Rule-Based Intrusion Detection System Using Logical Analysis Of Data

[1]Dr.B Rajesh Kumar, [2] Potlapati Haripriya

[1]Associate Professor, Mtech(Ph.D.),Department Of Computer Science And Engineering, PVKK Institute Of Technology, Anantapur, Andhra Pradesh, India.

[2]M.Tech Student, Department Of Computer Science And Engineering, PVKK Institute Of Technology, Anantapur, Andhra Pradesh, India.

ABSTRACT

The Increasing Prevalence And Complexity Of Cyber-Attacks Provide A Significant Danger To Organizational Network Infrastructures. This Study Responds To The Crucial Necessity For Efficient Intrusion Detection Systems (IDS) By Way Of Assessing Multiple Machine Learning Strategies Utilizing The NSL-KDD Dataset, A Well-Established Benchmark In Network Security. Making Use Of Support Vector Machine (SVM), Naive Bayes, Selection Tree, Random Forest, And Logical Analysis Of Data (LAD), Our Have A Look At Highlights LAD's Effectiveness In Intrusion Detection, With An Accuracy Of 83%. Increasing In This Basis, We Check Out Ensemble Tactics, Particularly The Voting Classifier That Integrates Random Forest And Adobos, Attaining An Exceptional Accuracy Of 100%. This Research Affirms The Importance Of Intrusion Detection Structures In Shielding Networks And Underscores The Potential Of Ensemble Techniques To Enhance Security Measures. Our Findings Highlight The Essential Characteristic Of Machine Learning In Strengthening Community Defenses, Imparting A Way For Stepped Forward Cyber Resilience And Proactive Threat Mitigation Techniques Within Organizations.

"Index Terms: Network Security, Machine Learning, Intrusion Detection System, Logical Analysis Of Data (LAD")

1. INTRODUCTION

In A Period Characterized By Using Rapid Expansion Of Internet Usage, Safeguarding Network Environments Has Gotten Step By Step Tough. Because Of The Increase In Security Threats, Especially Network Attacks, Organizations Are Facing An Urgent Necessity To Strengthen Their Cyber Defenses. This Urgency Is Emphasized Through The Emergence Of Transformational Technologies Like Cloud Structures, Which Have Broadened The Attack Surface And Revealed Networks To Numerous Unexpected Dangers. Therefore, Shielding Network Infrastructure Has Become A Critical Issue In Cybersecurity.

The Consequences Of Insufficient Network Safety Are Significant, Especially In Industries Where Key Structures, Such "Industrial Control Systems (Icss)", Are Vulnerable. "Industrial Control Systems (Icss)", Which Include Control Systems And Bodily Tactics, Are Often Linked Across Several Geographical Areas Thru Public Communication Networks. The Susceptibility Of These Systems To Cyber-Attacks Presents Not Simplest Financial Consequences But Also Endangers Human Lives, Especially In Protection-Critical "Cyber-Physical Systems (CPS)".

The Necessity To Establish Resilient Security Measures That Lessen The Probability Of Penetration Is Obvious. Although Reaching 100% Accuracy In Practical Situations Can Be Unattainable, The Emphasis Is On Growing

Systems That Possess Good Enough Precision To Pick Out Intrusions In Real-Time. The Upkeep Of Precious Statistics Throughout Intrusion Detection Is Fundamental To This Effort. Notwithstanding The Lifestyles Of Firewalls And Encryption Protocols, Adversaries Can Bypass These Safeguards, Highlighting The Need For Proactive Anomaly Detection Within The System.

In Mild Of These Troubles, "Intrusion Detection Systems (IDS)" Have Grown To Be Essential Devices For Monitoring Network Visitors And Detecting Capacity Threats. IDS Operates As A Vigilant Sentinel, Analyzing Incoming And Outgoing Packets For Any Nefarious Hobby That May Jeopardize Network Protection. 'Intrusion Detection Structures (IDS)" Are Widely Labeled Into Misuse "Intrusion Detection Systems (MIDS) And Anomaly Intrusion Detection Systems (AIDS)', Each Utilizing Special Approaches For Intrusion Detection.

MIDS Utilizes Installed Signatures Of Recognized Attacks To Discover And Hit Upon Anomalies In User Hobby, Whereas AIDS Identifies All Variations From Typical Conduct As Possible Risks. Acknowledging The Significance Of Comprehending Community Interest, We've Created A Behavioral-Based "Intrusion Detection System (IDS)" Utilising The "Logical Evaluation Of Statistics (LAD)" Approach. This Method Lets In Us To Identify Traits In The Community Surroundings, Helping In The Detection Of Suspicious Behaviors Suggestive Of Cyber-Attacks.

