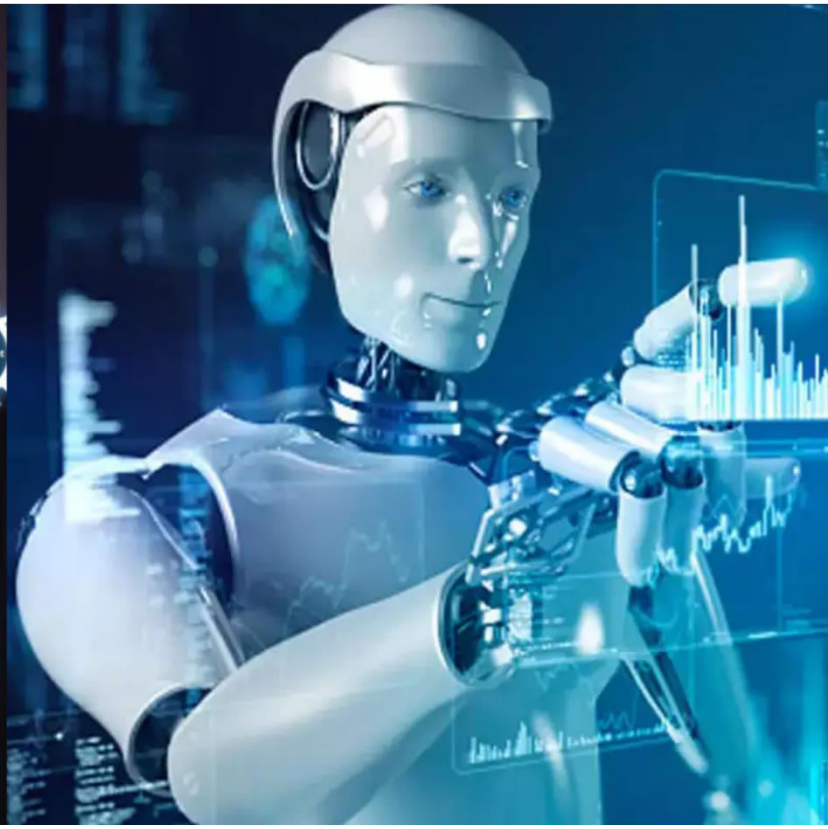
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404566|

Identification and Counteraction of Benign, DDOS, DOS, and MITM Utilizing AI Calculations

K. Muthulakshmi, K. Lakshmi Akhilesh

Assistant Professor, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, India

UG Student, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, India

ABSTRACT: There are three basic cyber threats, namely benign, Man-in-the-Middle (MiTM) attacks, distributed denial of service (DDoS), and denial of service (DoS). Attackers apply these to disrupt network infrastructure and data integrity. The catch is that early detection systems especially the ones that rely on traditional methods, easily get confused with the strategy lately adopted by attackers. This research therefore develops a layered architecture that uses algorithms-XGBoost and K-Nearest Neighbours (KNN) for real-time detection and mitigation of these threats. A classification-accurate XGBoost model is used to classify DDoS, DoS, and MiTM attacks whereas KNN is used to distinguish benign from harmful activity. Performance assessments show accuracy on the testing data of 94.88%, thus asserting the appropriateness of the models to secure network frameworks.

KEYWORDS: Cybersecurity Threats, Man-in-the-Middle (MiTM) attacks, distributed denial of service (DDoS), and denial of service (DoS), Machine Learning (ML), Bag of words.

I. INTRODUCTION

Regarding this, most current research concentrates on identifying and categorizing DDoS attacks using various mechanisms and a single controller. They also concentrate on accuracy or efficiency rather than both. In data centers, several controllers must be shielded from Benign, DDoS, DoS, and MiTM attacks. The tolerance level for network traffic varies among various controllers. One way to conceal the identity of the attacker in an attack of this nature is to spoof the source, often known as a phony source address. The attackers attempt to inundate the target with deceptive packets to facilitate the delivery of malicious packets. The following are the reasons behind these attacks: When there is a conflict between two groups or two individuals,[1] DDoS and DOS are powerful weapons that can be used to obstruct the opponent's applications and infrastructure. An individual may intentionally perpetrate an attack and engage in undesirable actions as a reaction to a perceived injustice through his assault. A terrorist group may endeavour to assault critical areas using cyber warfare, driven by political or geopolitical motives, to undermine the economic system. Numerous techniques for detecting, classifying, and mitigating DDoS, DoS, and MiTM assaults utilising machine learning algorithms are documented in the literature.

