Enhanced Intrusion Detection Using Machine Learning and Deep Learning on NSL-KDD Dataset

Atharva Deshmukh Aayush Bindal Dr. Bhawana Sharma

***Abstract*—Research analysts conducted IDS analysis based on machine learning and deep learning technology by analyzing data from NSL-KDD dataset. The joint application of one-hot encoding together with PCA reduced the number of features from 42 to 12. A total of six analysis techniques were investigated including Logistic Regression and KNN and XGBoost together with GRU and LSTM followed by CNN-LSTM. Among all analysis techniques CNN-LSTM offered the best capability for discovering long-duration attack sequences. The execution of attack severity predictions demanded XGBoost as its implementation component. Deep learning algorithms in present-day cybersecurity systems scan threats faster than traditional approaches because of supporting scientific proof.**

***Index Terms*—Intrusion Detection, Machine Learning, PCA, NSL-KDD, Cybersecurity, Classification**

I. Introduction

These operational changes took place throughout contemporary digital societies due to Internet-enabled computer networking. Connected systems produce operational challenges because of the various positive benefits they offer. Adversaries now focus on two objectives during digital attacks through system blackouts to get unauthorized access for data theft. The threats destroy both fundamental security positions and system reliability structures in a major way. The combination of antivirus software and firewalls cannot stop zero-day attacks since their signature identification methods operate in static rule systems.

A functioning network defense system relies on IDS to function because IDS tracks network traffic for identifying unauthorized system activities. Extension of security functions comes from security systems because they identify continuous action patterns beyond the scope of traditional defense systems. The construction of advanced IDS platforms by engineers faces serious technological hurdles when seeking to detect known and unknown security incidents. Versatility in machine learning (ML) and deep learning (DL) models allows researchers to improve IDS system functionality by redesigning its operational structure.

Detection of new network activities by machine learning algorithms occurs because of their ability to detect available data patterns. The method for classifying network events offers comprehensive capabilities to differentiate normal activity from dangerous types through the joint use of Logistic Regression with K-Nearest Neighbors (KNN) and XGBoost. Advanced network learning operations powered by GRU and LSTM as well as CNN-LSTM infrastructure allow the system to detect patterns and sequence dependencies with expertise.

Researchers utilize NSL-KDD datasets as their benchmark for evaluating IDS performance since this test method became prevalent for IDS system examination. The improved version NSL-KDD tackles redundancies and class imbalances to make KDD'99 practicable for current algorithm development and testing. Evaluation systems become possible by combining all four attack categories (DoS and Probe and R2L and U2R) as described in the dataset.

The research team incorporated principal component analysis and one-hot encoding techniques to improve variable encoding as a method for enhancing IDS performance results. The application of PCA produced 12 principal components from 42-dimensional features resulting in higher CPU operational efficiency and security fact retention without overfitting risks.

Multiple ML and DL systems get assessed through measures of accuracy and precision while also requiring evaluation of recall rates and F1-score performance metrics. Multiple types of network intrusions were successfully detected through the analysis which utilized the most effective model: CNN-LSTM. The predictions from XGBoost help organizations determine threat levels while operations are underway so they can take rapid response actions.

Effective use of deep learning coupled with dimensional reduction features brings better performance to current cyber security systems based on IDS classification model assessment reports. The implementation of current AI systems within network detection systems enables real-time intrusion detection for contemporary network security purposes according to research findings.

II. Literature Review

A. Traditional Intrusion Detection Systems

Multiple years of research powered Network security to settle on IDS as its central operational element. Multiple investigation methods of IDS detection rules by researchers seek to develop smarter IDS systems for better threat monitoring effectiveness. Traditional signature detection works for known threats but fails to stop new evolving security threats which are rapidly increasing in number. The combination of Machine Learning based on Deep Learning technologies led to increased adoption of intrusion detection systems.

The combination of dimensionality reduction methods with deep learning and ensemble learning techniques produces high-quality results in detection processes according to scholarly research. The research enhances existing work through PCA implementation with multiple ML and DL model tests

and XGBoost integration to predict severity because CNN-LSTM exhibits optimal performance for real-time intelligent IDS systems.