Area Information Is Essential For Defining Behavioral Styles Inside A Gadget. LAD, A Statistics-Centric Technique Added With The Aid Of Hammer Et Al., Gives A Comprehensive Framework For Sample Identification In Binary Datasets. With The Aid Of Using Ancient Records And Categorizing It Into Two Subsets "(D+ And D−), LAD" Enables The Recognition Of Patterns That Classify Observations Into Distinct Categories. This System Allows The Knowledge Of Device Conduct And Permits IDS To Perceive Intrusions In Real-Time.

2. LITERATURE SURVEY

The Literature On "Intrusion Detection Systems (IDS)" Includes Several Strategies And Processes Designed To Enhance Community Security Against Increasing Cyber Threats. This Literature Assessment Gives An Intensive Precis Of Contemporary Research Efforts, Emphasizing Significant Contributions, Technique, And Discoveries In The Topic.

Abrar Et Al. [5] Endorse A Machine Learning Methodology For Intrusion Detection Structures Using “NSL-KDD” Data File. Their Study Emphasizes The Possibilities Of Several Machine Learning Methods In Detection Of Disruption, Which Increases Community Security. LV Et Al. [6] They Represent Progressive Disruption Detection, So It Demonstrates The Flexibility Of Machine Learning Architectures In Disruption Detection.

Selection Trees Have Become A Significant Tool In Intrusion Detection Machine Studies. Kruegel And Toth [7] Look Into The Efficacy Of Decision Trees In Enhancing Signature-Based Intrusion Detection Structures. Their Research Highlights The Utility Of Selection Timber In Enhancing Accuracy And Efficiency Of Disturbance Detection Systems. Alazzam Et Al. [8] They Represent An Algorithm Of Selection Of Elements For Detection Detection Systems With Optimization Inspired By A Pigeon, And Therefore Offers Understanding Progressive Approaches To Improving Disturbance Detection Systems.

Patgiri Et Al. [16] Look At Intrusion Detection Systems Utilizing Machine Learning Methods, Presenting Widespread Insights Into The Efficacy And Usefulness Of Those Algorithms In Intrusion Detection. Their Research Advances The Expanding Field Focused On Utilizing Machine Learning To Improve Network Security.

Benchmark Datasets Are Essential For Assessing The Efficacy Of IDS Algorithms. Almseidin Et Al. [18] Create A Benchmark Collection Of Multi-Step Cyber Assaults For Intrusion Detection, Enabling Systematic Assessment And Comparison Of IDS Approaches. Their Dataset Constitutes A Significant Asset For Scholars And Practitioners In Cybersecurity.

Shakya [19] Presents An Improved Gray Wolf Feature Selection Approach Included With Machine Learning Type For Intrusion Detection In Wi-Fi Sensor Networks. Their Research Emphasizes The Want Of Function Selection In Raising Intrusion Detection System Efficiency And Precision In Environments With Limited Sources.

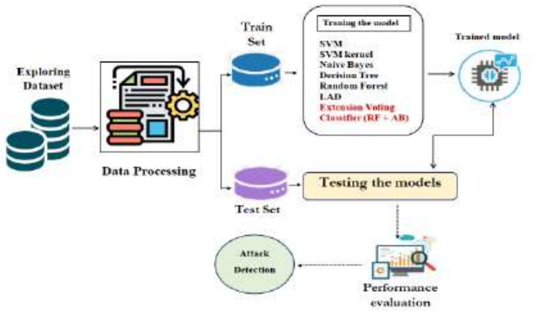
Together, These Studies Show The Complex Nature Of The Detection Research - Including Machine Learning Techniques, Approaches To Selecting Functions And Creation Of Benchmark Datasets. Researchers Seek To Enhance Intrusion Detection Via Numerous Techniques, Thereby Strengthening Network Security In A Progressively Interconnected And Susceptible Digital Environment.

3. METHODOLOGY

A) Proposed Work:

The Proposed Project Involves The Application Of "Logical Analysis Of Data (LAD)" As A Fundamental Method For Intrusion Detection In Network Systems. This Method Can Be Compared With Special Device Mastering Techniques, Which Include "Support Vector Machine (SVM), Naive Bayes, Decision Tree, And Random Forest, The Use Of The NSL-KDD" Dataset To Evaluate Its Overall Performance Thoroughly. The Recommended Gadget Utilizes LAD, A Data-Driven Technique For Spotting Patterns In Binary Datasets, To Discover Behavioral Styles That Signify Cyber Dangers. The Efficacy Of LAD In Identifying Intrusions May Be Assessed Thru Rigorous Experimentation And Comparative Evaluation In Opposition To Hooked Up Machine Learning Techniques. This Studies Aims To Decorate Intrusion Detection Systems By Way Of Clarifying The Potential Of LAD In Strengthening Network Security. This Work Goals To Clarify The Deserves And Weaknesses Of LAD Relative To Standard Machine Learning Methods To Beautify The Advent Of Extra Resilient And Green Intrusion Detection Systems Which Can Address Emerging Cyber Threats.

