International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# INTRUSION DETECTION SYSTEM USING DEEP LEARNING

*Hemant Mishra[1], Dr. Shikha Tiwari[2]*

Amity University Raipur (CG)

ABSTRACT:

Intrusion detection systems (IDS) rely on good data to function effectively. To streamline training and testing, using appropriate categorization models and data preparation techniques is crucial. Early detection of anomalies is easier when they're closely monitored. Deep learning and AI offer promising solutions, highlighting the need for a reliable outlier identification system with fast training cycles. A hybrid approach to feature selection improves data classification and prediction accuracy. A unified IDS architecture provides administrators with efficient tools for better decision-making. Statistical techniques and various strategies have been explored, with "tremendous reversal" proving most effective. Training on the NSL-KDD dataset yielded impressive results: 99.73% success rate, 40% data reduction, and 100% productivity increase. The proposed model outperforms existing methods with a 99.72% F1 score and an average training/testing time of 2.7 seconds, making it a strong candidate for real-world application.

**Keywords:** Intrusion Detection System (IDS) . Network Security ,Anomaly Detection ,Signature- based Detection ,, Deep Learning ,Feature Selection ,Data Preprocessing ,Normalization ,Classification.

## 1. INTRODUCTION:

Network security professionals face a relentless battle against ever-more sophisticated and frequent attacks. The ever-expanding volume of internet traffic creates a double-edged sword: it fuels communication but also exposes networks to a wider range of threats, both internal and external. Sifting through this massive amount of data for potential dangers is a constant struggle, demanding significant time and resources.

To address this growing complexity, the field of network security is exploring intelligent detection systems. These systems aim to maintain the accuracy of traditional intrusion detection systems (IDS) while minimizing the computational resources required.

**Here's a breakdown of the challenges and potential solutions:**

1. **The Data Deluge:** The sheer volume of network traffic makes it difficult to keep track of everything. Traditional methods struggle to analyze vast amounts of data efficiently, leaving vulnerabilities open.
2. **Evolving Threats:** Attackers areconstantly innovating, developing new tactics that can bypass existing security measures. Detection systems need to beadaptable to identify novel threats.
3. **False Positives and Negatives:** Existing IDS approaches, like signature-based and anomaly-based detection, can generate false positives (flagging harmless activity as malicious) and false negatives (missing actual attacks). These inaccuracies can overwhelm security personnel and reduce overall effectiveness.

### *The Role of Feature Selection:*

Feature selection is a crucial step inoptimizing IDS performance. It helps to:

- **Improve Efficiency:** By selecting the most relevant data points (features), the system can analyze information faster and with fewer resources.
- **Reduce Complexity:** High- dimensional data (data with many features) can be complex foralgorithms to handle. Feature selection simplifies the data, making it easier to identify patterns and improve accuracy.
- **Eliminate Noise:** Irrelevant data can obscure important details. Feature selection removes unnecessary information, allowing the system to focus on the most critical aspects of network traffic.

## Strategies for Effective FeatureSelection:

There are two main approaches to feature selection: filtering and wrapping.

- **Filtering Techniques:** These methods analyze the data independently of the chosen classification algorithm. They are generally faster and less computationally expensive.
- **Wrapper Techniques:** These methods involve evaluating feature subsets based on their effectiveness with a specific classification algorithm.While offering more flexibility, they can be more time-consuming.

### *Less Computational Power*

By using feature selection approaches to cut down on the size of a big dataset, system resource usage during model training and testing may be kept within reasonable bounds.

### *Improved Detection Accuracy*

In this paper, we suggest a hybrid approach with two distinct stages. We first employ dimensionality reduction methods based on feature selection using filters. As a result, we may shorten processing time while alsospeeding up processing. We classify thedata using a deep neural network (DNN) after choosing the most useful set of attributes to use [20-22]. By combining these methods, the IDS's overall performance is intended to be improved.

