International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I6P113

Volume 73 Issue 6, 149-156, June 2025

Original Article

A Hybrid Machine Learning approach for Analysis & Identification of Cyber Security Attacks

Satya Srinivas Maddipati[1*], A Siva Naga Ram Gopal[1], Rakesh Kancharla[2], PVVS Eswar Rao[1], DSV Prasad Uppalapati[1]

[1]*Department of CSE, Sasi Institute of Technology & Engineering, Andhra Pradesh, India.*
[2]*Department of CSE, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India.*

[*]*Corresponding Author : maddipativas@gmail.com*

Received: 03 December 2024 Revised: 24 May 2025 Accepted: 29 May 2025 Published: 28 June 2025

Abstract - *Providing security for resources in the internet is an essential task. Now a days, the major threats in the cyber world are Denial of Service (DoS), Malware and Intruders. These types of attacks must be predicted in advance with high accuracy using machine learning techniques. This research work analyses the network traffic patterns for cyber-attacks and identifies the type of attack. This work proposes apriori algorithm to extract frequent patterns from network traffic for cyber-attacks and also applies logistic regression to identify the type of attack. The results of proposed work compared with other machine learning algorithms like Decision trees, Random forest and support vector machines. The results of this work identified the network traffic frequent patterns with above 65% confidence and proved that the average accuracy was increased by 5% using proposed work.*

Keywords - *Denial of Service, Cyber-attacks, Machine Learning algorithms, Network traffic frequent patterns, Logistic regression.*

1. Introduction

1.1. Cybersecurity Threats and Detection Approaches

Cybersecurity threats have been escalating significantly in recent times. These threats can compromise local systems or networks by introducing malicious software, disrupting access to critical resources, or making them unavailable to legitimate users. Malware refers to malicious software designed to damage or gain unauthorized control over systems and data. Common cybersecurity threats include malware attacks, unauthorized system access by intruders, and Denial-of-Service (DoS) attacks.

1.1.1. Malware

Malware is a type of software intentionally created by cybercriminals to damage systems or steal sensitive data. It often infiltrates systems through deceptive advertisements or links, running silently in the background to capture confidential information such as passwords. This information is then transmitted to unauthorized third parties for exploitation. One of the most dangerous types of malware today is ransomware, which encrypts a victim's data using the attacker's public encryption key. Victims are then asked to pay a ransom, often in cryptocurrencies like Bitcoin, to receive the decryption key. Ransomware attacks have led to significant financial losses and have impacted the operations and reputations of several organizations, including cloud service providers.

1.1.2. Intruders

Intruders are unauthorized individuals or systems that attempt to breach network or local system security to access or manipulate data. They often exploit system vulnerabilities to steal sensitive information. Intrusion Detection Systems (IDS) are used to detect and mitigate such unauthorized access.

Types of IDS include:

1. Network-based IDS (NIDS): Monitors and analyzes network traffic to detect unusual patterns or anomalies.
2. Host-based IDS (HIDS): Periodically scans system files and logs to detect unauthorized access or changes.
3. Application-based IDS: Focuses on monitoring application traffic and user activity to identify suspicious behavior.

1.1.3. Denial of Service (DoS)

DoS attacks are designed to overwhelm servers or networks with excessive requests, thereby preventing legitimate users from accessing services. Attackers flood the system with traffic, consuming resources and leading to service disruption.

Types of DoS attacks include

1. Application-level Flooding: A large volume of service requests are sent using spoofed IP addresses to slow down

or crash the application.
2. Distributed Denial of Service (DDoS): Coordinated attacks using compromised devices (botnets or zombie machines) to flood a target with traffic.
3. Unintentional DoS: Occurs when legitimate users simultaneously access a resource during peak demand, unintentionally causing service interruptions.

1.2. Machine Learning Methods for Cyber Threat Detection

To counteract cybersecurity threats, early detection is essential. Machine learning techniques, including supervised and unsupervised learning, are widely used for this purpose. These methods can help in analyzing and recognizing abnormal network behavior.

1. Unsupervised Learning: Algorithms such as Apriori and FP-Growth are used for association rule mining, helping to identify recurring patterns in network traffic and detect anomalies without prior labeling.
2. Supervised Learning: Patterns identified through unsupervised methods are used to train models, such as decision trees, to classify the type and severity of threats.