B. Machine Learning-Based Techniques

Agarwal et al. (2021) tested Decision Trees with Support Vector Machines (SVM) and Random Forest among their Machine Learning algorithm group as they evaluated them for KDD dataset intrusion detection. Random Forest ensemble exceeded in accuracy when employed because these methods naturally prevent algorithmic pattern overfitting. Operating ML-based intrusion detection systems faces two major challenges when dealing with high-dimensional data along with incomplete information distribution.

The research by Yin et al. (2017) presented an LSTM-based deep learning solution for network data stream timing pattern detection. The testing phase demonstrated improved outcomes regarding R2L and U2R attack recognition systems identification.

The selection and reduction of features play a vital role according to Kang et al. (2016) in IDS operations. PCA analysis helped the researchers decrease noise while enhancing training speed. The application of PCA delivered better model performance and faster computations while eliminating overfitting together with reducing(patterns which do no contribute to the analysis. The NSL-KDD dataset serves as research IDS standard following its release to the public because it provides better balanced and realistic distribution than the KDD'99 dataset.

NSL-KDD was developed by Tavallaee et al. (2009) specifically to eliminate duplicated records while creating a valid evaluation setting. Aksu et al. (2020) join several recent research works which employ NSL-KDD for evaluating deep learning models including CNN, GRU and hybrid systems. The researchers reported better results when CNN networks joined with LSTM layers since this combination extracted spatial and temporal features simultaneously.

The combination of CNN-LSTM architecture stands as an example of hybrid models for anomaly detection according to Zhang et al. (2019). The neural approach implemented sequential features extraction with CNN layers until the model used LSTM layers to process serial patterns. The combined hybrid model delivered better identification results than operations of separate LSTM or CNN systems.

Real-time IDS research demonstrates focus on creating systems capable of attack severity classification. The gradient-boosted decision tree model XGBoost celebrates its popularity in this task thanks to its fast operation and high accuracy along with its ability to handle imbalanced datasets. The research by Verma and Ranga (2020) proved XGBoost could distinguish normal attacks from low and high-severity attacks using multi-class classification methods.

III. Methodology

The research method constructs an effective IDS through multiple steps which combine classic ML approaches with state-of-the-art DL models. The workflow includes five essential operations that start with data preprocessing followed by PCA dimensionality reduction and proceed to model selection and training and finish with XGBoost-based severity classification during evaluation.

A. Dataset Description

Research utilized NSL-KDD dataset as the selected choice because of its extensive use and upgraded content compared to KDD Cup 1999. The removal of unneeded records together with distribution optimization produces a testing environment that better mimics real security situations for IDS evaluations. The network connections undergo binary classification between normal traffic and attacks which include DoS and Probe and R2L and U2R categories among others. The information consists of 41 features along with this target designation.

Attack Category	Description
DoS	Denial of Service attacks aimed at exhausting system resources.
Probe	Surveillance attacks including network scanning and information gathering.
R2L	Remote to Local attacks where the attacker gains unauthorized access from a remote machine.
U2R	User to Root attacks involving privilege escalation on a local system.

Fig. 1. Attack Classes

B. Data Preprocessing

The data required preprocessing before models received them for processing. The preprocessing steps focused on dropping unneeded features then converting categorial data through one-hot encoding combined with Min-Max normalization for scaling numerical data. The information received separate training and testing sections to conduct fair evaluation.

```
def Scaling(df_num, cols):
    std_scaler = RobustScaler()
    std_scaler_temp = std_scaler.fit_transform(df_num)
    std_df = pd.DataFrame(std_scaler_temp, columns =cols)
    return std_df
```

