, meaning they may mistakenly identify normal traffic as an attack.

3

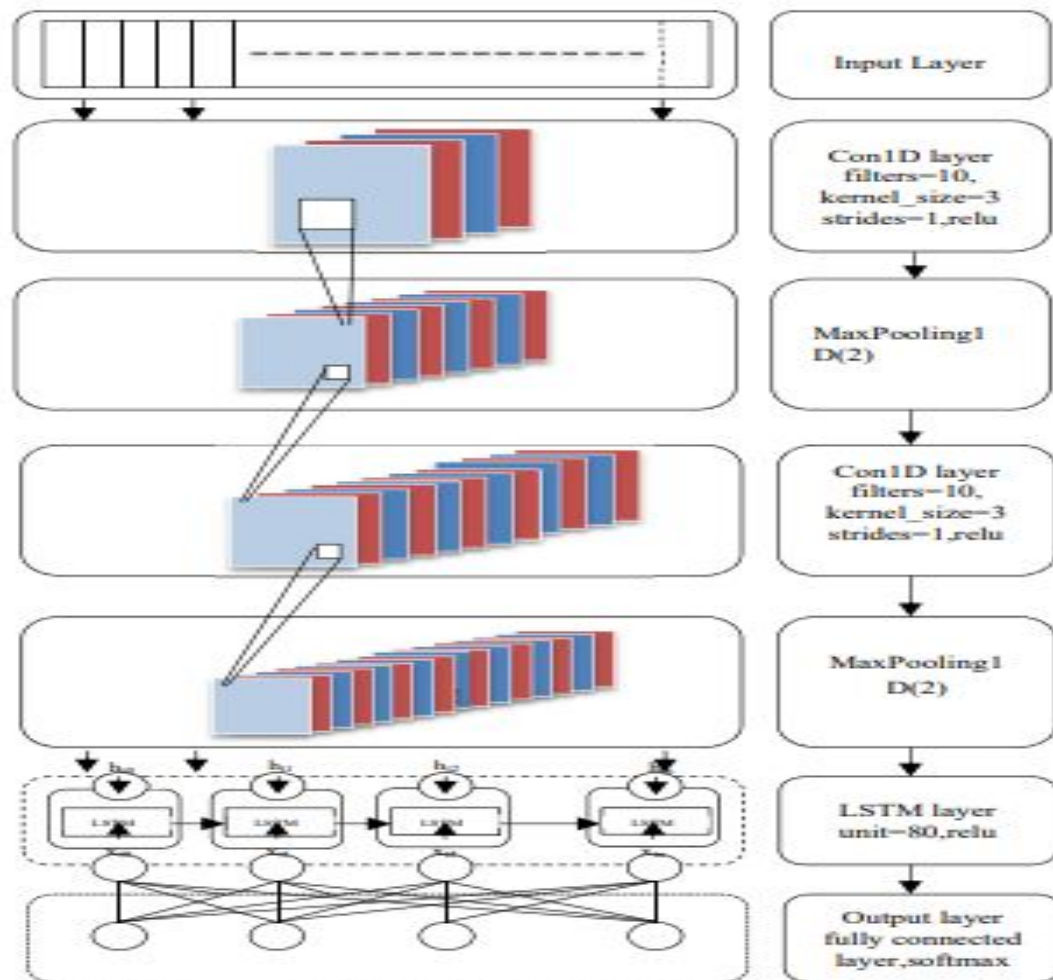
The proposed model was tested using the NSL-KDD dataset and achieved an impressive accuracy of 99.20%. This outperformed previous work and demonstrated the effectiveness of the deep learning approach in detecting DDoS attacks.

