RESEARCH PAPER

# Design and Implementation of Machine Learning Based Intrusion Detection System

**M BHARATHIRAJA [1*], EVANGELIN VINISHA R [2*], DARSHINI J [3*], DIVYA DHARSHINI S [4*], DHANALAKSHMI SHREKA P [5*]**

*1* Assistant Professor, Department of Computer Science and Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.*

*2* UG Scholar, Department of Computer Science and Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.*

*3* UG Scholar, Department of Computer Science and Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.*

*4* UG Scholar, Department of Computer Science and Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.*

*5* UG Scholar, Department of Computer Science and Engineering, V.S.B College of Engineering Technical campus, kinathukadavu, Coimbatore, Tamilnadu, India.*

***Abstract***— Cloud computing is commonly used by contemporary organizations due to the flexibility and reduced costs of cloud computing. Despite the advantages of cloud computing, cloud computing has several security challenges. Cloud computing is a distributed system with high dynamics, which makes cloud computing more vulnerable to cyber attacks, unauthorized access, and various attacks from the networks. The intrusion detection system is based on signature and rule-based systems. Because of this, the intrusion detection system is not effective in detecting new attacks. It learns from the data that has already been available and tries to learn how different types of attacks look. After this, it is capable of recognizing abnormal patterns in the network, which might mean that there is a potential threat in the system. The main purpose of this project is to ensure that there is a reduction in false alarms in the system. It is not easy to spot real alarms in the system if there is a high rate of false alarms. This is because it is not easy to monitor the system. This is where the reduction of false alarms is going to take place, making it easy to monitor the system. This system is also designed in a way that it can function well in cloud environments. This is because in cloud environments, there is a constant change in workload. It is not easy to deal with constant changes in workload. This is where machine learning comes in handy. Machine learning in cloud security makes it easy to detect attacks. This is because it is monitored in real time. This makes it easy to ensure that cloud computing is safe from different types of attacks.

***Keywords***— *Cloud Computing, Intrusion Detection System, Machine Learning, Network Traffic Analysis, Anomaly Detection, Cyber Security, False Alarm Reduction, Threat Detection.*

**How to cite this article**: Bharathiraja M, Vinisha ER, Darshini J, Dharshini SD, Shreka DP. Design and implementation of machine learning based intrusion detection system. Int J Drug Deliv Technol. 2026;16(74s): 286-292. DOI: 10.25258/ijddt.16.74s.32

## I. INTRODUCTION

The growth of digital communication has been tremendous in recent times. Currently, computer networks facilitate the delivery of critical services such as cloud computing, online transaction services, data storage services, online streaming services, and many other services related to smart devices. With the growing use of cloud technology, the level of network traffic is growing significantly.

However, the growth of digital communication has led to the emergence of cyber attacks and unauthorized access in computer networks. Hackers always look for opportunities to invade computer networks in order to access critical data. Due to this, the issue of cyber threats in cloud networks has become critical in ensuring the security of computer networks [1], [2].

Most of the traditional IDS uses mainly signature-based and rule-based approaches for intrusion detection [3]. Signature-based IDS performs well in detecting attacks that are already known, but these approaches are not effective in detecting unknown attacks. Signature-based IDS needs frequent updates of their database, and sometimes these IDS are not able to detect zero-day attacks that are not yet recorded.

Additionally, the number of false alarms produced by the rule-based IDS makes it difficult for the system administrator to easily identify the real attack [4]. As the complexity of the network increases, the traditional approaches are no longer enough for dealing with the sophisticated cyber attacks [5]. Some surveys have highlighted the limitations of conventional intrusion detection techniques and the need for advanced intelligent intrusion detection techniques [6].

To overcome these problems, various machine learning approaches have been explored for the improvement of intrusion detection systems [7], [8]. Machine learning algorithms are intelligent enough to learn from the historical data and improve their performance over time. Machine learning approaches are able to identify various patterns in the network traffic that differentiate between normal and abnormal behaviors [9].

In particular, the intrusion detection systems based on machine learning have the ability to learn and analyze the network traffic and detect abnormal patterns that may be a potential threat [10], [11]. After the analysis of various features such as the flow of the packets, the behavior of the network, and the pattern of the communication, the machine learning has the ability to classify the activities of the network as normal or malicious [12].

