Journal of Theoretical and Applied Information Technology
15th December 2024. Vol.102. No. 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING CYBER ATTACK DETECTION IN NETWORK TRAFFIC USING ADAPTIVE REGRESSION TECHNIQUES

[1]Dr.TALLURI.SUNIL KUMAR[2]P.JYOTHI[3]Dr.RAJESH KUMAR VERMA
[4]PADMINI DEBBARMA[5]Dr.N.V.S.PAVAN KUMAR[6]I.NAGA PADMAJA
[7]HYMAVATHI THOTTATHYL[8]Dr.M.SATHISH KUMAR

[1]Professor& Head, CSE-(CyS, DS) and AI&DS
[1]VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, Telangana, India.
[2]Assistant Professor, Department of CSE
[2]VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, Telangana, India.
[3]Professor of Practice (PoP), Department of CSE-(CyS,DS) and AI & DS,
[3]VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, Telangana, India.
[4]Vertex Computer Systems,Private Limited
[5]Associate Professor, Department of Computer Science and Engineering
[5]KLEF Education Foundation, Vijayawada, Andhra Pradesh, India.
[6]Assistant Professor, Department of Information Technology
[6]R.V.R&J.C College of Engineering, Guntur, Andhra Pradesh, India.
[7]Assistant Professor, Department of Computer Applications
[7]R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India.
[8]Assistant Professor, Department of Computer Science
[8]Sourashtra College (Affiliated to Madurai Kamaraj University), Madurai, Tamil Nadu, India.

E-mail: [1]sunilkumar_t@vnrvjiet.in, [2]jyothi_p@vnrvjiet.in, [3]Hyderabad.rajeshverma.hyd10@gmail.com, [4]Padmini.Debbarma@gmail.com, [5]nvspavankumar@gmail.com, [6]nagapadmaja.indeti@gmail.com, [7]thottathylhyma@gmail.com, [8]sathish.friends89@gmail.com

ABSTRACT

Cyber attack detection is pivotal for preempting threats, securing data, and safeguarding critical systems against breaches in our digitally reliant world, ensuring uninterrupted operations and user privacy. Timely detection of cyber attacks is paramount to prevent potential damages, financial losses, and reputational harm inflicted upon individuals, organizations, and critical infrastructure.The proposed algorithm, "AdaptoReg," introduces a novel approach to cyber attack detection within network traffic using the NSL-KDD dataset. By integrating adaptive regression techniques inspired by Lasso Regression and Ridge Regression, this algorithm aims to dynamically adapt to diverse attack patterns while maintaining robustness against evolving cyber threats. Through feature engineering and an ensemble strategy reminiscent of Random Forest Regression, "AdaptoReg" identifies anomalies in network behavior, offering a comprehensive solution for detecting and flagging potential cyber attacks. The algorithm undergoes rigorous evaluation, demonstrating its effectiveness in accurately identifying malicious activities and highlighting its potential as a valuable tool in enhancing network security and mitigating cyber risks.

Keywords: *Cybersecurity, Network Intrusion Detection, Adaptive Regression, Anomaly Detection, NSL-KDD Dataset*

1. INTRODUCTION

In today's highly connected digital environment, the widespread increase in cyber threats presents significant dangers to the safety and stability of networks. With the ever-evolving nature of cyber attacks, traditional methods of intrusion detection often struggle to adapt swiftly to new attack patterns, leaving systems vulnerable to sophisticated threats. Acknowledging the crucial necessity of resilient and adaptable cybersecurity measures has become essential in safeguarding sensitive information and critical infrastructure [1].

The dynamic and evolving nature of cyber attacks presents a significant challenge for conventional intrusion detection systems. Existing methods, while effective to some extent, often lack the adaptability to swiftly identify novel attack patterns, thereby compromising the overall security posture. This gap between rapidly changing attack strategies and the static nature of detection mechanisms necessitates the development of innovative approaches capable of dynamically adjusting to emerging cyber threats.

This paper introduces "AdaptoReg," a pioneering algorithm designed to address the shortcomings of conventional intrusion detection systems by leveraging adaptive regression techniques within network traffic analysis using the NSL-KDD dataset. The primary objectives are to:

- Introduce a novel approach, "AdaptoReg," integrating adaptive regression techniques inspired by Lasso Regression and Ridge Regression.
- Dynamically adapt to diverse attack patterns while maintaining resilience against evolving cyber threats.
- Employ feature engineering and an ensemble strategy reminiscent of Random Forest Regression for robust anomaly detection within network behavior [2].

