International Journal of Electrical and Computer Engineering (IJECE)
Vol. 16, No. 1, February 2026, pp. 437~449
ISSN: 2088-8708, DOI: 10.11591/ijece.v16i1.pp437-449

IDPS: A machine learning framework for real-time intrusion detection and protection system for malicious internet activity

Raisa Fabiha[1], Stein Joachim Reberio[1], Zubayer Farazi[1], Fernaz Narin Nur[2], Shaheena Sultana[1], A. H. M. Saiful Islam[1]
[1]Department of Computer Science and Engineering, Notre Dame University, Dhaka, Bangladesh
[2]Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh

Article Info

Article history:

Received Apr 7, 2025
Revised Oct 12, 2025
Accepted Nov 23, 2025

Keywords:

Intrusion detection
Machine learning algorithms
Network forensics
Packet analysis
Real-time Protection

ABSTRACT

With the increasing frequency and complexity of cyber threats, there is a pressing need for effective real-time solutions to detect and prevent malicious activities. This study introduces a novel machine learning-based architecture for real-time cybersecurity to enhance accurate identification and prevention of malicious cyber activities. The proposed framework combines advanced machine learning algorithms with Wireshark network traffic analysis to effectively detect and classify a wide range of cyberattacks, providing timely and actionable insights to cybersecurity professionals. A core component of this system is a prototype blocker, which is seamlessly integrated with Cisco infrastructure, enabling proactive intervention by blocking suspicious IP addresses in real-time. In addition, a user-friendly web application enhances system operability by offering intuitive data visualization and analytical tools, enabling rapid and informed decision-making. This comprehensive approach not only strengthens network security and protects digital assets but also equips defenders with the capability to respond effectively to the dynamic landscape of cyber threats.

Corresponding Author:

Fernaz Narin Nur
Department of Computer Science and Engineering, Daffodil International University
Dhaka, Bangladesh
Email: fernaznur@gmail.com

1. INTRODUCTION

The internet has become an essential component of everyday life in today's world, influencing nearly every aspect of society. People are more dependent on the internet than ever because to the advancement of smartphones, internet of things (IoT) devices, and fast connections. Because online communication is so widely used, a wide range of cyberthreats, such as ransomware, phishing, malware, and data breaches, can affect people, companies, and infrastructure [1]. Economic stability, security, and privacy are all seriously jeopardized by these challenges.

As network-related crimes increase, enhanced cybersecurity and monitoring are essential to combat these threats. Network forensics plays a key role by investigating security incidents, identifying vulnerabilities, and tracing the sources of cyber threats. It involves capturing and analyzing network traffic to uncover details about communication, such as source, destination, timing, and content [2], [3]. This approach is critical for responding to and preventing internet-related crimes. Packet analysis is a crucial method in network forensics to gather evidence and detect suspicions. network activities, including intrusion attempts, brute force, port scans, distributed denial-of-service (DDoS), and denial-of-service (DoS) [4], [5], [6].

Machine learning (ML) techniques combined with network forensics enhance cybersecurity by enabling faster and more efficient threat detection. Unlike traditional methods, which are time-consuming and may miss new attacks, machine learning can identify complex patterns and anomalies in network traffic. Studies, such as those by Naqash *et al.* [7] and Shivare *et al.* [8], show the effectiveness of machine learning-based intrusion detection systems (IDS), including hybrid models with convolutional neural networks (CNNs) and long short-term memory (LSTMs). Using supervised learning on datasets like Canadian Institute for Cybersecurity Intrusion Detection System 2017 dataset (CICIDS-2017) helps classify threats, while packet analysis allows for detecting zero-day attacks. Integration with real-time tools like Wireshark further strengthens threat detection and response capabilities.

Despite these advancements, most existing systems focus only on detection without implementing real-time mitigation strategies. There is a pressing need for intelligent, automated systems that can both detect and proactively respond to cyber threats in real-time. To address this gap, this paper proposes an advanced real-time intrusion detection and protection system (IDPS) that combines machine learning, network forensics, and automated blocking to detect, analyze, and mitigate cyber threats in real-time. The framework integrates network traffic analysis using Wireshark with machine learning algorithms to classify and block malicious activities, contributing to enhanced cybersecurity practices. Thaseen *et al.* [9] specifically analyzed Wireshark PCAP files, whereas our work uses the CICIDS-2017 dataset, which is widely recognized and consists of different types of attacks along with up-to-date network attack patterns.

The primary aim of this work is to develop a practical, scalable, and deployable machine learning-based framework that not only detects intrusions with high accuracy but also initiates automated network-level countermeasures. Our central analysis is that combining real-time packet analysis with ML-driven detection and autonomous blocking significantly enhances the effectiveness of intrusion detection systems. The key contributions of our work are as follows:

a. We have used the CICIDS-2017 dataset to train our intrusion detection model and employed Wireshark, a widely used packet-capturing and network analysis tool, to test the model's accuracy with real-time data.
b. We have detected abnormal packets that are automatically logged into a dynamically updated database, which helps prevent potential threats by storing details for further analysis and action.
c. We have developed an interactive web application for visualization and analysis, which provides real-time insights into normal and abnormal network packets, enhancing user understanding of network traffic.
d. A prototype blocker system is developed that retrieves malicious IP addresses identified from the database in real time and proactively blocks these addresses, thereby improving network security.
e. The proposed system demonstrated an accuracy of 81% in classifying network traffic, outperforming similar models in scalability and detection time.

The remainder of this paper is structured as follows: section 2 reviews the relevant literature and previous research in the field. Section 3 outlines the foundational concepts and the intuitive approach underlying our work. The detailed methodology is presented in section 4. Section 5 discusses the results obtained and provides a comprehensive analysis. Finally, section 6 concludes the paper and suggests directions for future research.