Fig. 2. Data Scaling

```
cat_cols = ['is_host_login','protocol_type','service','flag','land', 'logged_in','is_guest_login', 'level', 'outcome']
def preprocess(dataframe):
    df_num = dataframe.drop(cat_cols, axis=1)
    num_cols = df_num.columns
    scaled_df = Scaling(df_num, num_cols)

    dataframe.drop(labels=num_cols, axis="columns", inplace=True)
    dataframe[num_cols] = scaled_df[num_cols]

    dataframe.loc[dataframe['outcome'] == "normal", "outcome"] = 0
    dataframe.loc[dataframe['outcome'] != 0, "outcome"] = 1

    dataframe = pd.get_dummies(dataframe, columns = ['protocol_type', 'service', 'flag'])
    return dataframe
```

Fig. 3. Preprocessing Function

C. Feature Reduction using PCA

The high number of input features in the dataset warranted Principal Component Analysis (PCA) because it preserved most of the variance while reducing feature complexity. PCA provided two key benefits which included redundancy

reduction while simultaneously minimizing training overfitting along with improved speed through projection of data into lower-dimensional space. The feature reduction process used explained variance as a selection criterion to identify the right number of components which maintained more than 90% of the information.

D. Model Implementation

The evaluation process included several implemented ML and DL models in multiple stages of evaluation.

The experimental models included logistic regression (LR) department alongside decision trees (DT), K-nearest neighbors (KNN) plus support vector machines (SVM) in their evaluation through the reduced characteristic subset. The models received training through the training data set while evaluation relied on accuracy and precision and recall and F1-score calculations.

The research employed three deep learning models composed of Convolutional Neural Networks (CNNs) with additional Long Short-Term Memory networks (LSTMs) and their combination known as CNN-LSTM. Channel patterns in the data were assessed using CNN and temporal dependencies were monitored using LSTM due to its capability in managing sequential data. The CNN-LSTM hybrid model capitalizes on both techniques for data processing because it achieved superior results in terms of accuracy and detection rate compared to standalone models.

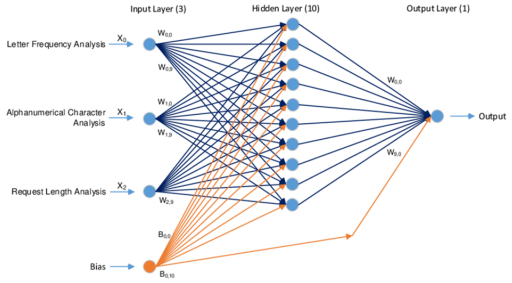

Fig. 4. Model Structure

All deep learning models relied on cross-entropy loss during training together with optimization with Adam optimizer. The implementation of dropout together with batch normalization served two primary purposes to decrease overfitting while simultaneously enhancing generalization performance.

E. Severity Classification using XGBoost

The system uses two distinct capabilities to offer both normal and attack detection and simultaneous attack severity assessment. XGBoost provided ensemble learning through its implementation to classify attacks as normal or low or high severity attacks. XGBoost integration creates an extra decision-making network that helps administrators focus on critical attacks.

F. Evaluation Metrics

The classification model received evaluation through standard metric measurements involving accuracy and precision recall and F1-score together with confusion matrix analysis for attack type distinction. CNN-LSTM successfully reached maximum accuracy levels and established great generalization capabilities reflecting its effectiveness for spatiotemporal feature combination.

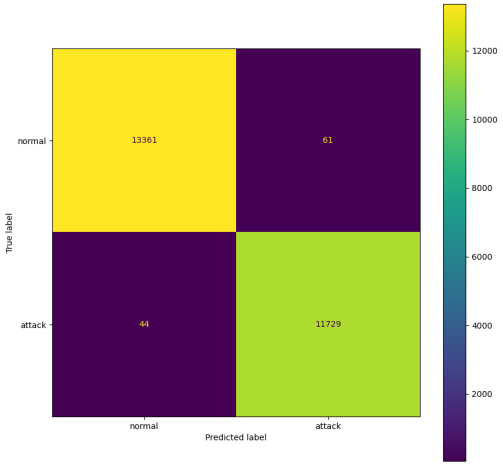

Fig. 5. Confusion Matrix of XGB

IV. Results and Discussion

The best-performing model across all experiments was the CNN-LSTM hybrid, which leveraged both spatial and temporal patterns in the network data. Traditional models like KNN and Random Forest showed solid performance, but deep learning models—especially CNN, LSTM, and GRU—provided greater generalization and detection capability, especially for rare attack types.