1.3. Dataset Description

The dataset used for analysis contains 40,000 entries, each with 25 features. These features cover various network parameters, including:

1. Traffic Metrics: Timestamps, source/destination IP addresses and ports, protocol type, packet details, traffic classification, and payload data.
2. Attack Classification: Identifies the type of attack (Malware, DDoS, Intrusion).
3. Attack Signature: Categorized as Known Pattern A or Known Pattern B.
4. Response Actions: Indicates whether the attack was logged, blocked, or ignored.
5. Severity Levels: Labeled as low, medium, or high.
6. Network Segments: Segment A, B, or C.
7. Log Sources: Logs may originate from either the server or the firewall.

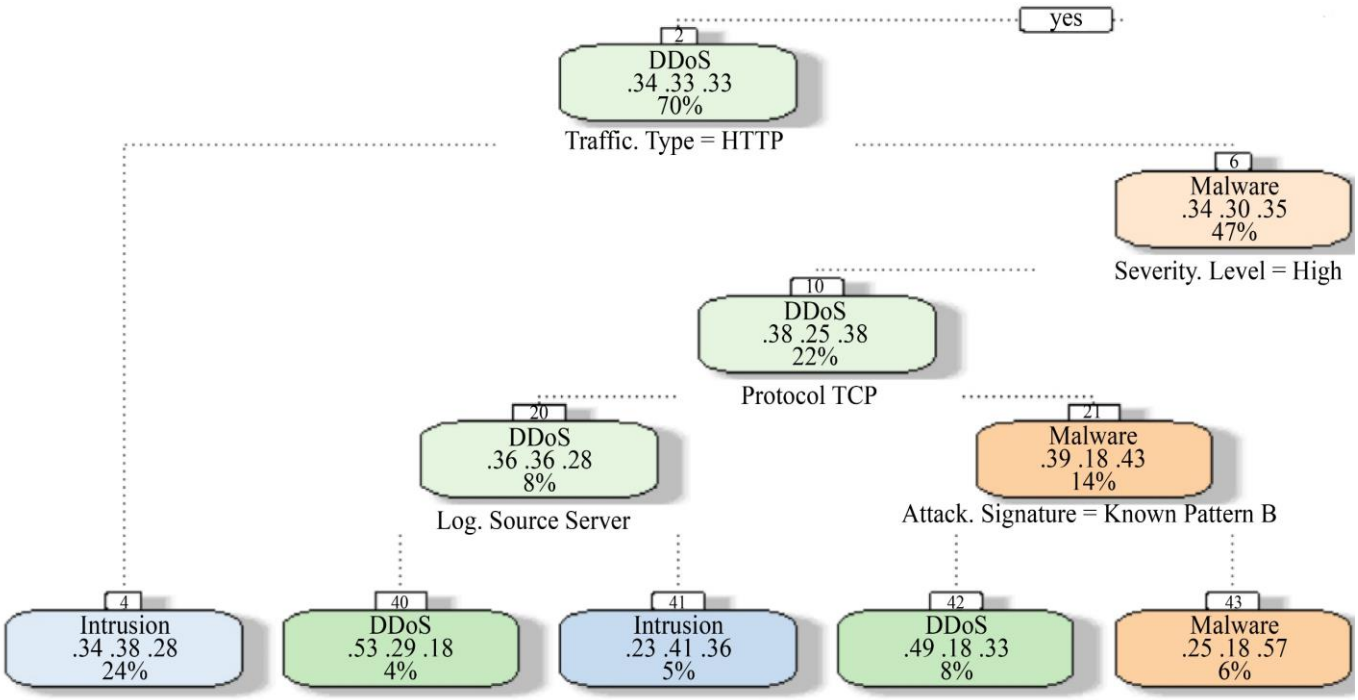

Fig. 1 Decision tree to classify cyber security threat

This paper is organized as follows: Chapter 2 presents a review of existing literature on the application of machine learning techniques to cybersecurity threat detection. Chapter 3 outlines the proposed methodology for identifying and analyzing cyber threats using machine learning. Chapter 4 discusses the results, comparing the proposed approach with existing models.

1.4. Research Gap

1. Identify the network pattens for various types of cyber security attacks
2. Improve the accuracy in prediction of cyber security attacks
3. Identify non-linear relationship between network pattens

2. Literature Review

2.1. DDoS Detection with Machine Learning

Machine learning techniques are increasingly used to detect cyber threats, particularly Distributed Denial of Service (DDoS) attacks. C. Malathi et al. [1] explored the use of machine learning algorithms for detecting coordinated attacks in IoT environments. Denial of Service attacks overwhelm servers with malicious traffic, disrupting services. R. A. Karthika et al. [2] employed various classifiers to accurately identify such threats.

