

Machine Learning Strategies for Mitigating Distributed Denial of Services Attacks

Vaishnav Gonare¹, Anup Ghunawat², Kiranraje Golekar³, Anup Ingle⁴, Vijay M Marathe⁵ and Vishal B Ambhore⁶

¹⁻⁶Vishwakarma Institute of Information Technology, Pune, India

Email: vaishnav.22110899@viit.ac.in, anup.22110878@viit.ac.in, kiranraje.22110680@viit.ac.in, anup.ingale@viit.ac.in, vijay.marathe@viit.ac.in, vishal.ambhore@viit.ac.in

Abstract—The security and availability of internet services are seriously threatened by denial-of-service (DoS) assaults, which interfere with the operations of authorized users and result in financial losses. The present investigation utilizes machine learning approaches to detect and avoid denial of service threats. We present a dynamic model for detecting and mitigating DoS assaults, including its distributed variant (DDoS), by examining multiple approaches and datasets. By utilizing ensemble techniques and machine learning algorithms like Support Vector Machines (SVM), we create a working prototype for real-time DoS attack detection and prevention. The effectiveness of the suggested method in precisely detecting and preventing denial-of-service (DoS) assaults is demonstrated by our experimental findings, which improve network infrastructure resilience and guarantee continuous service delivery.

Index Terms—DDoS attacks, IDS, NIDS, HIDS, Line Fitting Model.

I. INTRODUCTION

Since internet-based services are so widely used in today's digital world, there is a greater chance of security risks. One of the most common and disruptive types of cyberattacks is denial-of-service (DoS) attack. By overloading computational services' infrastructure, denial-of-service (DoS) attacks seek to prevent legitimate users from accessing them by depleting their resources. A successful DoS attack breaches the availability pillar of an organization's information security strategy, which has consequences that go beyond simple annoyance. The 2018 GitHub attack, a distributed type of Denial-of-Service (DDoS) attack, achieved an astounding volume of 1.35 Tbps, demonstrating the seriousness of the threat posed by DoS attacks.

Targeting protocols from the network and transport levels to the application layer, denial-of-service (DoS) attacks can appear at several layers of the Open Systems Interconnect (OSI) and TCP/IP models. Although there is a greater prevalence and body of research on attacks on lower layers, assaults on the application layer, especially variations on the HTTP protocol, are equally important and should be thoroughly investigated. DoS attacks can still affect database management systems (DBMSs), and one common technique used to jeopardize database integrity and availability is SQL Injection (SQLIA). It directly targets the database, in contrast to conventional network-based attacks, which presents a special difficulty for detection and mitigation attempts.

Although most research on attacks on networks, including packet analysis for anomaly detection, focuses on network-based assaults, attacks on database management systems (DBMSs) present difficulties because requests are encapsulated in valid packets.

As a result, DoS assaults directed against DBMSs may go unnoticed by conventional network-centric methodologies, underscoring the necessity for specialized detection methods. The use of machine learning (ML) techniques for cyber threat identification has become increasingly popular in response to the changing threat landscape. ML is a potent tool for detecting and thwarting cyberattacks, such as DoS and DDoS, because it allows computers to learn from data without the need for explicit programming. ML algorithms that have been trained on a variety of datasets can successfully identify patterns suggestive of malevolent.

Software Defined Networking (SDN) is a approach to network management that enables programmability, automation, and dynamic control of network resources through software abstraction. In traditional networking, network devices such as routers, switches, and firewalls are controlled and managed individually, often leading to complex configurations, limited scalability, and manual intervention for network changes.

The classification of traffic flows in today's IP networks has become an important research area with the adoption of Machine Learning (ML) techniques and Software Defined Networking (SDN) principles. Traditional methodologies including identifying traffic based on port number and payload inspection are not effective due to the dynamic and encrypted nature of current traffic. This project will attempt to utilize Supervised and Unsupervised ML algorithms to classify flows by their required bandwidth, required QoS, and their application based on various flow level details as features.