Thus, DDoS, DoS, and MiTM attacks become an important threat to the availability and reliability of services delivered online in the fast pace of cyber threats. The intent of the offenses is to flood target systems or networks with traffic to such a point that the intended systems or networks cannot be reached by authorised users.

Traditional methodologies of DDoS, DoS as well as MiTM attack detection and prevention are mostly static and not that sophisticated compared to these threats. The simplified research work simplifies the finding of Benign, DDoS, DoS as well as MiTM attacks through easier as well as more effective ways. It also shows that the machine learning approach is quite efficient. The results have solely relied on a single data set those forms one of the model's limitation. Hence, one can analyse a biased dataset to provide guidance on future improvements.

II. LITERATURE REVIEW

1. Research on Detection and Defense Strategy for DoS Attack based on BP Neural Network and Game Theory. The DoS attack BP neural network detection model selects several feature vectors of KDDCUP99 dataset with rigorous training, which could possibly identify DoS attacks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404566|

Algorithms: The model for detecting DoS attacks using BP neural networks
According to the simulation results, the proposed defensive plan and detection scheme can effectively prevent DoS attacks by improving the detection accuracy up to 99.977%.

2. Denial of Firewalling Attack (DoF): A Study of New Black Nurse Attack 2019
[2] In this research, the basics of the BlackNurse attack, how such attacks are generated in real life, and the impacts on the affected firewalls and networks are discussed. Performance evaluations are conducted using commercial models, namely the Cisco ASA 5540 and Juniper NetScreen SSG 20 firewalls.
Algorithms: Modelling of Time-To-Defend (TTD)
The evaluation is carried out to simulate the recommended defence mechanism against inexperienced and skilled BlackNurse attackers.

3. Low-Rate DoS Attacks: Identification, Protection, and Difficulties: A Survey (2020)
Classifies LDoS assaults and existing defence mechanisms based on the time domain and frequency domain in which detection and defence occur.
Algorithms: Naïve Bayes, Support Vector Machines
The proposed algorithms have accuracy values of 75.33% and 63.75% respectively.

4. Detection Technique for DDoS Attacks in High-Performance KNN against the Severity of DDoS Attacks in an SDN Network; (2020).
The approach will use an ML-based k-nearest-neighbours (KNN) algorithm that is improved in version to detect DDoS attacks.
Algorithms: The algorithm uses an optimised K-Nearest Neighbors (KNN).
The test results from the test-bed are given as follows, which shows that the probability for accurate detection is 88.69%.

5. Identification of DoS attacks utilising many characteristics in Software-Defined Networking (2020)
A novel methodology involves extracting six characteristics from the flow table and employing a back propagation (BP) neural network to develop the classifier.
Algorithms: Software Defined Network (SDN) architecture.
The experimental test-bed results show that the proposed method achieves an accurate detection probability of up to 98.9%.

6. Analysis of Denial-of-Service Attack and Countermeasures in Smart Grid Environment (2020)
Discloses a comprehensive and in-depth explanation of the various types of denial-of-service attacks, including a study of possible countermeasures, to encourage even more focused and coordinated research in this area because a lack thereof might have disastrous consequences.
Algorithms: Naive bayes, Decision Tree
The proposed algorithms have accuracy values of 67.11% and 83.54% respectively.

7. An Effective Intrusion Detection System Framework for Distributed Denial of Service Attacks in Software-Defined Networking Environment (2021)
This method prevents needless use of communication resources by enabling transmissions when a predetermined event is triggered. By using Lyapunov stability and linear matrix inequality (LMI) requirements, the asymptotic stability of the ET-based controller is formally shown.
Algorithms: Software Defined Network (SDN) architecture.
The proposed algorithms have accuracy values of 89.36% and 73.02% respectively.