Incremental learning, which builds classifiers from evolving data streams, was applied by V.M.R.M et al. [3] using the ARFC algorithm to improve detection rates. N. S. Deepak et al. [4] developed two models using Support Vector Machines and logistic regression-one to identify malicious users, and another to predict behavior by comparing offender and victim attributes. Cyber-Physical Systems (CPS), which integrate IoT devices with physical infrastructure, are especially vulnerable to DoS attacks. Z.N. Zarandi et al. [5] used deep neural networks to detect and isolate threats early in such systems. S.

K. Naing et al. [6] reviewed machine learning models for classifying DDoS attacks and found logistic regression to be particularly effective. S. Santhosh et al. [7] compared the performance of XGBoost and Random Forest for DDoS detection, concluding that XGBoost had higher accuracy. S. Vattikuti et al. [8] proposed Fast Entropy and attribute thresholding for anomaly detection. Ismail et al. [9] used the UNWS-np-15 dataset to evaluate Random Forest and XGBoost models, achieving around 89–90% accuracy.

A hybrid deep learning-based framework achieved 98.37% accuracy in detecting DDoS attacks [10]. Another approach separated normal and anomalous traffic to preserve service integrity during attacks [11]. J. Cheng et al. [12] proposed an ensemble method using multiple kernel learning to enhance adaptive detection. S. Balasubramaniam et al. [13] integrated Gradient Hybrid Leader Optimization to augment data, achieving high true positive and negative rates.

S. Sumathi et al. [14] designed a Long Short-Term Memory (LSTM)-based model optimized with Particle Swarm Optimization (PSO) for DDoS detection in cloud environments. L. Zhou [15] examined packet size patterns to distinguish between types of DDoS traffic. X. Yu et al. [16] introduced a semi-supervised approach combining spectral clustering and Random Forest to detect application-layer attacks. B. Jia et al. [17] used singular value decomposition followed by multiple classifiers-Random Forest, KNN, and CART-for hybrid detection. L. Xinlong [18] also applied hybrid deep learning techniques to identify malicious DDoS traffic. Halit Bakir et al. [19] extracted relevant features using neural network-based autoencoders and evaluated multiple classifiers like LightGBM, CART, and SVMs.

2.2. Malware Detection Using Machine Learning

Multiple studies have explored the detection of malware using machine learning. Halit Bakir et al. [19] utilized neural autoencoders for feature extraction, followed by traditional classifiers. Pharnika Bhat et al. [20] applied ensemble methods-bagging and boosting-for Android malware detection, with boosting achieving 98.08% accuracy. Hani Alomari et al. [21] developed a framework using SMOTE for class balancing, PCA for feature normalization, and LightGBM for malware classification. A. Abusnaina et al. [22] introduced a fine-grained deep learning model analyzing control flow graphs for high-accuracy detection in IoT networks.

D.O. Sahin et al. [23] tested Decision Trees, KNN, SVM, and Random Forest models, showing that linear regression models performed well without high complexity. H. Alamro et al. [24] proposed a stacked deep learning approach using LS-SVM, KELM, and RRVFL-NN, optimized via Hyperparameter Optimization (HPO). Z. Fang et al. [25] proposed DQFS, which integrates Deep Q-learning for automated feature selection, improving malware detection accuracy. H.-J. Zhu et al. [26] introduced a hybrid model using Merged Sparse Auto-Encoders and Stacked Denoising Autoencoders. A. Azmoodeh et al. [27] proposed a model translating opcode sequences into vector space for classification using eigenspace learning. T. Kim et al. [28] presented a multimodal deep learning framework that incorporates feature similarity and co-occurrence. Chin-Wei Tien et al. [29] employed statistical feature analysis and ML techniques to categorize IoT malware.

2.3. Intrusion Detection with Machine Learning

Deep learning techniques have also been extensively researched for intrusion detection. I. Ahmad et al. [32] applied multi-layer neural networks, SVM, and extreme learning methods. G. De Carvalho Bertoli et al. [33] introduced a five-stage framework called AB-TRAP, achieving an F1-score of 95% and an AUC of 98%. A. Guezzaz et al. [34] used neural networks to classify heterogeneous traffic using mathematical models. L. Zou et al. [35] proposed a two-stage model: hierarchical clustering for initial decision tree construction and TSVM for final classification. Abdullah Alsaeedi et al. [36] compared CART, Random Forest, Naïve Bayes, and SVM, concluding that CART and Random Forest outperformed others. Abdallah R. Gad et al. [37] used Chi-square tests, correlation matrices, and SMOTE for preprocessing, finding XGBoost superior for intrusion detection in IoT.