2. LITERATURE REVIEW

An intrusion detection system (IDS) is essential for cybersecurity, monitoring network traffic for malicious activities [10]. Detection techniques include packet analysis [11] and flow data analysis [3]. Signature-based IDS detects known threats but struggles with new attacks [9], while anomaly-based approaches use machines to identify zero-day threats [8]. Rule-based and cloud-based methods enhance real-time detection [12]. Machine learning techniques like K-nearest neighbors (K-NN), support vector machine (SVM), and convolutional neural network (CNN) improve accuracy [13], [8], and hybrid systems further enhance detection rates with reduced false positives. Recent studies propose integrated IDS models leveraging ML and rule-based approaches for robust security [14], [15].

Using sophisticated algorithms and in-depth examination of each packet's data, we have selected machine learning-based detection and packet analysis methods for intrusion detection in our study. By combining these strategies, we aim to improve intrusion detection systems' capability to identify and neutralize online threats. Using different strategies, a variety of machine learning models have been proposed on the CICIDS-2017 dataset. In order to identify network assaults in the CICIDS-2017 dataset, Panwar *et al.* [14] used eight supervised classification algorithms, including GaussianNB (GNB), BernoulliNB (BNB), decision tree (DT), K-nearest neighbors (K-NN), logistic regression (LR), support vector machine (SVM), random forest (RF), and stochastic gradient descent (SGD). Three machine learning models were created by Elmasri *et al.* [15] utilizing the local outlier factor (LOF), improved k-nearest neighbors (KNN) algorithms.

Various studies highlight the effectiveness of ML models in detecting network attacks using the CICIDS-2017 dataset [16], [17], [18], [19]. Wireshark, a powerful network protocol analyzer, is widely used for digital forensics and cybersecurity. Kamble *et al*. [20] demonstrated its utility in data collection and monitoring, while Soepeno [21] emphasized its superiority over TCPdump and NetFlow for real-time packet analysis. Dodiya *et al.* [22] utilized Wireshark to identify indicators of compromise (IOCs) for malware detection. Chaudhary *et al.* [23] explored network traffic analysis (NTA) with Wireshark, developing geolocation-based visualization for security tracking. Mabsali *et al.* [24] used Wireshark to detect TCP SYN flood attacks, analyzing traffic patterns and vulnerabilities. Our study builds on these insights by establishing a database to store packet details and developing a web application for intrusion detection analysis and visualization.

3. SYSTEM ARCHITECTURE

There can be many users in a network system that are connected via routers to servers. When an end user's device transmits a packet, it is processed as well as security checked by the default pre-configured router firewall system and then passed through the server's default gateway towards the destination device. Unfortunately, cybercriminals have become so advanced that they can easily break through that default security system and commit crimes without leaving a trace. Therefore, a more secure intelligent security approach is needed, and our IDPS is a suitable tool.

IDPS is trained using the K-NN ML Algorithm that checks various parameters of a packet passing through the server, and it tries to categorize the packet into either normal or non-normal packets. Normal packets are passed, while suspicious ones trigger IP blocking. A dynamic database stores suspicious packet data, which is then used to generate a command log for blocking those IPs in the router's firewall. This process repeats, updating the database with suspicious new data. In Figure 1, we see that our IDPS system is integrated into a network via a primary router. The IDS analyzes packet traffic, allowing normal packets to pass and isolating suspicious ones. Suspicious packet data is stored in a temporary database, which is then used to generate a command log for blocking malicious internet protocol (IP) addresses. Simultaneously, authorized personnel are alerted, enabling rapid IP blocking via the command log, ensuring network security and facilitating forensic analysis.

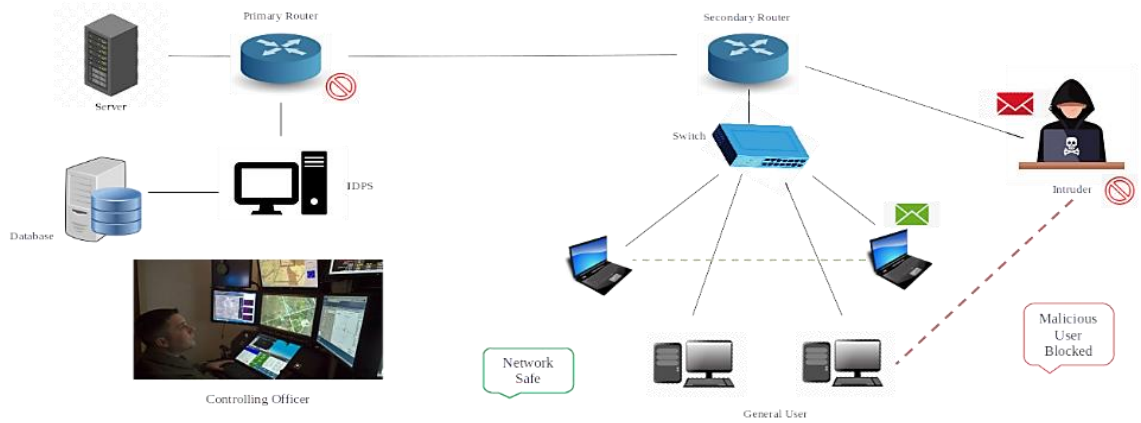


Figure 1. System architecture

4. METHODOLOGY

This section describes the proposed intrusion detection and protection system based on a real-time, machine learning-driven approach. The phases of the methodology are visualized in Figure 2. Real-time network traffic data is collected using wireshark, followed by rigorous cleaning and feature selection to prepare the data for the development of machine learning models. The trained model is then evaluated using Wireshark-captured data to assess its effectiveness in classifying benign and non-benign traffic. Finally, the deployed model predicts the nature of incoming traffic in real-time, enabling the identification of potential intrusions and the implementation of appropriate security measures.