B) System Architecture:



“Fig1 Proposed Architecture”

The System Architecture Consists Of Multiple Interconnected Components Designed For The Development And Assessment Of A Powerful "Intrusion Detection System (IDS)". The Dataset Is To Start With Explored To Recognise The Traits And Complexities Of The NSL-KDD Dataset, A Trendy Benchmark In Network Security. Subsequently, Data Processing Procedures Are Utilized To Preprocess The Dataset, Guaranteeing Its Appropriateness For Training And Testing The IDS Models. This Phase Include Operations Such Data Cleaning, Normalization, And Characteristic Extraction To Improve The First-Rate And Usability Of The Dataset For Further Analysis.

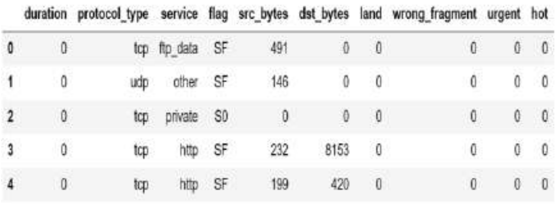
Thereafter, The System Advances To The Training Phase, At Some Stage In Which The IDS Models Are Skilled Making Use Of Various Machine Learning Methods, Which Include "Support Vector Machine (SVM)", Naive Bayes, Decision Tree, Random Forest, And "Logical Analysis Of Data (LAD)". Every Algorithm Is Independently Implemented To The Education Records, Permitting The Fashions To Learn And Perceive Patterns Function Of Normal Community Feature And Feasible Intrusions. This Various Collection Of Algorithms Gives Adaptability And Resilience In Detecting Various Intrusion Patterns, Therefore Enhancing The General Efficacy Of The IDS.

All Through The Trying Out Step, The Educated Models Are Assessed With A Wonderful Test Set To Determine Their Efficacy In Effectively Identifying Intrusions. Performance Measures Like "Accuracy, Precision, Recall, And F1-Score" Are Calculated To Evaluate The Effectiveness Of Every Model In Detecting Harmful Moves Within The Community. The System Ultimately Closes With The Aid Of Figuring Out Network Attacks Based On Predictions From The Trained IDS Models, So Offering Critical Insights Into Its Ability To Defend Against Cyber Threats.

C) Dataset Collection:

The "NSL-KDD" Dataset Is Essential For Intrusion Detection Research Within The Field Of Network Security. Derived From The "KDDCUP'99 Dataset, NSL-KDD" Provides A Standardized And Thorough Depiction Of Network Settings, Rendering It An Highest Quality Selection For Evaluating Intrusion Detection Models. "NSL-KDD", Brought By M. Tavallaee Et Al., Gives A Purified And Enhanced New Release Of Its Predecessor, Free From Redundant Or Duplicate Entries. "NSL-KDD" Consists Of 4 Precise Sub-Datasets: "Kddtest+, Kddtest-21, Kddtrain+, And Kddtrain+_20Percent", Encompassing A Variety Of Network Traffic Situations For Comprehensive Analysis.

The Dataset Incorporates 43 Features, Along With 41 Unbiased Variables Representing Traffic Input And Two Variables Indicating Class And Severity Ratings. The Class Attribute Categorizes Instances As Both Ordinary And Indicative Of Several Assault Techniques, Such As "Denial Of Service (Dos), Probe, User To Root (U2R), And Remote To Local (R2L)". Every Attack Type Shows Unique Attributes, Ranging From The Saturation Of Network Resources In Dos Assaults To The Covert Exam Of Vulnerabilities In Probe Attacks. "NSL-KDD" Gives A Comprehensive Categorization Of Attack Kinds And Their Behaviors, Enabling Sophisticated Analysis And Modeling Of Intrusion Detection Systems, Therefore Improving Network Security Protocols And Defense Strategies.



