Journal of Harbin Engineering University Vol 44 No. 8
ISSN: 1006-7043 August 2023

Detection and Prevention of Combined Teardrop and Back Attack using SVM and Hybrid CLSTM Algorithm

Nishwas M.[1], Santosh Kumar B. J.[2]
[1]Department of Computer Science
Amrita Vishwa Vidyapeetham,School of computing,
Mysuru Campus, Karnataka, India
[2]Department of Computer Science
Amrita Vishwa Vidyapeetham,School of computing,
Mysuru Campus, Karnataka, India

Abstract— A significant danger to service providers is an Attack through DDoS, or distributed denial of service. This kind of hack bombards the target with too many malicious requests, seeking to interfere and prevent legitimate users from using services. Due to higher operations and financial costs, a DDoS assault causes significant economic loss for enterprises and service providers. Recently, to stop DDoS attacks, numerous methods like IDS and firewall are implemented but they failed to detect many network layer attacks such as teardrop and back attack that makes server unavailable for legitimate users. To overcome the issue this paper uses recent trending approaches like machine learning and deep learning defending mechanism for detection of attacks which can be then integrated to secure servers to protect from combined teardrop and back attack. The study uses and compares two approaches one from machine learning algorithm SVM and other one from hybrid deep learning algorithm CLSTM which is combination of CNN and CLSTM and validates which can perform well in DDOS attack detection. The KDD cup dataset is fed into two approaches the methods concentrate on important feature selection which contributes to attack detection and accurate detection. The ML algorithm SVM provided 73% accuracy and deep learning approach gives 98% accuracy which proves usage of hybrid deep learning is best mechanism for teardrop and back attack detection. For the detected attacks the responsive system is implemented to notify admin with an email and block IPs of attacker system and generate signature for an attack.

Keywords— DDoS, Teardrop and back attack, Hybrid deep learning, Network function virtualization

I. INTRODUCTION

The frequency of cyberattacks has considerably increased in recent years, and they now pose a severe risk to people and businesses alike. One of the most occurring cyber-attack is Distributed Denial of Service (DDoS) which included teardrop and back attack which occurs in network and physical layer and can have a devastating impact on online services and websites. During DDoS attacks, a target webpage or network is bombarded with a massive volume of traffic, causing it to become inaccessible to legitimate users and make server inaccessible to respond for user requests.

The teardrop attack targets the vulnerability of IP fragmentation method and crashes system and back attack aims to create invisible entry point and tries to get unauthorized access of system use those system as botnet to generate traffic and make server busy, these two combinations of attack These assaults are frequently conducted through a "botnet" is collection compromised equipment, which the attacker can remotely control. Therefore, to stop such assaults from happening, it is essential for individual's organizations to exercise vigilance and have strong security measures in place.

The impact of DDoS attacks can be severe, ranging from financial losses for businesses to denial of service for critical online services such as healthcare and emergency services. As such, there is a pressing need for effective DDoS detection and mitigation techniques to be developed and implemented. This paper aims to explore various methods for DDoS attack detection and mitigation, with an emphasis on machine learning-based approaches. By developing and evaluating these techniques, we aim to

contribute to the ongoing effort to combat cyber-attacks and protect online services from disruption.

The contribution of the proposed system in the field of security are highlighted below.

I. A comparative model between single ML algorithm and Hybrid deep learning algorithm which uses Support Vector Machines (SVM) and Hybrid Deep Learning Algorithms (CNN + LSTM) in classifying Teardrop and Back DDoS attacks.

II. What are the most important features and patterns that contribute to the accurate classification of Teardrop and Back DDoS attacks using machine learning algorithms.

III. Detection and prevention of combined attack into three classes Teardrop, Back, Normal and blocking the IP and generating signature for detected attack.

The paper is divided into following segments – The related works/literature survey has been defined in section II,the Methodology has been discussed in section III, Results Analysis is described in section IV, Result comparison is described in section V, Deployment and Prevention Technique is described in section VI and conclusion has been laid out in section VII.