II. LITERATURE SURVEY

Gupta et al. (2013) examined the use of computational intelligence methods to create sophisticated intrusion detection systems for these kinds of networks. Their study showed that computational intelligence techniques might greatly improve IDS's detection capabilities. It was presented at the 2013 IEEE International Conference on Computational Intelligence and Computing Research. By utilizing these strategies, intrusion detection systems (IDS) can improve their capacity to detect and counteract security risks, thereby furnishing wireless networks with a stronger security structure.[1] Network security depends on the detection of types of attacks, including persistent echo attacks on UDP Port 7. The use of Ant Colony Optimization (ACO) techniques to create an intelligent detection system for these kinds of attacks was investigated by Gupta et al. (2014). Their research showed that ACO could successfully enhance the detection process, increasing its accuracy and efficiency. It was presented at the 2014 International Conference on Electronic Systems, Signal Processing, and Computing Technologies. By using this method, network security systems are better able to recognize and stop echo attacks, which increases the overall resilience of network infrastructures.[2] Gupta et al. (2014) investigated this integration and showed how it may enhance mechatronic systems' responsiveness and adaptability. The study's findings, which were showcased at the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques, context-aware systems that can change on their own. By offering a strong foundation for context-aware intelligence, this method not only improves system efficiency but also advances smart mechatronics networks.[3] Improving traffic flow is crucial to lowering congestion and enhancing urban mobility. Kolte et al. (2023) investigated the development of an adaptive signal control system for traffic management using Convolutional Neural Networks (CNN) and Graph Convolutional Networks (GCN). Their research, which was presented at the 2023 Asian Conference on Innovation in Technology, showed that traffic signal timings may be efficiently optimized by integrating CNN and GCN algorithms depending on current traffic conditions. This method improves the flexibility and effectiveness of traffic management systems, which results in less waits at intersections and smoother traffic flow.[4] Contribute to the field of intrusion detection by proposing a novel approach utilizing the naive Bayes algorithm and preprocessing techniques, demonstrating promising advancements in network security.[5] Contribute significantly by conducting a comparative study of various techniques, including support vector machines (SVMs), artificial neural networks (ANNs), multivariate adaptive regression splines (MARS), and linear genetic programs (LGPs), for intrusion detection. Their comprehensive analysis provides valuable insights into the performance and suitability of different AI techniques, offering a foundation for further advancements in IDS implementation and cybersecurity strategies.[6] Conduct a comprehensive survey of state-of-the-art Intrusion Detection Systems (IDSs) tailored for WSNs. Their analysis encompasses a range of IDSs, providing insights into their applicability, strengths, and weaknesses, while also outlining future research directions to bolster the security of WSNs.[7] Present a significant contribution by developing a machine learning-based system for detecting phishing websites with exceptional accuracy. Their approach leverages supervised learning, particularly the Random Forest technique, to analyze a combination of 26 features characteristic of phishing websites.[8] The paper proposes a Machine Learning Based Intrusion Detection System (IDS) for Software Defined Networks (SDNs) [9]. SDN environments introduce new security challenges, and this research investigates using machine learning to address

these vulnerabilities [10]. The authors designed a virtual testbed to simulate a real network environment for evaluating their IDS next paper proposes an Intrusion Detection System (IDS) that leverages Open-Source INTelligence (OSINT) knowledge to detect network threats. Then explores collaborative security and Peer-to-Peer (P2P) intrusion detection systems [11].

Discusses Advanced Metering Infrastructure (AMI) threats, intrusion detection requirements, and deployment recommendations [12]. It analyzes the unique challenges of AMI systems and proposes solutions for securing them [13].