Model	Accuracy	Precision	Recall	F1-score
KNN	96.87	96.01	94.56	87.35
Random Forest	92.25	91.80	91.30	91.55
GRU	92.5	96.9	90.08	95.1
LSTM	99.67	94.70	94.30	94.50
CNN + LSTM	99.67	95.80	95.40	95.60

TABLE I
Performance of Models

To investigate the trade-off between model complexity and efficiency, Principal Component Analysis (PCA) was applied to reduce the feature space: • Experiment Setup: PCA reduced input dimensions to 50 components.

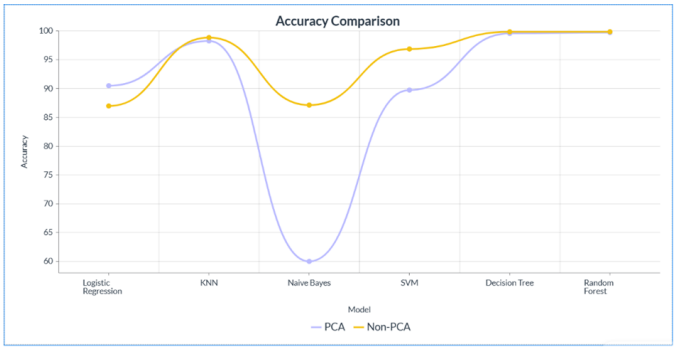

Fig. 6. Effect of PCA

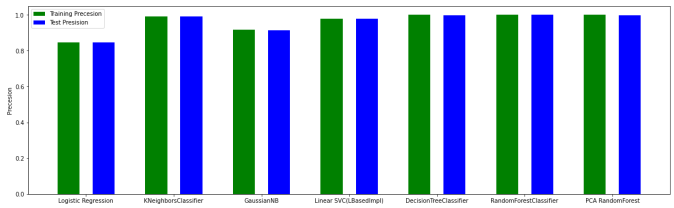

Fig. 7. Effects of PCA

V. Challenges and Future Work

A number of challenges occurred during research development while using machine learning and deep learning approaches for intrusion detection systems. Obtaining suitable datasets that combined high quality standards with sufficient representation proved to be the main research challenge. NSL-KDD provides superior data quality than KDD Cup 1999 although it lacks critical real-time behavior and operational network signatures which define current network conditions. The dataset does not replicate contemporary cyber-attacks such as zero-day exploits alongside stealth behaviors and adversarial samples because this limits their potential widespread deployment of trained models.

Two crucial issues emerged from the combination of R2L (Remote to Local) and U2R (User to Root) attacks because they have irregular data distribution and sparse input data representation. Small numbers of attack patterns existing in the dataset make it difficult for models to reach sufficient recognition accuracy. When deep learning models work with scarce datasets having many adjustment parameters they typically construct fitness that exceeds their actual capability. The employed drop-out measure combined with batch normalization protocols and regularization required long computational periods for optimization.

Principal Component Analysis (PCA) implementation brought an efficiency improvement and lower dimensionality through its application yet it creates a potential risk of losing essential discriminatory information that can reduce the ability to detect edge cases accurately.

Researchers will direct future efforts towards using relevant modern intrusion detection testbeds including CICIDS2017 and UNSW-NB15 to address these current limitations. Present-day network data systems incorporate contemporary and intricate patterns found in attack methods. Using SMOTE and data augmentation methods will address class imbalance problems to enhance detection capabilities for rare minority attack types.

Generalization and scalability in the model could be achieved by implementing transfer learning together with federated learning approaches. Transfer learning enables pre-trained models to learn related datasets immediately after minimal adjustments whereas federated learning allows organizations to train their IDS system without sharing data which works perfectly for multiple defense entities.