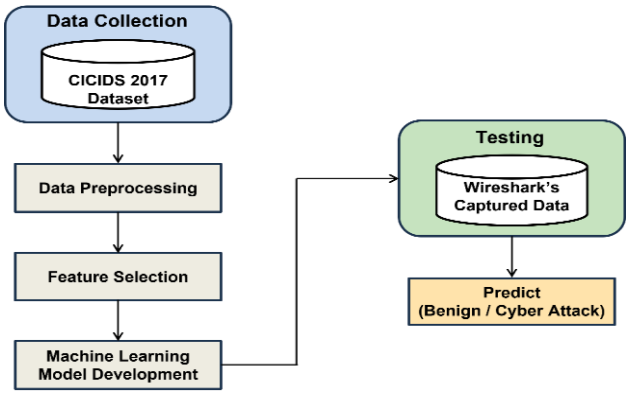


Figure 2. Phases of the methodology

4.1. Phases of methodology

4.1.1. Data collection process

To ensure model robustness and fairness, we have performed comprehensive data preprocessing, including cleaning, balancing, and splitting the dataset. The publicly available CICIDS2017 dataset (79 features) from CICIDS [11] is chosen for its recent network traffic data (5 days) encompassing diverse attacks, including DDoS [25], port scan [26], Botnet [27], Infiltration [28], web attacks: Brute Force Attack, XSS attack [29] and SQL injection attack [30]. Figure 3 describes the files contained within the CICIDS2017 dataset. This figure offers a comprehensive overview of the data structure and organization, enhancing understanding of the dataset's contents.

Name of the Files	Day Activity	Attacks Found	No. of Record
Monday-WorkingHours.pcap_ISCX.csv	Monday	Benign (Normal Human Activities)	5,29,918
Tuesday-WorkingHours.pcap_ISCX.csv	Tuesday	Benign	4,45,910
Wednesday-workingHours.pcap_ISCX.csv	Wednesday	Benign	6,92,704
Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX.csv	Thursday	Benign Web Attack - Brute Force, Web Attack - XSS, Web Attack - Sql Injection	1,70,367
Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX.csv	Thursday	Infiltration	2,88603
Friday-WorkingHours-Morning.pcap_ISCX.csv	Friday	Benign Botnet	1,91,034
Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv	Friday	PortScan	2,86,468
Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv	Friday	DDoS	2,25,746
		Total	28,30,751

Figure 3. Description of files containing the CICIDS 2017 dataset

4.1.2. Data preprocessing

The raw data is thoroughly cleaned, addressing the missing values by imputation and dividing them into training and testing sets for the model evaluation in an unbiased way. To address class imbalance, synthetic minority oversampling technique (SMOTE) is used to generate synthetic data points for the minority class, ensuring a balanced dataset for effective machine learning model training. This preprocessing step significantly improves the reliability of the model by reducing bias introduced by uneven class distribution.

4.1.3. Feature selection

Feature selection plays a crucial role in improving model efficiency and accuracy by identifying the most relevant network parameters for classification. After data pre-processing, a crucial step involves selecting the most informative features for intrusion detection. Rather than randomly choosing features, the selection focuses on those with clear significance to identify network threats. Key features such as 'Destination Port' (distinguishing network services), TCP flags (insights into connection and data flow), and 'Congestion Window Reduced' and 'ECN-Echo' (indicators of congestion control and network health) enhances the ability of the model to differentiate normal traffic from intrusions. As detailed in Table 1, this targeted selection ensures that the model learns relevant patterns for accurate detection.

Table 1. List of selected features

No	No feature name
1	Destination Port
2	Fin
3	Syn
4	Reset
5	Push
6	Acknowledge
7	Urgent
8	Congestion Window Reduced
9	ECN-Echo

4.1.4. Machine learning model development

To identify the best-performing model for our intrusion detection task, we have evaluated multiple classifiers based on standard performance metrics. Established classification algorithms (Gaussian naïve Bayes (GNB), decision tree (DT), random forest (RF), logistic regression (LR), gradient boosting, and K-nearest neighbors (K-NN)) are selected for their effectiveness in handling complex network traffic. The preprocessed data is split for training and testing, allowing each algorithm to optimize its parameters for accurate intrusion detection. Performance is evaluated using accuracy, precision, recall, and F1-score. Among the models evaluated, the K-NN achieves the highest precision (81%), as shown in Figure 4, making it the optimal choice for intrusion detection. Real-time detection capabilities of the framework are further assessed using established metrics, which demonstrate superior accuracy over existing approaches.

