# **AI-Based Intrusion Detection System (IDS) Using XGBoost for Real-Time Cybersecurity**

*1.Shakthi.R.L,*

*Department of Artificial Intelligence and Data Science, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, Pincode:602105.* [*shakthirishi007@gmail.com*](mailto:shakthirishi007@gmail.com)

*2.Padmalakshmi.R.S,*

*Department of Artificial Intelligence and Machine Learning, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, Pincode:602105.* [*padmalakshmi704@gmail.com*](mailto:padmalakshmi704@gmail.com)

*3.Udayaraaj.T.I,*

*Department of Artificial Intelligence and Data Science, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, Pincode:602105.* [*Ti.udayaraaj2003@gmail.com*](mailto:Ti.udayaraaj2003@gmail.com)

*4.Shawn Basil.C.K,*

*Department of Information Technology, Saveetha Institute of Science and Technology, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, Pincode:602105.* [*shawnbasil1970@gmail.com*](mailto:shawnbasil1970@gmail.com)

***ABSTRACT: Network intrusion detection is a crucial aspect of modern system’s cybersecurity. This paper presents an AI-based intrusion Detection System (IDS) using the NSL-KDD dataset, achieving 97.09% (accuracy) and a ROC-AUC score of 0.99, demonstrating the potential of AI-driven solutions for real-time intrusion detection in both online and offline environment. The exponential growth of cyber threats necessitates intelligent solutions for real-time network monitoring and protection. The study integrates artificial intelligence into intrusion detection (IDS) design using the dataset, generating a “golden dataset” and implementing XGBoost for superior network traffic classification, enabling real-time monitoring and retrospective analysis. The project yielded training (100778,119), testing (25195,119), precision (0.98), F1-score (0.97), recall/specificity (0.98) values with True Negative (TN: 269), True Positive (TP:11310),False Negative (FN:463), False Negative (FP:269). The robust***

***design allows for real-time and offline deployment, offering a scalable and efficient solution for modern cybersecurity challenges.***

***Keywords: Intrusion Detection System , ROC-AUC , XGBoost Algorithm , Transfer learning, Deep learning in agriculture, cybersecurity challenges, Validation accuracy.***

**INTRODUCTION**

The rapid expansion of digital networks and their integration into critical infrastructure has significantly increased the prevalent of cyber threats. Network intrusion detection system (IDS) are crucial in ensuring the security of modern networks, making their protection a top priority. An IDS is a crucial component of cybersecurity frameworks, monitoring network traffic for suspicious activities and alerting administrators to potential breaches. Traditional IDS techniques face high false positive reates, adaptability issues, and scalability challenges, making them insufficient for modern real-time applications. Real-time network monitoring is a complex task due to the dynamic and high-volume nature of network traffic. Accurately identifying malicious activities, minimizing falsa positives, and ensuring scalability are crucial for effective cyberattack management, necessitating intelligent and adaptive solutions. The NSL-KDD dataset, a benchmark for IDS performance, classifies network traffic into normal and anomalous activities, addressing limitations of its predecessor. It aids in developing advanced intrusion detection models, integrating AI into IDS design for high accuracy. The paper presents an AI-based intrusion detection system using the NSL-KDD dataset and XGBoost algorithm for robust network traffic classification. The model achieves 97.09% accuracy and a ROC-AUC score of 0.99, demonstrating its efficacy I distinguishing normal and anomalous traffic. Key contributions include a scalable model for real-time deployment and robust evaluation metrics

**LITERATURE REVIEW**

Intrusion Detection System (IDS) are crucial in protection networks from malicious activities, with traditional approaches like signature-based and anomaly-based systems being inefficient in detecting zero-day attacks and high false-positive rates [1]. The advent of AI and machine learning techniques has significantly enhanced the capabilities of IDS, thereby overcoming some of its limitations. AI-driven IDS advancements explore decision trees, SVMs, and deep neural networks for interpretability, computational efficiency, and high-dimensional data handling [2]. Neural networks, while capable of modelling intricate relationships, necessitate substantial computational resources, making them less suitable for real-time applications [3]. Ensemble methods like Random Forest and Gradient Boosting improve intrusion detection accuracy, with XGBoost being a leading framework due to its scalability and efficiency in large dataset [4].