Due to the learning ability, the machine learning has the potential to be effective in the improvement of the security of the cloud computing environment [13]. Recent studies have also explored advanced machine learning and deep learning architectures to further improve the detection accuracy of intrusion detection systems [14].

However, despite the advantages of the intrusion detection systems based on machine learning techniques, there are many challenges associated with the existing intrusion detection systems [15], [16]. For example, the majority of the existing intrusion detection systems produce a high number of false alarms, which may affect the efficiency of the system [17]. Additionally, the cloud environment is characterized by changing workloads and large volumes of data, which makes it challenging for the system to analyze the network traffic [18].

Therefore, there is a need for a more intelligent intrusion detection system that can analyze the network traffic while minimizing the number of false alarms [19]. Hybrid deep learning models have also been explored to enhance intrusion detection performance in modern network and IoT environments [20].

The major contribution of the project can be explained in the following ways:

- The development of an intrusion detection system that utilizes machine learning for the analysis of cloud network traffic.
- The automatic detection of abnormal patterns in the network traffic, which can be applied in the detection of any malicious activities.
- The minimization of false alarms in the system for accuracy purposes.

The objective of this project is to create a system for intrusion detection that can monitor the network and detect any suspicious activity in the cloud environment using machine learning. The system can detect abnormal activity in the network based on the patterns of the network traffic. The system can identify potential security threats by analyzing the patterns of the network traffic. By using the pre-collected data from the network, the system can detect both normal and abnormal attacks.

## II. Related Works

Samriya et al. [1] proposed a machine learning-based network intrusion detection optimization approach for cloud computing environments, highlighting how optimized ML models can improve detection accuracy and enhance security in cloud-based systems. A deep learning-based method was also proposed to enhance network security by detecting and mitigating cyber-attacks, demonstrating that advanced learning models can improve the detection capability of intrusion detection systems [2].

Imran Hidayat et al. [3] conducted an experimental comparison of various machine learning algorithms for intrusion detection and highlighted their effectiveness in distinguishing between normal and malicious network behaviors. An adaptive and scalable Distributed Denial-of-Service (DDoS) detection system using hierarchical machine learning techniques was also developed to enhance detection accuracy in distributed computing environments [4].

Andrea Pinto et al. [5] presented a comprehensive survey on intrusion detection systems based on machine learning techniques for protecting critical infrastructure. Different machine learning algorithms used in IDS were also reviewed, emphasizing their ability to analyze network traffic patterns and identify abnormal activities efficiently [6].

Mary et al. [7] proposed a secure-aware routing protocol for reliable network communication, focusing on improving network security and performance. A comprehensive survey of machine learning methods used in intrusion detection systems also discussed how intelligent algorithms can improve network threat detection [8].

Kasongo and Sun [9] explored various machine learning techniques used for network-based intrusion detection systems and highlighted their ability to detect complex attack patterns. Different machine learning algorithms were also evaluated and compared based on their performance in identifying cyber-attacks in network traffic [10].

Xinwei Yuan et al. [11] introduced a framework to enhance the adversarial robustness of deep learning-based intrusion detection systems. An experimental review of neural network-based approaches for network intrusion management also discussed their effectiveness in detecting sophisticated cyber threats [12].

Benamor et al. [13] conducted a comparative study of machine learning algorithms for intrusion detection in IoT networks and analyzed their performance in detecting various attack types. A machine learning-based intrusion detection system was also developed to improve network security by identifying abnormal traffic patterns [14].

Ramesh et al. [15] performed a comparative analysis of different datasets and feature reduction techniques for improving intrusion detection performance in cybersecurity systems. The application of machine learning techniques in computer networks was also investigated to enhance the detection of malicious activities [16].

Khan et al. [17] proposed a hybrid deep learning-based intrusion detection system designed for IoT networks, combining multiple learning techniques to improve detection accuracy. A systematic literature study on machine learning techniques for intrusion detection also identified key challenges and research opportunities [18].