A. V. Turukmane et al. [38] developed a complete pipeline including Min-Max normalization, Modified SVD for feature extraction, and a MultiSVM classifier. Md. A. Hossain et al. [39] proposed a stacking ensemble model using RF, Gradient Boost, Adaboost, and XGBoost, which achieved 99% accuracy.

3. Methodology

3.1. Data Preprocessing

In the initial stage, feature engineering is applied to extract significant attributes from the dataset, eliminating redundant ones such as user details, device metadata, proxy information, timestamps, alerts, and geolocation data.

3.2. Proposed Approach

The methodology involves identifying frequent traffic patterns using a custom algorithm named Find Frequent Itemsets, which analyzes traffic characteristics such as protocol type, traffic classification, network segment, and log source. The dataset is divided into training and testing subsets using k-fold cross-validation. Logistic regression is then used to train a classifier on the training data.

The model's performance is evaluated on the test set. Figure 2 illustrates the architectural design of the proposed system.

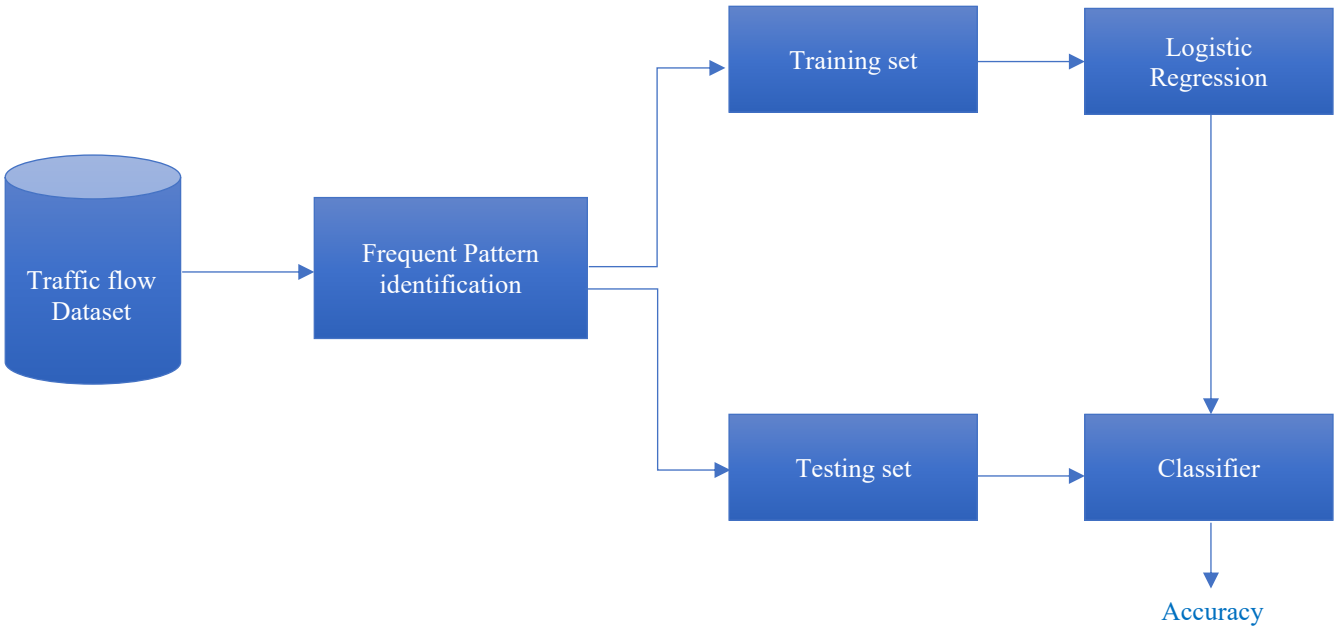

Fig. 2 Architecture diagram of proposed methodology

3.3. Algorithm

```
FindFrequencyItemsets(Dataset,globalConfidence)
for i = 1 to ncol(Dataset)
        Itemsets[i]<-split(Dataset[,i])
for i=1 to ncol(Dataset)
 for j= 1 to i
                (Cand_itemset[k,j],
        itemsetConfidence)=FrequencyDetermine(Itemset[i:
        j], j)
                if(itemsetConfidence>globalConfidence)
         Output(Candidate_itemset[k,j])

Algorithm: FrequencyDetermine(Itemset[i:j],j)
for l=i to j
 for m=1 to l
 frequency=Count(Match(Itemset(l:m))
 confidence=frequency/nrow(Dataset)
return (Itemset[i:j],confidence)
Algorithm: CyberAttackTypeIdentification
{
globalConfidence=0.65;
Dataset<-load("cyberthreats.csv")
frequentItemsets=
FindFrequencyItemsets(Dataset,globalConfidence)
data_train=(Dataset,0.7)
data_test=(Dataset,0.3)
data_train_input=data_train[,1:n-1]
data_train_target=data_train[,n]
data_test_input=data_test[,1:n-1]
data_test_target=data_test[,n]
lgr_model=fit.logisticRegression(data_train_input,data_train
_target)
model_output=predict(lgr_model,data_test_input)
Accuracy=Match(data_test_target,model_output)/nrow(data_
test)
Error rate=1-Accuracy
Output(Accuracy)
Output(Error rate)
```

4. Results & Discussion

This section presents frequent patterns (Network traffic features) identified by proposed methodology. Figure 3 shows the frequent patterns for various types of cyber threats and Table 1 represents Network Traffic Frequent Patterns along with confidence values.