II. LITERATURE SURVEY

There have been numerous studies on nevertheless; most have primarily concentrated on conventional or particular network environments. Defending versus distributed denial of service attacks using Machine learn techniques. Even some researches have highlighted outmoded attack types that don't apply to service providers nowadays or have solely examined cloud computing environments without discussing the ML approaches utilized. One study by Vishwakarma et al. [1] did discuss the application of machine learning (ML) methods in IoT and SDN to prevent DDoS attacks systems, although this was restricted to those two domains. The research only looked at published techniques and was restricted to the cloud environment. Osanaiye et al. [2] evaluated defense mechanisms for DDOS attack in the setting of secure cloud computing and offered many anomaly detection techniques that were published Like Salim et al. [3], this survey was restricted to the IoT environment and left out the various ways that ML is applied as a mitigation approach. Salim et al. looked at DDoS mitigation strategies with respect to IoT ecosystem and developed standards for putting into practice effective techniques to protect IoT devices from DDoS attack for various DDoS assaults. Security issues, DDoS attack strategies, and mitigation techniques that cloud & fog computing must address were investigated by Chaudhary and others [4] solutions for DDoS defense were examined in cloud & fog computing context. But the creators of the majority of the examined publications included in this article talked about outdated detection methods rather than employing ML strategies to counter DDoS attacks. It is crucial to remember that attackers are capable of carrying out several sorts of DDoS attacks, so designing and developing a defense against them shouldn't be constrained to a single attack type. Modern technologies are also used by many systems today because of their benefits, such as flexibility, scalability, & cost savings [5], [6]. a revolutionary deep learning algorithm by Haider et al [7]. DDoS attack detection model for convolutional neural networks. A benchmark dataset was used to verify the model, and it was compared to other approaches such as RNN, hybrid (RBM+SVM), SVM, & LSTM. The findings demonstrated demonstrating that the proposed model outperformed the competition with a 99.45% accuracy rate. In contrast, Elsayed, Dev, and Jurcut [8] thoroughly examined the drawbacks of the machine learning techniques DDoS assaults are currently being recognized in SDN systems. They examined four strategies: J48 surpassed the J48, Random Forest and Naive Bayes as the best method for detecting attacks in SDN systems. In a thorough analysis of 70 different DDoS attack detection & mitigation strategies, Singh and Behal [9] separated them into artificial neural network-based techniques, machine learning techniques, and other categories of information theory-based strategies, learning-based strategies, and other approaches. In addition to emphasizing the issues and research gaps in this area, the paper offered compelling solutions for researchers. In a different study, Sales et al. [10] created a smart detection system that classifies data utilizing the Random Forest Tree Algorithms. When the system's performance was tested, the researchers discovered

that it performed better than other systems that were already known to exist in the literature.

MACHINE LEARNING

Machine Learning, which falls under the umbrella of artificial intelligence, employs statistical models to generate predictions. It is distinguished in the computer's capacity to learn without human intervention and is frequently referred to as forecasting or predictive analytics explicit programming. The process involves utilizing algorithms to analyze historical or empirical data and produce outputs based on the analysis. Some approaches involve working with "training data" to improve the algorithms' performance over time by learning and predicting.

DEEP LEARNING

Deep learning, which uses neural networks with many layers, tries to analyze and replicate the activity of the human brain by analyzing and learning from enormous volumes of data. The accuracy of predictions made by a neural network with just one layer can be improved by adding hidden layers. Deep learning enables automation and the completion of analytical and physical activities without the need for human intervention, making it a crucial component of many AI systems and services. Deep learning technology is used in both standard products and services like digital assistants, voice-activated TV remote controls, including detection of credit card fraud as well as cutting-edge innovations like self-driving cars.

Machine learning vs. Deep Learning

To produce predictions, machine learning algorithms utilize structured, labeled data. This indicates that particular features are characterized from the model's input data and arranged in tables. However, by preliminary processing it to put it into an organized style, machine learning may also employ unorganized information such as text & photos. Deep learning algorithms, on the other hand, can process unstructured information without the requirement for pre-processing, simplifying feature extraction, and lowering reliance on human specialists. For instance, a deep learning algorithm can categorize different pets based on their distinguishing features, such as their ears. The order of features in machine learning is manually defined by a human expert.