**TABLE - 1**

| Strategy | Benefits | Drawbacks |
|---|---|---|
| **Wrapper Approach** | - Providesthe mostrelevant feature subset | - Slower due to increased processing |
|  | - Can improvesystem accuracy | - More proneto overfitting |
| **Filter Method** | - Quickanalysis with low overfitting | - May notalways selectthe most relevant |

## RELATED WORK :

The cyberwar rages on, demanding ever- more sophisticated defenses. Intrusion detection systems (IDS) stand as a vital line of defense, constantly monitoring network traffic for malicious activity. Researchers are wielding the power of machine learning and deep learning to identify these threats. From Deep Belief Networks (DBNs) excelling at high-dimensional data analysis to hybrid DNN models trained on diverse attack types, the arsenal of detection techniques is growing.

However, the challenge is not just about identifying threats, but doing so quickly. Modern hackers operate with speed, and IDSs need to keep pace. Scalable hybrid systems are being developed to handle massive real-time data streams and raise immediate alarms. But raw data volume presents another hurdle. Feature selection techniques, like filter-based and wrapper- based approaches, are crucial for sifting through this data and pinpointing the key indicators of an attack. By streamlining the data, these techniques allow IDSs to focus on the most critical information, boosting detection accuracy and efficiency.

The future of network security lies in this powerful marriage of cutting-edge machine learning, deep learning, and meticulous feature selection. As the threat landscape continues to evolve, ongoing research and innovative approaches are paramount to staying ahead of the curve and safeguarding our digital world.

## METHODOLOGY :

The proposed methodology involves data preprocessing, feature selection, and DNN classification. Data normalization and scaling are performed to standardize input features. Feature selection techniques like chi-square, ANOVA, and PCA are applied to extract relevant features for intrusion detection. The DNN model is trained and tested using the NSL-KDD dataset, with activation functions optimized for classification tasks.

**FIGURE – 1:**

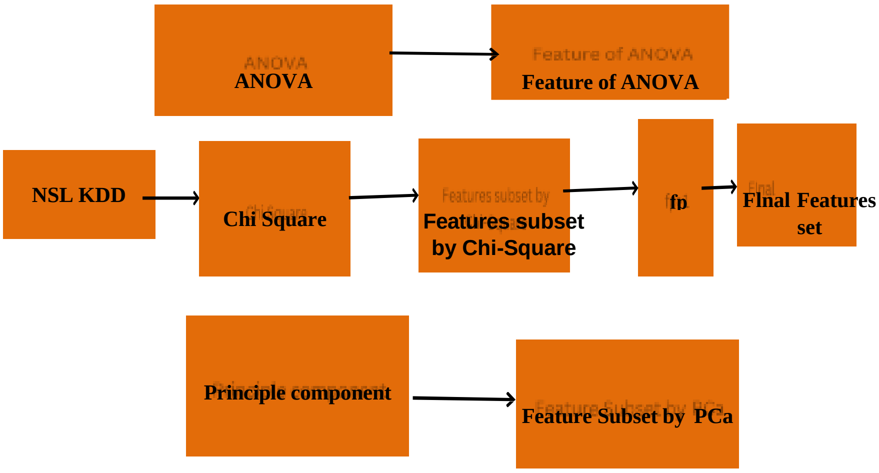

**Figure 1 Block diagram of the proposedmodel**

The image depicts a flowchart related to feature selection methods and their sequence in data processing for a dataset named NSL KDD. The flowchart shows three parallel processes that start from the NSL KDD dataset and lead to a final feature set

***Data Collection andPreprocessing:***

Data Acquisition: The NSL-KDD dataset isutilized as the basis for training and testingthe intrusion detection system (IDS). Data Normalization: Before feeding the data intothe deep learning model, normalization techniques like min-max scaling are appliedto ensure that all features are on a similar scale, which aids in the convergence and effectiveness of the deep learning model.

***Feature Selection Techniques:***

Filter-Based Approaches: Statistical methods such as the chi-squared test, analysis of variance (ANOVA), and principal component analysis (PCA) are employed for feature selection. These techniques help in identifying the most relevant features that contributesignificantly to intrusion detection.