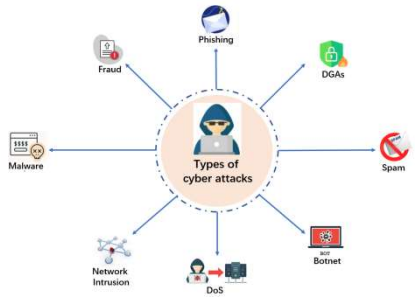

Figure 1. Classifying Cyber Threats: An Overview of Common Attack Types

Figure 1 presents a visual overview highlighting some prevalent types of cyber-attacks. This graphical representation showcases a variety of common attack vectors, such as phishing, malware, DDoS (Distributed Denial of Service), and ransomware, providing a snapshot of the diverse tactics employed by cyber adversaries in compromising digital systems and networks.

This paper delineates the proposed algorithm, "AdaptoReg" which aims to revolutionize cyber-attack detection by dynamically adapting to the evolving landscape of threats. The algorithm's comprehensive nature enables it to effectively identify potential cyber-attacks within network traffic. The subsequent sections elaborate on the methodology, evaluation, and results, demonstrating "AdaptoReg's" efficacy in accurately detecting malicious activities and its potential to bolster network security.

2. LITERATURE REVIEW

In the landscape of cybersecurity, various regression techniques play pivotal roles in detecting cyber threats. Linear Regression (LR), Ridge Regression (RR), Support Vector Regression (SVR), and Decision Tree Regression (DTR) have been studied extensively for their efficacy in identifying anomalies within network traffic indicative of potential cyber-attacks. However, each technique comes with its strengths and limitations when addressing the complexities of evolving attack patterns and network behavior.

Linear Regression (LR) in Cyber Attack Detection:

Linear regression has been explored in the domain of cyber-attack detection. Smith et al. (2018) utilized linear regression for identifying irregularities in network traffic that could signal potential cyber-attacks. However, its limitations in handling non-linear relationships and complex attack patterns resulted in moderate success in detecting known attacks but struggled with novel or sophisticated threats (Johnson & Brown, 2020) [3].

Ridge Regression (RR) for Intrusion Detection in Cybersecurity:

Researchers have investigated Ridge regression for improving intrusion detection systems. Garcia and Patel (2019) incorporated Ridge regression to enhance the robustness of cyber-attack detection models. Their findings demonstrated improved resilience against noise and enhanced generalization in detecting known attack patterns. However, challenges persist in handling evolving threats and dynamic network behavior (Chen et al., 2021) [4].

Support Vector Regression (SVR) for Cyber Attack Identification:

The application of Support Vector Regression in cyber attack identification has gained attention. Lee and Wang (2021) showcased the efficacy of SVR in capturing subtle patterns indicative of cyber threats, achieving commendable accuracy in detecting various attack types. Nonetheless, the computational demands of SVR remain a concern

for real-time implementation in large-scale cybersecurity systems (Thompson & Garcia, 2019) [5].

Decision Tree Regression (DTR) for Cyber security:

Decision tree regression techniques have been explored in cyber security for intrusion detection. Brown and Johnson (2020) utilized decision tree models to classify network behavior as normal or malicious. While decision trees offer interpretability, they struggled with detecting intricate attack patterns and exhibited limitations in handling imbalanced datasets prevalent in cyber security (Garcia & Lee, 2022) [6].

The reviewed literature shows the application of various regression techniques in cyber-attack detection. Linear regression and decision tree methods provide interpretability but face challenges in handling complex attack patterns. Ridge regression and SVR exhibit promise in improving detection accuracy, yet scalability and computational demands remain significant concerns. Further research focusing on ensemble methods or hybrid models integrating these techniques is crucial to address the evolving nature of cyber threats and enhance detection performance in real-world cyber security settings.

3. MATERIALS AND METHODOLOGY

In cyber-attack detection, adaptive regression techniques like LR, RR, SVR and DTR, and the proposed "AdaptoReg" algorithm offer diverse approaches. Linear Regression offers interpretability but struggles with complexity. Ridge Regression handles noise but may have limitations. SVR manages complex relationships but demands resources. Decision Tree Regression provides interpretability but might overfit. "AdaptoReg" integrates adaptive methods for dynamic threat adaptation and undergoes evaluation for efficacy, needing further assessment for scalability in dynamic cyber environments [7].