Block Diagram



Proposed Solution

- The research paper proposes a new deep learning classification method that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) for DDoS attack detection.
- CNNs are effective at extracting features from sequential data, such as network traffic data. They can identify patterns in the data that may be indicative of an attack.
- LSTMs are a type of recurrent neural network (RNN) that can learn long-term dependencies in data. This is important for DDoS attack detection, as attacks may unfold over time.
- The proposed model combines the strengths of CNNs and LSTMs to achieve high accuracy in DDoS attack detection. The model consists of seven layers:
 - An input layer that pre-processes the data.
 - A convolutional layer that extracts features from the data.
 - A max pooling layer that reduces the number of parameters and helps prevent overfitting.
 - These convolutional and max pooling layers are repeated to learn more complex features.
 - An LSTM layer that learns long-term dependencies in the data.
 - A fully connected layer that classifies the data as a DDoS attack or normal traffic.



Tools Used for Implementation

- Deep learning techniques:
 - Convolutional Neural Networks (CNNs)
 - Long Short-Term Memory (LSTM)
- The specific software libraries used for implementation may not be mentioned in the research paper, but common libraries for deep learning include TensorFlow, PyTorch, and Keras.

Result Analysis

- The research paper reports that the proposed CNN-LSTM model achieved an accuracy of 99.20% on a standard benchmark dataset for DDoS attack detection.
- This accuracy is higher than the accuracy achieved by other existing methods, such as CNN or LSTM used alone.

The suggested CNN's performance for each fold

<i>Fold</i>	<i>Accuracy</i>	<i>Precision</i>	<i>Recall</i>	<i>F1 score</i>
1	97.67	97.94	97.92	97.92
2	97.80	93.77	83.67	83.72
3	97.74	83.80	83.65	83.72
4	97.83	84.16	83.55	83.85
5	97.75	98.23	97.78	98.00
Mean	97.76	91.58	89.31	89.44
Median	97.75	93.77	83.67	83.85
Standard deviation	0.061	7.160	7.793	7.776

The suggested LSTM's performance for each fold

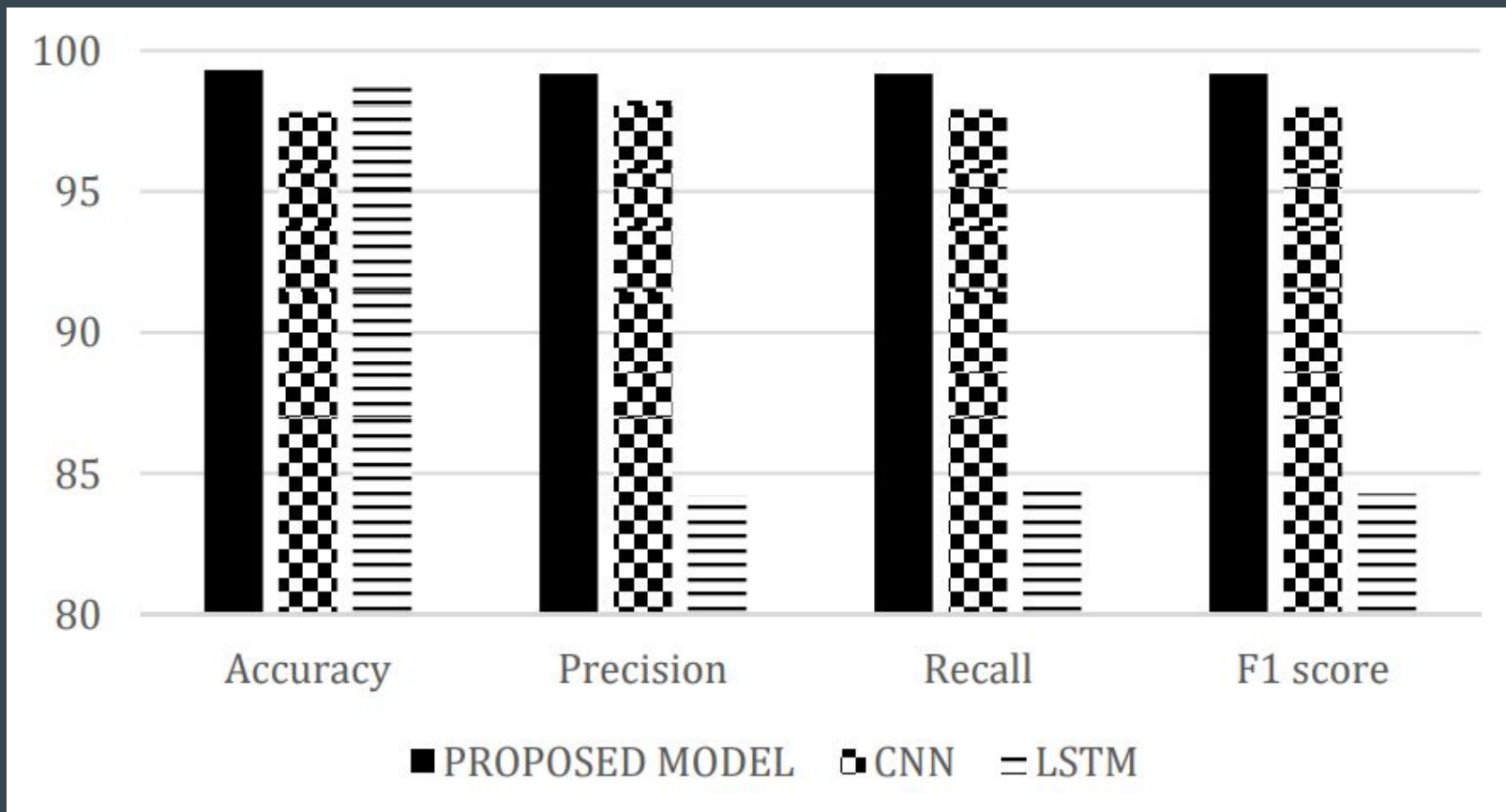
<i>Fold</i>	<i>Accuracy</i>	<i>Precision</i>	<i>Recall</i>	<i>F1 score</i>
1	97.55	83.12	81.30	82.17
2	98.57	83.87	83.66	83.75
3	98.23	79.19	83.91	81.10
4	98.97	84.19	84.39	84.28
5	92.93	67.38	59.96	61.95
Mean	97.25	79.55	78.64	78.65
Median	98.23	83.12	83.66	82.17
Standard deviation	2.471	7.092	10.513	9.421