**A. Deep Neural Network (DNN) Model for Classification:**

Architecture Design: A deep neuralnetwork (DNN) model is designed withmultiple hidden layers to capture complex relationships and patterns within the network traffic data. Activation Functions: The DNN model utilizes rectified linearunit (ReLU) activation functions for thehidden layers and a sigmoid activation function for the output layer. ReLU helps inovercoming the vanishing gradient problemand enables efficient learning of non-linear features.

Training Process: The DNN model is trained using the NSL-KDD dataset, wherethe training data is fed through the networkin batches. The model optimizes its parameters using techniques like backpropagation and gradient descent tominimize classification errors.

Evaluation and Testing: After training, the DNN model is evaluated using a separate validation dataset to assess its generalization performance. Testing involves feeding unseen data to the trained model to classify network traffic intonormal and anomalous categories.

**B. Algorithm Implementation:**

Deep Learning Algorithm: The proposed deep learning-based intrusion detectionalgorithm focuses on learning intricate patterns and anomalies from the network traffic data. It leverages the capabilities of deep neural networks to enhance detection accuracy and reduce false positives.

Integration of Feature Selection Results:The features selected through statistical techniques like chi-square, ANOVA, and PCA are integrated into the DNN model toimprove its efficiency in detecting and classifying network intrusions.

**C. Experimental Validation:**

The performance of the deep learning- based IDS is evaluated using metrics such as accuracy, precision, recall, and F1 score.These metrics provide insights into the model's effectiveness in identifying bothknown and novel intrusion patterns. Comparison with Traditional Methods: Theperformance of the deep learning approachis compared with traditional machine learning methods and other state-of-the-art intrusion detection techniques to showcase its superiority in terms of accuracy and computational efficiency.

Here's a structured table based on the provided methodology incorporating deep learning concepts in intrusion detection research:

**Table-2**

| Stage | Description |
|---|---|
| **Data Collection and Preprocessing** | - Utilize the NSL-KDD dataset for training and testing the IDS.<br>- Apply data normalization techniques like min-max scaling. |
| **Feature Selection Techniques** | - Use filter-based approaches such as chi-squared test, ANOVA, and PCA for featureselection. |
| **Deep Neural Network (DNN) Model** | - Design a DNN architecture with multiple hidden layers.<br>- Utilize ReLU activation for hidden layers and Sigmoid for output layer.<br>- Train the DNN model using backpropagation and gradient descent.<br>- Evaluate the model's performance using a separate validation dataset. |
| **Algorithm Implementation** | - Implement a deep learning-based intrusion detection algorithm.<br>- Integrate selected features from feature selection techniques into the DNN model.<br>- Assess the model's performance using metrics like accuracy, |

| | |
|---|---|
| | precision, recall, and F1 score. |
| **Experimental Validation** | - Compare the deep learning approach with traditional methods and state-of-the-art IDS techniques.<br>- Evaluate the model's ability to detect both known and novel intrusion patterns.<br>- Validate the model's superiority in accuracy and computational efficiency. |

### *3.3. Deep Neural Network Model forClassification*

Following data cleansing, a Deep Neural Network (DNN) is utilized to categorize thecollected information. Advances in deepneural network technology have simplifiedthe detection of anomalies and potentialthreats across various contexts. A typical DNN model comprises three layers: an input layer, a hidden layer, and an output layer. During training, the DNN optimizes its parameters to improve efficiency and reduce false positives. The multi-layeredstructure of DNNs enables them to efficiently analyze large datasets, enhancing pattern recognition capabilities. The output layer of the DNN utilizes a sigmoid activation function, while rectified linear unit (ReLU) activation functions are used in the hidden layers. The choice of activation functions greatly impacts the DNN's performance in training and classification tasks. In this study, a DNN model integrating three Convolutional Neural Networks (CNNs) is proposed. Eachlevel within the DNN-CNN model performs distinct tasks to effectively evaluate and interpret the data. The Adam optimizer is employed during training to enhance the DNN model's performance andconvergence.