III. DISTRIBUTED DENIAL SERVICE OF ATTACK

Attackers using distributed networks of hacked devices to flood targeted servers or networks with malicious traffic are known as Distributed Denial of Service (DDoS) invaders, and they position a solemn threat to cybersecurity. In contrast to customary denial-of-service attacks, which stem from a single source, distributed denial-of-service attacks leverage the combined might of disparate and unconnected devices, such as servers, PCs, and Internet of Things devices, arranged into botnets for coordinated attacks. These assaults, which might take the form of HTTP or ICMP floods, are designed to deplete the target's resources to the point where genuine users are unable to access it, so impairing vital services. Thanks to machine learning, enterprises may now use sophisticated intrusion detection systems to instantly analyze network traffic patterns and identify and stop DDoS attacks. Organizations can effectively protect themselves by implementing a multi-layered defensive strategy and encouraging cooperation within the cybersecurity community. Public DoS/ DDoS attacks types are ICMP (Ping), TCP-SYN, and UDP floods, HTTP floods.

A. Internet Control Message Protocol (ICMP) Ping Flood Assault

A common kind of denial-of-service (DoS) attack is known as an "ICMP flood," in which an overwhelming amount of Internet Control Message Protocol (ICMP) packets are directed towards a target server, exceeding its ability to process and reply to valid requests. Attackers try to deplete the server's resources by abusing the ping tool, which can cause serious slowdowns or system failures. The network bandwidth is overloaded by this deluge of ICMP packets, impairing the server's capacity to manage TCP/IP traffic efficiently.

B. TCP-SYN Flood Assault

When someone launches a TCP SYN flood attack, they bombard the server with SYN packets, struggling to begin a linking but not finishing the handshake. The influx of unfinished connections depletes the server's resources, making it incapable of fulfilling valid requests. As a result of having too many "half-open" connections, the server becomes more susceptible to new connection attempts. This might prevent reliable clients from connecting to the server, which would disrupt services.

C. UDP Flood Assault

Attackers using UDP floods bombard a target server with UDP datagrams aimed at arbitrary open ports. As open ports may not always be known to admins, the server responds to the flood of information. The problem gets worse when every UDP packet is met with an ICMP "unreachable" response, which floods the network environment with spoof source IP addresses. This increases the attack's impact and jeopardizes the stability of the network even more.

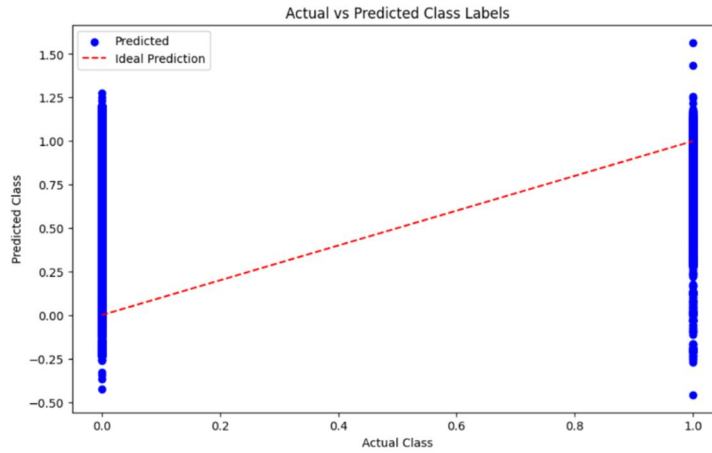
IV. PREVENTING DDOS ATTACK USING MACHINE LEARNING

A. Line Fitting Model

Our goal is to identify and stop DDoS attacks, and we use machine learning's (ML) line fitting model as a strong protection. Our goal is to find unusual patterns in network traffic data that could be signs of impending DDoS attacks by utilizing machine learning (ML) technologies, most especially line fitting models. Using a dataset that is obtained from websites such as Kaggle, this method entails training the line fitting model on a variety of network traffic patterns, encompassing both typical and malicious circumstances.

The line fitting model examines several characteristics taken out of the network traffic data, including protocol abnormalities, capacity use, and packet speeds.

The model may successfully highlight abnormal activity that could indicate an ongoing DDoS attack by detecting deviations from established traffic patterns. By continuously monitoring and analyzing incoming network traffic, the line fitting model may quickly identify possible threats and trigger alarms, allowing for preemptive intervention to lessen the impact of DDoS attacks.



