[ICAETBM-2024]
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Detection of DDoS Attack Using ML

Prof. Vivek Nagargoje, Vaibhav Patil, Giri Anant, Sandesh Sabale, Sumit Kekan
Dept. Of Information Technology Nutan Maharashtra Institude of Engineering and Technology, Pune, India

ABSTRACT
This paper explores the field of detecting Distributed Denial of Service (DDoS) attacks, which is an essential component of network security in the current digital environment. With the proliferation of sophisticated cyber threats, there is a pressing requirement for robust detection mechanisms to safeguard network infrastructures. This study examines the effectiveness of machine learning techniques, specifically K-Nearest Neighbours (KNN) and Support Vector Machines (SVM), in detecting DDoS attacks amidst the vast amount of network traffic. By meticulously analyzing datasets encompassing vital features such as IP Length, Time-To-Live (TTL), Protocol, TCP Source/Destination Ports, Length, and Window Size, we unveil the potential of these algorithms in discerning malicious traffic patterns. Through rigorous model training and evaluation, our results underscore the accuracy and reliability of KNN and SVM in detecting DDoS attacks, thus bolstering network security measures. Furthermore, we showcase the deployment of trained models within a Flask application framework, enabling real-time detection and mitigation of potential threats. The paper itself acts as a testament to the efficacy of machine learning in fortifying network defenses against DDoS attacks, paving the way for enhanced cybersecurity paradigms in the digital age.

keywords - Distributed Denial of Service (DDoS) attacks, network security, machine learning, K-Nearest Neighbors (KNN), Support Vector Machines (SVM), feature analysis, model training, Flask application, cybersecurity

I. INTRODUCTION

The stability and security of network infrastructures around the world are being threatened by the increase in Distributed Denial of Service (DDoS) assaults[4,5]. DDoS attacks aim to prevent authorised users from accessing the target system by flooding it with traffic, so disrupting the regular operation of online services[6,7]. These attacks can result in severe financial losses, damage to reputation, and potential data breaches for the targeted organizations[8].

In response to the growing threat of DDoS attacks, the development of effective detection and mitigation strategies has become paramount[9]. Conventional DDoS detection techniques, such signature-based and rule-based systems, frequently find it difficult to keep up with the attackers' constantly changing strategies[10]. A potential substitute is provided by machine learning (ML) algorithms, which use data-driven methods to identify unusual network activity that could be a sign of DDoS attacks[11,12].

This paper presents a comprehensive study on the application of ML algorithms, specifically K-Nearest Neighbors (KNN) and Support Vector Machines (SVM), for the detection of DDoS attacks. These algorithms were chosen because they can analyse network traffic

Copyright © 2024 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)**

data and identify patterns that indicate malicious activity. By training on labeled datasets containing both normal and attack traffic, KNN and SVM models can learn to distinguish between benign and malicious network behavior.

An overview of DDoS assaults and their effects on network infrastructure is given at the outset of the paper. It then delves into the fundamentals of KNN and SVM algorithms, explaining their principles of operation and suitability for DDoS detection tasks. The dataset used for training and evaluation purposes is described, highlighting the importance of feature selection and preprocessing techniques in preparing the data for model training.

Next, the paper discusses the implementation of KNN and SVM models within a Flask application, allowing for real-time DDoS detection and prediction. The system architecture and workflow are presented, detailing the steps involved in data collection, preprocessing, model training, and inference. Additionally, the paper explores the performance metrics used to evaluate the effectiveness of the models, including accuracy, precision, recall, and F1-score.

Finally, the paper concludes with a discussion on the strengths and limitations of KNN and SVM algorithms for DDoS detection, along with future research directions in this field. Overall, this study provides valuable insights into the application of ML techniques for enhancing network security and mitigating the impact of DDoS attacks on critical infrastructure.

II. LITERATURE REVIEW

Paper 1: DDoS Simulation: Empowering Targets through Simulated Attacks

Alternate Name: Understanding DDoS Attacks through Simulation

Description:

In order to improve potential targets' readiness for DDoS attacks, this research paper presents the idea of a DDoS simulation platform. The gateway, as demonstrated by ddos attack. Online, serves as a platform for simulating DDoS attacks and providing insightful information to aid targeted in realising their limitations and develop effective mitigation strategies. The study examines Layer 7 attacks, describes how the simulation portal was created and used, and talks about intentions to add Layer 4 attacks and increase the number of attack sites in the future. By leveraging simulated attacks, this approach aims to empower organizations to proactively defend against DDoS threats and minimize the impact of potential attacks on their online services.