### *3.4. Algorithm*

- Deep Learning for Intrusion Detection in Networks is the first algorithm.
- We will focus on the NSL-KDDTrain++2 dataset first.
- Next, gather and arrange the data:
- Use the min-max approach to normalizenumerical properties.
- The encoding of textual properties usesdummy encoding.
- Choosing Specific Attributes
- Choose the traits that are most relevant(f_n) using the Chi-Square test.
- You may use analysis of variance (f_a) toimprove feature sets.
- To further condense features, one can useprincipal component analysis (f_p).
- The fourth stage is to compose a list of characteristics that are shared by all three types.

Continue to step five, classifying. The Deep Neural Network (DNN) should next be tested on the NSL-KDD Binary Classification Dataset. Your DNN model's output layer should be Sigmoid, and the input and hidden layers should be ReLU. Ask about the output's categorization at number eight. Number nine, keep going.

The proposed technique utilizes a deep learning-based framework to locate and prioritize characteristics that aid in the identification of network intrusions. Beforeutilizing a dataset for classification, it is crucial to decide which characteristics to include in it. In order to determine which aspects of the data are most important, the algorithm uses a variety of statistical techniques, including the Chi-Square test, One-way Analysis of Variance, and Principal Component Analysis. Once thetraits have been narrowed down, they are sent into a Deep Neural Network (DNN) tobe classified. The NSL-KDD Binary Classification Dataset is used for training and testing the DNN model that features ReLU activation for the hidden layers and Sigmoid activation for the output layer. Thesuggested approach improves the network'ssecurity and dependability by using deep learning to recognize and classify network intrusions more accurately using improvedfeature selection techniques.

### *3.5. Dataset Description*

Figure 4 illustrates the binary class distribution within the NSL-KDD dataset, which serves as a standard benchmark in the fields of anomaly detection and intrusion detection. Compared to the KDD99 dataset, NSL-KDD exhibits a more balanced distribution and less extreme value ranges. With two distinct labels, the dataset is well-suited for tasks requiringbinary categorization. The dataset comprises a total of 41 features used in the classification process, with both trainingand validation conducted on this dataset distribution of the binary classes is crucial as it ensures equal representation of both normal and anomalous instances. This balance allows the model to learn from both types of examples, reducing bias and enhancing the reliability of classificationoutcomes. Thus, the NSL-KDD dataset'scharacteristics make it highly suitable for training and evaluating intrusion detection models.

**FIGURE – 2:**

Anomaly
Normal

Figure 2 illustrates a simplified flowchart depicting the inner workings and data flowof a typical DNN model. This visualizationhelps understand how the network dynamically adjusts detection parametersduring the learning process. Integrating the feature selection expertise of the intrusion detection system with the capabilities of a complex DNN model has significantly improved the system's ability to detect and classify potentially harmful activities on a network.

containing 125,974 instances. Each instance represents a unique network action or connection. In the context of intrusion detection, the binary class distribution

distinguishes between "normal" and "anomalous" or "benign" and "malicious" occurrences. Maintaining a balanced

## Experimental Result And Discussion

In this section, we will demonstrate theadvantages of the proposed model. Each approach consists of three phases: preprocessing, feature selection, and classification. Preprocessing involves preparing data for analysis. During the feature selection phase, input data is reduced by 60%, leading to improved efficiency as noisy and redundant components are eliminated. This reduction enhances the model's performance significantly.Comparing to previous detection methods, our categorizationresults show superiority. We further delve into the outcomes of our feature selection and classification analyses below.

### *Feature Selection Results*

After the data has been normalized, dimensionality reduction may begin. To achieve this feat of feature reduction, we employ three widely used feature selection techniques. These methods don't provide adequate insight into the entire dataset. As the last parameter in the classification method, we employed a characteristic that was present in all three categories. The findings from all three studies aresummarized in Table 2. The steps that mustbe taken to choose characteristics are laid out in Table 2. The greatest accuracy is reached using the proposed feature selection technique, as shown in Table 3. Our recommended method for selecting features produces a dataset with low false- positive rates, high classification accuracy,high precision, and high recall of genuine positives.