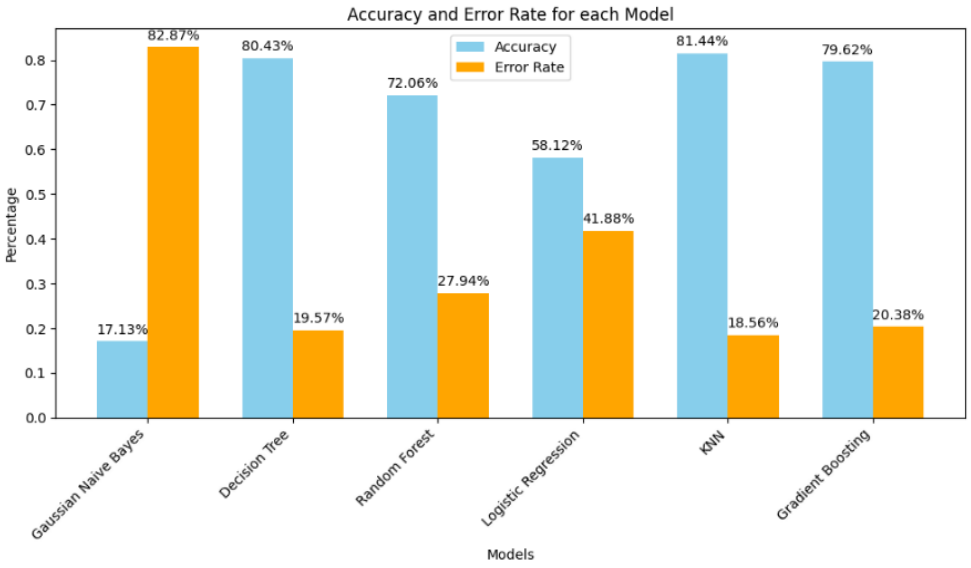
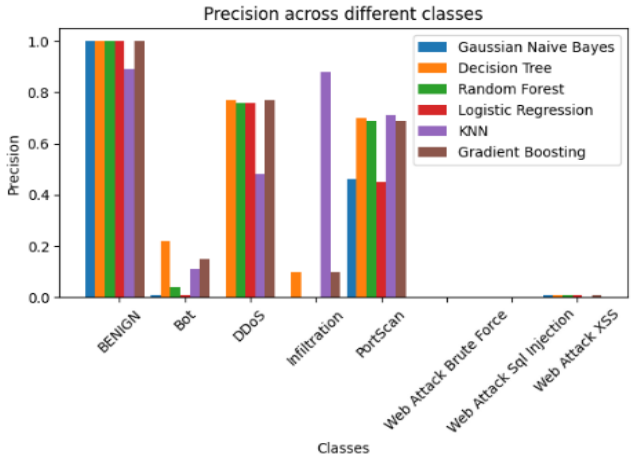


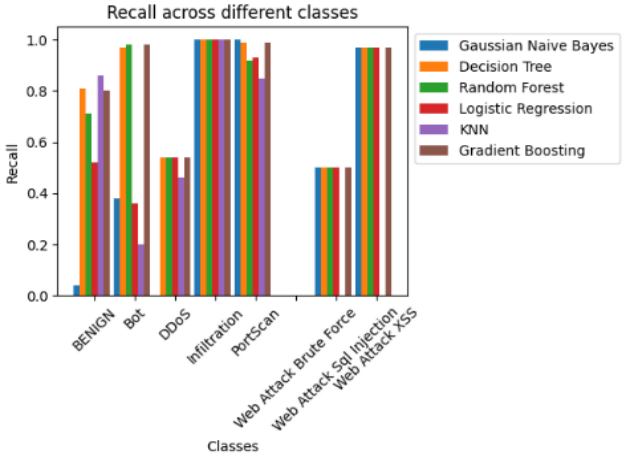
Figure 4. Comparison of accuracy and error rate between algorithms

Incorporating K-NN, the proposed framework is rigorously evaluated for real-time malicious activity detection using established metrics (precision, recall, F1-score, accuracy). Promising results indicate superior accuracy compared to existing approaches for protecting online environments. We present

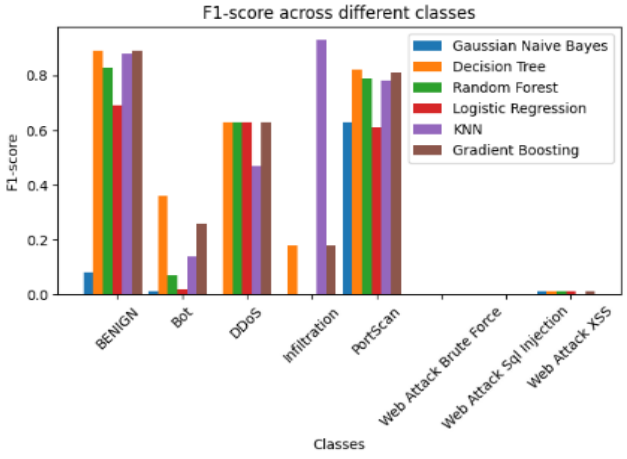
comparisons of precision, recall, and F1-score for each algorithm to analyze framework performance in different metrics. Precision evaluates the accuracy of intrusion detections, recall measures how well actual intrusions are identified, and F1-score balances both. As shown in Figure 5, different algorithms excel in specific scenarios: naive Bayes performs well for benign traffic (precision) in Figure 5(a), infiltration (recall) in Figure 5(b) and PortScan (F1-score) in Figure 5(c), while K-NN struggles with Bot attacks. These variations highlight the trade-offs in algorithm selection for intrusion detection.



(a)



(b)



(c)

Figure 5. Comparison of machine learning algorithms based on (a) precision, (b) recall, and (c) F1-score

4.1.5. Testing using the wireshark PCAP file

Wireshark, a powerful network analyzer [31], is used to capture over 10,000 data points in 7 hours for real-time traffic analysis. The data are pre-processed, including feature selection, imputation, and scaling, to optimize them for machine learning. K-NN is chosen for its superior accuracy in intrusion detection, and its performance is evaluated to validate its effectiveness in distinguishing benign from malicious traffic, enhancing network security.

5. WEB APPLICATION AND PROTOTYPE DEVELOPMENT

After validating the effectiveness of the machine learning model, we have focused on integrating it into a deployable system for practical use. We have chosen a web application for its accessibility and cross-platform compatibility, enabling seamless cybersecurity data analysis for all users. With intuitive tools and visualizations, it simplifies complex insights, empowering non-technical users to evaluate security posture and make informed decisions in Figure 6.