Jayalaxmi et al. [19] presented a survey on intrusion detection systems based on machine learning and deep learning approaches, highlighting their effectiveness in improving network security. Various machine learning and deep learning architectures used in intrusion detection

systems were also analyzed, discussing their potential in enhancing detection performance [20].

However, despite the above advancements, existing intrusion detection systems have several challenges in the cloud environment. Some of the challenges associated with existing intrusion detection systems in the cloud environment include the difficulty of maintaining high detection accuracy while keeping the false alarm rate low.

In addition, some intrusion detection systems have difficulties in adapting to the dynamic nature of the cloud environment. In cloud-based intrusion detection systems, these techniques improve detection of attacks and monitoring of the network; however, these techniques' effectiveness is limited by the following reasons:

- Some traditional intrusion detection systems heavily rely on signatures, hence failing to detect new types of cyber attacks.
- Some of these intrusion detection systems do not take into account the dynamics of cloud computing, including changes in network traffic, resources, and scalability of systems.

Considering the aforementioned factors, the objective of the paper is to design a machine learning intrusion detection system that will monitor network traffic patterns and identify any abnormalities within the network.

## III. Proposed Methodology

### A. Overview

In the proposed methodology, it is suggested that an intrusion detection system based on machine learning would be developed to ensure the security of cloud computing. This system would monitor the behavior of the network traffic. In the proposed system, it is suggested that the machine learning model would learn from the historical data of the network. This would help in detecting abnormal behavior in the network, which might lead to attacks. It is suggested that the proposed system would be able to detect known as well as unknown attacks. This would help in increasing the accuracy of the detection system.

### B. System Architecture

The system architecture for the proposed project will be focused on enhancing the security of the cloud computing environment through the implementation of a machine learning-based intrusion detection system, as shown in Fig. 1. The different components involved in the system will be the administrator, the cloud computing environment, the data collection module, the preprocessing unit, the feature extraction module, and the machine learning detection engine. Network traffic data will be collected from the cloud computing environment and fed into the preprocessing unit to remove any unwanted data. The feature extraction module will then identify the necessary attributes to be considered for the intrusion detection process. The machine learning model will then analyze the data to identify whether the network traffic is normal or not.

The system architecture uses a machine learning-based intrusion detection system (IDS) to monitor network traffic in a cloud computing environment. Network data is collected from the cloud, preprocessed, and important features are extracted for analysis by the machine learning model. Based on the detection result, the system either allows normal traffic or blocks malicious attacks and generates an alert.

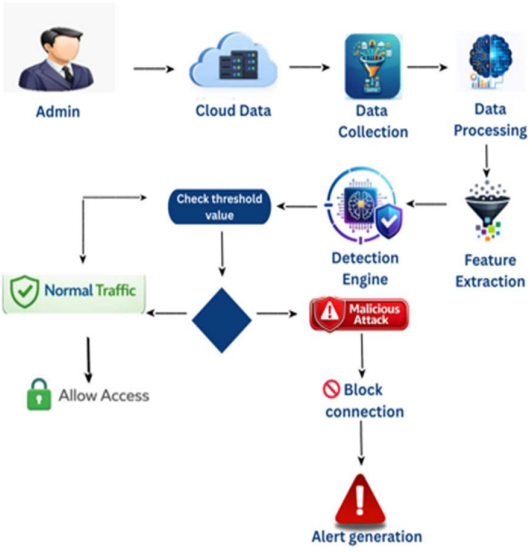


Fig. 1. System Architecture

### C. Machine Learning Based Intrusion Detection Algorithm

The proposed system uses machine learning techniques to detect malicious activities in cloud networks. The algorithm analyzes network traffic data and learns patterns from historical datasets to identify abnormal behavior. In this approach, the system continuously monitors incoming network traffic and classifies it as normal or malicious. In addition, the system recognizes significant features from the network traffic, which include the source and destination IP address, protocol type, packet size, and duration of the connection. The above features are used to improve the accuracy of the intrusion detection process. The machine learning model compares the network traffic with the patterns it has learned to recognize the threats in real-time, thereby preventing unauthorized access to the cloud environment.