Models for machine learning & deep learning can do learning under supervision, unsupervised learning, as well as reinforcement learning, among other types of learning. Labeled datasets are necessary for supervised learning in order to classify or predict, while unsupervised learning detects patterns in the data without the need for labeled datasets. Reinforcement learning involves a model that improves its accuracy for carrying out a task in a setting based on user feedback so as to optimize the reward.

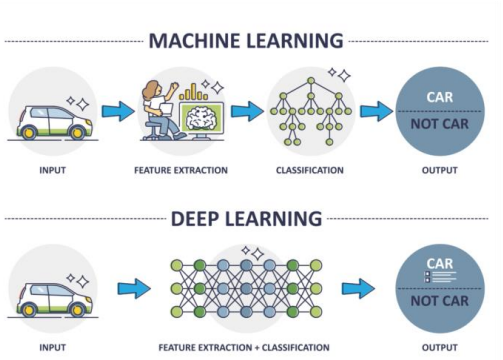

Figure 1: Machine learning vs. Deep Learning

III. METHODOLOGY

The proposed Method made an experiment on how efficient ML and deep learning models are in detecting DDOS attacks. The methodology is divided into two models one is based on Machine learning algorithm SVC which comes under SVM and the other one is CLSTM which is combination of CNN, the experiment analyzes the effect of using ML and Deep Learning algorithms for detection of combined teardrop ana back attack, the aim of the model is to do experiment on testing the efficiency of ML and deep learning models for combined teardrop and back attack detection and deploy the best model to detect attacks.

Building efficient algorithm for Teardrop and Back attack detection consists of five main modules Preprocessing, Feature selection, Model development and Model evaluation by considering which models are evaluated and deployment of efficient model to achieve secure system, for the

prevention method attack IP notification, hash code generation and blocking mechanism is implemented.

A. Feature Selection

while building model research difficulty lies in feature selection which can affect accuracy of model due to the presence of irrelevant and redundant attributes. The dataset used is KDD cup dataset for DDOs attacks, to overcome that issue, we are using one of the ensembled machine learning algorithm called Extra Tree Classifier which uses decision trees and trained by using AutoML tool, using this model the algorithm achieves reduction in bias and most relevant features are selected. This method achieves selection of features from 42 to 26 relevant features based on feature importance score the selected features are ranked according to feature relevance importance, the rank and score is visualized in below line plot.

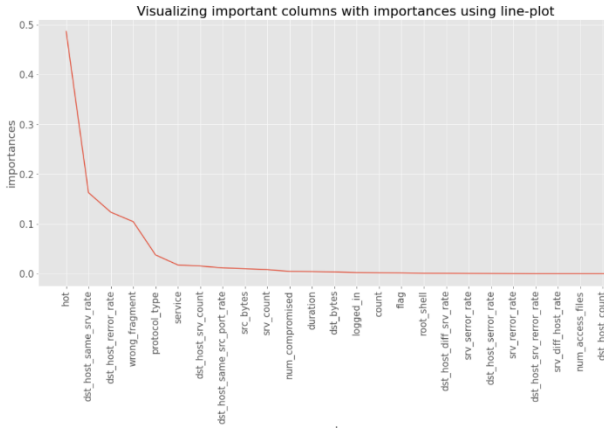

Figure 2: Visualization of important features from dataset

B. Model Development

The model development has two proposed models from ML and deep learning which are SVC and hybrid Conv.LSTM deep learning algorithms using which efficiency of ML and deep learning model for DDOS attack detection is analyzed.

The first model is SVC which comes under Support Vector Machine (SVM)

a. Support Vector Classifier

Support Vector Classifier (SVC) is a well-liked machine learning method applied to categorization challenges. This model of supervised learning analyzes data and classifies it into two or more classes. The SVC algorithm uses a hyperplane to divide the various classes and increase their margin of separation. It works by identifying the optimal decision boundary that distinguishes between the classes with the greatest margin, where this margin is the separation between that decision boundary & the nearest data points for each class.

