SCIENTIFIC OASIS

Decision Making: Applications in Management and Engineering

ISSN: 2560-6018, eISSN: 2620-0104

SECURING NETWORKS: ADVANCEMENT IN INTRUSION DETECTION, AODV, CLUSTER-BASED ROUTING, USING MACHINE LEARNING TECHNIQUES.

Mrs.V.Deepa[1], Dr.N.Radha[2]

[1]Ph.DScholar,Department of Computer Science, PSGR Krishnammal College for Women
deepa.rskumar@gmail.com

[2] Department of Data Analytics, PSGR Krishnammal College for Women

Abstract

In today's interconnected world, network security remains a paramount concern, necessitating constant advancements in intrusion detection and routing protocols. This journal explores the forefront of network security with a focus on the integration of machine learning techniques such as KNN (K-Nearest Neighbors), AMODV (Adaptive Multiobjective Optimization-based Detection of Anomalies in Network Traffic), and IDS (Intrusion Detection System) into traditional approaches. Beginning with an examination of state-of-the-art intrusion detection models like KNN-IDS, the journal delves into the intricacies of ad hoc multipath distance vector (AODMV) routing, cluster-based routing protocols, and their incorporation with intrusion detection systems. Through detailed analyses and case studies, it elucidates the challenges and opportunities inherent in securing networks against evolving threats. Furthermore, the journal investigates the synergistic potential of machine learning techniques in enhancing the efficacy and adaptability of intrusion detection and routing systems. By synthesising theoretical insights with practical implementations of KNN, AMODV, IDS, and routing protocols like CBRP (Cluster-Based Routing Protocol), this work provides a comprehensive overview of the latest advancements in network security, offering valuable insights for researchers, practitioners, and policymakers alike.

Keywords: Intrusion Detection System, Data Mining, Cluster-based Routing protocol, K-nearest neighbour, ad hoc multipath distance vector (AODMV) routing.

I. Introduction

Intrusion Detection Systems (IDS) play a crucial role in identifying irregularities and network attacks, becoming increasingly significant in network security [1]. Various techniques such as machine learning, deep learning, and data mining are employed for intrusion detection, enhancing accuracy and response capabilities [2] [3]. Anomaly detection methods are utilised to identify deviations from normal behaviour in network traffic, signalling potential security

breaches [4]. Machine learning models like Decision Trees and Neural Networks, along with ensemble methods such as Random Forest, are implemented for developing effective intrusion detection systems [2] [5]. Challenges include high false positive rates and model interpretability issues, with ongoing research focusing on improving accuracy and efficiency in intrusion detection systems [1].

Anomaly-based intrusion detection models often incorporate Attribute-Oriented Data Mining and Visualization (AODMV) techniques for effective analysis [1]. AODMV aids in enhancing detection accuracy by visualising and analysing network traffic patterns, enabling the identification of potential security threats [2]. AODMV techniques are utilised for feature selection and fusion, optimising the input data for intrusion detection models [3]. Integration of AODMV in intrusion detection models leads to improved model efficiency, enabling better classification of network anomalies [4]. AODMV methods help in addressing class imbalance issues in intrusion detection datasets, contributing to enhanced performance and accuracy [4].

Incorporating cluster-based routing protocols enhances intrusion detection models by organising sensor nodes into clusters for efficient data transmission and analysis [1]. Cluster-based routing facilitates better network monitoring and anomaly detection by enabling nodes within clusters to collaborate in detecting intrusions and sharing information [2]. The use of cluster-based routing protocols in intrusion detection models improves scalability, allowing for effective monitoring of large-scale wireless sensor networks (WSNs) [3]. Cluster-based models optimise resource allocation by distributing tasks among cluster heads, leading to efficient intrusion detection and response mechanisms [4]. The collaborative nature of cluster-based routing protocols contributes to reducing false positive rates in intrusion detection systems, ensuring accurate threat identification [5].

Intrusion detection models leverage data mining concepts for effective threat detection and classification [1] [2]. Data mining algorithms, such as Decision Trees, Neural Networks, and K-nearest neighbours, are applied to identify patterns and anomalies in network traffic for intrusion detection [2] [3]. Data mining methods contribute to enhancing detection accuracy by analysing network data and identifying potential security breaches [2] [3]. Data mining techniques, like anomaly detection, play a crucial role in spotting deviations from normal behaviour and alerting to potential security breaches in intrusion detection systems [1] [2]. Data mining concepts are utilised for feature selection and fusion, optimising input data for intrusion detection models and improving overall performance [2] [3].