Our infrastructure features a well-designed XAMPP database that stores critical security data, including detected threats and IP addresses, ensuring efficient data management for proactive threat mitigation. A prototype blocker system, implemented using Cisco Packet Tracer in Figure 7, blocks malicious IPs identified by the IDPS system. This integrated framework enhances cybersecurity by enabling real-time threat detection and response, safeguarding digital assets.

Non-BENIGN Predictions

Destination Port	Fin	Syn	Reset	Push	Acknowledgment	Urgent	Congestion Window Reduced	ECN-Echo	KNN Prediction
2720.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
21.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
2720.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
21.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
2720.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
2720.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
2720.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
2720.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
2720.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS
2720.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	DDoS

Figure 6. Non-benign prediction in a table on website

Figure 7. Blocker system prototype in CISCO

6. PERFORMANCE AND RESULT ANALYSIS

K-nearest neighbors (KNN), chosen for its high accuracy (81%), powers our web-based intrusion detection system in real time. It integrates with a secure database to logged threats and block malicious IP addresses proactively, while also providing clear visualizations for security professionals to take action.

6.1. System features

Our feature selection process aims to identify the most impactful features for intrusion detection. While an exhaustive comparison with all recent works is beyond the scope of this paper, Table 2 provides a breakdown of key features employed in our system. This table highlights some of the features utilized by our system for intrusion detection. We may incorporate additional features based on our specific network environment and threat landscape to further optimize the model's performance.

Table 2. Feature comparison with recent works

References	ML	Real-time data	Web application	Prototype
Chaudhary *et al.* [23]	×	✓	✓	×
Mabsali *et al.* [24]	×	✓	×	×
Thockchom *et al.* [32]	✓	×	×	×
Thaseen *et al.* [9]	✓	✓	×	×
IDPS	✓	✓	✓	✓

6.2. System accuracy

Our system prioritizes accuracy, achieving 81% in classifying traffic. Figure 8 compares our model's accuracy with a recent network intrusion detection system (NIDS) [9]. While both show similar accuracy for smaller datasets, ours exhibits better scalability with larger data volumes (2,830,743 vs. 1,130 instances in [9]), suggesting superior generalization. This robustness is further enhanced by our system's proactive prevention capabilities (malicious IP blocking) that extend beyond mere intrusion detection.

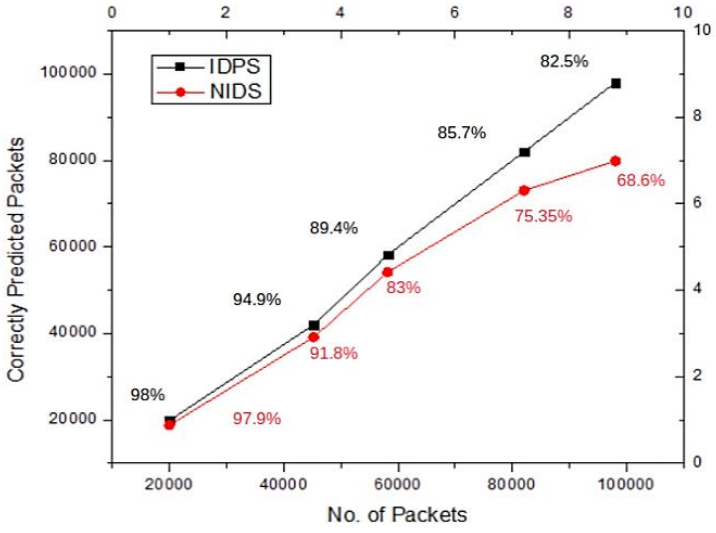


Figure 8. Accuracy matrix

6.3. Detection time

Our system emphasizes real-time performance, with a detection time scale proportional to the number of packets analyzed, as illustrated in Figure 9. This capability ensures that our system responds more rapidly compared to a recent NIDS [9], particularly when handling larger data volumes. The reduced detection time is crucial as it allows for swift mitigation of security threats, thereby enhancing the overall security posture and minimizing potential damage. This efficiency in processing and response is vital to maintaining robust network security, enabling the timely identification and neutralization of malicious activities.

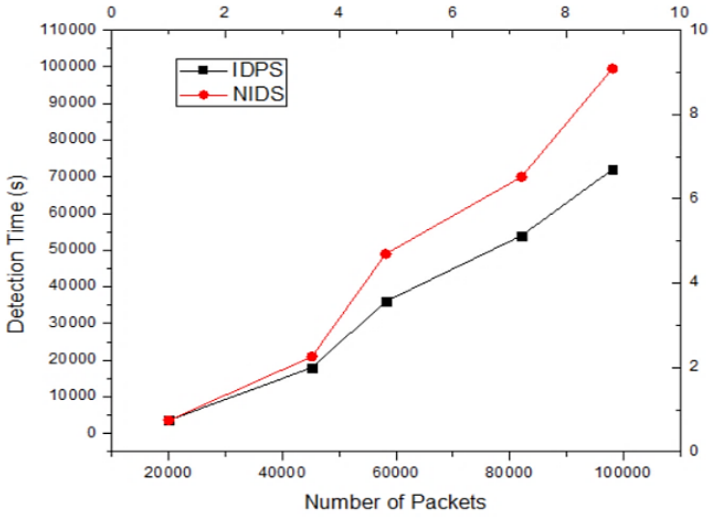


Figure 9. Detection time comparison

6.4. User feedback

User feedback is crucial for IDPS improvement. We gathered feedback from 10 users, most of them recommending the system, as shown in Figure 10. This feedback loop informs future development efforts to improve usability and effectiveness against evolving cyber threats.