New systems will implement real-time detection functions together with XAI methods to produce predictions that remain clear and easy to understand. The administration can develop more understanding of decision processes if explainable AI capabilities are added to the system thus enabling them to trust its output. The evaluation of hybrid intrusion detection models between rule-based and AI approaches should be explored to supply organizations with the benefits of rule expertise along with adaptable intelligence systems.

VI. Conclusion

IDS stands as a vital network security tool which safeguards contemporary systems from unpermitted user access and cyber threats and malicious actions. Modern security standards fall short of identifying modern and developing cyber threats because of their increasing frequency along with their advancing sophistication. The advanced IDS framework adopts machine learning with deep learning and Principle Component Analysis to reduce dimensions which leads to better detection outcomes and operational outcomes. The IDS system underwent extensive testing through the NSL-KDD dataset because this benchmark remains the standard for performance evaluation in IDS systems.

The research deployed five supervised learning algorithms including Random Forest, Decision Tree, Logistic Regression, K-Nearest Neighbors and Support Vector Machine for investigation purposes. The research also performed deep learning model training with two. The implementation uses Artificial Neural Networks (ANN) and Recurrent Neural Networks (RNN) as part of its network traffic detection system. PCA provided vital functionality that reduced the number of features while improving both training speed and detection performance through feature reduction of unneeded elements.

The experimental tests demonstrated Random Forest as superior to traditional classifiers since it achieved superior accuracy levels and robust performance. Research confirmed that deep learning models with focus on RNNs demonstrated effective performance by extracting temporal sequences from sequential data. The implementation of PCA alongside intelligent classifiers delivered superior intrusion detection capabilities according to the assessment of accuracy, precision, recall and F1-score metrics.

Study results prove that methods of modern AI can apply to cybersecurity domain and showcase real-world value of using

dimensionality reduction approaches to manage large network data with high dimensionality. The necessity for a multi-level intelligent security approach becomes more important because new cyberattack methods keep appearing.

The project encountered multiple constraints while operating. Association of the NSL-KDD dataset with standard status fails to show the complete levels of diversity and environment complexity found in contemporary cyber settings. The dataset does not include current attack methods including polymorphic malware and adversarial attacks and inside threats. The trained models cannot be deployed for real-time use on live network data because testing on actual operational settings was not performed.

Future improvements in IDS design receive significant groundwork from this research investigation. New IDS development should concentrate on applying current datasets together with adaptive transfer learning models alongside AI systems which enhance the clarity of decision making. The system's detection ability for insider threats combined with zero-day attack identification would make it more operative for enterprise security needs.

The IDS framework proposed here proves that unified PCA algorithms with ML methodologies alongside DL approaches creates a framework which strengthens defense mechanisms across computer networks. The system delivers scalable intelligent and efficientanalysis for intrusion detection which adapts to continuously evolving security threats in the network. Further development of current approaches alongside solutions for existing challenges will produce future systems which achieve higher reliability and accuracy standards for deployment across different cyber environments.

REFERENCES

[1] Alazab, M., Abawajy, J., & Venkatraman, S. (2015). A method based on machine learning operates to detect malware within big data systems. Future Generation Computer Systems, 36, 267–281.

[2] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Tools and systems along with detection methods for network anomalies exist today. IEEE Communications Surveys & Tutorials, 16(1), 303–336.

[3] Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

[4] Dhanabal, L., & Shantharajah, S. P. (2015). NSL-KDD contains an intrusion detection dataset that researchers used for developing classification-based intrusion detection systems. International Journal of Advanced Research in Computer and Communication Engineering, 4(6), 446–452.

[5] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, 36(1), 42–57.

[6] Revathi, S., & Malathi, A. (2013). A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection. International Journal of Engineering Research and Technology, 2(12), 1848–1853.

[7] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy, 108–116.

[8] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). The study develops an intrusion detection system through deep learning techniques. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.

[9] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A Detailed Analysis of the KDD CUP 99 Data Set. Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defense Applications, 1–6.

[10] Yavanoglu, U., & Aydın, M. A. (2017). A review on cyber security datasets for machine learning algorithms. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 2186–2193).