II Related works

The author analyses new methods of skyline queries on secured cloud databases also hybrid immune algorithms to enhance database security. Introducing the merging Danger Theory(DT) and Negative Selection Algorithm(NSA) for intrusion detection with high effectiveness. This new algorithm achieves high intrusion detection activities and a low false positive rate; moreover

enhances the capability to identify insider threads and prevent data breaches. Guarantee confidentiality, integrity, and availability of sensitive data and prevent breaches. [1].

The author focuses on network intrusion detection systems using machine learning methods. The multinomial classification model uses various performance evaluation metrics. Multiple algorithms are used here, such as decision tree, K Nearest Neighbour, and random forest classifiers. Logical regression achieved the best intrusion detection accuracy of 83.76%; decision trees provide an understanding of detected intrusion patterns [2].

The author reviews various intrusion detection systems techniques and datasets with data mining and research opportunities. The review focuses on using deep learning techniques for cybersecurity applications. The Proposal Uses a comprehensive approach using the CNN algorithm and CSE-CIC-IDS2018 dataset in this web application firewall, which provides 83.5% accuracy on NSL-KDD. The work aims to enhance the accuracy and reliability of detecting cyber-attacks on networks [3].

Analyses Metaverse security using blockchain and machine learning techniques. Proposes a decentralised collaborative intrusion detection system for Metaverse security. Addresses scalability and SPoF issues in traditional security approaches. Outlines key challenges and future research directions for Metaverse security. Develop a decentralised intrusion detection system based on blockchain and federated learning. MSecureChain resists up to 33 byzantine nodes with 99% accuracy. Offers efficiency under poisoning attacks and is resistant to SPoF. Decentralised collaborative intrusion detection system based on blockchain and federated learning. Training process with stochastic gradient descent for model adaptability. Security solutions include IDS, access control, identity authentication, and malware detection. Decentralised collaborative intrusion detection system based on blockchain and federated learning. Training process with stochastic gradient descent for model adaptability. Security solutions include IDS, access control, identity authentication, and malware detection [4].

MLSTL-WSN enhances intrusion detection in wireless sensor networks. Achieved accuracy rates of 99.78% in binary and 99.92% in multiclass. Utilises ML techniques with SMOTE-TomekLink for balanced dataset and accuracy. Novel intrusion detection model with high accuracy rates. Combines ML techniques with SMOTE-TomekLink for balanced datasets. Acknowledges limitations despite impressive model performance. SMOTE-TomekLink algorithm for balancing datasets. Feature scaling through standardisation for consistent input features. SMOTE-Tomek resampling technique to mitigate overfitting and underfitting. Ensemble method with Random Forest, decision tree, MLP, KNN, XGB, LGB. Enhances intrusion detection accuracy in WSNs using ML techniques. Safeguards data integrity in healthcare, industrial control systems, and monitoring. Balances imbalanced WSN datasets effectively for improved intrusion detection [5].

Enhances intrusion detection accuracy in WSNs using ML techniques. Safeguards data integrity in healthcare, industrial control systems, and monitoring. Balances imbalanced WSN datasets effectively for improved intrusion detection. Reviews machine learning-based intrusion detection systems for network security. Aims to aid developers in understanding Network Intrusion Detection System development. The adoption of machine learning-based intrusion detection systems is emphasised. The proposed system shows high accuracy and F1-Score. Machine learning for network content analysis to detect intrusions. Preprocessing, feature selection, parameter optimisation, and classification phases. Classification algorithms like Random Tree, AdaBoost, KNN, and SVM were utilised. Removal of non-numeric or symbolic features in dataset preprocessing. Machine learning for network content analysis to detect intrusions. Preprocessing, feature selection, parameter optimisation, and classification phases. Classification algorithms like Random Tree, AdaBoost, KNN, and SVM were utilised. Removal of non-numeric or symbolic features in dataset preprocessing[6].