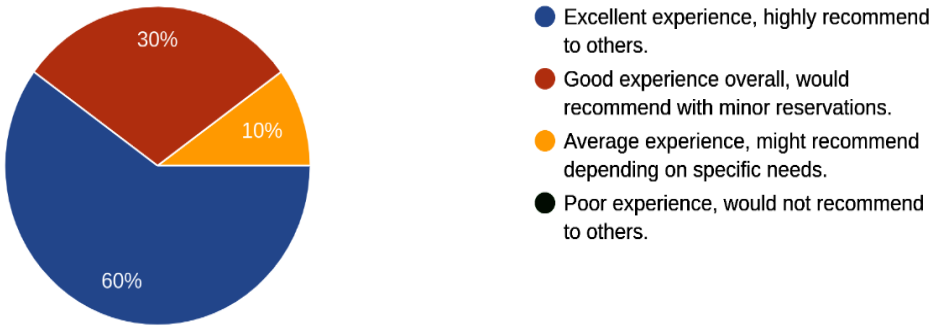


Figure 10. User feedback

7. CONCLUSION

This study proposed an intelligent, real-time intrusion detection and protection system (IDPS) that integrates machine learning, network forensics, and automated response mechanisms to detect and mitigate malicious network activities. As stated in the Introduction, the primary objective was to develop a practical and deployable framework capable of accurate intrusion detection and timely mitigation, and the results and discussion confirm that this objective has been successfully achieved. The experimental evaluation demonstrates that integrating packet-level traffic analysis with a trained machine learning model and dynamic IP blocking enhances both detection accuracy and real-time protection in modern networks.

The findings validate the compatibility between the expected outcomes and the achieved results, highlighting the effectiveness of combining machine learning with real-time network traffic analysis. Based on these results, future research may focus on improving detection accuracy through advanced learning models, integrating edge computing and federated learning for scalability, and deploying the system in real-world network environments. Overall, the proposed framework provides a strong foundation for developing intelligent and scalable cybersecurity solutions applicable to enterprise networks, smart infrastructures, and research-driven security platforms.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to the Department of Computer Science and Engineering, Notre Dame University Bangladesh, and the Department of Computer Science and Engineering, Daffodil International University, for providing the necessary academic environment, laboratory facilities, and institutional support that made this research possible. The authors further acknowledge the developers and maintainers of the CICIDS-2017 dataset and the Wireshark community for making high-quality tools and datasets publicly available, which significantly supported the experimental evaluation of this work.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This study was conducted through the collaborative efforts of all authors. Raisa Fabiha, Stein Joachim Reberio, and Zubayer Farazi contributed to the conceptualization, methodology design, software development, formal analysis, investigation, data curation, and writing of the original draft. They were primarily responsible for dataset preparation, model implementation, experimental evaluation, and initial manuscript drafting. Fernaz Narin Nur contributed to conceptualization, methodology refinement, formal analysis, visualization, writing, review and editing, supervision, and project administration, and also served as the corresponding author, overseeing the overall research direction and ensuring manuscript quality and coherence. Shaheena Sultana contributed to investigation, formal analysis, writing, review and editing, visualization, and supervision, providing critical academic insights and feedback to strengthen the analytical and presentation aspects of the study. A. H. M. Saiful Islam contributed to investigation, resources, writing, review and editing, supervision, and project administration, supporting experimental validation and contributing to the refinement of the research outcomes. All authors have read and approved the final version of the manuscript and agree to be accountable for all aspects of the work.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Raisa Fabiha	✓	✓	✓	✓	✓	✓	✓		✓		✓			
Stein Joachim Reberio	✓	✓	✓	✓	✓	✓	✓		✓		✓			
Zubayer Farazi	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓			
Fernaz Narin Nur	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	
Shaheena Sultana						✓	✓			✓	✓	✓	✓	
A. H. M. Saiful Islam						✓	✓			✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The authors state no conflict of interest.

INFORMED CONSENT

This study did not involve human participants, personal data, or identifiable information. Therefore, informed consent was not required for this research.

ETHICAL APPROVAL

This study did not involve human participants, animals, or the use of personally identifiable data. Therefore, ethical approval from an institutional review board or ethics committee was not required.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request. The publicly available CICIDS-2017 dataset used in this study can be obtained from the Canadian Institute for Cybersecurity.

REFERENCES

[1] G. Tsochev, R. Trifonov, O. Nakov, S. Manolov, and G. Pavlova, "Cyber security: Threats and challenges," in *2020 International Conference Automatics and Informatics, ICAI 2020 - Proceedings*, 2020, pp. 1–6. doi: 10.1109/ICAI50593.2020.9311369.

[2] S. Qureshi, S. Tunio, F. Akhtar, A. Wajahat, A. Nazir, and F. Ullah, "Network forensics: a comprehensive review of tools and techniques," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, pp. 879–887, May 2021, doi: 10.14569/IJACSA.2021.01205103.

[3] E. Özeri and M. İskefiyel, "Detection of DDoS attack via deep packet analysis in real time systems," in *2nd International Conference on Computer Science and Engineering, UBMK 2017*, 2017, pp. 1137–1140. doi: 10.1109/UBMK.2017.8093526.

[4] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Forensic Science International: Digital Investigation*, vol. 32, p. 200892, 2020, doi: 10.1016/j.fsidi.2019.200892.

[5] R. Fabiha, S. J. Reberio, Z. Farazi, F. N. Nur, and S. Sultana, "A machine learning framework for real-time intrusion detection for malicious internet activity," in *2024 6th International Conference on Sustainable Technologies for Industry 5.0, STI 2024*, 2024, pp. 1–6. doi: 10.1109/STI64222.2024.10951140.