4.1. Frequent Patterns for Different Cyber Security Threats

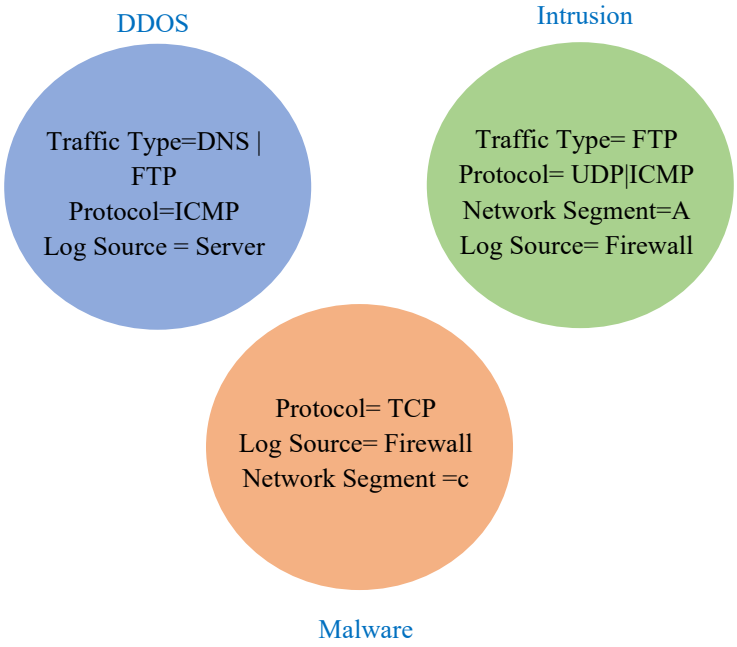

Fig. 3 Frequent patterns for different cyber security threats

Table 1. Network traffic frequent patterns along with confidence values

S.No	Network Traffic Frequent Pattern	Confidence
1	{Network Segment=Segment C, Log Source=Firewall} {Attack Signature=Known Pattern B} => {Type of attack=DDoS}	0.67
2	{Packet Type=Control, Traffic Type=DNS}, {Log Source=Server} => {Type of attack=DDoS}	0.67
3	{Traffic Type=DNS, Log Source=Firewall}, {Packet Type=Data} => {Type of attack=DDoS}	0.68
4	{Traffic Type=FTP, Log Source=Server}, {Packet Type=Data} => {Type of attack=DDoS}	0.75
5	{Packet Type=Data, Traffic Type=FTP}, {Log Source=Server} => {Type of attack=DDoS}	0.66
6	{Protocol=ICMP, Attack Signature=Known Pattern A}, {Log Source=Server} => {Type of attack=DDoS}	0.66
7	{Protocol=ICMP, Attack Signature=Known Pattern A} {Log Source=Firewall} => {Attack Type= Intrusion}	0.75
8	{Traffic Type=FTP, Attack Signature=Known Pattern B} {Log Source=Firewall} => {Attack Type= Intrusion}	0.72
9	{Attack Signature=Known Pattern A, Network Segment=Segment A}, {Packet Type=Data} => {Attack Type= Intrusion}	0.71
10	{Protocol=UDP, Attack Signature=Known Pattern A}, {Packet Type=Data} => {Attack Type= Intrusion}	0.69
11	{Protocol=UDP, Packet Type=Data}, {Attack Signature=Known Pattern A} => {Attack Type= Intrusion}	0.69
12	{Action Taken=Ignored, Log Source=Server}, {Packet Type=Data} => {Attack Type= Intrusion}	0.7
13	{Protocol=ICMP, Severity Level=High}, {Packet Type=Data} => {Attack Type= Intrusion}	0.68
14	{Protocol=ICMP, Severity Level=High}, {Log Source=Firewall} => {Attack Type= Intrusion}	0.68