Paper 2: A Comprehensive Survey of DDoS Attacks: Evolution, Mitigation, and Emerging Trends

Alternate Name: Exploring DDoS Landscape: Evolution and Mitigation Strategies

Description:

This survey paper provides a comprehensive overview of Distributed Denial of Service (DDoS) attacks, addressing their evolution, mitigation strategies, and emerging trends. It offers insights into the growing threat landscape of DDoS attacks, emphasizing their impact on the availability and integrity of online services. The paper discusses various types of DDoS attacks and presents recommendations for mitigating these threats. The study summarises past studies and highlights their flaws, making it a valuable resource for scholars and practitioners who seek to understand and address the challenges posed by DDoS attacks. It emphasises how crucial it is to continue researching and innovating in order to create efficient defences against DDoS attacks that are always changing.

Paper 3: Analysis of DDoS Attacks on IoT Architecture

Alternate Name: Understanding DDoS Threats in IoT Networks

Description:

The classification of Distributed Denial of Service (DDoS) attacks in the context of Internet of Things (IoT) architecture is the main topic of this research study. By

examining attacks across different layers of the IoT architecture and analyzing their operational mechanisms and execution tools the study attempts to close knowledge gaps in the literature and offer guidance for developing strong defenses against DDoS assaults against IoT devices. The paper's findings contribute to enhancing understanding of DDoS threats in IoT environments and offer recommendations for bolstering security defenses. Through a thorough examination of attack characteristics and defense strategies, the paper sheds light on the evolving landscape of DDoS attacks on IoT architecture and highlights the need for proactive defense mechanisms to safeguard IoT ecosystems.

Paper 4: A Simulation-based Analysis Study for DDoS Attacks on Computer Networks

Alternate Name: Exploring DDoS Attack Scenarios through Simulation

Description:

This research paper delves into the realm of Denial of Service (DoS) attacks, particularly focusing on Distributed Denial of Service (DDoS) attacks, can flood the target with an excessive number of bogus requests, causing disruptions to system operations. The paper elucidates the fundamental principles underlying DDoS attacks and provides insights into their operational mechanics. Through the utilization of simulation tools, specifically OPNET, the paper constructs practical models simulating DDoS attacks over various Internet protocols such as VoIP, FTP, and HTTP. By conducting experiments across different scenarios, the paper unveils the effects of DDoS attacks on network performance and evaluates the efficacy of firewall configurations in mitigating these attacks. The findings underscore the importance of proactive defense measures and the role of simulations in understanding and combating DDoS threats in computer networks.

Paper 5: Enhancing Resilience against DDoS Attacks in SDN-based Supply Chain Networks Using Machine Learning

Alternate Name: Machine Learning-driven Resilience in SDN-enabled Supply Chains against DDoS Attacks

Description:

This paper explores the vulnerability of supply chain networks to Distributed Denial of Service (DDoS) attacks and proposes a novel approach leveraging Software-Defined Networking (SDN) and machine learning to bolster their resilience against such threats. Due to the way they connect, supply chain networks are vulnerable to DDoS attacks, which could disrupt operations and result in large financial losses. SDN offers a centralized control mechanism that enables dynamic traffic rerouting, which can enhance the network's ability to withstand DDoS attacks. By integrating machine learning techniques for DDoS attack detection and mitigation within an SDN framework, the paper aims to improve the effectiveness of defense mechanisms. Through empirical evaluation, the paper assesses the performance and efficacy of these techniques, shedding light on their potential to strengthen the security posture of supply chain networks in the face of evolving DDoS threats

Paper 6: A Review of DDoS Attack Detection and Prevention Mechanisms in Clouds

Alternate Name: Examining DDoS Defense Strategies for Cloud Environments

Description:

This paper presents a comprehensive review of Distributed Denial of Service (DDoS) attack detection and prevention mechanisms tailored for cloud computing environments. With the widespread adoption of cloud services, ensuring their resilience against DDoS attacks is paramount to maintaining service availability and integrity. The paper systematically analyzes various strategies employed to detect, prevent, and mitigate DDoS attacks in cloud

environments, providing insights into their strengths, limitations, and suitability for different deployment scenarios. By synthesizing existing research findings and identifying gaps in current approaches, the paper offers valuable guidance for researchers and practitioners seeking to bolster the security of cloud-based infrastructures against DDoS threats. Through a critical examination of the state-of-the-art in DDoS defense mechanisms, the paper contributes to advancing the field of cybersecurity in cloud computing and lays the groundwork for future research endeavors aimed at enhancing DDoS resilience in cloud environments.