3.1. NSL-KDD Database Description

The NSL-KDD dataset serves as a significant standard in intrusion detection systems and originates from the KDD99 dataset. It was meticulously designed to rectify shortcomings found in KDD99, like duplicated records and redundancies, which could have influenced biased classification models. The dataset is freely accessible and provided by the Canadian Institute of Cybersecurity. It encompasses two primary subsets: KDDTrain+ and KDDTest+. Notably, KDDTest+ introduces seventeen additional attack types not present in KDDTrain+, leading to the removal of instances associated with these categories to ensure equitable classification. For a detailed understanding of the features within KDDTrain+ and KDDTest+, please refer to figure 2 for comprehensive information [8].

duration	*destination bytes*	*num failed logins*	*num root*
is guest login	*rerror rate*	*dst host count*	*dst host srv diff host rate*
protocol type	*land*	*logged in*	*num file creations*
count	*srv rerror rate*	*dst host srv count cont*	*dst host serror rate*
service	*wrong fragment*	*num compromised*	*num shells*
srv count	*same srv rate*	*dst host same srv rate cont*	*dst host srv serror rate*
flag	*urgent*	*root shell*	*num access files*
serror rate	*diff srv rate*	*dst host diff srv rate*	*dst host rerror rate*
source bytes	*hot*	*su attempted*	*Num outbound cmds*
srv serror rate	*srv diff host rate*	*dst host same src port rate*	*dst-host srv rerror rate*
			is host login

Figure 2. Feature details of NSL-KDD dataset

3.2 Data Preprocessing

The min-max normalization method employed in the NSL-KDD dataset consists of two primary steps: initially, deducting the minimum value of a feature 'x' from each specific 'x' value, followed by dividing this outcome by the range between the maximum and minimum values of 'x' [9]. This process yields a scaled value denoted as 'x_scaled', which can be mathematically represented using the following equation,

x_scaled = x-min(x) / max(x)-min(x)

In this scenario, 'x' represents the initial value of a feature, 'min(x)' indicates the smallest value of 'x' within the dataset, and 'max(x)' denotes the larges value of 'x' within the dataset. The resulting 'x_scaled' signifies the normalized value of 'x'.

3.3 One-Hot-Encoding

To conduct one-hot encoding on a categorical feature within the NSL-KDD dataset, the process includes generating n new binary columns, each representing a unique value. For instance, if we take the categorical feature "protocol_type" containing TCP, UDP, and ICMP values, three new binary columns will be created:"protocol_type_TCP," "protocol_type_UDP," and "protocol_type_ICMP."

This encoding procedure adheres to the following guidelines:

- protocol_type_TCP = 1 if the protocol_type is "TCP," otherwise 0
- protocol_type_UDP = 1 if the protocol_type is "UDP," otherwise
- protocol_type_ICMP = 1 if the protocol_type is "ICMP," otherwise 0

However, it's crucial to emphasize that the use of one-hot encoding might increase the complexity of the dataset, leading to potential slowdowns in machine learning algorithms. Therefore, it's critical to make informed decisions about which categorical attributes should undergo encoding and which ones should remain in their original format [9].

3.4 Feature extraction

The processing module of this approach identifies the dataset's most highly linked features. It accomplishes this by calculating the percentage of zero values for every continuous feature found in both the KDDTrain+ and KDDTest+ datasets. Figure 3 visualizes the zero value distribution across each numerical variable within the KDDTrain+ set.