1. Initialization
   - At the beginning, the dataset containing network traffic information is loaded.
   - The machine learning model parameters are initialized before training.
   - The system environment and the libraries for data processing and machine learning are configured to enable the proper execution of the algorithm.
2. Data Preprocessing
   - The collected network data is cleaned by removing missing or irrelevant values.
   - Data normalization and transformation are performed to prepare the dataset for model training.
3. Feature Extraction
   - Important features are selected from the dataset to improve detection performance.
   - Feature extraction helps reduce data complexity and enhances model efficiency.
4. Model Training

- The processed dataset is used to train the machine learning model.
- The model learns patterns of both normal and malicious network traffic.

5. Intrusion Detection
   - The trained model analyzes incoming network traffic.
   - Based on learned patterns, the system classifies traffic as normal or malicious.
6. Alert and Response
   - If normal traffic is detected, access to the network is allowed.
   - If malicious activity is detected, the system blocks the connection and generates an alert for the administrator.
7. Continuous Monitoring
   - The system continuously monitors the network to ensure there is ongoing protection from cyber attacks.
   - As new network data is being generated, the system processes the data and enhances its detection capability.
   - This enables the system to keep up with new cyber attacks and maintain its security level.

The proposed system uses machine learning for detecting and classifying network traffic, as shown in Fig. 2. The system uses network data and features as input for detecting normal or malicious activities. The system enhances the accuracy of the detection, minimizes false alarms, and increases security in the cloud environment.

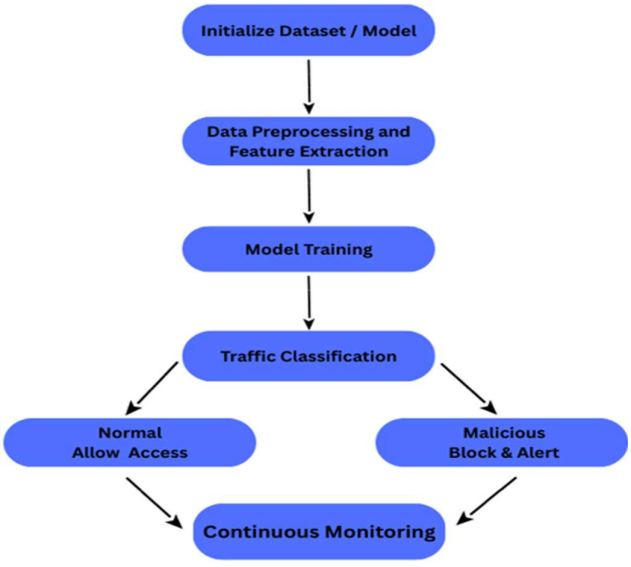


Fig. 2. Machine-Learning Based Intrusion Detection

*D. Detection and Alert Management*

Detection and alert management are important components of the proposed machine learning based intrusion detection system. The system analyzes network traffic and classifies it as normal or malicious. When malicious activity is detected, the system blocks the connection and generates alerts, enabling the administrator to monitor and respond to security threats effectively.

*M-L BASED NETWORK INTRUSION DETECTION SYSTEM ALGORITHM*

1. Initialize the ML model parameters (weights for neural networks, or hyperparameters for other ML models).
2. Load dataset and preprocess features (normalize numeric features, encode categorical features).
3. Split dataset into training and testing sets.
4. Train the ML model on the training set.
5. For each incoming network packet or flow:
   1. Extract relevant features (source IP, destination IP, protocol, packet size, etc.).
   2. Input features into the trained ML model.
   3. Predict the class of traffic: Normal or Attack.
   4. If predicted as Attack:
      - Generate an alert for the administrator.
      - Optionally block the connection or isolate the source IP.
   5. Else, allow the connection.
6. Update model periodically with new labeled data (online learning or batch retraining).
7. End

*ADAPTIVE M-L BASED INTRUSION DETECTION SYSTEM FOR MOBILE NETWORKS ALGORITHM*

1. Initialize network simulation with nodes, links, and traffic flows.
2. Assign mobility patterns for each node (e.g., Random Waypoint Model).
3. For each time step t:
4. Update node positions:

$$Pi(t) = Pi(t-1) + Vi(t) * \Delta t \quad (1)$$

Where Pi(t) = Position of node *i* at time *t,*
Pi(t-1) = Previous position of node *i,*
Vi(t) = Velocity of node *i* at time *t,*
Δt = Time step

5. For each packet:
6. Extract features: source/destination IP, protocol, payload size, connection duration.
7. Predict class using ML model:

$$y = f(X) \quad (2)$$

Where X = feature vector,
y = prediction (Normal/Attack).