Figure(A): Line fitting output of DDOS

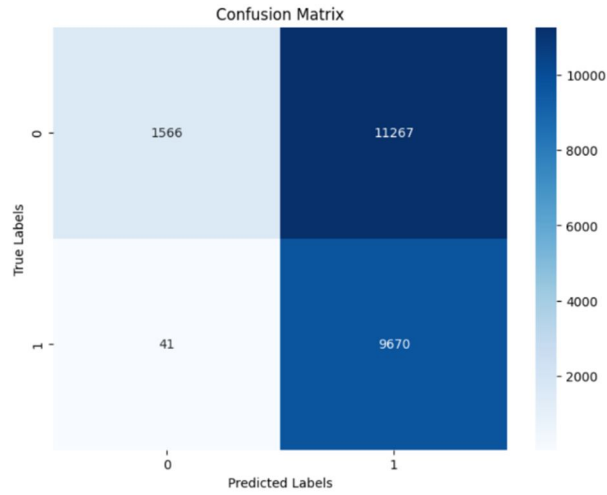


Figure (B): Confusion matrix of DDOS

We forecast the necessary detection accuracy by estimating the number of real DDoS attackers from our dataset. It is possible to precisely estimate prospective dangers by analyzing the dataset, which provides insights into attack characteristics and prevalence. We use dataset insights to create predictive models by leveraging sophisticated machine learning techniques, such as line fitting models. These methods predict the number of DDoS attackers using variables like attack history and network traffic patterns. The utilization of statistical methods and visual aids enhances comprehension of assault dynamics and boosts the precision of predictive models. This data-driven strategy fortifies cybersecurity against DDoS attacks and enables proactive resource allocation.

V. RESULT ANALYSIS

The following metrics are used to evaluate the quality of machine learning algorithms:

- **Accuracy:** The ratio of correctly confidential instances to the total number of instances. It is considered using the equation

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad \dots(1)$$

- **Precision:** The ratio of correctly forecast positive instances to the total forecast positive instances. It is considered using the equation

$$\text{Precision} = \frac{TP}{TP+FP} \quad \dots(2)$$

- Recall: The ratio of correctly forecast positive instances to the total actual positive instances. It is considered using the equation:

$$\text{Recall} = \text{TP} / (\text{TP} + \text{FN}) \quad \dots(3)$$

- F1-score: The harmonic mean of precision and recall, representing the balance between them. It is considered using the equation:

$$\text{F1-score} = (2 \times \text{Recall} \times \text{Precision}) / (\text{Recall} + \text{Precision}) \quad \dots(4)$$

With a in height recall of 99% and a precision of 46%, our line fitting model exhibits an accuracy of 49%. The model's high recall score indicates that, despite its relatively low precision, it is excellent at detecting true positive cases. With an F1 score of 0.63, which considers both precision and recall, there is a moderate balance between the two criteria. These findings imply that while the model is successful in collecting DDoS attack instances, it still must be improved to correctly identify actual positive events while reducing false positives

```
Accuracy: 0.49840312278211496
Precision: 0.46186177580360127
Recall: 0.995777983729791
F1 Score: 0.631036282954842
```

Figure (c): Accuracy precision recall output of DDOS

VI. INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) alerts security professionals about packets incoming and leave-taking a monitored network. IDSs sniff network packets to understand network activities. They can be hardware or software-based, monitoring network traffic and detecting potential attacks [4, 10]. IDS software typically monitors packets, detects suspicious activities, records events, and sends informs to the network administrator. IDSs are classified into three types: network- created, host- created, and hybrid created.