Resultant tables

The suggested in the Proposed Model's performance for each fold

<i>Fold</i>	<i>Accuracy</i>	<i>Precision</i>	<i>Recall</i>	<i>F1 score</i>
1	99.21	92.01	99.10	94.36
2	99.31	99.18	99.18	99.18
3	99.11	99.03	98.99	99.01
4	99.19	84.75	84.78	84.77
5	99.20	84.71	84.79	84.75
Mean	99.20	91.94	93.37	92.41
Median	99.20	92.01	98.99	94.36
Standard deviation	0.071	7.188	7.835	7.250

The performance comparison between CNN, LSTM, and the proposed model based on mean



Advantages

- The proposed CNN-LSTM model offers several advantages over existing methods for DDoS attack detection:
 - **High accuracy:** The model achieves a high accuracy rate in detecting DDoS attacks.
 - **Improved detection of complex attacks:** The model can effectively detect complex DDoS attacks, including those that distribute traffic across multiple sources.
 - **Ability to learn from data:** The model can learn from new attack patterns and improve its detection accuracy over time.

Current Limitations

- The research paper does not explicitly discuss limitations of the proposed model. However, some potential limitations of deep learning models in general include:
 - **High computational cost:** Training deep learning models can require significant computational resources.
 - **Data dependency:** The performance of deep learning models depends on the quality and quantity of training data.
 - **Potential for overfitting:** Deep learning models can overfit to training data, leading to poor performance on unseen data.

Applications

- The proposed CNN-LSTM model can be used in a variety of real-world applications for DDoS attack detection, such as:
 - Protecting critical infrastructure, such as power grids and financial systems, from DDoS attacks.
 - Securing enterprise networks from DDoS attacks that can disrupt business operations.
 - Improving the security of cloud computing environments.