Paper 7: Challenges of DDoS Attack Mitigation in IoT Devices by Software Defined Networking (SDN)

Alternate Name: Addressing DDoS Vulnerabilities in IoT Devices through SDN

Description:

In this paper, the authors delve into the pressing issue of Distributed Denial of Service (DDoS) attacks targeting Internet of Things (IoT) devices and explore potential mitigation strategies leveraging Software Defined Networking (SDN). As IoT deployment continues to proliferate, the security of connected devices becomes increasingly critical, with DDoS attacks posing a significant threat to their availability and integrity. The paper identifies the unique challenges associated with mitigating DDoS attacks in IoT environments and proposes the use of SDN as a viable approach to enhance security defenses. By centralizing network control and enabling dynamic traffic management, SDN offers promise in mitigating DDoS threats while preserving the lightweight nature of IoT devices. The authors evaluate existing DDoS mitigation techniques and their applicability to SDN-based IoT architectures, highlighting the need for adaptive decision-making and continuous monitoring to thwart evolving DDoS attack vectors. Through a comprehensive analysis of the security implications and challenges inherent in securing IoT devices against DDoS attacks, the paper contributes valuable insights to the field of IoT security and lays the groundwork for future research in this area.

Paper 8: A Secured Botnet Prevention Mechanism for HTTP Flooding Based DDoS Attack

Description:

This paper focuses on addressing the threat posed by HTTP flooding-based Distributed Denial of Service (DDoS) attacks, which inundate target servers with illegitimate HTTP requests, thereby disrupting network operations. The authors highlight the vulnerability of computer network-connected devices to such attacks and propose a novel botnet prevention mechanism to bolster network security. By integrating invisible challenge and Resource Request Rate algorithms into the application layer, the proposed mechanism aims to mitigate HTTP flooding-based DDoS attacks while allowing genuine incoming traffic to reach the server. The paper emphasizes the importance of proactive measures to prevent DDoS attacks, particularly in light of the growing prevalence of such attacks and their detrimental impact on network availability and resources. Through simulation-based analysis and experimentation, the authors demonstrate the effectiveness of the proposed botnet prevention mechanism in safeguarding against HTTP flooding-based DDoS attacks, offering a promising solution for enhancing network resilience and mitigating the financial and operational repercussions of DDoS incidents.

Paper 9: Detection and Mitigation of Low and Slow DDoS attack in an SDN environment

Abstract:

Attacks such as Distributed Denial of Service (DDoS) attempt to interfere with network activities by overloading target servers with packets or by using vulnerabilities to deplete resources. While volume-based DDoS attacks are relatively easy to detect due to abnormal packet flow, low and slow DDoS attacks pose a significant challenge as they maintain connections for extended periods, mimicking genuine traffic. In this

research, a method for identifying and countering the low-latency DDoS assault known as Slowloris in an SDN context is proposed. The suggested remedy entails data analysis and the identification of low- and slow-traffic DDoS attack patterns through communication between the SDN controller and the detection and mitigation module. By leveraging the centralized control mechanism of SDN, the solution aims to enhance the network's resilience against low and slow DDoS attacks, thereby mitigating their impact on network availability and performance. Through experimental validation and analysis, the paper demonstrates the effectiveness of the proposed approach in detecting and mitigating low and slow DDoS attacks, offering valuable insights for strengthening network security in SDN environments.

Paper 10: Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain.

Abstract:

With the rapid advancement of blockchain technology, securing blockchain networks against Distributed Denial of Service (DDoS) attacks has become increasingly critical. Traditional DDoS detection and defense mechanisms are primarily centralized, posing limitations in effectively combating DDoS attacks in blockchain networks. This research presents a unique lightweight DDoS assault detection technique based on heterogeneous ensemble learning in blockchain networks called Anti-D chain, to address this difficulty. The Anti-D chain leverages a distributed and decentralized approach, incorporating heterogeneous ensemble learning strategies such as AdaBoost and Random Forest. Lightweight classifiers like CART and ID3 are integrated into the ensemble learning algorithm to enhance the detection accuracy and robustness against DDoS attacks. By harnessing the power of blockchain technology and ensemble learning, the Anti-D chain offers a scalable and effective solution for accurately identifying DDoS attack patterns in peer-to-peer (P2P) networks. Experimental results demonstrate the superior performance of the proposed detection method in terms of precision, recall, F-score, true positive rate, false positive rate, and ROC curve analysis, highlighting its potential for bolstering DDoS defense mechanisms in blockchain networks.