The paper focuses on AI algorithms for network threat detection and defence. Discusses intrusion detection technology and the K-means clustering algorithm. Focus on AI algorithms for network security intrusion detection and defence. Introduces improved k-means clustering model for network security detection. Emphasises the importance of intrusion detection technology in network security. Improved k-means algorithm enhances network intrusion detection accuracy. Reduced false positive rate in network anomaly detection. Improved k-means clustering algorithm for network security detection model. Visualisation of data in 3D with clusters set to 10. Improved k-means algorithm enhances network intrusion detection accuracy. Reduces false positive rates in network anomaly detection [7].

Advanced IoT intrusion detection using deep learning with LSTM architecture. Achieved peak accuracy of 0.997 on test data. The model shows stability in loss and accuracy metrics. Comparative analysis approves the effectiveness of the proposed approach. IDS for IoT security using deep learning on CICIDS2017 dataset. The model achieves 0.997 accuracy, resilient to Gaussian noise. Comparative analysis confirms the model's effectiveness in diverse threat scenarios. Deep learning techniques with LSTM architecture for intrusion detection. Utilised the CICIDS2017 dataset for training and testing intrusion detection models. Evaluation metrics included sparse categorical cross-entropy loss and accuracy. The model's resilience to Gaussian noise was assessed for accuracy maintenance. [8].

ML-IDS enhances security in medical IoT devices, using PSO-AdaBoost for detection. The proposed ML-IDS combines PSO and AdaBoost for malware detection. It achieves high recall value with superior accuracy, Precision, and recall. Enhances security in medical IoT devices, improving patient outcomes. PSO and AdaBoost-based intrusion detection system. Feature selection, training classification models, and performance evaluation. Data imbalance, generalisation, scalability, and false positives are limitations [9].

Proposed unsupervised intrusion detection system for in-vehicle communication networks. Combines autoencoders and fuzzy C-means for efficient intrusion detection. Achieved high accuracy on various intrusion detection datasets. Outperforms existing methods without requiring labelled datasets. Proposed unsupervised intrusion detection system for in-vehicle communication networks. Combines autoencoders and fuzzy C-means for lightweight intrusion detection. Achieved high accuracy on various intrusion detection datasets. Outperforms existing methods without requiring labelled datasets. Achieved 75.51% accuracy on the ML350 in-vehicle intrusion dataset. Outperformed existing methods with high accuracies on various intrusion detection datasets. The proposed method is generalised, robust, and effective for real-time deployment. Unsupervised intrusion detection with autoencoders and fuzzy C-means clustering. Host-based intrusion detection system for zero-day attacks. Comparison of clustering algorithms like K-means, GMM, and FCM. [10]

APFed enhances FL for intrusion detection in maritime sensor networks. The paper discusses APFed for intrusion detection in maritime meteorological sensor networks. APFed improves local unknown attack detection and personalised performance. The experiment validates APFed's superiority in MMSN intrusion detection. APFed improves local unknown attack detection without significant personalised performance degradation. APFed demonstrates superiority in FL for MMSN intrusion detection. Adaptive, personalised federated learning for intrusion detection in maritime networks. Lightweight Group Convolutional Neural Network (LGCNN) intrusion detection model [11].

Optimised deep learning approach for network intrusion detection using big data. Method tested on various datasets, proving adaptability and reliability. Methods used Ensemble SVM, CGO, CNN-LSTM, Bi-LSTM. Utilised ResNet152 for intrusion detection after feature extraction. Various techniques like Ensemble SVM, CNN-LSTM, and Bi-LSTM were compared. Enhances security breach detection through effective feature selection methods. Addresses risks to data safety and asset protection from IoT intrusions [12].

DCRNN with IGOA enhances intrusion detection system accuracy. Feature selection using NBGOA improves classification accuracy and processing time. DCRNN enhances network security through intrusion detection with feature selection. The proposed system outperforms existing models in classification accuracy and processing time. Ensemble learning model for intrusion detection with high accuracy achieved. J48, Multinomial NB, Logistic regression, Random forest, Proposed method. The proposed system outperformed existing models in accuracy and processing time. Achieved accuracy of 99.17%, false alarm rate of 0.87%. The detection rate of 99.8% against numerous subsets of assault data. Enhances network security through intrusion detection using DCRNN. Achieves high accuracy with fewer resources and processing power. Outperforms existing deep learning approaches in intrusion detection. Provides efficient classification of various attack types [13].