### *Classification Results*

For binary classification, the suggested DNN model performs better than its forerunners in terms of accuracy, precision,recall, and F1 score. Table 4 presents the model's outstanding results, which are the highest accuracy ever reported for a research of this kind (99.73%). The confusion matrix may be used to demonstrate how well the suggested model performs at accurately classifying data from the network once it has been put into use. The significant differences between the proposed method and state-of-the-art deep learning and machine learning techniques are outlined in Table 6. Results indicate thatthe suggested model is superior to the reference models and ought to be followed as the benchmark for categorizing networks and carrying out intrusion detection. The assessment findings, which are shown in Figures 5 and 6, demonstrate that the suggested model surpasses cutting-edge deep learning and machine learning techniques. The proposed method consistently outperforms the state-of-the- art methods in terms of accuracy, precision,recall, and F1 score, and it also shortens thetesting period.

**FIGURE - 3**

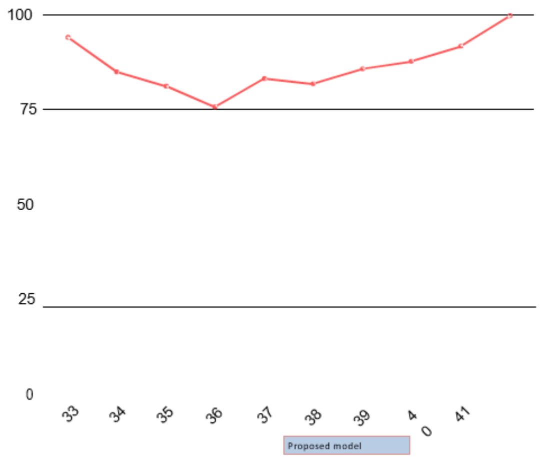

**Figure 3: A comparison of the suggestedmodel's accuracy with other models**

Figure 7 displays our method's performance in comparison to that of standard machine learning models. Our suggested model outperforms all other machines andinstructional methods already in use. The complexity of network data is a challenge for machine learning algorithms.

**Figure 4 depicts how the proposedstrategy stacks up against machine learning methods.**

### *Computational Time*

The proposed deep neural network model stands out from previous deep learning and machine learning models due to its notably faster training and testing times. While feature selection methods aid in reducing input dimensionality, they also guide the model to concentrate on crucial information. Our suggested method strikes a balance between precision and computational efficiency, unlike alternative methods that may overly emphasize precision. This balance makes it suitable for practical applications in network intrusion detection, where considerations of both accuracy and computational resources are crucial.

## CONCLUSION AND FUTUREWORK

This study proposes deep learning as an effective method for intrusion detection, offering a novel technique to safeguard network data from various threats. Our approach utilizes a robust detection model that integrates feature selection and classification methods, leading to enhanced performance. Beyond traditional metrics like accuracy, precision, recall, and the F1 score, our approach emphasizes the importance of resource conservation by leveraging feature selection algorithms to remove unnecessary data. Consequently, our model exhibits significantly reduced training and testing times compared to other alternatives. Future research directions may include evaluating our model's performance on diverse datasets, particularly those with multiple classes, to assess its adaptability across different scenarios. Exploring additional feature selection techniques could further enhance the model's ability toaccurately predict events. These efforts aimto strengthen our current findings and contribute to the ongoing advancements in intrusion detection systems.

## REFERENCES:

1. Alabdulwahab, S., & Moon, B. (2020). Feature selection methods simultaneously improve the detection accuracy and model building time of machine learning classifiers. Symmetry, 12(9), 1424.

2. Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). A review of intrusion detection system using machine learning approach. International Journal of Engineering Research and Technology,12(1), 8–15.