8. An Enhanced Protocol for Consensus in Delayed Multi-Agent Systems with Unbounded Network Message Saturation and Aperiodic Denial-of-Service Cyber Attacks (2021)
Secondly, the alterations in communication topologies resulting from frequent aperiodic DoS cyber-attacks are considered, which may disrupt communication chains and cause network paralysis in MASs.
Algorithms: Random Forest Algorithm, SVM
The proposed algorithms have accuracy values of 98.36% and 75.02% respectively.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404566|

9. Detection and Prevention of Low-Rate Denial-of-Service Attack Overview (2022)
This new attack vector, referred to as LDoS (Low-rate Denial of Service) attacks, is potentially more destructive than its predecessor because it is harder to recognise and combat than its predecessor.
Algorithms: SVM, or support vector machine; RF, or random forest
The precision values of the proposed algorithms are 88.55% and 93.80%, respectively.

10. Machine Learning Algorithms-Based Anomaly Detection Intrusion Detection System for Denial-of-Service Attack Identification in Internet of Things Networks (2022)
The adaptive threshold technique was taken to develop a resilient adaptive event-triggered mechanism that aims at reducing the transmissions and fighting the aperiodic DoS attacks.
Algorithms: Random Forest, Support Vector Machine
The accuracy values for the proposed algorithms are 99.80% and 98.55% respectively.

11. MSR-DoS: An Adaptive Framework Based on Modular Square Roots to Reduce Denial of Service (DoS) Attacks in 5G-Enabled Car Networks (2022)
In this study, a modular square root-based method for mitigating denial-of-service (DoS) attacks in 5G-enabled car networks is presented.
Algorithms: Modular Square Root (MSR) Algorithms
Thus, the proposed MSR-DoS method reduces 99.80% and 98.55% of the computation overhead for message verification and signature reduction, respectively.

12.Source-Side Identification of DDoS Attacks Using LSTM Collaborations, (2022).
To prevent performance degradation due to chaotic source-side network, adaptation uses the proposed architecture and the LSTM-based adaptive threshold for each source-side network.
Algorithms: KNN, Decision Tree
The exact accuracy values of the proposed algorithms are 78.08% and 81.69% respectively.

13. Safe Control for Groups of Vehicles under the DoS attack using Observers (2023)
It is an observer system with the use of sensor data of vehicles to monitor the condition of vehicles. The idea is to reduce the effect of DoS attacks. This makes the group of vehicles more resilient and better at dealing with such attacks.
Algorithms: K-Means Clustering, ERF-KMC Algorithm
The proposed algorithm achieves accuracy rates of 85.33% and 83.75% respectively.

14. Event-Triggered H∞ Control to Protect Offshore Structures from DoS Attacks: A Comparison (2023)
As a result, the system being studied is a type of switching time-delay system. To ensure the system remains stable internally, a set of necessary conditions has been developed. These conditions are meant to produce an H∞ controller that is event-triggered and can counter attacks.
Algorithm: K-means clustering, Regression trees
The accuracy ratio achieved by the proposed algorithm is 81.93% and 69.75% in that order.

15. Control of DC microgrid based on consensus with a distribution of event-triggering mechanism during DoS cyber-attack (2023)
This mechanism transmission takes place to minimize wastage of communication resources when certain events occur. The stability of ET controller in the null system is verified using Lyapunov stability consider linear matrix inequality LMI condition.
Algorithm: For chemical classification to apply in these chemical Algorithm decision tree
The accuracy values of the proposed algorithm were found to be 89.36% and 73.02% respectively.

III. PROBLEM STATEMENT

The modern cyber security world is characterized by rapid changes with several different threats tending toward attacks classified as denial of service (DoS) or a distributed denial of service (DDoS) which endangers the available and reliable state of service. Such attacks are meat to incapacitate the system or network in question rendering it useless to

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404566|

any genuine users. Traditional strategies for detecting and mitigating DDoS and DoS attacks, such as rules or signatures-based approaches, are often ineffective given the fast-evolving and intricate nature of these threats. The focus is on coming up with better and more flexible solutions which can tell the difference between normal traffic and the one that is intended for an assault to help in improving the network safety and lessening the effects of such attacks on crucial services and infrastructures.