Lightweight IDSs for IoT using SGDC and feature selection algorithms. Achieved 92.69% accuracy, reduced features by 79.93%. Enhances IoT security and privacy, safeguarding sensitive data. Lightweight IDSs for IoT devices using SGDC and feature selectors. Achieved 92.69% accuracy, reduced features by 79.93%. Enhances IoT security and privacy safeguards sensitive data. Lightweight IDSs with SGDC and four feature-selection algorithms.Feature selection based on correlation coefficients using backward elimination. Dataset realism and representativeness were crucial for training IDSs. Careful selection of feature selection algorithms and regression models is essential. Enhances IoT security with lightweight IDSs for resource-constrained devices. Improves accuracy and energy efficiency in detecting cyber attacks. Reduces dataset dimensionality while maintaining high accuracy levels [14].

The proposed IDS uses DBDE-QDA for feature selection and a speedy ensemble classifier. Achieves high detection rates with lower computational cost than state-of-the-art. DBDE-QDA reduces dimensionality significantly but may slightly decrease detection rates. IDS aims for high detection rates with reduced computational cost. The proposed system uses swift wrapper feature selection and a speedy ensemble classifier. Achieved competitive detection rates with lower computational costs. IDS aims for high detection rates with reduced computational cost. The proposed system uses swift wrapper feature selection and a speedy ensemble classifier. Achieved competitive detection rates with lower computational costs. The proposed IDS achieves 95%-97.4% detection rates for the NSL-KDD dataset. DBDE-QDA reduces dimension by 60.97%-82.92% for the NSL-KDD dataset. The proposed IDS competes with state-of-the-art methods in detection rate. QDA model limitations in handling categorical and nominal attributes. Slight decrease in detection rates in some intrusion detection datasets [15].

Framework enhances intrusion detection with Grey Wolf Optimization and Entropy-Based Graph. Outperforms existing methods with a 94.6% detection rate and 0.35% false positives. Framework enhances intrusion detection with Grey Wolf Optimization and Entropy-Based Graph. Outperforms existing methods with a 94.6% detection rate and 0.35% false positives. Grey Wolf Optimization Entropy-Based Graph Classification. Soft Computing method integration. GWO-EBG method achieved a detection rate of 94.6% and 0.35% false-positive rate. Outperformed EBG, KNN, SVM, and GRNN in various performance measures [16].

AFHO enabled DL for NIDS using AFHO, FHO, and DMN. Achieved high Precision, Recall, and F-measure in intrusion detection. AFHO enabled DL for NIDS using Wireless Network and DMN. AFHO combines AOA and FHO for feature selection. DMN achieves 93.7% precision, 97.7% recall, and 95.6% F-measure. Archimedes Fire Hawk Optimization (AFHO) for feature selection. Deep Maxout Network (DMN) for intrusion detection. AFHO-enabled DL for NIDS achieved 93.7% precision and 97.7% recall. AFHO optimised feature selection, DMN for intrusion detection. Resistance to zero-day assaults not examined and improved. The system's execution time did not improve with more nodes [17].

III Implementation methods

To validate the proposed algorithm's effectiveness, we implemented a comprehensive network security system integrating state-of-the-art intrusion detection models and routing protocols.

KNN-based Intrusion Detection System with AMODV and CBRP Algorithm.

Dataset Preparation: Step 1: *Prepare a dataset containing features of network traffic, such as source and destination IP addresses, protocol, packet size, and more, along with their corresponding labels (normal or malicious).*

Feature Selection: Step 2: *Select relevant features from the dataset to be used for intrusion detection.*

Training Phase:

Step 3: *Normalise the dataset to ensure all features are on the same scale.*

Step 4: *Split the dataset into a training set and a test set.*

Step 5: *Train intrusion detection models like KNN, AMODV, or IDS using the selected features from the labelled dataset.*

Testing Phase:

Step 6: *When a new instance of network traffic is observed:*

- *Extract relevant features from the new instance.*

Step 7: *Apply intrusion detection techniques (KNN, AMODV, or IDS) to determine whether the traffic is normal or malicious:*

a. For KNN:

i. Calculate the Euclidean distance between the new instance and all other instances in the dataset:

- *For each instance in the training set:*
- *Calculate the Euclidean distance between the new instance and the current instance.*

ii. Select the k nearest neighbours based on the calculated distances.

- *Sort the distances in ascending order and select the top k instances.*

iii. Determine the majority class among the k nearest neighbours.