3. Shah, F., Anwar, A., AlSalman, H., Hussain, S., & Al-Hadhrami, S. (2022). Artificial intelligence as a service for immoral content detection and eradication.Scientific Programming, 2022, 6825228.
4. Tang, C., Luktarhan, N., & Zhao, Y.(2020). SAAE-DNN: deep learning methodon intrusion detection. Symmetry, 12(10), 1695.
5. Wang, X., Yin, S., Li, H., Wang, J., & Teng, L. (2020). A network intrusion detection method based on deep multi-scaleconvolutional neural network. InternationalJournal of Wireless Information Networks,27(4), 503–517.
6. Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep learning approach combining sparse autoencoder with SVM for network intrusion detection.IEEE Access, 6, 52843–52856.
7. Ingre, B., & Yadav, A. (2015). Performance analysis of NSL-KDD dataset using ANN. In 2015 International Conference on Signal Processing and Communication Engineering Systems (pp. 92–96). Guntur, India: IEEE.
8. Kainat, J., Ullah, S. S., Alharithi, F. S., Alroobaea, R., Hussain, S., & Nazir, S. (2021). Blended features classification of leaf-based cucumber disease using image processing techniques. Complexity, 2021, 9736179.
9. Iqbal, J., Hussain, S., AlSalman, H., Mosleh, M. A., & Ullah, S. S. (2021). A computational intelligence approach for predicting medical insurance cost. Mathematical Problems in Engineering, 2021, 1162553.
10. Li, Z., Qin, Z., Huang, K., Yang, X., & Ye, S. (2017). Intrusion detection using convolutional neural networks for representation learning. In ICONIP 2017: Neural Information Processing,International Conference on NeuralInformation Processing (pp. 1–11). Springer, Cham.
11. Tama, B. A., Comuzzi, M., & Rhee, K.
H. (2019). TSE-IDS: a two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. IEEE Access, 7,94497–94507.
12. Choudhary, S., & Kesswani, N. (2020). Analysis of KDD-Cup’99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. Procedia Computer Science, 167, 1561–1573.
13. Farahnakian, F., & Heikkonen, J. (2018). A deep auto-encoder based approach for intrusion detection system. In 2018 20th International Conference on Advanced Communication Technology(ICACT) (pp. 178–183). Chuncheon,Korea (South): IEEE.
14. Boutaba, R., Salahuddin, M. A., Limam, N., et al. (2018). A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. Journal of Internet Services and Applications, 9(1), 1–99.
15. Lakhina, S., Joseph, S., & Verma, B. (2010). Feature reduction using principal component analysis for effective anomaly– based intrusion detection on NSL-KDD.Citeseer.
16. Rawat, D. B., & Reddy, S. R. (2017). Software defined networking architecture, security and energy efficiency: A survey. IEEE Communications Surveys & Tutorials, 19(1), 325–346.
17. Khan, M. Z., Naseem, R., Anwar, A., et al. (2022). A novel approach to automate complex software modularization using a fact extraction system. Journal ofMathematics, 2022, 8640596.
18. Srba, I., & Bieliková, M. (2012). Encouragement of collaborative learning based on dynamic groups. In 21st Century Learning for 21st Century Skills.
19. Kantardzic, M. (2011). Data Mining: Concepts, Models, Methods, and Algorithms. John Wiley & Sons.
20. Hussain, D., Ismail, M., Hussain, I., Alroobaea, R., Hussain, S., & Ullah, S. S. (2022). Face mask detection using deepconvolutional neural network andMobileNetV2-Based transfer learning. Wireless Communications and Mobile Computing, 2022, 1536318.
21. Kumar, S., Jain, A., Rani, S., Alshazly, H., Idris, S. A., & Bourouis, S. (2022). Deep neural network based vehicle detection and classification of aerial images. Intelligent Automation and Soft Computing, 34(1), 119–131.
22. Aa, M., Hamdi, M., Bourouis, S., Rastislav, K., & Mohmed, F. (2022).
Evaluation of neuro images for the diagnosis of Alzheimer’s disease using deep learning neural network. Frontiers in Public Health, 10, 834032.