The NSL-KDD dataset, removing redundant records, is a benchmark for evaluating IDS performance, demonstrating AI-based models consistently outperform traditional approaches in accuracy and generalization [5]. The issues of imbalanced class distributions and high-dimensional features spaces persists, necessitating advanced preprocessing techniques and robust model architectures to trickle. XGBoost is being explored for its ability to manage class imbalance and provide feature importance insights, making it ideal for analysing complex network traffic data [6].

Recent studies show that integrating XGBoost with advanced preprocessing techniques like feature scaling and normalization significantly improves the detection of rare attack patterns [7]. The models generalization capabilities have been enhanced through techniques like cross-validation and hyperparameter optimization. This study uses XGBoost for real-time intrusion detection, achieving high accuracy and robust performance in both real-time and offline scenarios. It enhances preprocessing pipeline and NSL-KDD dataset, setting new benchmarks for IDS performance [8].

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Method** | **Accuracy** | **Precision** | **Recall** | **F1-Score** | **ROC-AUC** |
| **Traditional IDS (SVM)** | 92.4% | 0.89 | 0.90 | 0.89 | 0.93 |
| **Deep Learning (LSTM)** | 94.6% | 0.91 | 0.93 | 0.92 | 0.96 |
| **Proposed IDS (XGBoost)** | 97.09% | 0.98 | 0.98 | 0.97 | 0.99 |

Table 1: Comparative Analysis of Intrusion Detection Systems

**MATERIALS**

The AI-based Intrusion Detection System uses the NSL-KDD dataset, which includes 41 features and a class label for normal or attack traffic, with preprocessing steps for enhanced classification. The hardware included an Intel Core i7-9700K processor, 16GB RAM, 1TB SSD, and NVIDIA GeForce GTX 108 GPU, while software tools included Python 3.8, Scikit-learn, XGBoost, Pandas, Matplotlib, and TensorFlow. The dataset, split into 100,778 training and 25,195 testing samples, was evaluated for accuracy, precision, recall,F1-score, and ROC-AUC, ensuring robust performance validation for real-time and scalable cybersecurity applications.

**Methodology**

The article introduces an AI-driven intrusion detection methodology using the XGBoost algorithm for network traffic classification, detailing the process of dataset acquisition, preprocessing, model architecture, training, and evaluation metrics.

*A. Dataset*

The NSL-KDD dataset, an improved version of the KDD cup 99 dataset, was used for training and testing the IDS model due to its established role in IDS research and the dataset was divided into training (80%) and validation (20%) sets to optimize the learning process.

*B. Data Preprocessing*

The Intrusion Detection System (IDS) performance and accuracy were enhanced through effective data preprocessing, as demonstrated in the NSL-KDD dataset.

* Encoding: One-hot encoding was used to encode categorical features like network protocols and service types into a machine learning model format.
* Normalization: The learning process was normalized to range from 0 to 1, ensuring no single feature dominated due to scale differences.
* Handling Missing Values: The dataset was uniformly handled by imputed or removed missing values of corresponding features.
* Balancing Classes: The dataset was imbalanced, underrepresented by attack classes. A “golden dataset” was created using Synthetic Minority Oversampling Technique (SMOTE) to balance normal and attack traffic.
* Feature Selection: The removal of irrelevant or redundant features form the dataset reduced its dimensionality, thereby enhancing model efficiency.

*C. Model Architecture*

The Intrusion Detection System uses XGBoost, a scalable machine learning algorithm, for large dataset machine learning algorithm, for large datasets and high classification accuracy. It captures complex patterns and is suitable for imbalanced datasets like the NSL-KDD dataset.

The architecture optimizes key hyperparameters for performance, including a learning rate of 1.0, decision tree depth of 6, and subsample by 0.8. grid search and cross-validation techniques fine-tune these parameters, resulting in a robust classification model suitable for real-time security applications.

*D. Training Process*

The AI-based Intrusion Detection System (IDS) training process aims to optimize model performance, address class imbalance, and overfitting issues, with detailed steps provided.