	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot
0	0	tcp	ftp_data	SF	491	0	0	0	0	0
1	0	udp	other	SF	146	0	0	0	0	0
2	0	tcp	private	S0	0	0	0	0	0	0
3	0	tcp	http	SF	232	8153	0	0	0	0
4	0	tcp	http	SF	199	420	0	0	0	0

"Fig 2 NSL KDD Dataset"

D) Data Processing:

Data Processing Is An Essential Segment Inside The Preparation Of The NSL-KDD Dataset For The Training And Evaluation Of Intrusion Detection Algorithms. This Segment Entails Utilizing The Panda's Dataframe, An Effective Instrument For Managing Based Facts, To Trade And Enhance The Dataset According To Precise Specs.

Pandas Dataframe: The Pandas Dataframe Is The Principal Data Structure Utilized For Processing The "NSL-KDD" Dataset. It Facilitates The Efficient Management Of Tabular Data, Including Competencies For Data Modification, Cleansing, And Transformation.

Dropping Unwanted Columns: A Crucial Element Of Data Processing Entails Recognizing And Eliminating Extraneous Columns That Do Not Resource The Intrusion Detection Goal. Those Columns May Include Extraneous Functions Or Metadata That May Not Yield Significant Insights For Differentiating Among Normal And Malicious Network Behavior. By Judiciously Omitting Positive Columns, The Dataset Is Optimized, Diminishing Computing Burden And Enhancing The Efficacy Of Subsequent Research.

E) Visualization:

Visualization Is Essential For Expertise The Attributes And Distributions Of Data In The "NSL-KDD Dataset". Utilizing The Seaborn And Matplotlib Packages, Visualizations Are Produced To Offer Clean Representations Of Numerous Properties And Their Interrelations. Seaborn And Matplotlib Are Strong Python Packages For Generating Informative And Aesthetically Pleasing Visualizations. Seaborn Provides Elevated Abstractions Based On Matplotlib, Streamlining The Advent Of Intricate Visuals.

Distribution Plots: Seaborg's Distort Function Is Employed To Graph Histograms And Kernel Density Estimations, Facilitating The Visualization Of Numerical Feature Distributions Within The Dataset.

Count Plots: The Countplot Function In Seaborn Is Utilized To Illustrate The Frequency Of Express Data, Such As Assault Classes, Facilitating The Detection Of Class Imbalances.

Pair Plots: The Pairplot Function In Seaborn Produces Pair's Scatterplots For Numerical Data, Assisting Inside The Exam Of Potential Relationships And Patterns Across Variables.

F) Label Encoding:

Label Encoding Is Utilized To Convert Class Variables Into Numerical Codecs, Facilitating Compliance With Machine Learning Methods That Necessitate Numerical Inputs. The Label Encoder Class From The Sickie-Learn Library Is Hired To Transform Specific Labels Into Numerical Values. This Technique Ensures Consistent Encoding Of Categorical Variables Throughout The Dataset.

G) Feature Selection:

Feature Choice Is Essential For Developing A Success Intrusion Detection Models, Focusing On Determining The Most Pertinent Elements That Differentiate Normal From Malicious Community Traffic.

Selectpercentile Using Mutual Info Classify: Selectpercentile, Along With Mutual Data Class, Is Employed For Function Choice. Mutual Data Quantifies The Dependence Between Variables, Facilitating The Identification Of Useful Features That Demonstrate A Robust Correlation With The Goal Variable (I.E., Class Labels). With The Aid Of Choosing The Best Percentile Of Features In Line With Mutual Information Scores, Redundant Or Pointless Characteristics Are Eliminated, Enhancing The Efficiency And Interpretability Of The Intrusion Detection Models.

H) Algorithms:

Support Vector Machine (SVM): "Vector Machine Support (SVM)" Is Asked For Classification And Regression Tasks ". It Works By Determining Hyperplane, Which Best Separates Many Classes Inside The Element Space And Therefore Optimizes The Limit Between Them.

SVM Kernel: The SVM Kernel Is An Enhancement Of The SVM Technique That Facilitates Nonlinear Decision Barriers Through Transforming Enter Data Into A Better-Dimensional Area. Not Unusual "Kernel Functions Comprise Linear, Polynomial, Radial Basis Function (RBF)", And Sigmoid.

Naive Bayes: Based On The Independence Of The Element, Naive Bayes Is A Probability Method Of Classification Developed From Bayes' Sentence. Naive Bayes, On The Other Hand, Is Quite Simple And Works Quite Well In Many Applications In The Real World; This Is Particularly Suitable For Tasks Of Text Classification.

Decision Tree: This Choice Tree Is Used Method Of Learning Supervised Type And Regression. In Order To Maximize The Cleanliness Of The Class In Each Node Of The Leaves, It Creates A Structure Similar To A Tree Recursively By Distributing The Area Depending On The Most Informative Characteristics.