8. If malicious, log alert and optionally block the connection.
9. Update traffic statistics:

$$\text{Accuracy} = \frac{\text{Number of Correct Predictions}}{\text{Total Number of Predictions}} \quad (3)$$

Where μ = mean of normal traffic feature,

σ = standard deviation.

10. Adjust thresholds dynamically based on node density Dn and speed $\bar{V}$:

$$\text{Threshold } t = \text{Base Threshold} \cdot (1 + k \cdot Dn \cdot \bar{V}) \quad (4)$$

Where Dn = Node Density,
$\bar{V}$ = Average Node Speed.

11. Monitor Link Quality and update detection parameters:

$$\text{Link Quality} = \frac{\text{Successful Packets}}{\text{Total Packets}} \quad (5)$$

12. Periodically retrain ML model with newly observed patterns.
13. End for each packet.
14. End for each time step.
15. Repeat simulation until network evaluation completes.
16. Update detection model and thresholds as needed.
17. Ensure real-time adaptation to node mobility.
18. End.

## IV. Perfomance Analysis

### A. *Analysis of Accuracy in Detecting*

The accuracy level of the detection mechanism of the IDS in ML-based IDS indicates how effectively the IDS can differentiate between normal and malicious traffics in the network. The accuracy level can be found using the following formula:

$$\text{Accuracy} = \frac{\text{Number of Correct Predictions}}{\text{Total Number of Predictions}} \times 100 \quad (6)$$

In In Fig. 3, the x-axis represents the number of network packets or time intervals, while the y-axis shows detection accuracy (%). Higher accuracy indicates better performance in identifying intrusions.

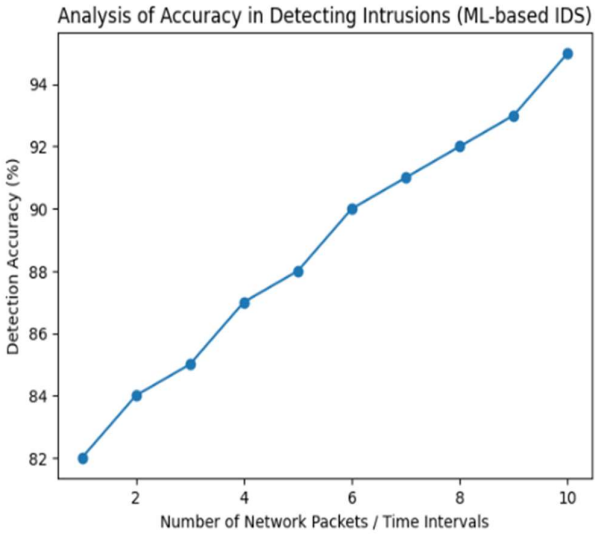


Fig. 3.Analysis of Accuracy in Detection

### B. *Scalability Analysis*

Scalability tests assess the ability of the IDS to cope with increased traffic volume or a larger network size. In this case, the IDS is subjected to increased packet rates, the number of nodes, or the number of active connections. Fig. 4 shows that the ML-based IDS has a high detection accuracy even under a larger workload.

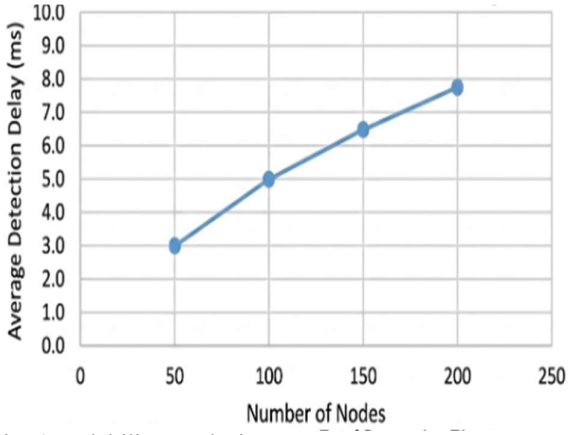


Fig. 4.Scalability Analysis

$$\text{Average Detection Delay} = \frac{\text{Total Processing Time}}{\text{Total Packets Analyzed}} \quad (7)$$

- Processing Delay: Time taken to classify each packet.
- Resource Utilization: CPU and memory usage are monitored to ensure the system can function efficiently on real-time network devices.