23. Aldweesh, A., Derhab, A., & Emam, A.
Z. (2020). Deep learning approaches foranomaly-based intrusion detection systems:a survey, taxonomy, and open issues. Knowledge-Based Systems, 189, 105124.

24. Scarfone, K., & Mell, P. (2007). Guideto intrusion detection and prevention systems (IDPS). NIST Special Publication,800(2007), 94.

25. Gao, N., Gao, L., Gao, Q., & Wang, H. (2014). An intrusion detection model basedon deep belief networks. In 2014 Second International Conference on Advanced Cloud and Big Data (pp. 247–252). Huangshan, China: IEEE.

26. Potluri, S., & Diedrich, C. (2016). Accelerated deep neural networks for enhanced intrusion detection system. In 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1–8). Berlin, Germany: IEEE.

Kim, J., Shin, N., Jo, S. Y., & Kim, S.
27. H. (2017). Method of intrusion detection using deep neural network. In 2017 IEEE International Conference on Big Data and Smart Computing (BigComp) (pp. 313– 316). Jeju, Korea: IEEE.

28. Zeng, Y., Gu, H., Wei, W., & Guo, Y. (2019). Deep-full-range: a deep learningbased network encrypted trafficclassification and intrusion detection framework. IEEE Access, 7, 45182–45190.

29. Maithem, M., & Alazab, M. (2021). Network intrusion detection system using deep neural networks. In Journal of Physics: Conference Series (Vol. 1804, No.1, p. 12138). IOP Publishing.

Vinayakumar, R., Alazab, M., Soman,
30. K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550.

31. Jo, S., Sung, H., & Ahn, B. H. (2016).
31. A comparative study on the performance of SVM and an artificial neural network in intrusion detection. Journal of the Korea Academia-Industrial Cooperation Society, 17(2), 703–711.

32. Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2016). Deep learning approach for network intrusion detection in software defined networking. In 2016 InternationalConference on Wireless Networks and Mobile Communications (WINCOM) (pp. 258–263). Fez, Morocco: IEEE.

Su, T., Sun, H., Zhu, J., Wang, S., & Li,
33. Y. (2020). BAT: deep learning methods onnetwork intrusion detection using NSL- KDD dataset. IEEE Access, 8, 29575– 29585.

34. Yu, Y., & Bian, N. (2020). An intrusiondetection method using few-shot learning. IEEE Access, 8, 49730–49740.

35. Kshirsagar, D., & Kumar, S. (2021). Anefficient feature reduction method for the detection of DoS attack. ICT Express, 7(3),371–375.

Ahmadi, S. S., Rashad, S., & Elgazzar,
36. H. (2019). Efficient feature selection for intrusion detection systems. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 1029–1034). New York, NY, USA: IEEE.

37. Liu, X., Li, T., Zhang, R., Wu, D., Liu, Y., & Yang, Z. (2021). A GAN and feature selection-based oversampling technique forintrusion detection. Security and Communication Networks, 2021, 9947059.

38. Osanaiye, O., Ogundile, O., Aina, F., &Periola, A. (2019). Feature selection forintrusion detection system in a cluster- based heterogeneous wireless sensor network. Facta Universitatis, Series: Electronics and Energetics, 32(2), 315–330.

39. Gottwalt, F., Chang, E., & Dillon, T. (2019). CorrCorr: a feature selection method for multivariate correlation network anomaly detection techniques.Computers & Security, 83, 234–245.

40. Vinutha, H. P., & Poornima, B. (2018).Analysis of feature selection algorithms for
Naïve Bayes classifier using NSL-KDD.International Journal of Engineering andManufacturing Science, 8(1), 167–175.

41. Dawoud, A., Shahristani, S., & Raun, R. (2018). Deep learning and software-defined networks: Towards secure IoT architecture. Internet of Things, 3-4, 82–89.

42. Bhattacharya, S., & Selvakumar, S. (2015). LAWRA: a layered wrapper featureselection approach for network attack detection. Security and Communication Networks, 8(18), 3468.