A. Network-created IDSs

Network-created IDS (NIDS) are essential for an organization's security [24]. They detect a wide range of attacks at the application, network, and transport layers, and monitor unexpected services across multiple applications. Additionally, NIDSs monitor network traffic and secure systems from network-based threats without violating network policies [11]. However, NIDSs often struggle to process entire network packets, leading to incomplete analyses and significant delays in high-speed, high-load environments [11]

B. Host-created IDSs

Host-created IDS (HIDS) monitor events on local machines and are versatile, being installable on servers, workstations, and notebooks, unlike NIDS. HIDSs monitor malicious activities and events within the host, situated at network endpoints with anti-threat applications like spyware detection, firewalls, and antivirus software [11]. Disadvantages include consuming system resources, potential conflicts with existing security policies, difficulty in analyzing multiple computers, maintenance challenges in large networks, vulnerability to being disabled after compromise, and the need for reboots after installation or updates, which many essential servers cannot support [5]

C. Anomaly-created IDS

Anomaly-created IDSs require foundational information and system knowledge. These systems excel in gathering evidence, such as statistics, data, facts, and figures, to form baselines during the learning period. The reference point profile represents the normal behavior of the supervised system, advanced as the IDS learns the environment [9]. This environment can include networks, users, and systems. During this learning period, the IDS creates a normal outline of the monitored system. Anomaly-based IDSs classify anomalies into two main types: Protocol-based anomalies and Application/Payload-based anomalies. These classifications help in detecting deviations from the established normal behavior, ensuring effective intrusion detection [9].

D. Signature-created IDSs

Signature-created intrusion detection, or rule-based detection, uses predefined signatures of known attacks to identify malicious activity in network traffic. Derived from historical attack data, these signatures match

incoming network packets or system logs. Signature-based IDS effectively detects known threats and common attack patterns, making it essential for a comprehensive security posture. However, its effectiveness is limited to predefined signatures, making it vulnerable to zero-day exploits and polymorphic malware. This limitation underscores the need for additional detection methods.

VII. IMPLEMENTATION

Intrusion detection plays a critical role in safeguarding computer systems and networks against unauthorized access and malicious activities. One of the widely used datasets for intrusion detection research is the NSL-KDD dataset, developed by Tavallaee et al. (2009) as an enhancement to the earlier KDD Cup'99 dataset. The KDD dataset, while extensive, suffered from a significant issue of duplicate packets, which skewed the accuracy of intrusion detection models.

Tavallaee et al. identified that approximately 78% and 75% of network packets in the training and testing subsets of the KDD dataset were duplicates. This duplication led to biases in machine learning algorithms, favouring normal instances, and hindering the detection of irregular and potentially harmful network activities. To address this challenge, the NSL-KDD dataset was crafted by eliminating duplicate records from the KDD Cup'99 dataset.

The NSL-KDD dataset comprises 125,973 accounts in the training set and 22,544 accounts in the test set, providing a substantial amount of data for robust intrusion detection model training and evaluation. With 22 different intrusion attack types and 41 attributes (features), including 21 attributes describing the connection itself and 19 attributes characterizing the nature of connections within the same host, the NSL-KDD dataset offers a comprehensive and diverse dataset for intrusion detection research.

Implementing intrusion detection using the NSL-KDD dataset involves pre-processing the data to address issues such as duplicate records and feature engineering to select relevant attributes. Machine learning algorithms, such as Random Forest classifiers, Support Vector Machines (SVM), or Neural Networks, can be trained on the pre-processed dataset to learn patterns indicative of normal and malicious network behavior.

Furthermore, techniques such as Random Oversampling and Recursive Feature Elimination (RFE) can be employed to address class imbalance and select the most relevant features for model training, respectively. Once trained, the model's performance can be evaluated using metrics such as recall, accuracy, precision and F1-score to assess its effectiveness in detecting intrusions accurately while diminishing incorrect positives and incorrect negatives.

VIII. RESULTS

The evaluation results provide valuable acumens into the performance of different machine learning models for the task of intrusion detection, specifically targeting the "Normal DoS" class.