In Fig. 4, the x-axis represents the number of nodes in the network, and the y-axis represents the average detection delay (ms). As the number of nodes increases, the detection delay gradually increases. This shows that the ML-based IDS can handle larger networks while maintaining stable performance.

### C. *Analysis of False Alarm Rate*

The analysis of the false alarm rate is an evaluation of the rate at which the intrusion detection system incorrectly identifies normal network traffic as an attack. The rate of false alarms can affect the efficiency of the intrusion detection system since system administrators can spend a lot of time dealing with false alarms. Therefore, the rate of false alarms needs to be minimized to ensure the efficiency of the intrusion detection system.

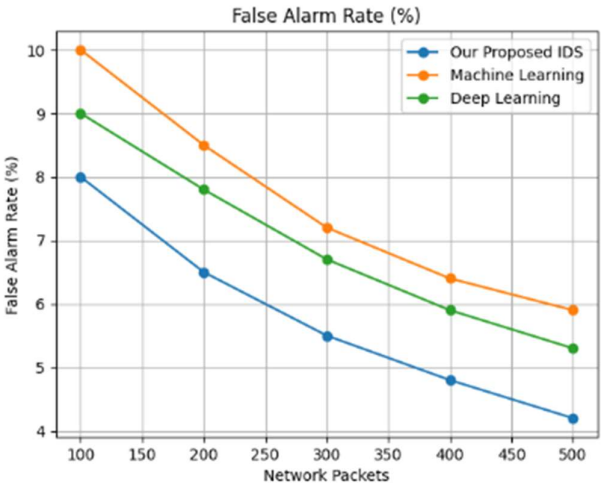


Fig. 5.False Alarm Rate

In Fig. 5, the x-axis represents the number of network nodes or traffic instances, and the y-axis represents the false alarm rate. A lower false alarm rate indicates better IDS performance.

## V. Conclusion

The Machine Learning-based Intrusion Detection System (IDS) indicates its potential in enhancing network security through the detection of malicious activities with fewer false positives and false negatives. The system is able to monitor network activities continuously and analyze patterns in order to identify various types of attacks, including known and unknown attacks. The IDS is also able to adapt dynamic changes in network conditions through machine learning algorithms, which enable it to improve accuracy in detecting attacks through dynamic changes in detection thresholds. The results indicate that the proposed ML-based IDS improves system reliability and optimizes system resources through the minimization of unnecessary packet inspection processes. In the future, various advanced machine learning algorithms, including deep learning, reinforcement learning, and feature selection algorithms, can be employed in order to improve detection accuracy. The proposed system can also be enhanced in order to cater to various large-scale networks, including IoT networks, which makes it scalable and adaptable to dynamic network environments.

## References

[1] Samriya, J.K., Kumar, S., Kumar, M., Wu, H. and Gill, S.S., "Machine learning-based network intrusion detection optimization for cloud computing environments," IEEE Transactions on Consumer Electronics, 70(4), pp.7449-7460, 2024.

[2] Jino, R.F., Paulsamy, A.M., Shanmugam, G. and Vishwakarma, R.K., "Enhancing network security: a deep learning-based method to detect and diminish attacks," International Journal of Electronic Security and Digital Forensics, 17(5), pp.631-645, 2025.

[3] Hidayat, I., Ali, M.Z. and Arshad, A., "Machine learning-based intrusion detection system: an experimental comparison," Journal of Computational and Cognitive Engineering, 2(2), pp.88-97, 2023.

[4] Manivannan, K., Jayanthi, S., Kavitha, T., Geetha, M., Mary, P.A. and Nelson, S. "Towards Adaptive and Scalable DDoS Detection in Distributed System using Tuned Hierarchical Machine Learning Techniques". In 2025 International Conference on Computing and Communications (COMPUTINGCON) (pp. 1-6). IEEE, 2025, September.