Conclusion

The research paper concludes that the proposed CNN-LSTM model represents a significant advancement in DDoS attack intrusion detection. By integrating the feature extraction capabilities of Convolutional Neural Networks (CNNs) with the long-term dependency learning of Long Short-Term Memory (LSTM) networks, the model demonstrates a high level of accuracy in identifying DDoS attacks, including complex ones with distributed traffic sources. This amalgamation addresses limitations observed in existing methods, particularly in detecting sophisticated attacks. Furthermore, the model's capacity to learn from data suggests potential adaptability to new attack patterns, thereby maintaining effectiveness over time. Overall, the CNN-LSTM hybrid model presents a promising avenue for enhancing DDoS attack detection and mitigating their impact on networks and systems.

Future Enhancement

- **Incorporate additional features:** The model currently focuses on network traffic data. It could be further improved by incorporating additional features, such as flow rate, packet size distribution, and destination IP addresses.
- **Explore transfer learning:** Transfer learning techniques could be used to leverage the model's capabilities for detecting other types of cyber attacks.
- **Investigate real-time detection:** The current research focuses on offline detection. Future work could explore adapting the model for real-time detection of DDoS attacks.
- **Test against adversarial attacks:** Adversarial machine learning techniques could be used to test the robustness of the model against attackers who try to evade detection.
- **Large-scale deployment:** The research evaluates the model on benchmark datasets. Future work could involve deploying the model in real-world network environments and evaluating its performance at scale.


The comparison of proposed model with many state-of-the-art approaches in term of accuracy

<i>No</i>	<i>Name</i>	<i>Year</i>	<i>Accuracy (%)</i>	<i>Technique</i>
1	Our proposed model	current	99.20	Proposed Hybrid Model
2	Yusof et al. [24]	2017	91.7	DCF + CSE
3	Kushwah and Ali [25]	2017	96.3	ANN + black hole optimization algorithm
4	Igbe et al. [26]	2017	98.6	DCA
5	Derakhsh et al. [27]	2018	82.44	GA
6	Hoon et al. [28]	2018	93.26	DRF
7	Idhammad et al. [29]	2018	98.23	semi-supervised

8	Anjum and Shreedhara [30]	2019	93.26	semi-supervised
9	Mukhametzyanov et al. [31]	2019	97.94	NN
10	Verma et al. [32]	2019	98.23	MAD+RF
11	Hosseini and Azizi [33]	2019	98.9	hybrid technique
12	Das et al. [15]	2019	99.1	Ensemble technique
13	Ma et al. [21]	2020	92.99	CNN
14	P.-K.-Y.[34]	2020	96.7	AIS
15	Bhardwaj et al. [35]	2020	98.43	AE+DNN
16	B. and S. [36]	2020	98.74	LVQ+DT

References

- [1] Bharot, N. et al.: DDoS Attack Detection and Clustering of Attacked and Non-attacked VMs Using SOM in Cloud Network. In: International Conference on Advances in Computing and Data Sciences. Springer, 2019, pp. 369-378
- [2] Baykara, M., Das, R.: A Novel Hybrid Approach for Detection of WebBased Attacks in Intrusion Detection Systems. International Journal of Computer Networks and Applications, 4(2), 2017, pp. 62-76
- [3] ISSA, Ahmed Sardar Ahmed, and Zafer ALBAYRAK. "CLSTMNet: A Deep Learning Model for Intrusion Detection." Journal of Physics: Conference Series. Vol. 1973, No. 1, IOP Publishing, 2021
- [4] Özalp, A. N et al.: Layer-based examination of cyber-attacks in IoT. International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2022, pp. 1-10
- [5] Hyder, H. K., Lung, C. H.: Closed-Loop DDoS Mitigation System in Software Defined Networks. DSC 2018 - 2018 IEEE Conf. Dependable Secur. Comput., 2019, pp. 1-6
- [6] Musotto, R., Wall, D. S.: More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. Trends Organ. Crime, 2020



THANK YOU