15	{Network Segment=Segment C}, {Log Source=Firewall} => {Attack Type= Malware}	0.71
16	{Packet Type=Control, Severity Level=High}, {Log Source=Firewall} => {Attack Type= Malware}	0.73
17	{Severity Level=High, Log Source=Firewall}, {Packet Type=Control} => {Attack Type= Malware}	0.75
18	{Packet Type=Control, Action Taken=Blocked}, {Log Source=Firewall} => {Attack Type= Malware}	0.75
19	{Packet Type=Control, Network Segment=Segment C}, {Log Source=Firewall} => {Attack Type= Malware}	0.77
20	{Network Segment=Segment C,Log Source=Firewall}, {Packet Type=Control} => {Attack Type= Malware}	0.74

21	{Packet Type=Data, Severity Level=Low}, {Attack Signature=Known Pattern B} => {Attack Type= Malware}	0.72
22	{Protocol=TCP, Attack Signature=Known Pattern A}, {Packet Type=Control} => {Attack Type= Malware}	0.78
23	{Attack Signature=Known Pattern A, Network Segment=Segment C}, {Log Source=Firewall} => {Attack Type= Malware}	0.84
24	{Protocol=TCP, Packet Type=Data}, {Attack Signature=Known Pattern B} => {Attack Type= Malware}	0.76
25	{Action Taken=Logged, Severity Level=Medium}, {Log Source=Firewall} => {Attack Type= Malware}	0.72
26	{Action Taken=Logged, Network Segment=Segment B}, {Packet Type=Data} => {Attack Type= Malware}	0.8

Figure 4 presents frequency plots of various patterns of different cyber security threats and Table 2, 3 presents the confusion matrix and accuracy, precision and recall values of various machine learning algorithms.

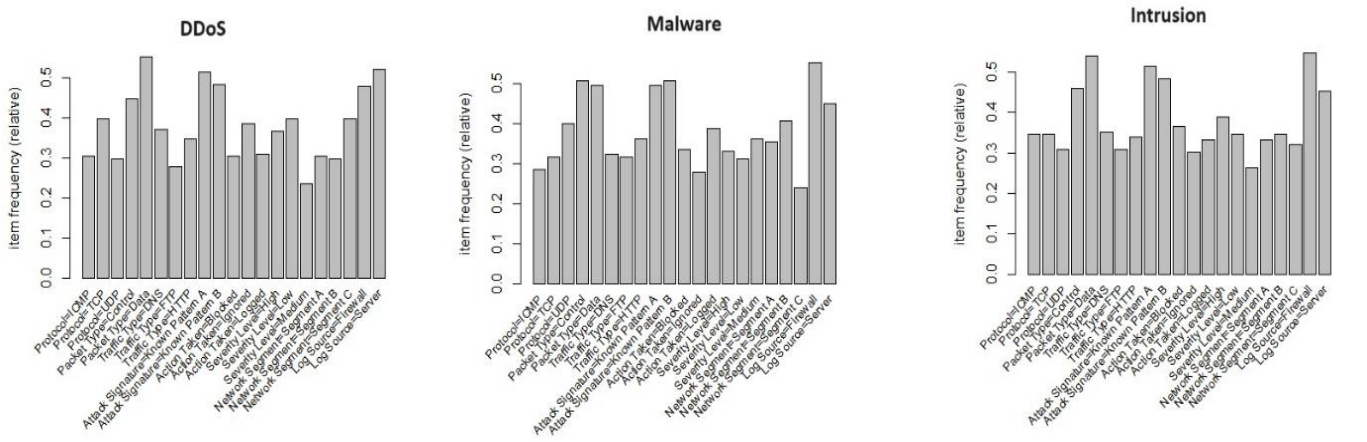

Fig. 4 Frequency plots for network traffic patterns

Table 2. Confusion matrix of proposed model (Apriori + Logistic regression)