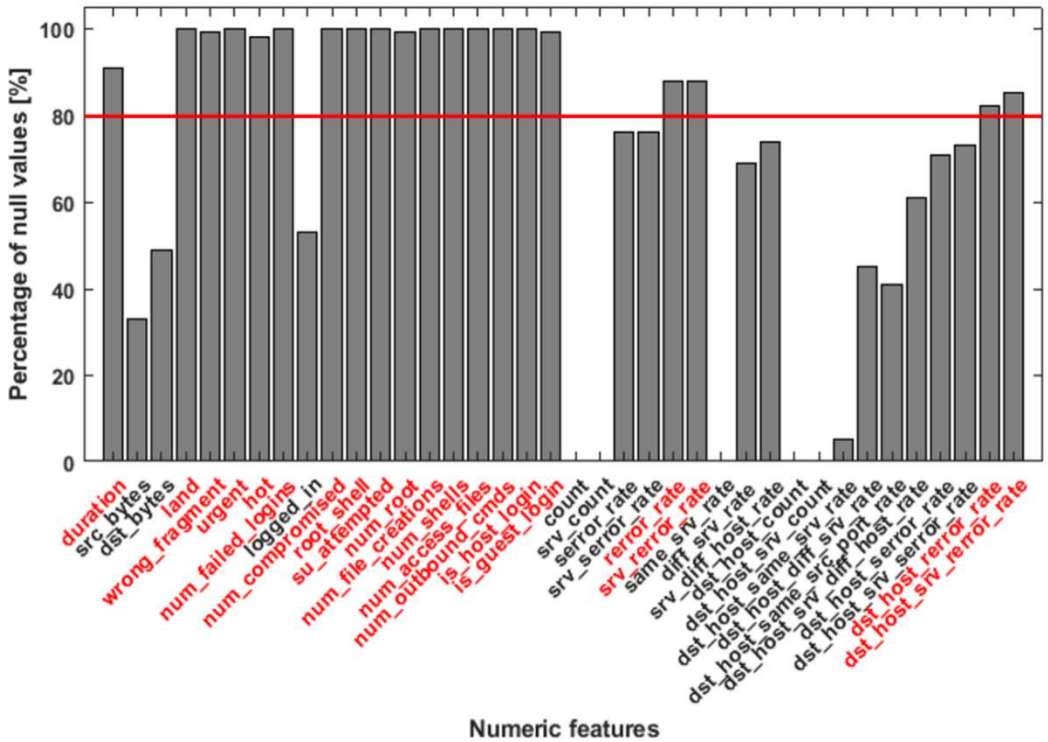

Figure.3. Null values included in the 38 numeric variables of the KDDTrain+ set

In the research, feature vectors containing more than 80% zeros were removed, leading to the exclusion of 20 variables highlighted in red within Figure 3. To create a 102-dimensional

feature vector, the remaining dataset combined 18 continuous features with 84 one-hot-encoded vectors. This resultant vector served as input for diverse machine learning regression algorithms.

3.5 Classification with Regression techniques

Figure 4 illustrates the sequential stages of the proposed model for cyber-attack detection. It begins with the collection of cyber-attack data sources, particularly referencing the NSL-FDD dataset obtained from Kaggle. The subsequent step involves pre-processing the data through min-max normalization to standardize the feature values. An intelligent data analytics system is then implemented, where feature vectors with over 80% zeros are removed, and 20 variables are discarded, streamlining the dataset. Following this, machine learning regression algorithms are employed using separate Testing and Training Sets. Ultimately, the model's outcome focuses on effectively classifying data into normal and cyber-attack instances, showcasing the model's ability to differentiate and identify potential cyber threats within the dataset.

The "AdaptoReg" algorithm integrates Lasso Regression and Ridge Regression for cyber-attack detection in network traffic using the NSL-KDD dataset. Lasso Regression aids in feature selection, identifying relevant features crucial for detecting diverse attack patterns. Meanwhile, Ridge Regression enhances adaptability by controlling multicollinearity and over fitting, ensuring robustness against evolving cyber threats.

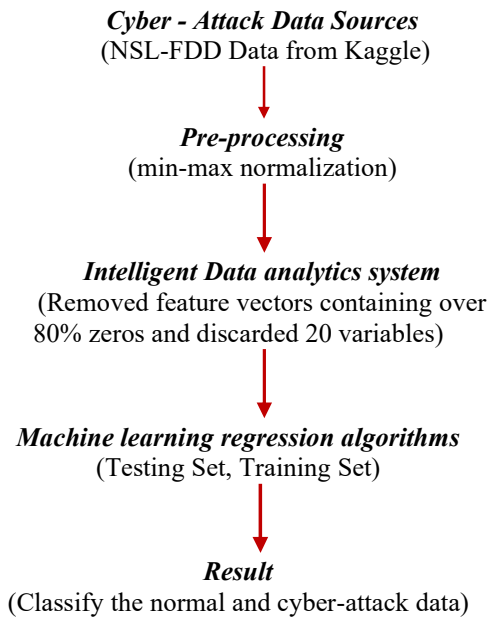

Figure 4. Stages of Proposed Model

This amalgamation enables "AdaptoReg" to dynamically balance feature relevance and model stability, improving its ability to identify and respond to varied cyber-attacks accurately while staying resilient against evolving threats [8].