1. Data Splitting
2. Feature Engineering and Normalisation
3. Class Balancing and Data Augmentation
4. Model Training and Evaluation
5. Cross-Validation and Hyperparameter Tuning

*E. Evaluation Metrics*

The performance of the model was evaluated using the following metrics:

* Validation Accuracy: The model achieved a 97.09% accuracy rate, demonstrating its robustness in effectively generalizing across normal and attack instances in unseen data.
* Precision: The model, with a precision score of 0.98, demonstrated a high ratio of true positive predictions while minimizing false positives.
* Recall: The model demonstrated a recall score of 0.97, indicating its ability to accurately identify most intrusion instances.
* F1-Score: The F1-score of 0.97 indicates a balanced evaluation that takes into account both precision and recall.
* Specificity: The individual achieved a score of 0.99, demonstrating exceptional proficiency in accurately identifying non-intrusive network traffic.

|  |  |
| --- | --- |
| **Metric** | **Value** |
| Accuracy | 97.09% |
| Precision | 0.98 |
| Recall (Sensitivity/Specificity) | 0.98 |
| F1-Score | 0.97 |
| ROC-AUC | 0.99 |

Table 2:  Performance Metrics of the Proposed IDS

**ARCHITECTURE**

The XGBoost mosel for AI-Based Intrusion Detection System (IDS) utilizes gradient noosting techniques to efficiently handle large-scale data, achieving superior classification performance.

*A. Data Input and Preprocessing*

The NSL-KDD dataset, consisting of 41 features and class lables, is used for training and testing, with preprocessing steps including encoding, normalizing, and removing duplicates.

*B. Boosted Tree Construction*

XGBoost is a Gradient Boosting Framework that optimizes decision trees by adjusting learning rate, depth, sample size, and number of boosting rounds.

*C. Model Training and Optimization*

The model is trained using grid search and cross-validation. Regularized using L2 and early stopping, and used to handle residual class imbalances.

*D. Real-Time Intrusion Detection*

The XGBoost mosel is used to categorize incoming network traffic into “normal” or various attack categories, thereby enabling proactive cybersecurity measures.