[5] Pinto, A., Herrera, L.C., Donoso, Y. and Gutierrez, J.A., "Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure," Sensors, 23(5), p.2415, 2023.

[6] Bajpai, A., Singh, A., Kansal, V., Prakash, S., Yang, T. and Rathore, R.S., "Blockchain-enabled real-time intrusion detection framework for a cyber-physical system," In 2024 International Conference on Decision Aid Sciences and Applications (DASA) (pp. 1-7). IEEE, 2024.

[7] Mary, P.A., Maalini, D., Manivannan, K., Umamaheswari, K., Balaji, S. and Deepak, R., "A Secure Aware Routing Protocol for Efficient and Reliable FPANETS," in 2024 First International Conference on Software, Systems and Information Technology (SSITCON) (pp. 1-6). IEEE, 2024.

[8] Al-Haija, Q.A. and Droos, A., "A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT)," *Expert Systems*, *42*(2), p.e13726, 2025.

[9] Chua, T.H. and Salam, I., "Evaluation of machine learning algorithms in network-based intrusion detection system," arXiv preprint arXiv:2203.05232, 2022.

[10] Manivannan, K., Ramkumar, K. and Krishnamurthy, R., "Enhanced AI based diabetic risk prediction using feature scaled ensemble learning technique based on cloud computing," SN Computer Science, 5(8), p.1123, 2024.

[11] Yuan, X., Han, S., Huang, W., Ye, H., Kong, X. and Zhang, F., "A simple framework to enhance the adversarial robustness of deep learning-based intrusion detection system," Computers & Security, 137, p.103644, 2024.

[12] Sathyanarayanan, M., Manivannan, K., Mithin, K., Manoj, G., Mugesh, M. and Kishore, N., "Design and Implementation of a Cybersecurity Framework for Encrypted File Management System," in 2025 6th International Conference for Emerging Technology (INCET), IEEE, 2025.

[13] Benamor, Z., Seghir, Z.A., Djezzar, M. and Hemam, M., "A comparative study of machine learning algorithms for intrusion detection in IoT networks," Revue d'Intelligence Artificielle, 37(3), pp.567-576, 2023.

[14] Mari, A.G., Zinca, D. and Dobrota, V., "Development of a machine-learning intrusion detection system and testing of its performance using a generative adversarial network," Sensors, 23(3), p.1315, 2023.

[15] Ramesh, T.R., Jackulin, T., Kumar, R.A., Chanthirasekaran, K. and Bharathiraja, M., "Machine learning-based intrusion detection: A comparative

analysis among datasets and innovative feature reduction for enhanced cybersecurity," International Journal of Intelligent Systems and Applications in Engineering, 12(12s), pp.200-206, 2024.

[16] Dina, A.S. and Manivannan, D., "Intrusion detection based on machine learning techniques in computer networks," Internet of Things, 16, p.100462, 2021.

[17] Khan, N.W., Alshehri, M.S., Khan, M.A., Almakdi, S., Moradpoor, N., Alazeb, A., Ullah, S., Naz, N. and Ahmad, J., "A hybrid deep learning-based intrusion detection system for IoT networks," Math. Biosci. Eng, 20(8), pp.13491-13520, 2023.

[18] Rehman, H.M.R.U., Liaquat, S., Gul, M.J., Jhandir, M.Z., Gavilanes, D., Vergara, M.M. and Ashraf, I., "A systematic literature study of machine learning techniques based intrusion detection: datasets, models, challenges, and future directions," Journal of Big Data, 12(1), p.264, 2025.

[19] Shrivastava, V. and Chaturvedi, A.K., "A survey on intrusion detection system based on machine learning and deep learning," In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE, 2023.

[20] Thankappan, M., Narayanan, N., Sanaj, M.S., Manoj, A., Menon, A.P. and Krishna, M.G., "Machine Learning and Deep Learning Architectures for Intrusion Detection System (IDS): A Survey," In 2024 1st International Conference on Trends in Engineering Systems and Technologies (ICTEST) (pp. 01-06). IEEE, 2024.