43. Raman, M. G., Somu, N., Kirthivasan, K., Liscano, R., & Sriram, V. S. (2017). Anefficient intrusion detection system based on hypergraph-genetic algorithm for parameter optimization and feature selection in support vector machine. Knowledge-Based Systems, 134, 1–12.

44. Mohammadi, S., Mirvaziri, H., Ghazizadeh-Ahsaee, M., & Karimipour, H.(2019). Cyber intrusion detection by combined feature selection algorithm. Journal of Information Security andApplications, 44, 80–88.

45. Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2019). An adaptive ensemble machine learning model for intrusion detection. IEEE Access, 7, 82512–82521.

46. Yin, C., Zhu, Y., Fei, J., & He, X.(2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961.

47. Torabi, M., Udzir, N. I., Abdullah, M. T., & Yaakob, R. (2021). A review on feature selection and ensemble techniques for intrusion detection system. InternationalJournal of Advanced Computer Science andApplications, 12(5), 2.

48. Wang, Z., Liu, Y., He, D., & Chan, S. (2021). Intrusion detection methods based on integrated deep learning model. Computers & Security, 103, 102177.

49. Usman, S. M., Latif, S., & Beg, A.(2019). Principle components analysis for seizures prediction using wavelet transform. International Journal of Advanced and Applied Sciences, 6(3), 50–55.

50. Usman, S. M., Khalid, S., & Aslam, M.
H. (2018). Epileptic seizures prediction using scalp EEG signals. Biocyberneticsand Biomedical Engineering, 41(1), 211– 220.

51. Usman, S. M., Khalid, S., Jabbar, S., & Bashir, S. (2021). Detection of preictal statein epileptic seizures using ensemble classifier. Epilepsy Research, 178, 106818.

52. Usman, S. M., Khalid, S., & Bashir, Z. (2021). Epileptic seizure prediction using scalp electroencephalogram signals. Biocybernetics and BiomedicalEngineering, 41(1), 211–220.

53. Usman, S. M., Khalid, S., Bashir, S., & Bashir, Z. (2021). A deep learning based ensemble learning method for epileptic seizure prediction. Computers in Biology and Medicine, 136, 104710.

54. 54. Nazir, A., & Khan, R. A. (2021). A novel combinatorial optimization based feature selection method for network intrusion detection. Computers & Security,102, 102164.

55. Dina, A. S., & Manivannan, D. (2021).Intrusion detection based on Machine Learning techniques in computer networks.Internet of Things, 16, 100462.

56. Shah, F., Liu, Y., Anwar, A., et al. (2022). Machine learning: the backbone of intelligent trade credit-based systems. Security and Communication Networks, 2022, 7149902.

57. Haq, I. U., Anwar, A., Rehman, I. U., etal. (2021). Dynamic group formation with intelligent tutor collaborative learning: anovel approach for next-generation collaboration. IEEE Access, 9, 143406– 143422.

58. Iwendi, C., Maddikunta, P. K., Gadekallu, T. R., Lakshmanna, K., Bashir,
K., & Piran, M. J. (2021). A metaheuristic optimization approach for energy efficiency in IoT networks. Software: Practice and Experience, 51(12),2558–2571.

59. Chang, C. Y., Bhattacharya, S., Vincent, P. M. R., Lakshmanna, K., &

Srinivasan, K. (2021). An efficient classification of neonates cry using extremegradient boosting-assisted grouped-support-vector network. Journal of Healthcare Engineering, 2021, 7517313.

60. Kaluri, R., Rajput, D. S., Xin, Q., et al.(2021). Rough sets-based approach for predicting battery life in IoT. arXiv preprintarXiv:2102.06026.

61. Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2018). A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection. Computers & Security,75, 36–58.

62. Ahmad, S., Arif, F., Zabeehullah, Z., & Iltaf, N. (2020). Novel approach using deep learning for intrusion detection and classification of the network traffic. In 2020 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA) (pp. 1–6). Tunis, Tunisia: IEEE.