III. ARCHITECTURE

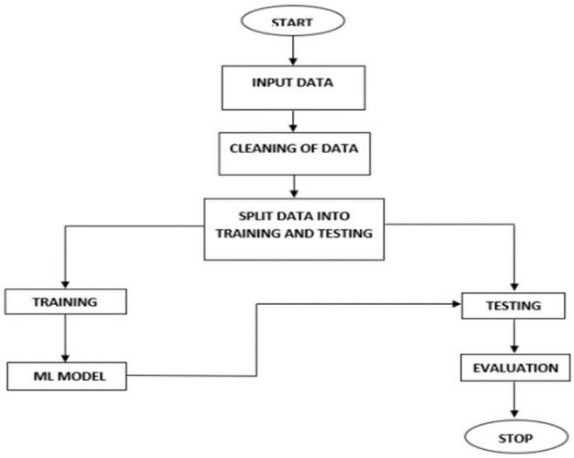

Fig: architecture

I. ER DIGRAM

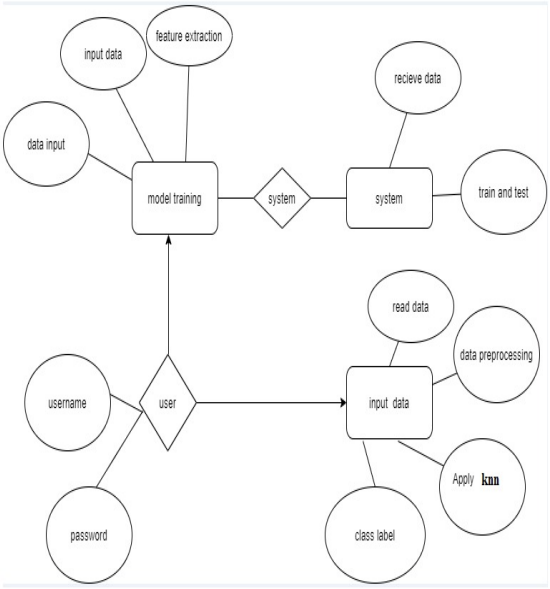

Fig: Er diagram

II. DATASET DESCRIPTION

The dataset utilized in this study comprises network traffic data captured from both normal network activity and Distributed Denial of Service (DDoS) attack scenarios. It is an essential part of machine learning model evaluation and training for the identification of harmful network activity. The dataset contains a diverse range of features extracted from network packets, providing valuable insights into the characteristics of benign and attack traffic.

Each entry in the dataset represents a network packet and includes various attributes that encapsulate key aspects of network communication. These attributes include but are not limited to frame length, IP header length, IP length, IP time-to-live (TTL), IP protocol type, TCP source and destination ports, TCP length, TCP window size, and various TCP flags. Additionally, the dataset includes labels indicating whether each packet corresponds to normal network traffic or a DDoS attack.

The two primary categories of the dataset are DDoS attack traffic and regular network traffic. The normal network traffic category comprises packets exchanged during routine network communication, including activities such as web browsing, email communication, and file transfers. These packets exhibit typical patterns and characteristics associated with legitimate network behavior.

In contrast, the DDoS attack traffic category contains packets generated during simulated DDoS attack scenarios. These packets are intentionally crafted to overwhelm the target system's resources and disrupt its normal operation. Distinctive patterns, like abnormally high packet rates, big packet sizes, and strange protocol behaviour, are frequently seen in DDoS attack traffic.

One of the critical aspects of preparing the dataset involves ensuring a balanced representation of both normal and attack traffic samples. This balance helps prevent model bias and ensures robust performance during training and evaluation. Additionally, data preprocessing techniques may be applied to the dataset to address issues such as missing values, outliers, and feature scaling, thereby enhancing the quality of the input data for machine learning algorithms.