- *If the majority class is 'malicious', predict that the new instance of network traffic is malicious.*
- *Otherwise, predict that the new instance of network traffic is not malicious.*

b. For AMODV:

i. Use the trained AMODV model to evaluate the new instance and determine whether it is normal or malicious.

c. For IDS:

i. Use the trained IDS model to classify the new instance of network traffic as normal or malicious.

Incorporation with CBRP:

Step 8: CBRP can be used to optimise the routing of data packets between sensor nodes in a wireless network.

- *Intrusion detection techniques like KNN, AMODV, or IDS can be used to detect malicious network traffic.*
- *CBRP can then be used to efficiently transmit this information to the appropriate nodes in the network.*

Feature Selection: We selected relevant features from the dataset to be used for intrusion detection, including [Bandwidth, Residual Energy, Traffic, Hop count, Round Trip Time, Total number of packets forward, Total number of packets received, Total number of packet drop, Total number of packet in communication, Minimum Received signal strength, Standard Received signal strength, Node Type].

Intrusion Detection Models: We employed several machine learning-based intrusion detection models, including KNN-IDS (K-Nearest Neighbors Intrusion Detection System). We trained the KNN model using the selected features from the labelled dataset. During training, we normalised the dataset to ensure all features were on the same scale. We split the dataset into a training set and a test set. The KNN algorithm was used to classify network traffic as normal or malicious. AMODV (Adaptive Multiobjective Optimization-based Detection of Anomalies in Network Traffic): We trained the AMODV model using the selected features from the labelled dataset. During training, the model optimised multiple objectives simultaneously to achieve better detection performance. When a new instance of network traffic was observed, the AMODV algorithm evaluated it using the trained model to determine whether it was normal or malicious. IDS (Intrusion Detection System): We trained an IDS model using the selected features from the labelled dataset. The IDS model was used to classify network traffic as normal or malicious.

IV Experimental Result

The conducted experiments using real-world network traffic data to evaluate the performance of our integrated network security system. Here, the model name calls it IDS_KNN (Intrusion Detection System_K-nearest neighbour), IK_AMODV (Intrusion Detection System_K-nearest neighbour with AMODV), and IKA_CBRP (Intrusion Detection System_K-nearest neighbour with AMODV, and CBRP).

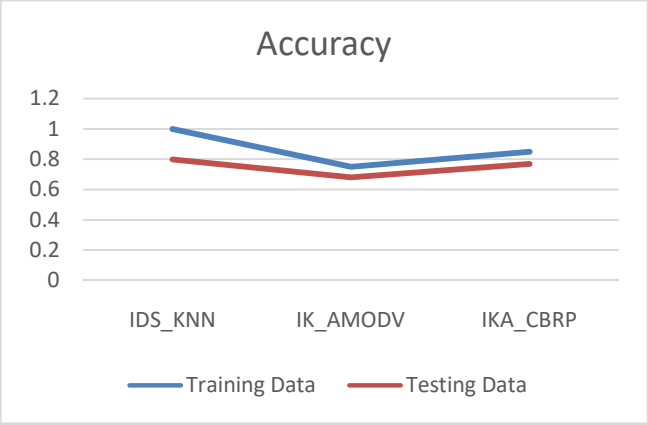

Fig 4.1 Accuracy

Figure 4.1 shows the accuracy of the training and testing datasets. IDS_KNN: Achieved perfect accuracy (100%) on the training data and 80% accuracy on the testing data.IK_AMODV: Achieved 75% accuracy on the training data and 68% accuracy on the testing data.IKA_CBRP: Achieved 85% accuracy on the training data and 77% accuracy on the testing data.