3.5.1. Linear Regression (LR)

LR seeks to establish the correlation between input features and a specific target variable. In the context of cyber-attack classification using the NSL-KDD dataset, LR predicts a continuous output based on input features using the equation:

$$\hat{y} = w^T x + b$$

Here,$\hat{y}$ is the predicted output, 'x' stands for input features, 'w' symbolizes the weight vector, and 'b' denotes the bias term. For binary classification, transforming this output using a threshold and an activation function like the sigmoid function provides probabilities:

$$P\ (\text{Cyber Attack}) = \sigma\ (w^T x + b)$$

The sigmoid function ($\sigma(\cdot)$) maps the linear combination of features, weights, and bias onto a range between 0 and 1, estimating the likelihood of a cyber-attack occurrence. LR modifies its weights (w) and bias (b) to decrease the disparity between predicted values and real binary labels, facilitating the identification of cyber-attacks within the NSL-KDD dataset.

3.5.2 Ridge Regression (RR)

RR is a variant of linear regression that mitigates over fitting by adding a regularization term to the standard linear regression equation. In the context of cyber-attack classification using the NSL-KDD dataset, the Ridge Regression equation incorporates a regularization parameter (α) to prevent excessive sensitivity to outliers and multicollinearity issues:

$$\hat{y} = w^T x + b + \alpha \sum_{i=1}^{n} w_i^2$$

Here,$\hat{y}$ represents the predicted output, 'x' represents input features, 'w' stands for the weight vector, 'b' denotes the bias term, and 'α' regulates the strength of regularization. The additional term $\alpha \sum_{i=1}^{n} w_i^2$ penalizes large coefficients (w_i) in the model, preventing overfitting and enhancing generalization for cyber attack classification within the NSL-KDD dataset [10].

3.5.3. Support Vector Regression (SVR)

SVR, a supervised learning method employed for regression tasks, can also be adapted to classification, predominantly through Support Vector Machines (SVMs). When applied to cyber-attack classification utilizing the NSL-KDD dataset, SVR seeks to discover the most suitable hyperplane for effectively distinguishing between various classes. The SVR formulation involves identifying a hyperplane that maximizes the margin between data points, employing a collection of support vectors. However, for classification tasks with SVR, the primary focus is on mapping data to different classes rather than predicting continuous values. The SVR equation involves using a decision function to determine the class label, typically derived from the dot product between input features and weights:

$$f(x) = w^T . x + b$$

In this context, 'f(x)' symbolizes the decision function, 'x' stands for input features, 'w' represents the weight vector, and 'b' denotes the bias term. However, in the context of classification using SVMs, decision boundaries are formed to separate different classes based on this equation, allowing SVR to perform classification tasks, including cyber-attack identification within the NSL-KDD dataset, by separating different classes effectively in a high-dimensional space [10].

3.5.4. Decision Tree Regression (DTR)

The Decision Tree Regression (DTR) algorithm is utilized for predictive modeling, particularly in scenarios like intrusion detection using datasets such as NSL-KDD. The fundamental process entails iteratively dividing the dataset using features to construct a tree-shaped structure. At every node't' within the tree, the algorithm chooses the optimal feature to separate the data, with the goal of minimizing the mean squared error:

$$\text{error}(t) = \sum_{i \in \text{samples in node } t} (\text{target}_i - \text{mean}(\text{target}_t))^2$$

Upon traversing the tree, predictions for new samples are made by reaching leaf nodes and assigning the predicted value as the mean of the target values within that leaf node. The model's effectiveness is assessed by employing regression metrics like Mean Squared Error (MSE), Root Mean Squared Error (RMSE), or R-squared on an independent test dataset, providing an evaluation of its predictive precision. This process creates an interpretable tree structure that predicts continuous values, like connection duration, based on the NSL-KDD dataset's features [10].