SVC is a powerful algorithm for dealing with complex datasets, because it can handle high-dimensional feature spaces and non-linear data. It is also known for its ability to handle large datasets efficiently, thanks to the use of the kernel trick, which allows it to project the data into a higher-dimensional without really figuring out each point's coordinates in that space. However, SVC can be sensitive to the choice of kernel function and regularization parameters, which can affect its performance.

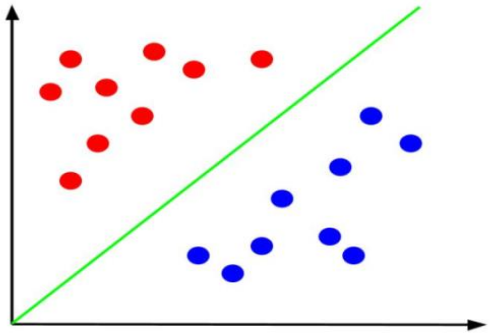

Figure 3: Architecture of Support Vector Classifier

The first model developed is using ML algorithm Support Vector Classifier where the data is preprocessed to remove null, redundant data, for the filtration of irrelevant feature Extra Tree Classifier is used then the model is trained and tested with data to predict data into three classes Teardrop, Back and Normal classes where the model achieved overall 73% accuracy.

The second proposed model is using hybrid CNN-LSTM

b. Convolution Long Short-Term Memory

Convolutional Long Short-Term Memory (ConvLSTM) networks combine the temporal learning of LSTM networks with the spatial training of convolutional neural networks (CNNs). Serial information processing is done using ConvLSTM such as videos and satellite images, which have both temporal and spatial dependencies. ConvLSTM is an extension of the standard LSTM network, which has been widely used for processing sequential data. LSTM networks use a memory cell to store information about past inputs and use gates to regulate the information flow into and out of the cell. However, LSTM networks are designed to process one-dimensional sequential data, such as text, and cannot easily handle spatial data, such as images. ConvLSTM introduces convolutional operations to the LSTM network to enable it to handle spatial data. It replaces the matrix multiplication operation in the LSTM cell with a convolutional operation, allowing the network to learn spatial features from the input data. The convolutional operation is performed in both the state-to-state and input-to-state transitions, allowing the network to capture both spatial and temporal dependencies. ConvLSTM has been successfully used in various applications, such as video processing, weather forecasting, and motion analysis. It has shown to be effective in capturing complex spatial and temporal patterns in data, and can handle variable-length sequences of inputs. However, ConvLSTM is a complex model that requires significant computational resources and large amounts of training data.

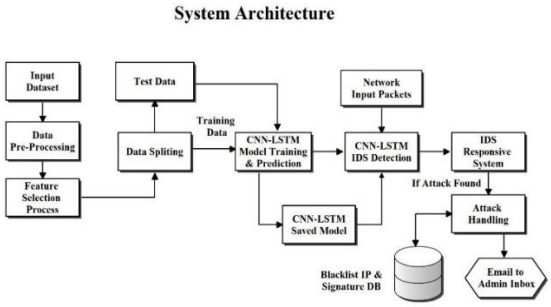

Figure 4: Architecture of Convolutional Long Short-Term Memory

The dataset used is KDD cup dataset for DDOS attack detection, the model is preprocessed to remove all null and redundant values and the main important features are fetched using Extra Tree Classifier is fed into CLSTM model where data is divided into test data and train data and model is trained using CLSTM algorithm. Then the model is integrated into system for CNN-LSTM IDS detection after that the detected attacks will be handled by IDS responsive system for attack handling and admin will be notified with attack detection.

IV. RESULT ANALYSIS

The experimental result of ML and deep learning models are discussed in this section.