Researchers and practitioners can create efficient DDoS detection systems by using the dataset as the basis for training and testing machine learning models. By analyzing the characteristics of normal and attack traffic patterns, machine learning models can learn to differentiate between benign and malicious network behavior, enabling timely detection and mitigation of DDoS attacks in real-world environments.

III. MODEL TRAINING AND EVALUATION:

From a framework of DDoS attack detection, model training involves the process of training machine learning algorithms using the prepared dataset to develop predictive models capable of distinguishing between normal network traffic and DDoS attack traffic. This section outlines the steps involved in model training and evaluation, highlighting key considerations and methodologies.

Feature Selection and Extraction:

Before training the models, it is essential to identify relevant features from the dataset that contribute to distinguishing between normal and attack traffic. Features such as IP length, TTL, protocol type, TCP source and destination ports, TCP length, and window size are commonly utilized for this purpose. Feature extraction techniques may be employed to transform raw data into meaningful feature representations suitable for model training.

Data Splitting:

To evaluate the effectiveness of the trained models, the dataset is split into testing and training sets. Typically, a significant portion of the dataset is allocated for training (e.g., 70-80%), while the remainder is reserved for testing. This ensures that the models are evaluated on

unseen data to provide an unbiased estimate of their performance.

Model Selection:

Various machine learning algorithms can be employed for DDoS attack detection, including Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Random Forests, and Gradient Boosting Machines. The selection of an algorithm is contingent upon various aspects, including the type of data, computational effectiveness, and the intended balance between interpretability and accuracy. Hyperparameter Tuning:

Hyperparameters are variables that govern the behaviour of machine learning algorithms but are not learned during training. Model performance can be increased by optimising hyperparameters using strategies like random or grid search. Common Among the hyperparameters are the quantity of neighbors in KNN, the kernel type in SVM, and the number of trees in Random Forests.

Model Training:

Once the algorithm and hyperparameters are selected, the model is trained using the training data. In order to reduce prediction errors and increase predictive accuracy, the model learns patterns and correlations between features and labels in the dataset during training.

Model Evaluation:

After training, the performance of the trained model is evaluated using the testing data. Evaluation measures that are frequently used to evaluate a model's performance in properly classifying normal and attack traffic include accuracy, precision, recall, F1-score, and area under the ROC curve (AUC-ROC). Additionally, techniques such as cross-validation may be employed to obtain more reliable performance estimates.

IV. PERFORMANCE ANALYSIS

To determine the trained model's advantages, disadvantages, and potential areas for development, its performance is examined. Insights gained from performance analysis can inform further iterations of the model training process, potentially leading to enhanced detection capabilities and robustness against evolving DDoS attack strategies.

V. RESULT

Feature Selection: The selected features for detecting DDoS attacks were 'ip.len', 'ip.ttl', 'ip.proto', 'tcp.srcport', 'tcp.dstport', 'tcp.len', and 'tcp.window_size'.

1. Support Vector Machine (SVM):

   Accuracy: 97.55%

   SVM achieved an accuracy of 97.55% in detecting DDoS attacks using the selected features.

2. K-Nearest Neighbors (KNN):

   Accuracy: 99.60%

   KNN achieved an impressive accuracy of 99.60% in detecting DDoS attacks using the same set of features.

CONCLUSION:

In conclusion, the process of DDoS attack detection involves leveraging machine learning techniques to develop robust models capable of accurately distinguishing between normal network traffic and malicious attack traffic. Throughout this paper, we have explored various aspects of DDoS attack detection, including dataset preparation, model training, and evaluation.

Firstly, we discussed the importance of dataset preparation, highlighting the need to collect and preprocess network traffic data to extract relevant features for model training. Features such as IP length, TTL, protocol type, and TCP characteristics play a crucial role in characterizing network traffic and detecting anomalies indicative of DDoS attacks.

Next, we delved into the model training process, where we explored different machine learning algorithms such as SVM, KNN, and XGBoost. The choice of algorithm is influenced by various parameters, including desired

performance metrics, computing efficiency, and dataset characteristics. Each method has pros and cons of its own. We then discussed the evaluation of trained models, emphasizing the importance of assessing performance using appropriate metrics such as accuracy, precision, recall, and AUC-ROC. Rigorous evaluation ensures that the deployed models can effectively differentiate between normal and attack traffic while minimizing false positives and false negatives.