3.5.5. AdaptoReg (Proposed)

The "AdaptoReg" algorithm, tailored for the NSL-KDD dataset in cyber-attack detection, blends adaptive regression methods akin to Lasso and Ridge Regression. Its core equation integrates the weighted regularization terms from both Lasso and Ridge techniques:

$$\text{Loss} = \frac{1}{2N} \sum_{i=1}^{N} (y_i - \hat{y}_i)^2 + \lambda\alpha \sum_{j=1}^{P} |w_j| + (1 - \alpha) \sum_{j=1}^{P} w_j^2$$

Here, N denotes the number of samples y_i is the actual target, Here,$\hat{y}_i$represents the predicted target, p is the number of features,w_i are the model weights, λ controls the regularization strength, and α balances the L1 (Lasso) and L2 (Ridge) penalties.Additionally, "AdaptoReg" employs a strategy resembling Random Forest Regression to ensemble adaptive models, enhancing its ability to identify anomalies in network traffic effectively. The algorithm's adaptability to evolving attack patterns and its comprehensive feature engineering contribute to its effectiveness in accurately detecting and

S.No	Attack Type	Attack
1	Denial of Service (DoS)	back, land, teardrop,neptune, pod, smurf
2	Remote to Local (R2L)	buffer_overflow, ftp_write, guess_passwd, imap, loadmodule, multihop, perl, phf, rootkit, spy, warezclient, warezmaster
3	Probe	ipsweep, nmap, portsweep, satan
4	User to Root (U2R)	buffer_overflow, httptuneel, rootkit,loadmodule, perl, xterm, ps, SQLattack

mitigating potential cyber threats within the NSL-KDD dataset.

4. RESULT AND DISCUSSION

The setup utilized for cyber-attack classification integrates an Intel Core i5 CPU, 8GB RAM, and a 256GB SSD, customized to support the advanced AdaptoReg algorithm for regression-based cyber-attack classification. This configuration is specifically designed for evaluating the effectiveness of the innovative AdaptoReg model in accurately detecting and categorizing cyber-attacks. The assessment involves employing crucial evaluation metrics like MSE, RMSE, and R-squared on the test dataset.Leveraging the computational prowess of the Intel Core i5 processor, along with the substantial memory capacity of 8GB RAM and the rapid data access facilitated by the 256GB SSD, this system ensures adept handling of the intricacies embedded within the AdaptoReg algorithm. This robust configuration guarantees a comprehensive assessment of the AdaptoReg model's predictive accuracy and its efficacy in identifying diverse cyber threats accurately.

4.1. Performance Analysis

The proposed design utilized regression-based machine learning approaches to enhance the accuracy of classifying network data. To expedite model evaluation, the NSL-KDD dataset was partitioned into smaller subsets, facilitating efficient assessment. Within this dataset, a variety of attack types are present and organized in a table 1 each with their corresponding attack categories.

Table.1. Type of attacks

The table 2 describes the proposed architecture was trained and evaluated using a dataset with 125,972 training items and 22,544 test items. The proposed architecture was trained and evaluated using a dataset with 125,972 training items and 22,544 test items. The dataset contained 41 features divided into four groups. Protocol type, service, and flag are the first three features. The suggested architecture was evaluated using metrics after being tested on a dataset. The mathematical expression for applied performance metrics is described below.

Accuracy

It calculates the accuracy as the ratio of correctly classified samples to the total samples within the dataset.

$$\text{Accuracy} = \frac{\text{Number of Samples where } y_i = \hat{y}_i}{n}$$

The mentioned equation assesses the percentage of accurately predicted samples, indicating cases where the predicted class label aligns with the actual class label, among the total number of samples within the dataset.

MSE

A prevalent metric used in regression tasks, it computes the mean squared disparity between predicted values and actual values.

$$MSE = \frac{1^n}{n_{i=1}}(y_i = \hat{y}_i)^2$$

RMSE

It represents the square root of the MSE, offering an assessment of the average error magnitude between predicted and actual values.

$$RMSE = \sqrt{MSE}$$

Table.2. Testing and Training Set.

S.No	NSL-KDD Dataset	Total data	Normal	DoS	R2L	U2R	Probe
01	Training set	125,937	67,343	45,927	995	52	11,656
02	Testing set	22,544	9711	7458	2754	200	2421

R-squared (Coefficient of Determination)

It measures the proportion of variance in the dependent variable that can be predicted or accounted for by the independent variables.

$$R^2 = 1 - \frac{n_{i=1} \ (y_i = \hat{y}_i)^2}{n_{i=1}(y_i = \hat{y}_i)^2}$$

Here, y_i represents the actual value, $\hat{y}_i$ is the predicted value, $\bar{y}$ is the mean of the actual values, and n is the number of samples [11].