[6] F. Humaira, M. S. Islam, F. N. Nur, and K. A. Hussain, "A comprehensive study on machine learning algorithms for wireless sensor network security," in *2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020*, 2020, pp. 1–6. doi: 10.1109/ICCCNT49239.2020.9225659.

[7] T. Naqash, S. H. Shah, and M. N. U. Islam, "Statistical analysis-based intrusion detection system for ultra-high-speed software-defined network," *International Journal of Parallel Programming*, vol. 50, no. 1, pp. 89–114, 2022, doi: 10.1007/s10766-021-00715-0.

[8] I. Shivhare, J. Purohit, V. Jogani, S. Attari, and M. Chandane, "Intrusion detection: a deep learning approach," *arXiv preprint arXiv:2306.07601*, 2023, doi: 10.48550/arXiv.2306.07601.

[9] I. S. Thaseen, B. Poorva, and P. S. Ushasree, "Network intrusion detection using machine learning techniques," in *International Conference on Emerging Trends in Information Technology and Engineering, ic-ETITE 2020*, 2020, pp. 1–7. doi: 10.1109/ic-ETITE47903.2020.148.

[10] M. Tiwari, R. Kumar, A. Bharti, and J. Kishan, "Intrusion detection system," *Encyclopedia of Computer Graphics and Games*, vol. 5, p. 1008, Apr. 2024, doi: 10.1007/978-3-031-23161-2_300686.

[11] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, vol. 2018-Janua, pp. 108–116. doi: 10.5220/0006639801080116.

[12] V. Kumar, D. Sinha, A. K. Das, S. C. Pandey, and R. T. Goswami, "An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset," *Cluster Computing*, vol. 23, no. 2, pp. 1397–1418, 2020, doi: 10.1007/s10586-019-03008-x.

[13] M. Paricherla, M. Ritonga, S. R. Shinde, S. M. Chaudhari, R. Linur, and A. Raghuvanshi, "Machine learning techniques for accurate classification and detection of intrusions in computer network," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2340–2347, Aug. 2023, doi: 10.11591/eei.v12i4.4708.

[14] S. S. Panwar, Y. P. Raiwani, and L. S. Panwar, "An intrusion detection model for CICIDS-2017 dataset using machine learning algorithms," in *2022 International Conference on Advances in Computing, Communication and Materials, ICACCM 2022*, 2022, pp. 1–10. doi: 10.1109/ICACCM56405.2022.10009400.

[15] T. Elmasri, N. Samir, M. Mashaly, and Y. Atef, "Evaluation of CICIDS2017 with qualitative comparison of machine learning algorithm," in *Proceedings - 2020 IEEE Cloud Summit, Cloud Summit 2020*, 2020, pp. 46–51. doi: 10.1109/IEEECloudSummit48914.2020.00013.

[16] M. Alrowaily, F. Alenezi, and Z. Lu, "Effectiveness of machine learning-based intrusion detection systems," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11611 LNCS, Cham: Springer, 2019, pp. 277–288. doi: 10.1007/978-3-030-24907-6_21.

[17] M. K. Baklizi *et al.*, "Web attack intrusion detection system using machine learning techniques," *International journal of online and biomedical engineering*, vol. 20, no. 3, pp. 24–38, Feb. 2024, doi: 10.3991/ijoe.v20i03.45249.

[18] M. F. Kamarudin Shah, M. Md-Arshad, A. Abdul Samad, and F. A. Ghaleb, "Comparing FTP and SSH password brute force attack detection using k-nearest neighbour (k-NN) and decision tree in cloud computing," *International Journal of Innovative Computing*, vol. 13, no. 1, pp. 29–35, May 2023, doi: 10.11113/ijic.v13n1.386.

[19] J. Coronel Gaviro and A. Boukhamla, "CICIDS2017 dataset: performance improvements and validation as a robust intrusion detection system testbed," *International Journal of Information and Computer Security*, vol. 1, no. 1, p. 1, Aug. 2021, doi: 10.1504/ijics.2021.10039325.

[20] D. Kamble, S. Rathod, M. Bhelande, A. Shah, and P. Sapkal, "Correlating forensic data for enhanced network crime investigations: Techniques for packet sniffing, network forensics, and attack detection," *Journal of Autonomous Intelligence*, vol. 7, no. 4, 2024, doi: 10.32629/jai.v7i4.1272.

[21] R. A. A. P. Soepeno, "Wireshark: An effective tool for network analysis," *CYBV - Introductory Methods of Network Analysis*, no. September. pp. 1–15, 2023. doi: 10.13140/RG.2.2.34444.69769.

[22] B. Dodiya and U. K. Singh, "Malicious traffic analysis using Wireshark by collection of indicators of compromise," *International Journal of Computer Applications*, vol. 183, no. 53, pp. 1–6, 2022, doi: 10.5120/ijca2022921876.

[23] I. Chaudhary *et al.*, "Network traffic analysis using Wireshark," *International Advanced Research Journal in Science, Engineering and Technology (IARJSET)*, vol. 10, no. 2, pp. 144–148, 2023.

[24] N. A. Mabsali, H. Jassim, and J. Mani, "Effectiveness of Wireshark tool for detecting attacks and vulnerabilities in network traffic," in *1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)*, 2023, pp. 114–135. doi: 10.2991/978-94-6463-110-4_10.

[25] A. A. Abdulrahman and M. K. Ibrahem, "Evaluation of DDoS attacks detection in a new intrusion dataset based on classification algorithms," *Iraqi Journal of Information and Communications Technology*, vol. 1, no. 3, pp. 49–55, Feb. 2019, doi: 10.31987/ijict.1.3.40.