To resolve the issues identified above, machine learning methods are proposed in the detection and protection against Man-in-the-Middle (MITM) attacks, Distributed Denial of Service (DDoS) and Benign denial of service attacks. The aim of this system is to improve the time of response and accuracy of detection. This system employs real-time data input through network traffic, which is then assessed using machine learning methods such as K-Nearest Neighbours (KNNs), XgBoost that are capable of recognizing complex attack patterns.

The solution under consideration employs a multi-tiered approach, combining advanced machine learning algorithms with real-time data analysis to detect and counteract threats such as DDoS, Man-in-the-Middle (MITM), and benign ones. The methodology comprises multiple crucial elements, one of which is alerting others of an attack.

1. Real-Time Data Collection and Processing:
Data Sources - Several network traffic sources, including routers, firewalls, intrusion detection/prevention systems (IDS/IPS), and network logs, provide real-time data to the system.
Preprocessing - Raw data undergoes preprocessing steps, such as data cleaning, normalization, and feature extraction, to ensure high-quality inputs for machine learning models. Packet capture can be performed using tools such as Wireshark or Tshark whereas preprocessing is done using Python bandwidth libraries like Pandas or Scikit-learn.

2. Creating new features:
Some useful features like size of packets, source and destination Ips, number of requests nd types of said requests etc are extracted and altered in order to optimise the given model's ability to detect and classify attacks.
Using, for instance, NumPy and Scipy, statistical and temporal features are also calculated to detect abnormal behaviour of the network.

3. Choosing and Educating of Machine Learning Model:
Supervised Learning – As a first step, and a few standard supervised learning techniques are applied on labeled datasets for a large number of times wherein Support Vector Machines (SVM), K-Nearest Neighbours (KNN) and the like techniques are employed.
Unsupervised Learning – In addition to the above, several kinds of unsupervised learning are also used by the system for the purpose of mimicking or generating 'new' attacks where in the case if K-Means clustering is used for the Autoencoders application to detect traffic patterns anomalies.
The training takes place with the use of Scikit-learn and TensorFlow/Keras especially for the models which are deep learning based, while Jupyter Notebooks are used as the working environment.

4. Model Evaluation and Tuning
Model metrics for example accuracy, precision, recall, and F-1 score are used to evaluate the models developed to ensure that there is good separation between the normal and the attack data.
Hyperparameters are tuned using Cross-Validation and Grid Search techniques as applicable, those techniques increasing the performance of models with respect to detection accuracy and response time.

5. Real-Time Monitoring and Counteractions
The system can perform real time classification of the incoming and outgoing network traffic using the trained models.
In case of an attack, the system quickly adapts network parameters such as rerouting existing path, changing firewall settings or altering access control policies, when required to reduce the level of the threat. Open Daylight and ONOS network management systems, for instance Software Defined Networking (SDN) controllers, allow for reconfiguration of the network on the fly.

6. Clinical Practice Guidelines for the Management of Anomalies and Diabetic Foot: A Combination of Anomaly Detection Based and Signature Detection Based Attacks

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404566|

The system applies hybrid detection shields comprising also signature detection techniques, to increase hallmark detection capabilities and decrease any false alarm rates.
In this case, Snort or Suricata tools are designed for the signature-based approach detection, while the systems are additionally supported by the anomaly detection models to present new forms of undesired weapons previously unknown.

7. The Progression of Endless Learning and Tuning
The new attack approaches identified with the help of unsupervised techniques in this approach are added to the supervised learning phase which aids in reloading and retraining the incumbent models from time to time.
This helps in the faster recognition of the threats and helps in updating the system based on the recognition of different threats.

8. Deployment and Governance Monitoring
The entire framework is deployed on a scalable architecture and microservices using Docker and Kubernetes enabling deployment and scaling across different networks with ease.
Prometheus and Grafana help in monitoring the performance of the system and the metrics of attack detection by providing the user with an up-to-date view of the security status.

This methodology entails both the old-fashioned and the sophisticated methods by fusing an array of learning algorithms and tools for network management in real time to shield against complicated cyber-attacks.