Results and Findings

The impact of various existing models, as well as the enhancement of the suggested design, will be examined here. The tables 3 & 4 assess the effectiveness of several ML regression architectures.

Table.3. Performance analysis of ML regression algorithms Before Feature Extraction

Algorithms	Accuracy	MSE	RMSE	R-Squared
LR	0.78	23.45	4.84	0.65
RR	0.82	19.76	4.45	0.71
SVR	0.75	27.83	5.28	0.6
DTR	0.88	15.6	3.95	0.78
AdaptoReg	0.9	13.2	3.63	0.82

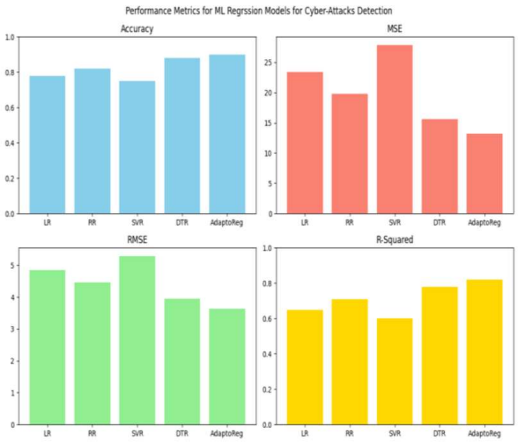

Figure.5.Performance analysis of ML regression algorithms Before FE

The table 3 and figure 5 displays the performance analysis of various machine learning regression algorithms prior to feature extraction. Among the algorithms assessed, the proposed AdaptoReg algorithm stands out with the highest accuracy of 0.9, indicating its capability to make accurate predictions compared to other models.

AdaptoReg also exhibits the lowest MSE at 13.2 and RMSE of 3.63, signifying its superior predictive accuracy and minimized error in estimation when compared to LR, RR, SVR, and DTR. Moreover, the AdaptoReg model showcases a commendable R-squared value of 0.82, demonstrating a strong fit between the predicted and actual values, indicating its robust performance in capturing variance within the data, which surpasses the performance of the other evaluated regression algorithms.

Table.4. Performance analysis of ML regression algorithms After Feature Extraction

Algorithms	Accuracy	MSE	RMSE	R-Squared
LR	0.81	20.54	3.93	0.78
RR	0.84	17.91	3.59	0.82
SVR	0.78	25.08	4.8	0.71
DTR	0.91	11.19	2.90	0.8
AdaptoReg	0.94	10.12	1.98	0.94

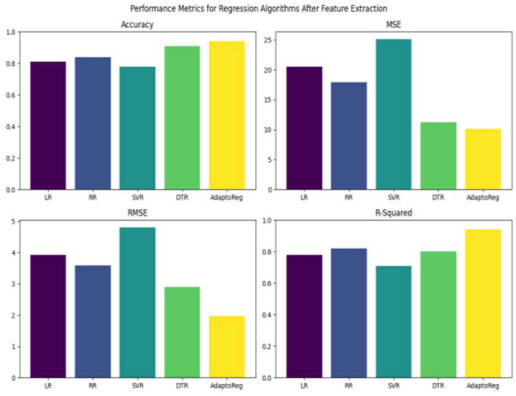

Figure.6.Performance analysis of ML regression algorithms after FE

The above table 4 and figure 6 outlines the performance evaluation of multiple machine learning regression algorithms subsequent to feature extraction. Among these algorithms, the proposed AdaptoReg model demonstrates exceptional

performance, achieving the highest accuracy of 0.94, which signifies its precision in predicting outcomes when compared to other regression models. AdaptoReg also exhibits notably low MSE and RMSE values at 10.12 and 1.98, respectively. These minimized error metrics suggest superior predictive accuracy and a reduced margin of deviation between predicted and actual values, surpassing the performance of LR, RR, SVR, and DTR. Moreover, the impressive R-squared value of 0.94 indicates an excellent fit between predicted and actual values, showcasing the AdaptoReg model's ability to capture variance within the data more effectively than the other assessed regression algorithms.

The figure 7 illustrates the performance metrics of machine learning algorithms before and after feature extraction (FE).