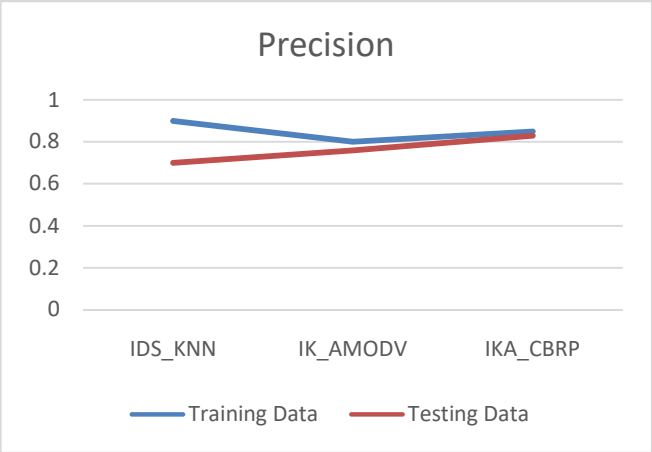

Fig 4.2 Precision

Figure 4.2 shows the Precision of the training and testing datasets. IDS_KNN: Precision of 90% on the training data and 70% on the testing data.IK_AMODV: Precision of 80% on the training data and 76% on the testing data.IKA_CBRP: Precision of 85% on the training data and 83% on the testing data.

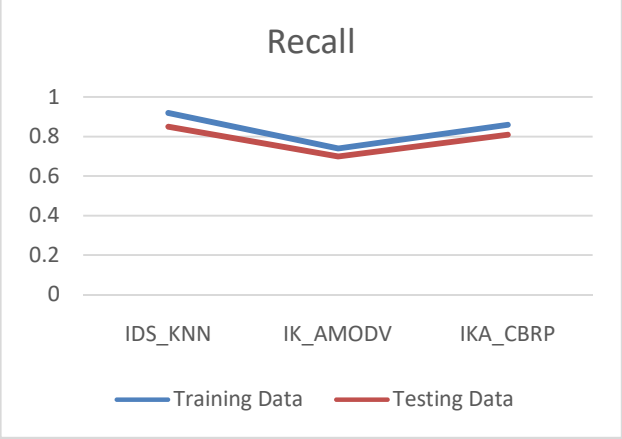

Fig 4.3 Recall

Figure 4.3 shows the Recall of the training and testing datasets. IDS_KNN: Recall 92% of the training data and 85% of the testing data.IK_AMODV: Recall 74% of the training data and 70% of the testing data.IKA_CBRP: Recall of 86% on the training data and 81% on the testing data.

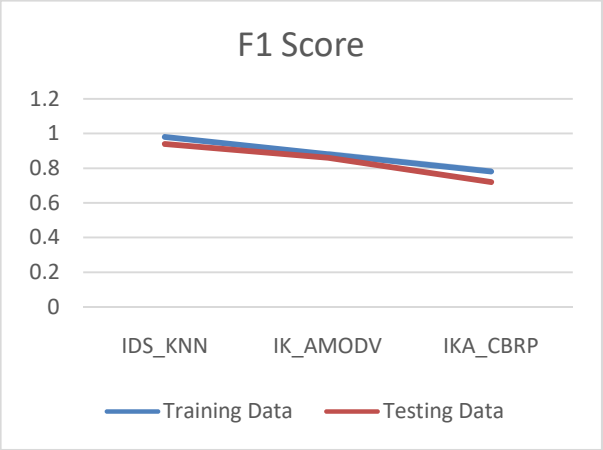

Fig 4.4 F1 Score

Figure 4.4 shows the accuracy of the training and testing datasets. IDS_KNN: F1 Score of 98% on the training data and 94% on the testing data.IK_AMODV: F1 Score of 88% on the training data and 86% on the testing data.IKA_CBRP: F1 Score of 78% on the training data and 72% on the testing data.

These experimental results demonstrate that the integration of machine learning-based intrusion detection models such as KNN-IDS and AMODV with routing protocols like CBRP significantly enhances the efficacy and adaptability of network security systems. The system showed improved accuracy in detecting and mitigating network attacks while efficiently routing data packets in a wireless network.

V Conclusion

In conclusion, our research presents a comprehensive approach to network security, integrating machine learning-based intrusion detection models and routing protocols. The experimental results demonstrate the effectiveness of the proposed approach in enhancing network security against evolving threats. We believe that our work provides valuable insights for researchers, practitioners, and policymakers in the field of network security.

Reference

[1] K. U, S. C. Karuturi, A. Veeramaneni, S. Balasubramanian, and T. Srivani, 'Adaptive Database Intrusion Detection Using Danger Theory and Negative Selection', *SSRN Journal*, 2024, doi: 10.2139/ssrn.4778512.

[2] S. P. Singh, N. Kumar, A. Kumar, P. Agrawal, V. Ghosh, and D. Singh, 'An Efficient Machine Learning-based Analytical Approach for Network Intrusion Detection System', *SSRN Journal*, 2024, doi: 10.2139/ssrn.4772570.