IV. CHALLENGES

- Advancement of Attacks Strategies: Attacks such as DDoS, DoS, MiTM attacks are on the rise with several methods being employed by attackers to avoid detection systems. The system needs to learn how to pace itself with the trends in attacking and modify itself to appropriate the attack patterns as they occur.
- Strategies for Management of False Positives: A proper detection apparatus needs to ensure minimal false positive occurrences so as to preserve the normal flow of traffic across the network. This is only achievable by employing artificial intelligence techniques that can discriminate in a meaningful manner between the good and bad traffic.

Scalability: Because the size and complexity of networks has increased over time the detection system needs to be scalable so that it can process large amounts of information with ease. This includes improving the machine learning models' performance while maintaining their precision.
Anomaly Detection: Any flooding attack or MiTM campaign is likely to exhibit some unusual form of network traffic. For that reason, the system ought to be able to identify such anomalous patterns through the management of normal and abnormal behaviours.

V. IMPLEMENTATION

1.KNN, or K-Nearest Neighbour

KNN is the most common algorithm in Machine learning, pattern recognition and several other areas. KNN is used to classification related jobs. This method is also called as an instance based algorithm (also termed as lazy learning). All training data samples are kept until new observations need to be classified; a model or classifier is not created immediately. This attribute of a lazy learning algorithm renders it superior than eager learning, which develops a classifier prior to the classification of fresh observations. This attribute of a lazy learning algorithm renders it superior than eager learning, which develops a classifier prior to the classification of fresh observations. This technique is particularly important when dynamic data necessitates rapid changes and updates. KNN was utilised with various distance measures.
Step I: Supply the feature space to the neural network for training.

Step II: Calculate distance utilising the Euclidean distance formula

Step III: Determine the values calculated using the Euclidean distance so that, for each i = 1, 2, 3,.., k, d i ≤ d i + 1.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404566|

Step IV: Depending on the characteristics of the data, technique will be applied or vote cast.

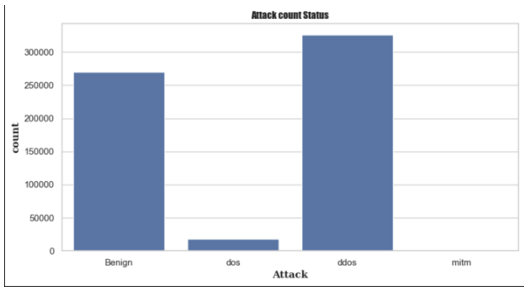
Step V: The proportion and standard of data supplied to KNN determine the value of the constant K, which refers to the nearest neighbors, K. K value is kept low for small sized datasets and kept high for large sized datasets where appropriate.

2. XGBoost

XGBoost is another machine learning algorithm that implements the idea of multiple small decision trees by considering their functional approximations. The role of each tree is to improve on the mistakes made by the previous trees, so with every cycle, the combination improves and the performance of the model overall increases. This procedure is referred to as boosting.

XGBoost is used to classify different types of network traffic (Benign, DDoS, DoS, and MiTM). It learns patterns in the data to identify each type correctly, though it sometimes gets confused between similar attack types (like DDoS and DoS).

i. Data Input: focuses on loading the network traffic data (packet details, traffic patterns) and spreadsheets into the XGBoost model and the available data is labeled as Benign, DDoS, DoS, MiTM.
ii. Initialize Trees: XGBoost procedure initially creates a basic decision tree with the aim of categorizing the given data. This tree may not be very precise in its classification at the beginning.
iii. Calculate Errors: Once the first tree completed the prediction process, XGBoost considers the outcome. Specifically, it pays attention to those points which have been classified correctly, as well as those that were erroneous. It concentrates on the errors.
iv. Build New Trees: As new trees are built; each tree seeks to correct the errors introduced by the previous tree. The trees are linearly combined, and the final output prediction is optimized.
v. Repeat the Process: This approach is repeated until enough trees are constructed by the model (according to the maximum number of boosting rounds). With every new tree, the classification becomes more accurate.
vi. Final Prediction: When all the trees have been created XGBoost utilises all available trees in order to formulate a prediction for each instance of network traffic (Benign, DDoS, DoS and MiTM).
vii. Evaluate the Model: This model can also be evaluated based on how well its predictions agree with actual outcomes determined from a confusion matrix, or accuracy rates. It will provide the number of instances that were marked the way and incorrectly so.