[26] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. A. Usman, "Machine learning classification of port scanning and DDoS attacks: A comparative analysis," *Mehran University Research Journal of Engineering and Technology*, vol. 40, no. 1, pp. 215–229, 2021, doi: 10.22581/muet1982.2101.19.
[27] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet attack detection in IoT using machine learning," *Computational Intelligence and Neuroscience*, vol. 2022, no. 4, pp. 743–754, 2022, doi: 10.1155/2022/4515642.
[28] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics (Switzerland)*, vol. 12, no. 6, p. 1333, 2023, doi: 10.3390/electronics12061333.
[29] V. S. Stency and N. Mohanasundaram, "A study on XSS attacks: intelligent detection methods," *Journal of Physics: Conference Series*, vol. 1767, no. 1, p. 12047, 2021, doi: 10.1088/1742-6596/1767/1/012047.
[30] R. Zuech, J. Hancock, and T. M. Khoshgoftaar, "Detecting SQL injection web attacks using ensemble learners and data sampling," in *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021*, 2021, pp. 27–34. doi: 10.1109/CSR51186.2021.9527990.
[31] N. Alsharabi, M. Alqunun, and B. A. H. Murshed, "Detecting unusual activities in local network using snort and Wireshark tools," *Journal of Advances in Information Technology*, vol. 14, no. 4, pp. 616–624, 2023, doi: 10.12720/jait.14.4.616-624.
[32] N. Thockchom, M. M. Singh, M. Moirangthem, and U. Nandi, "A novel ensemble learning-based model for network intrusion detection," *Complex \& Intelligent Systems*, vol. 9, no. 5, pp. 5693–5714, 2023, doi: 10.1007/s40747-023-01013-7.

BIOGRAPHIES OF AUTHORS

Raisa Fabiha received her bachelor of science in computer science and engineering from Notre Dame University Bangladesh (2020–2024). Currently, she is pursuing an executive master's degree in information technology at the Institute of Information Technology, University of Dhaka (session: 2024-2025, Spring). Her academic and professional interests include cloud infrastructure, machine learning, and cybersecurity, and she actively explores innovative solutions in these fields. Committed to continuous learning, Raisa stays up to date with emerging technologies and aims to contribute to cutting-edge research and advances in information technology. She can be contacted at email: raisa202120004@student.ndub.edu.bd.

Stein Joachim Reberio completed his bachelor of science in computer science and engineering from Notre Dame University Bangladesh, where he studied from 2020 to 2024. He works as a Software Development Engineer in Test at Stardust Telecom Ltd., a sister company of the Confidence Group. Stein has a strong background in software development and testing, where he applies his skills to enhance product quality and reliability. He is passionate about technology and actively participates in projects that involve innovative testing methodologies and automation tools. Mr. Reberio is committed to professional growth and constantly seeks opportunities to expand his software engineering and testing practices. He can be contacted at email: stein202120001@student.ndub.edu.bd.

Zubayer Farazi received his B.Sc. degree in computer science and engineering from Notre Dame University Bangladesh, Dhaka, Bangladesh, in 2024. He is passionate about scalable web applications and back-end optimization. Zubayer has worked on various development projects, earning recognition for his problem-solving skills. His research interests include cybersecurity, API design, and cloud technologies. He can be contacted at email: zubayer202120003@student.ndub.edu.bd.

Fernaz Narin Nur received her B.Sc. (Hons) from the Department of CSE, Jahangirnagar University, Bangladesh, in 2008 and her M.S. from the Institute of Information Technology, University of Dhaka, Bangladesh in 2010. She obtained her Ph.D. degree from the Department of CSE, University of Dhaka, Bangladesh, in 2017. In her professional life, she is a professor at the Daffodil International University in the Department of CSE. She is a passionate researcher in the fields of wireless sensor networks, directional wireless sensor networks, Ad Hoc networks, MAC protocols, cloud computing, the internet of things, machine learning. She has published a good number of research papers in international conferences and journals. She is a widely traveled personality and a novice golfer at Army Golf Club. She is a member of the Green Networking Research Group, IEEE, Internet Society, and Bangladesh Women in IT. She can be contacted at email: fernaznur@gmail.com.

Shaheena Sultana is an academic who is currently employed as the Women's IT Leadership specialist of the ICSETEP Project, which is funded by the Asian Development Bank through the University Grants Commission (UGC), Ministry of Education, Bangladesh. This project aims to empower women in Bangladesh's tech sector and enhance software engineering education. She is on leave from her position as a professor in the Department of Computer Science and Engineering at Notre Dame University Bangladesh (NDUB). She earned her Bachelor of Science in Electrical and Electronic Engineering from Khulna University of Engineering and Technology (KUET), followed by a Master of Science and a Ph.D. in Computer Science and Engineering from Bangladesh University of Engineering and Technology (BUET). Dr. Shaheena started her academic career at KUET, where she worked from 2001 until 2017. She then moved to NDUB in 2018. She has published research papers in international conferences and journals. Her research expertise includes graph drawing, graph theory, algorithm design, VLSI design, embedded systems, social network analysis, and applied artificial intelligence, covering different practical domains. She is a member of IEEE, WIE, and BWIT. She can be contacted at email: zareefas.sultana@gmail.com.

A. H. M. Saiful Islam received the B.Sc. degree from the Department of Computer Science and Engineering, Khulna University, Bangladesh, in 2003, and the M.S. degree from North South University, Bangladesh, in 2011. He is now working as a Professor in the Department of Computer Science and Engineering, Notre Dame University Bangladesh. His research interests include machine learning, IoT, discrete mathematics, software engineering, and data mining. He can be contacted at email: saiful@ndub.edu.bd.