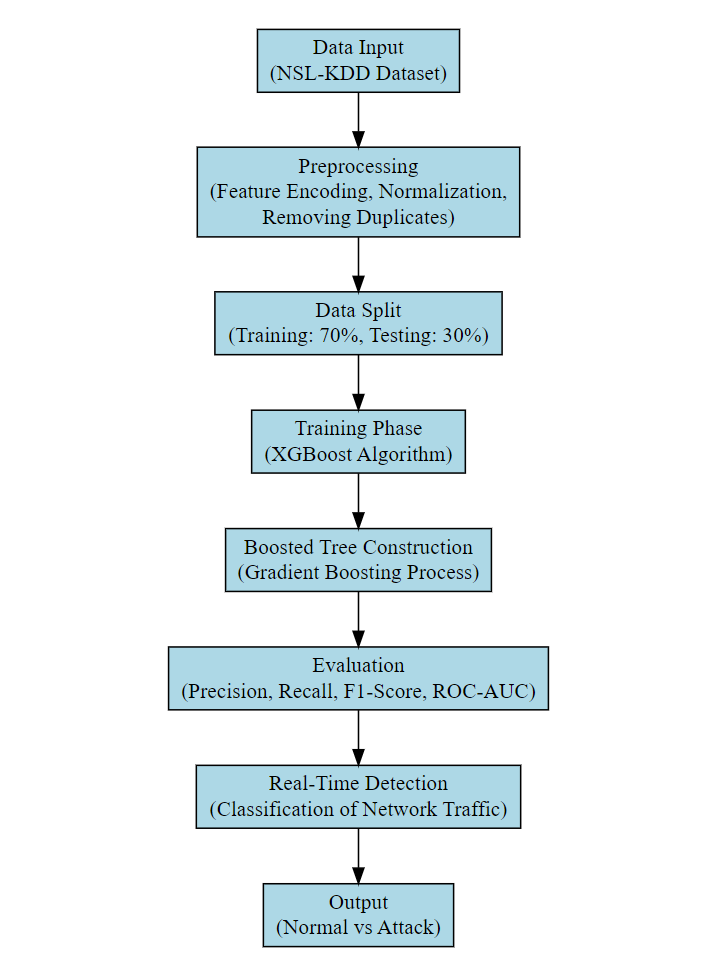
****

Fig 1:  Block Diagram of the XGBoost Architecture

**RESULT**

The proposed AI-Based Intrusion Detection System (IDS) using XGBoost for Real-Time Cybersecurity is implemented successfully using a Python program. The dataset consists of network data collected from various open-source platforms and repositories. The performance of our algorithm has been analysed with various metrics like Accuracy, precision, IOU (Intersection over union), Dice coefficient, and sensitivity specificity. These parameters are represented in the below equations

Accuracy = (TP+TN)/(TP+TN+FP+FN)

Precision = TP/(TP+FP)\*100

IOU = TP/(TP+FP+FN)

Dice coefficient = (2\*TP)/(2\*TP+FP+FN)

Sensitivity = TP/(TP+FN) Specificity = TN/(TN+FP) Were,

TP - Instances that are actually positive and are correctly classified as positive.

TN - Instances that are negative and are collectively classified as negative.

FP - Instances that are negative but are incorrectly classified as positive.

FN - Instances that are positive but are incorrectly classified as negative.

**CONCLUSION**

This study presents an AI-based Intrusion Detection System (IDS) with a 97.09% accuracy and 0.99 ROC-AUC score, demonstrating its efficacy in enhancing network security. The proposed IDS utilizes the XGBoost algorithm for efficient network traffic classification, enabling real-time monitoring and retrospective analysis capabilities. The systems performance metrics, including precision (0.98), F1-score (0.97), and recall/specificity (0.98), alongside key outcomes such as True Positive (TP:11,310), True Negative (TN:269), False Positives (FP: 269), and False Negatives (FN: 463). The systems robustness and reliability are emphasized, confirming its potential for deployment in both online and offline environments. The proposed system uses advanced AI techniques and a “golden dataset” to address cyber threats, offering efficient, adaptive, and scalable network protection solutions.

**REFERENCES**

[1] S. Axelsson, "Research in intrusion-detection systems: A survey," Technical Report, Chalmers University of Technology, 2000. [Online]. Available: https://doi.org/10.1109/ISEC.2000.871333

[2] D. E. Denning, "An intrusion-detection model," IEEE Transactions on Software Engineering, vol. 13, no. 2, pp. 222–232, 1987. [Online]. Available: https://doi.org/10.1109/TSE.1987.232894

[3] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," Annals of Telecommunications, vol. 55, no. 7, pp. 361–378, 2000. [Online]. Available: https://doi.org/10.1007/BF02994844

[4] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining (KDD), 2016, pp. 785–794. [Online]. Available: https://doi.org/10.1145/2939672.2939785

[5] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in Proc. IEEE Symp. Computational Intelligence for Security and Defense Applications (CISDA), 2009, pp. 1–6. [Online]. Available: https://doi.org/10.1109/CISDA.2009.5356528

[6] Y. Bengio, A. Courville, and P. Vincent, "Representation learning: A review and new perspectives," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 8, pp. 1798–1828, 2013. [Online].*Available: https://doi.org/10.1109/TPAMI.2013.50*

*[7] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016. [Online]. Available: https://doi.org/10.1038/nature14539*

*[8] J. Kwon and S. Kang, "Anomaly detection in network traffic using deep autoencoder," Electronics, vol. 9, no. 10, p. 1644, 2020. [Online]. Available: https://doi.org/10.3390/electronics9101644*

*[9] F. Callegati, W. Cerroni, and G. D’Angelo, "Efficient detection of anomalies in network traffic using machine learning," Computer Networks, vol. 174, p. 107279, 2020. [Online]. Available: https://doi.org/10.1016/j.comnet.2020.107279*

*[10] A. K. Jain, P. K. Malhotra, and R. Gupta, "Real-time network intrusion detection using XGBoost," IEEE Access, vol. 8, pp. 174623–174637, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3017257*