Actual/Predicted	Actual		
Predicted	**DDoS**	**Malware**	**Intrusion**
DDoS	14250	287	386
Malware	204	16147	146
Intrusion	252	134	8194

Table 3. Accuracy of various machine learning models

Name of the Algorithm	Accuracy	Precision	Recall
Decision Tree	0.91	0.78	0.85
Random Forest	0.95	0.82	0.86
Support Vector Machines	0.90	0.65	0.72
Apriori + Logistic Regression	0.964	0.92	0.94

5. Conclusion

Analysing and identifying cyber security attacks in advance is a major challenge. The proposed work analysed the network traffic patterns for cyber security attacks using apriori algorithm with confidence level grater than 65% and identified the type of cyber security attack using logistic regression with 97% accuracy. The results of proposed work compared with other existing machine learning algorithms and proved that the accuracy was increased by 5% compared to other machine learning algorithms.

Acknowledgement

We would like to thank Management, Principal for encouraging research towards identification of cyber security attacks.

Data Availability

The dataset used in the research is downloaded from open dataset repository from the following URL https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks

Funding statement

Sasi Institute of Technology & Engineering has sponsored an amount of 55,500 Rupees (Indian currency) for the research carried in this paper.

References

[1] C. Malathi, and I. Naga Padmaja, "Identification of Cyber Attacks Using Machine Learning in Smart IoT Networks," *Materials Today: Proceedings*, vol. 80, pp. 2518-2523, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] R.A. Karthika, and M. Maheswari, "Detection Analysis of Malicious Cyber Attacks Using Machine Learning Algorithms," *Materials Today: Proceedings*, vol. 68, pp. 26-34, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Veeramanickam M.R.M. et al., "Streamed Incremental Learning for Cyber Attack Classification using Machine Learning," *2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, Dehradun, India, pp. 1-5, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Nrusimhadri Sai Deepak et al., "Analyze and Forecast the Cyber Attack Detection Process using Machine Learning Techniques," *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Coimbatore, India, pp. 1732-1738, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Zohre Nasiri Zarandi, and Iman Sharifi, "Detection and Identification of Cyber-Attacks in Cyber-Physical Systems Based on Machine Learning Methods," *2020 11th International Conference on Information and Knowledge Technology (IKT)*, Tehran, Iran, pp. 107-112, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Soe Kalayar Naing, and Tin Thein Thwel, "A Study of DDOS Attack Classification Using Machine Learning Classifiers," *2023 IEEE Conference on Computer Applications (ICCA)*, Yangon, Myanmar, pp. 108-112, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] S. Santhosh, M. Sambath, and J. Thangakumar, "Detection of DDOS Attack Using Machine Learning Models," *2023 International Conference on Networking and Communications (ICNWC)*, Chennai, India, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sakshi Vattikuti et al., "DDoS Attack Detection and Mitigation using Anomaly Detection and Machine Learning Models," *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, Bangalore, India, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Ismail et al., "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, pp. 21443-21454, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Asmaa A. Elsaeidy, Abbas Jamalipour, and Kumudu S. Munasinghe, "A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City," *IEEE Access*, vol. 9, pp. 154864-154875, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Jieren Cheng et al., "Adaptive DDoS Attack Detection Method Based on Multiple-Kernel Learning," *Security and Communication Networks*, vol. 2018, no. 1, pp. 1-19, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[12] S. Balasubramaniam et al., "Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing," *International Journal of Intelligent Systems*, vol. 2023, no. 1, pp. 1-16, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] S. Sumathi, R. Rajesh, and Sangsoon Lim, "Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection," *Journal of Sensors*, vol. 2022, no. 1, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Lu Zhou et al., "Low-Rate DDoS Attack Detection Using Expectation of Packet Size," *Security and Communication Networks*, vol. 2017, no. 1, pp. 1-14, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] Xiang Yu et al., "Web DDoS Attack Detection Method Based on Semisupervised Learning," *Security and Communication Networks*, vol. 2021, no. 1, pp. 1-10, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Bin Jiae et al., "A DDoS Attack Detection Method Based on Hybrid Heterogeneous Multiclassifier Ensemble Learning," *Journal of Electrical and Computer Engineering*, vol. 2017, no. 1, pp. 1-9, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[17] Li Xinlong, and Chen Zhibin, "DDoS Attack Detection by Hybrid Deep Learning Methodologies," *Security and Communication Networks*, vol. 2022, no. 1, pp. 1-7, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Hoda El Merabet, and Abderrahmane Hajraoui, "A Survey of Malware Detection Techniques