Graph. 1. - Attack count Status

The bar graph depicts the number of distinct attack categories present in the collected data. Most occurrences belong to the category of benign events, which amount to over 250,000. This indicates that there are a lot of benign or non-attack events. Similarly, DDoS and its variants also show a high count, that is more than 300,000, which is a major worry in the case of this type of attack. In contrast, DoS shown attacks appear to be the most infrequent, indicating their occurrence is quite rare. But strikingly, the attacks that are well-known as MITM, do not present any count at all. To sum up, the graph clearly presents an uneven distribution of the attacks throughout the timeline, with most of them being non-hostile and DDoS attacks instances.

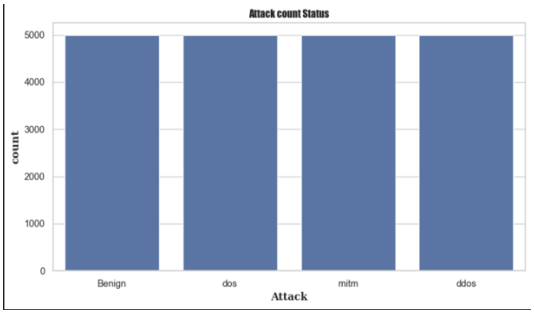
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404566|



Graph. 2. - Attack count Status

The bar graph clearly indicates that all four attack types are identical with a frequency of occurrence of 5000. The uniformity of the height of the bars indicates that there is no skew in the dataset that is, every attack type like Benign, DDoS, DoS, and MiTM, occurs with the same number of instances. Such balanced representation reinforces that no one attack type is predominant andtherefore provides better ease in analysing the distribution of attacks in the data set.

VI. CONCLUSION & FUTURE WORK

In order to improve network security against new cyber threats, research on machine learning methods for Benign, Denial of Service (DoS), Man-in-the-Middle (MiTM), and Distributed Denial of Service (DDoS) attack detection and prevention is essential. The complexities inherent in these attacks require creative solutions that utilise machine learning capabilities. This research aims to tackle these issues and enhance the creation of a resilient and adaptable detection system.

This research employs a hybrid methodology for assault detection. Verifies that the implemented solution aligns with SDN specifications by leveraging the controller's capabilities and the principle that all unmatched packets are directed to the controller. Additionally employs flow statistics, distinctive to SDN, to assist with anomaly detection. Owing to resource constraints, SDN uses a machine learning-based flow-based intrusion detection system that is pre-trained and achieves 98–99% detection accuracy. Due to numerous false positives associated with machine learning detection, entropy computation is intended to augment the flow intrusion detection system (flowIDS). Combining the two approaches made it easier to create a module that gives the controller the ability to identify and neutralise most risks. When applied to real-time network data, the proposed method shows a 99% detection accuracy and a 14% false positive rate, confirming its accuracy and effectiveness.

REFERENCES

1. Bindra, N.; Sood, M. Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset. Autom. Control. Comput. Sci. 2019, 53,419–428
2. Usha, G., Narang, M., Kumar, A. (2021). Detection and Classification of DistributedDoS Attacks Using Machine Learning. In: Smys, S., Palanisamy, R., Rocha, Á.,Beligiannis, G.N. (eds) Computer Networks and Inventive CommunicationTechnologies. Lecture Notes on Data Engineering and CommunicationsTechnologies, vol 58. Springer, Singapore.
3. Gote, A., & Mendhe, V. (2024). Enhancing Resilience: A Solution Framework for Handling Third-Party Service Disruptions in FinTech Mobile Applications. Journal Homepage: http://www. ijmra. us, 14(02).
4. Saini, P.S.; Behal, S.; Bhatia, S. Detection of DDoS attacks using machine learning algorithms. In Proceedings of the 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 12–14 March2020; IEEE: Piscataway, NJ, USA, 2020;
5. Sambangi, S.; Gondi, L. A Machine Learning Approach for DDoS (Distributed Denialof Service) Attack Detection Using Multiple Linear Regression. Proceedings 2020,63, 51.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details