[3] C. T. Dhumal and Dr. S. V. Pingale, 'Analysis of Intrusion Detection Systems: Techniques, Datasets and Research Opportunity', *SSRN Journal*, 2024, doi: 10.2139/ssrn.4749820.

[4] V. T. Truong and L. B. Le, 'Security for the Metaverse: Blockchain and Machine Learning Techniques for Intrusion Detection', *IEEE Network*, pp. 1–1, 2024, doi: 10.1109/MNET.2024.3351882.

[5] Md. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, 'MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs', *Int. J. Inf. Secur.*, Mar. 2024, doi: 10.1007/s10207-024-00833-z.

[6] A. Amodei, D. Capriglione, G. Cerro, L. Ferrigno, G. Miele, and G. Tomasso, 'A Measurement Approach for Inline Intrusion Detection of Heartbleed-Like Attacks in IoT Frameworks', *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–10, 2023, doi: 10.1109/TIM.2023.3282662.

[7] K. Wei, H. Zang, Y. Pan, G. Wang, and Z. Shen, 'Strategic Application of AI Intelligent Algorithm in Network Threat Detection and Defense', vol. 4, no. 1, 2024.

[8] R. Morshedi, S. M. Matinkhah, and M. T. Sadeghi, 'Intrusion Detection for IoT Network Security with Deep learning', *JAIDM*, no. Online First, Mar. 2024, doi: 10.22044/jadm.2023.13539.2471.

[9] Z. Sun, G. An, Y. Yang, and Y. Liu, 'Optimised machine learning enabled intrusion detection 2 system for internet of medical things', *Franklin Open*, vol. 6, p. 100056, Mar. 2024, doi: 10.1016/j.fraope.2023.100056.

[10] K. N, V. Ravi, and V. Sowmya, 'Unsupervised intrusion detection system for in-vehicle communication networks', *Journal of Safety Science and Resilience*, vol. 5, no. 2, pp. 119–129, Jun. 2024, doi: 10.1016/j.jnlssr.2023.12.004.

[11] X. Su and G. Zhang, 'APFed: Adaptive, personalised federated learning for intrusion detection in maritime meteorological sensor networks', *Digital Communications and Networks*, p. S2352864824000191, Feb. 2024, doi: 10.1016/j.dcan.2024.02.001.

[12] D. Suja Mary, L. Jaya Singh Dhas, A. R. Deepa, M. A. Chaurasia, and C. Jaspin Jeba Sheela, 'Network intrusion detection: An optimised deep learning approach using big data analytics', *Expert Systems with Applications*, vol. 251, p. 123919, Oct. 2024, doi: 10.1016/j.eswa.2024.123919.

[13] G. Sai Chaitanya Kumar, R. Kiran Kumar, K. Parish Venkata Kumar, N. Raghavendra Sai, and M. Brahmaiah, 'Deep residual convolutional neural Network: An efficient technique for intrusion detection system', *Expert Systems with Applications*, vol. 238, p. 121912, Mar. 2024, doi: 10.1016/j.eswa.2023.121912.

[14] J. Azimjonov and T. Kim, 'Stochastic gradient descent classifier-based lightweight intrusion detection systems using the efficient feature subsets of datasets', *Expert Systems with Applications*, vol. 237, p. 121493, Mar. 2024, doi: 10.1016/j.eswa.2023.121493.

[15] E. Zorarpaci, 'A fast intrusion detection system based on swift wrapper feature selection and speedy ensemble classifier', *Engineering Applications of Artificial Intelligence*, vol. 133, p. 108162, Jul. 2024, doi: 10.1016/j.engappai.2024.108162.

[16] D. Srivastava, R. Singh, C. Chakraborty, S. Kr. Maakar, A. Makkar, and D. Sinwar, 'A framework for detection of cyber attacks by the classification of intrusion detection datasets', *Microprocessors and Microsystems*, vol. 105, p. 104964, Mar. 2024, doi: 10.1016/j.micpro.2023.104964.

[17] B. S. Rani, S. Vairamuthu, and S. Subramanian, 'Archimedes Fire Hawk Optimization enabled feature selection with deep maxout for network intrusion detection', *Computers & Security*, vol. 140, p. 103751, May 2024, doi: 10.1016/j.cose.2024.103751.