A. Classification Report for SVM

	precision	Recall	f1 Score	Support
Normal	**0.61**	**0.36**	**0.46**	**207**
Back	**0.62**	**0.82**	**0.71**	**263**
Teardrop	**1.00**	**1.00**	**1.00**	**181**
Macro avg	**0.75**	**0.73**	**0.72**	**651**
Weighted avg	**0.72**	**0.73**	**0.71**	**651**
Overall Accuracy	**73**			**651**

Table 1: Classification Report - Support Vector Classifier

The report shows how well a classification model performs on a dataset with three classes: normal, back, and teardrop. The precision for normal is 0.61, indicating that 61% of the instances classified as normal are actually normal. The recall for normal is 0.36, meaning that the model correctly identifies 36% of the normal instances. For back, the precision is 0.62, indicating that 62% of the instances classified as back are actually back, the model correctly recognizes

82% of back instances, according to the recall of 0.82. For teardrop, the precision and recall are both 1.00, meaning that the model correctly identifies all instances of this class. The overall accuracy of the model is 0.73, indicating that 73% of the instances in the dataset are correctly classified. The macro average F1-score, this equals 0.72 for the recall and precision harmonic mean. 0.71 is the weighted average F1 score. Taking into account the class imbalance in the dataset.

Confusion Matrix- SVM

A table called the matrix of confusion is used to assess the effectiveness of categorization models. The total amount of correct and incorrect guesses for each class is listed. The four categories are true positives, fake positives, true negatives, & fake negatives. Where the matrix's rows show the actual class labels, and the columns display predicted class labels. The values on the diagonal are correct predictions, while off-diagonal values are incorrect predictions. The confusion matrix provides crucial information about the model's the variables memory, accuracy, precision, and F1 score, which calculated using its values.

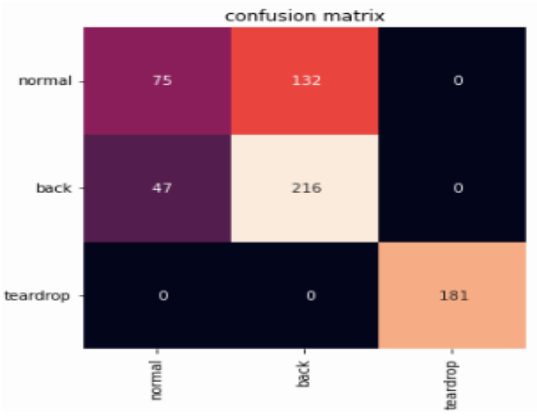

Figure 5: Confusion Matrix - Support Vector Classifier

B. *Classification report for CLSTM*

	precision	Recall	f1 Score	Support
Normal	**1.00**	**0.93**	**0.96**	**207**
back	**0.95**	**1.00**	**0.97**	**263**
teardrop	**1.00**	**1.00**	**1.00**	**181**
Macro avg	**0.98**	**0.98**	**0.98**	**651**
Weighted avg	**0.98**	**0.98**	**0.98**	**651**
Overall Accuracy	**0.98**			**651**

Table 2: Classification report- Convolutional Long Short-Term Memory

The table 2 represents the performance of a classification model that has been trained on a dataset containing three classes: normal, back, and teardrop. The precision of the model indicates that it is very good at predicting the correct class for each label, with an overall accuracy of 98%. The recall of the model is high for all classes, with a F1-score of 0.96, 0.97 and 1.00 for normal, back and teardrop, respectively. In conclusion, the model has a high accuracy and is performing well in predicting all three classes