based on Machine Learning," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 1, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Halit Bakır, and Rezan Bakır, "DroidEncoder: Malware Detection Using Auto-Encoder Based Feature Extractor and Machine Learning Algorithms," *Computers and Electrical Engineering*, vol. 110, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Parnika Bhat, Sunny Behal, and Kamlesh Dutta, "A System Call-Based Android Malware Detection Approach with Homogeneous & Heterogeneous Ensemble Machine Learning," *Computers & Security*, vol. 130, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Hani AlOmari, Qussai M. Yaseen, and Mohammed Azmi Al-Betar, "A Comparative Analysis of Machine Learning Algorithms for Android Malware Detection," *Procedia Computer Science*, vol. 220, pp. 763-768, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Jagsir Singh, and Jaswinder Singh, "A Survey on Machine Learning-Based Malware Detection in Executable Files," *Journal of Systems Architecture*, vol. 112, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Ahmed S. Shatnawi, Qussai Yassen, and Abdulrahman Yateem, "An Android Malware Detection Approach Based on Static Feature Analysis Using Machine Learning Algorithms," *Procedia Computer Science*, vol. 201, pp. 653-658, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Ahmed Abusnaina et al., "DL-FHMC: Deep Learning-Based Fine-Grained Hierarchical Learning Approach for Robust Malware Classification," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 3432-3447, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Durmus Ozkan Sahın, Sedat Akleylek, and Erdal Kilic, "LinRegDroid: Detection of Android Malware Using Multiple Linear Regression Models-Based Classifiers," *IEEE Access*, vol. 10, pp. 14246-14259, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Hayam Alamro et al., "Automated Android Malware Detection Using Optimal Ensemble Learning Approach for Cybersecurity," *IEEE Access*, vol. 11, pp. 72509-72517, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Zhiyang Fang et al., "Feature Selection for Malware Detection Based on Reinforcement Learning," *IEEE Access*, vol. 7, pp. 176177-176187, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[28] Huijuan Zhu et al., "A Hybrid Deep Network Framework for Android Malware Detection," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 12, pp. 5558-5570, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] Amin Azmoode, Ali Dehghantanha, and Kim-Kwang Raymond Choo, "Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 88-95, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] TaeGuen Kim et al., "A Multimodal Deep Learning Method for Android Malware Detection Using Various Features," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 773-788, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[31] Chin-Wei Tie et al., "Machine Learning Framework to Analyze IoT Malware Using ELF and Opcode Features," *Digital Threats: Research and Practice*, vol. 1, no. 5, pp. 19, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[32] Jan Lansk et al., "Deep Learning-Based Intrusion Detection Systems: A Systematic Review," *IEEE Access*, vol. 9, pp. 101574-101599, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[33] Iftikhar Ahmad et al., "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," *IEEE Access*, vol. 6, pp. 33789-33795, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[34] Gustavo De Carvalho Bertoli et al., "An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System," *IEEE Access*, vol. 9, pp. 106790-106805, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[35] Azidine Guezzaz et al., "Mathematical Validation of Proposed Machine Learning Classifier for Heterogeneous Traffic and Anomaly Detection," *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 18-24, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[36] Li Zou et al., "HC-DTTSVM: A Network Intrusion Detection Method Based on Decision Tree Twin Support Vector Machine and Hierarchical Clustering," *IEEE Access*, vol. 11, pp. 21404-21416, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[37] Abdullah Alsaeedi, and Mohammad Zubair Khan, "Performance Analysis of Network Intrusion Detection System using Machine Learning," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 12, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[38] Abdallah R. Gad et al., "A Distributed Intrusion Detection System using Machine Learning for IoT based on ToN-IoT Dataset" *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 13, no. 6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[39] Anil Vitthalrao Turukmane, and Ramkumar Devendiran, "M-MultiSVM: An Efficient Feature Selection Assisted Network Intrusion Detection System using Machine Learning," *Computers & Security*, vol. 137, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[40] Md. Alamgir Hossain, and Md. Saiful Islam, "Ensuring Network Security with a Robust Intrusion Detection System Using Ensemble-Based Machine Learning," *Array*, vol. 19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[41] Ricardo Misael Ayala Molina, "On Ransomware Family Attribution Using Pre-Attack Paranoia Activities," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 19-36, 2022. [CrossRef] [Google Scholar] [Publisher Link]