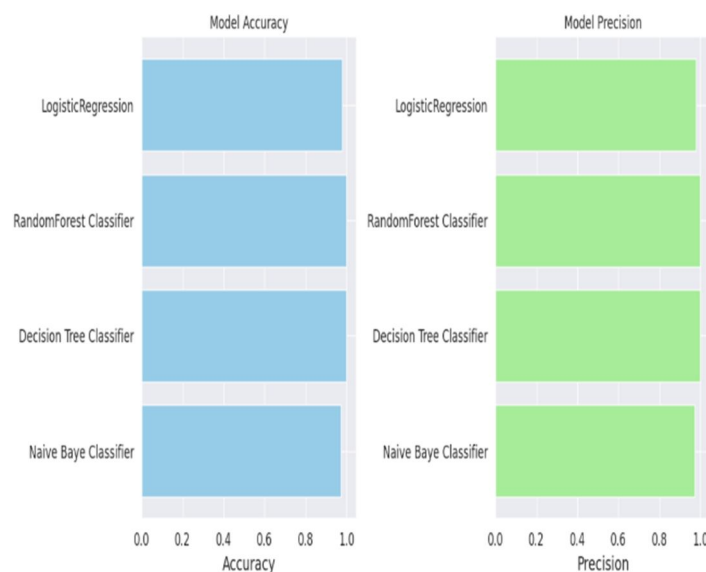


Figure (D): Accuracy precision output of DDOS using NIDS

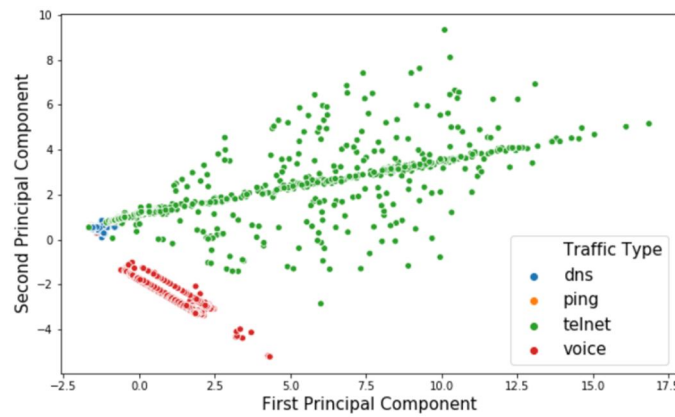


Figure (E): First component vs Second component

The Decision Tree Classifier and Random Forest Classifier demonstrated exceptional performance, achieving near-perfect accuracy with mean cross-validation scores of approximately 99.98%. These models showcased remarkable accuracy rates of 99.99%, accurately classifying all instances of both '0.0' (Normal) and '1.0' (DoS) classes. Their precision scores of 99.99% further emphasize their ability to correctly identify positive cases, underscoring their robustness and effectiveness in intrusion detection.

The Naive Bayes Classifier also delivered strong results, with a mean cross-validation score and accuracy of approximately 97.38%. While it displayed slightly lower performance compared to the Decision Tree and Random Forest models, it still achieved a high precision score of 97.38%, indicating its capability to accurately predict positive cases.

Similarly, the Logistic Regression model exhibited commendable performance, with a mean cross-validation score and accuracy of around 98.08%. Despite some misclassifications observed in the confusion matrix, the model achieved a precision score of 98.10%, indicating its ability to correctly identify positive cases.



Figure (F): Confusion matrix of traffic type

The supervised Logistic Regression model was the first machine learning algorithm to be used. Predicting categorical target variables is its intended use. When there are multiple targets, it selects the target with the highest probability of occurring. Typically, the result is a binary value. With an accuracy of more than 99.54%, logistic regression functioned remarkably well in our program. The decision boundaries that were created using the first two Principal Components make it evident why the accuracy is so high.