Throughout this paper, we have underscored the significance of continuous refinement and improvement in DDoS detection systems. As cyber threats evolve and adversaries employ sophisticated attack strategies, it is essential to adapt and enhance detection mechanisms to stay ahead of emerging threats.

In summary, the development of accurate and reliable DDoS detection systems requires a comprehensive understanding of network traffic patterns, robust model training methodologies, and rigorous performance evaluation. By leveraging machine learning techniques and adopting a proactive approach to cybersecurity, organizations can effectively mitigate the risks posed by DDoS attacks and safeguard their network infrastructure against malicious threats.

VI. REFERENCES

[1] Aliyev, R. (2023). DDoS Simulation: Empowering Targets through Simulated Attacks. In 2023 IEEE 17th International Conference on Application of Information and Communication Technologies (AICT). IEEE. DOI: 10.1109/AICT59525.2023.10313188

[2] Kumar Sharma, A., & Kumar, R. (2024). A Comprehensive survey of DDoS Attacks: Evolution, Mitigation and Emerging trend. In 2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC). IEEE. DOI: 10.1109/PARC59193.2024.10486696

[3] Kaur, K., & Ayoade, J. (2023). Analysis of DDoS Attacks on IoT Architecture. In 2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). IEEE. DOI: 10.1109/EECSI59885.2023.10295766

[4] Kokane, C., Babar, S., & Mahalle, P. (2023, March). An adaptive algorithm for polysemous words in natural language processing. In Proceedings of Third International Conference on Advances in Computer Engineering and Communication Systems: ICACECS 2022 (pp. 163-172). Singapore: Springer Nature Singapore.

[5] Kokane, C. D., Mohadikar, G., Khapekar, S., Jadhao, B., Waykole, T., & Deotare, V. V. (2023). Machine Learning Approach for Intelligent Transport System in IOV-Based Vehicular Network Traffic for Smart Cities. International Journal of Intelligent Systems and Applications in Engineering, 11(11s), 06-16.

[6] Kokane, C., Babar, S., Mahalle, P., & Patil, S. (2022). Word sense disambiguation: A supervised semantic similarity based complex network approach. Int J Intell Syst Appl Eng, 10(1s), 90-94.

[7] Kokane, C.D., Babar, S.D., Mahalle, P.N., Patil, S.P. (2023). Word Sense Disambiguation: Adaptive Word Embedding with Adaptive-Lexical Resource. In: Chaki, N., Roy, N.D., Debnath, P., Saeed, K. (eds) Proceedings of International Conference on Data Analytics and Insights, ICDAI 2023. ICDAI 2023. Lecture Notes in Networks and Systems, vol 727. Springer, Singapore. https://doi.org/10.1007/978-981-99-3878-0_36

[8] Kokane, C. D., & Sachin, D. (2021). Babar, and Parikshit N. Mahalle." Word Sense Disambiguation for Large Documents Using Neural Network Model.". In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE.

[9] Kokane, C. D., & Sachin, D. (2020). Babar, and Parikshit N. Mahalle." An adaptive algorithm for lexical ambiguity in word sense disambiguation.". In Proceeding of First Doctoral Symposium on Natural Computing Research: DSNCR.

[10] Kokane, C.D., Babar, S.D., Mahalle, P.N. (2021). An Adaptive Algorithm for Lexical Ambiguity in Word Sense Disambiguation. In: Patil, V.H., Dey, N., N. Mahalle, P., Shafi Pathan, M., Kimbahune, V.V. (eds) Proceeding of First Doctoral Symposium on Natural Computing Research. Lecture Notes in Networks and Systems, vol 169. Springer, Singapore. https://doi.org/10.1007/978-981-33-4073-2_11

[11] Kokane, C., Babar, S., Mahalle, P. (2023). An Adaptive Algorithm for Polysemous Words in Natural Language Processing. In: Reddy, A.B., Nagini, S., Balas, V.E., Raju, K.S. (eds) Proceedings of Third International Conference on Advances in Computer Engineering and Communication Systems. Lecture Notes in Networks and Systems, vol 612. Springer, Singapore. https://doi.org/10.1007/978-981-19-9228-5_15

[12] C. D. Kokane, S. D. Babar and P. N. Mahalle, "Word Sense Disambiguation for Large Documents Using Neural Network Model," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1-5, doi: 10.1109/ICCCNT51525.2021.9580101.