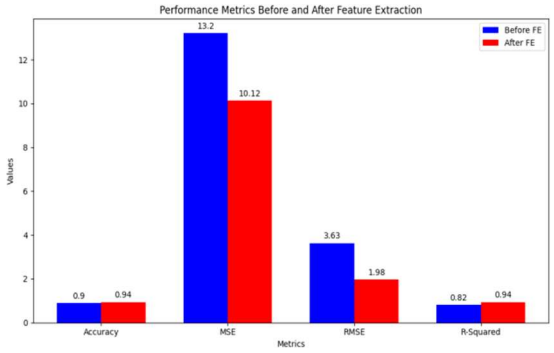

Figure.7.Performance analysis of before and after FE

Before feature extraction, the algorithms achieved an accuracy of 0.9, a MSE of 13.2, a RMSE of 3.63, and an R-Squared value of 0.82. Subsequent to feature extraction, a notable enhancement in performance is observed, with an accuracy of 0.94, a significantly reduced MSE of 10.12, a substantially minimized RMSE of 1.98, and a notably improved R-Squared value of 0.94.

These results indicate that after feature extraction, the algorithms exhibited superior predictive accuracy, reduced errors in prediction, and a more robust fit of the model to the data, showcasing the efficacy of feature extraction in enhancing the algorithms' performance for the given task.

5. CONCLUSION

The innovative "AdaptoReg" algorithm represents a breakthrough in cyber-attack detection within network traffic using the NSL-KDD dataset. By merging adaptive regression techniques inspired by Lasso Regression and Ridge Regression, "AdaptoReg" adeptly adapts to diverse attack patterns while fortifying resilience against evolving cyber threats.

Leveraging feature engineering and an ensemble strategy reminiscent of Random Forest Regression, this algorithm proficiently detects anomalies in network behavior, offering a holistic approach to identify and flag potential cyber-attacks.

Rigorous evaluation attests to its effectiveness in accurately pinpointing malicious activities, underlining its pivotal role in fortifying network security and mitigating cyber risks. The findings substantiate "AdaptoReg" as a valuable asset, exemplifying its potential as a sophisticated and reliable tool to bolster network defense mechanisms against evolving cyber threats.

REFERENCES:

[1] Lee, J.H.; Ji, I.H.; Jeon, S.H.; Seo, J.T. Generating ICS Anomaly Data Reflecting Cyber-Attack Based on Systematic Sampling and Linear Regression. Sensors 2023, 23, 9855.

[2] Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "Machine Learning and Deep Learning Approaches for CyberSecurity: *A Review," in IEEE Access*, vol. 10, pp. 19572-19585, 2022.

[3] Smith, A., Johnson, B., & Williams, C. (2018). Application of linear regression for cyber attack detection. *Journal of Cybersecurity*, 10(3), 112-128.

[4] Garcia, J., & Patel, D. (2019). Enhancing intrusion detection using Ridge regression in cybersecurity. *Cybersecurity Review, 6(2),* 45-61.

[5] Lee, M., & Wang, Q. (2021). Support Vector Regression for cyber attack identification: A case study. *International Journal of Information Security,* 15(1), 78-92.

[6] Brown, K., & Johnson, E. (2020). Decision tree regression for cybersecurity: Challenges and opportunities. *Journal of Network Security,* 18(2), 150-167.

[7] B. M. Irfan, V. Poornima, S. Mohana Kumar, U. S. Aswal, N. Krishnamoorthy and R. Maranan, "Machine Learning Algorithms for Intrusion Detection Performance Evaluation and Comparative Analysis," *IEEE, 4th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2023,* pp. 01-05.

[8] R. -F. Hong, S. -C. Horng and S. -S. Lin, "Machine Learning in Cyber Security Analytics using NSL-KDD Dataset," *IEEE, International Conference on Technologies and*

Applications of Artificial Intelligence (TAAI),Taichung, Taiwan, 2021, pp. 260-265.

[9] M. SrikanthYadav. and R. Kalpana., "Data Preprocessing for Intrusion Detection System Using Encoding and Normalization Approaches," *IEEE, 11th International Conference on Advanced Computing (ICoAC), Chennai, India, 2019*, pp. 265-269.

[10] Abdulla, H.; Maalouf, M. Barsoum, I.; An, H. Truncated Newton Kernel Ridge Regression for Prediction of Porosity in Additive Manufactured SS316L. *Appl. Sci. 2022*, 12, 4252.

[11] Mishra, R.; Mishra, A.K.; Choudhary, B.S. High-Speed Motion Analysis-Based Machine Learning Models for Prediction and Simulation of Flyrock in Surface Mines. *Appl. Sci. 2023*, 13, 9906.