III. CONCLUSIONS

Finally, a thorough examination of DoS and DDoS attacks is presented here, along with a variety of machine learning methods that are used to counter these threats. Through the examination of current attacks, the classification of attack kinds, and the determination of signs and underlying reasons, the research offers significant understanding into addressing DoS-related issues. Robust detection techniques, such deep learning

algorithms, are becoming increasingly important as IPv6 networks become more widely used and network data progressively gets more complicated. Even while machine learning methods have produced encouraging results, they can yet be improved, especially in terms of responding to changing assault tactics. Subsequent initiatives will concentrate on putting out novel models to support intrusion detection systems (IDS) and improve DDoS assault detection. DoS/DDoS assaults are becoming more frequent on social media and the internet, which emphasizes how important it is to have efficient detection and mitigation techniques. Protecting computer systems from potential disruption requires a thorough understanding of the underlying causes and detection techniques of these threats. Our experiment shows promising results in accurately recognizing and mitigating such threats consuming machine learning models based on network traffic data. We attain a high prediction accuracy rate of 99% by utilizing ensemble-learned models, demonstrating the effectiveness of our suggested strategy in strengthening network defenses and lessening the effect of DoS/DDoS attacks.

REFERENCES

- [1] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur and A. Ingle, "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks," 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, India, 2013, pp. 1-7, doi: 10.1109/ICCIC.2013.6724156
- [2] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, A. Ingle and V. Ambhore, "Intelligent Perpetual Echo Attack Detection on User Datagram Protocol Port 7 Using Ant Colony Optimization," 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, Nagpur, India, 2014, pp. 419-424, doi: 10.1109/ICESC.2014.82..
- [3] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, A. Ingle and P. Gawande, "Towards context-aware smart mechatronics networks: Integrating Swarm Intelligence and Ambient Intelligence," 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, 2014, pp. 64-69, doi: 10.1109/ICICT.2014.6781254.
- [4] S. Kolte, A. Ingle, K. Kshirsagar, P. G. Gawande, K. A. Kumbhar and R. S. Kawchale, "Traffic Flow Optimization Using CNN and GCN for Adaptive Signal Control," 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), Ravet IN, India, 2023, pp. 1-4, doi: 10.1109/ASIANCON58793.2023.10269944.
- [5] S Faizal Mukhtar Hussain. R. Karthikeyan S.Ramamoorthi, I.Sheik Arafat S.Syed Musthafa Gani - Denial of Service Attack Analysis using Machine Learning Techniques(2023).
- [6] D. A. Effendy, K. Kusriani, and S. Sudarmawan - Classification of intrusion detection system (IDS) based on computer network. (2017)
- [7] S. Mukkamala and A. H. Sung - A comparative study of techniques for intrusion detection. (2003).
- [8] I. Butun, S. D. Morgera, R. Sankar - A Survey of Intrusion Detection Systems in Wireless Sensor Networks. (2014).
- [9] A. Alswailem, B. Alabdullah, N. Alrumayh, A. Alsedrani - Detecting Phishing Websites Using Machine Learning. (2019).
- [10] I. Vacas, I. Medeiros and N. Neves, "Detecting Network Threats using OSINT Knowledge-Based IDS," 2018 14th European Dependable Computing Conference (EDCC), Iasi, Romania, 2018, pp. 128-135, doi: 10.1109/EDCC.2018.00031C.
- [11] M. E. Locasto, J. J. Parekh, A. D. Keromytis, and S. J. Stolfo, "Towards collaborative security and P2P intrusion detection," Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, West Point, NY, USA, 2005, pp. 333-339, doi: 10.1109/IAW.2005.1495971.
- [12] Abubakar, A., & Pranggono, B. (20?). Machine Learning Based Intrusion Detection System for Software Defined Networks. Department of Engineering and Mathematics, Sheffield Hallam University, Sheffield, S1 1WB, U.K.
- [13] Grochocki, D., Huh, J. H., Berthier, R., Bobba, R., Sanders, W. H., Cárdenas, A. A., & Jetcheva, J. G. (2012). AMI Threats, Intrusion Detection Requirements and Deployment Recommendations. Information Trust Institute, Coordinated Science Laboratory, and Electrical and Computer Engineering Department University of Illinois at Urbana-Champaign, Fujitsu Laboratories of America, Inc
- [14] Ashoor, A. S., & Gore, S. (n.d.). Importance of Intrusion Detection System (IDS). Department of Computer Science, Pune University.