Confusion Matrix – CLSTM

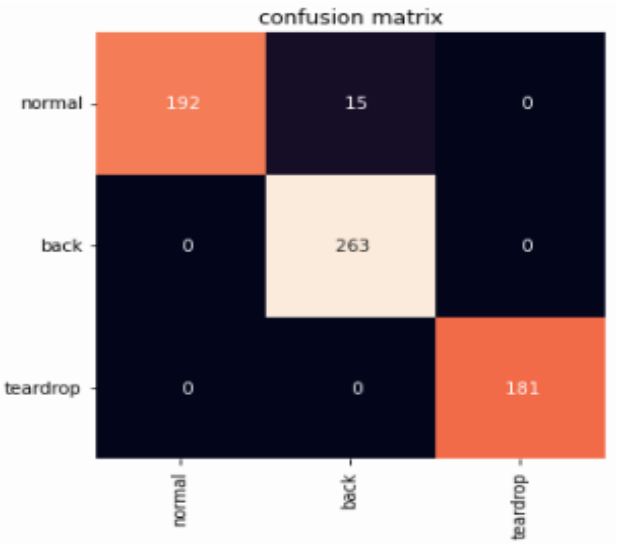

Figure 6: Confusion Matrix - Convolutional Long Short-Term Memory

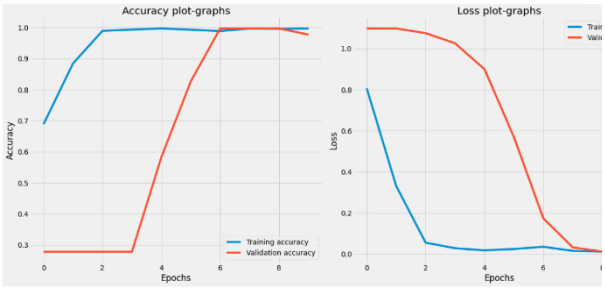

Figure 7: Accuracy and Loss plot graph of CLSTM of 10 Epochs

V. RESULT COMPARISON

The comparison of ML and deep learning models which are SVM and CLSTM are discussed in this section

Sl.no	Model	Precision	Recall	F1 Score	Accuracy
1	SVM	0.75	0.73	0.72	0.73
2	CLSTM	0.98	0.98	0.98	0.98

Table 3: Comparison of models

The accuracy of the SVC model recorded 0.75, the recall recorded 0.73, the F1 score was 0.72, and the precision got was 0.73. On the other hand, the CLSTM model has a precision value of 0.98, a recall score of 0.98, an F1 score of 0.98, and a precision score of 0.98. The results show that the CLSTM model outperforms the SVC model in all analysis parameters. The CLSTM model is a better model for a given task because it is more accurate and reliable than the SVC model.

VI. MODEL DEPLOYMENT AND PREVENTION

Once the model is developed and result of methods are compared, we got Conv.LSTM works better than SVM so model is deployed using CLSTM algorithm and for prevention method the model will block the IPs of teardrop and back attack and prevent it from sending further request to network, In the next step of prevention the model will generate Hash Code for detected attacks which helps in enhanced attack detection and prevention.

Figure 8: Responsive Intrusion System Website-List of all clients

Figure 9: Responsive Intrusion System Website-List of detected and blocked clients

The figure 8 and 9 represents responsive intrusion system where details of detected attacks from model will be recorded and prevented and those details will be further used for network security.

VII. CONCLUSION

DDoS such as teardrop and back attack can have a severe negative effect on Internet service providers and businesses, leading to huge financial losses. As a result, machine learning (ML) and hybrid deep learning methods are more frequently utilized to create clever, intelligent systems that can resist these attacks. The comparative results of the two models considered in this study, SVM and CLSTM, the CLSTM model performs very well across a number of criteria with accuracy of 98%, which includes recall, precision, F1 score, & accuracy. outperforms the SVM model on upon all these dimensions, and makes it a fine model for the work of this that conveys message of deep learning algorithm are best for DDOS attack detection and hybridization of deep learning algorithms can give best accuracy in detection. The report also makes a number of recommendations for future study to

assist the research community in creating efficient security systems that can fend off various DDoS attacks. Overall, it is essential to continue researching and developing new and innovative techniques to combat the ever-evolving threat of DDoS attacks.

The future scope of this project is to train a model with other most occurring DDOS attack types and integrate this model in hardware to implement the model in real time PCs.

REFERENCES

1. R. Vishwakarma and A. K. Jain, ‘‘A survey of DDoS attacking techniques and defense mechanisms in the IoT network,’’ Telecommand. Syst., vol. 73, no. 1, pp. 3–25, Jul. 2019.
2. O. Osanaiye, K.-K.-R. Choo, and M. Dlodlo, ‘‘Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework,’’ J. Netw. Compute. Appl., vol. 67, pp. 147–165, May 2016
3. M. M. Salim, S. Rathore, and J. H. Park, ‘‘Distributed denial of service attacks and its defenses in IoT: A survey,’’ J. Supercomput., vol. 76, no. 7, pp. 5320–5363, Jul. 2020, Doi: 10.1007/s11227-019-02945-z
4. D. Chaudhary, K. Bhushan, and B. B. Gupta, ‘‘Survey on DDoS attacks and defense mechanisms in cloud and fog computing,’’ Int. J. E-Services Mobile Appl., vol. 10, no. 3, pp. 61–83, Jul. 2018
5. T. Alharbi, A. AL Juhani, and H. Liu, ‘‘Holistic DDoS mitigation using NFV,’’ in Proc. IEEE 7th Annu. Compute. Commune. Workshop Conf. (CCWC), Las Vegas, NV, USA, Jan. 2017, pp. 1–4, Doi: 10.1109/CCWC.2017.7868480.
6. T. Alharbi, A. AL Juhani, H. Liu, and C. Hu, ‘‘Smart and lightweight DDoS detection using NFV,’’ in Proc. Int. Conf. Compute Data Anal. (ICCDA), Lakeland, FL, USA, 2017, pp. 220–227.
7. S. Haider et al., “A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks,” IEEE Access, vol. 8, pp. 53972– 53983, 2020.
8. M. S. Elsayed, S. Dev, and A. D. Jurcut, “Machine Learning Techniques for Detecting Attacks in SDN,” arXiv preprint arXiv: 1910.00817, 2019.
9. J. Singh and S. Behal, “Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions,” Computer Science Review, vol. 37, p. 100279, 2020.
10. F. Sales et al., “Smart Detection: An Online Approach for DoS / DDoS Attack Detection Using Machine Learning,” Security and Communication Networks, vol. 2019, 2019.
11. Acharya, A. A., Arpitha, K. M., & Kumar, B. S. (2016). An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in MANET. *International Journal of Engineering and Technology (IJET)*, *8*(2).
12. Kumar, B. S., & Sinha, S. (2022, June). An Intrusion Detection and Prevention System against DOS Attacks for Internet-Integrated WSN. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 793-797). IEEE.
13. Kumar, B. S., & Gowda, V. S. (2022, July). Detection and Prevention of UDP Reflection Amplification Attack in WSN Using Cumulative Sum Algorithm. In *2022 IEEE International Conference on Data Science and Information System (ICDSIS)* (pp. 1-5). IEEE.
14. Sreelakshmi, K., Anand, S., & Sinha, S. (2019). Black hole attack in mobile ad hoc network–analysis and detection. *IJRTE Access*, *7*.
15. Kumar, B. S., & Gowda, V. S. (2022, July). Detection and Prevention of UDP Reflection Amplification Attack in WSN Using Cumulative Sum Algorithm. In *2022 IEEE International Conference on Data Science and Information System (ICDSIS)* (pp. 1-5). IEEE.
16. Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017, June). Enhanced cloud data security using AES algorithm. In *2017 International Conference on Intelligent Computing and Control (I2C2)* (pp. 1-5). IEEE.
17. Lakshmi, H. N., Anand, S., & Sinha, S. (2019). Flooding attack in wireless sensor network-analysis and prevention. *International Journal of Engineering and Advanced Technology*, *8*(5), 1792-1796.
18. Kumar, S., & Sinha, S. (2022, September). Machine Learning based Robust Techniques to Detect DDoS Attacks in WSN. In *2022 International Conference on Intelligent*

Innovations in Engineering and Technology (ICIIET) (pp. 294-300). IEEE.

19. R. Abhijith and B. J. Santhosh Kumar, "First Level Security System for Intrusion Detection and Prevention in LAN," *2021 2nd International Conference for Emerging Technology (INCET)*, Belagavi, India, 2021, pp. 1-5, Doi: 10.1109/INCET51464.2021.9456259.
20. Sinha, S. (2021, July). Impact of DoS attack in IoT system and identifying the attacker location for interference attacks. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)* (pp. 657-662). IEEE.
21. Madhav, A., & Akhil, K. M. (2022, September). RSSI based Localization and Evaluation using Support Vector Machine. In *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 509-515). IEEE.