Random Forest: The Technique Of Learning A File Called Random Forest Creates Several Decision -Making Trees During Training And Generates Class Mode For Type Or Average Prediction Of Individual Trees In Regression. It Reduces Excessive Amounts And Therefore Improves The Generalization And Resistance Of The Model.

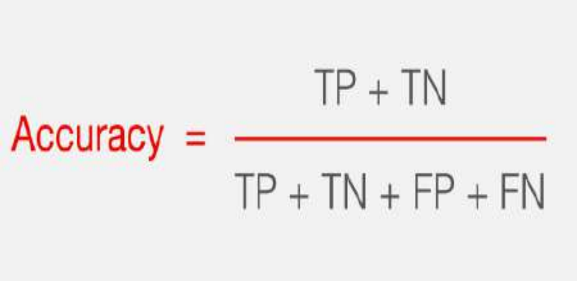
Logical Analysis Of Data (LAD): "Logical Analysis Of Data (LAD)" Is A Data-Centric Method Employed For Sample Identity In Binary Datasets. It Discerns Patterns That Categorize Observations Into Distinct Classifications, Facilitating The Identification Of Abnormalities Suggestive Of Cyber-Attacks Inside Network Systems.

Voting Classifier (RF + AB): The Combination Of Several Base Estimates - Including "Random Forest (RF) And Adaboost (AB)" - The Voting Classifier Is An Access To A File Learning To Improve The General Performance And Robustness Of The Model. It Creates The Final Prediction Of The Aggregation Of Individual Predictions Through The System Of Most Voting.

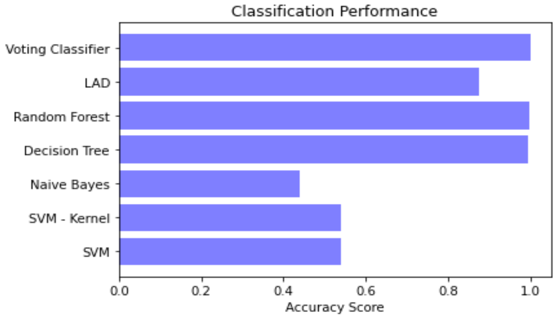
4. EXPERIMENTAL RESULTS

Accuracy: The Accuracy Of The Check Is Its Ability To Relatively Separate The Patient From Healthy Cases. One Must Determine The Ratio Of Real Positives To Real Negatives In All Evaluated Cases To Evaluate The Validity Of The Test. Mathematically It Can Be Mentioned As:

"Accuracy = TP + TN TP + TN + FP + FN".



$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

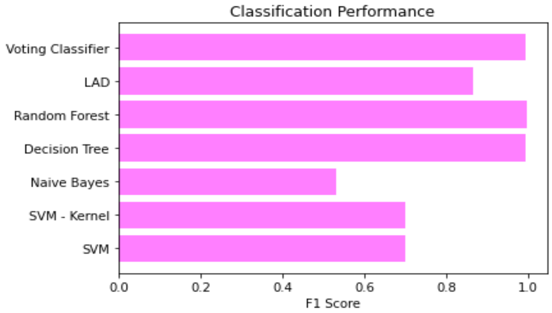


“Fig 3 Accuracy Comparison Graphs”

F1-Score: In Machine Learning, The Score F1 Is A Measure Of The Model Accuracy. It Combines The Modeling And Accuracy Measurement. The Frequency Of Actual Predictions Created By The Model Throughout The Data File Is Calculated By The Metric Of Accuracy.

$$\textbf{F1 Score} = \frac{2}{\left(\frac{1}{\text{Precision}} + \frac{1}{\text{Recall}}\right)}$$

$$\textbf{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

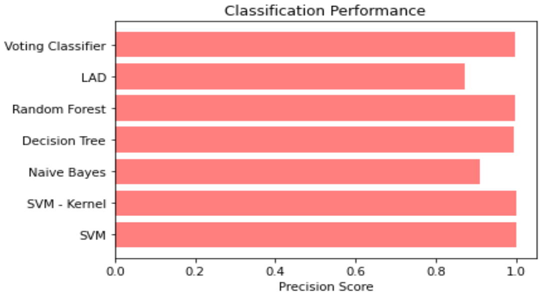


“Fig 4 F1 Score Comparison Graphs”

Precision: Accurate Percentage Measures As It Should Be Classified Among High -Quality Diagnosed Cases. The Formula For Computational Accuracy Is Like:

“Precision = True Positives/ (True Positives + False Positives) = TP/ (TP + FP)”

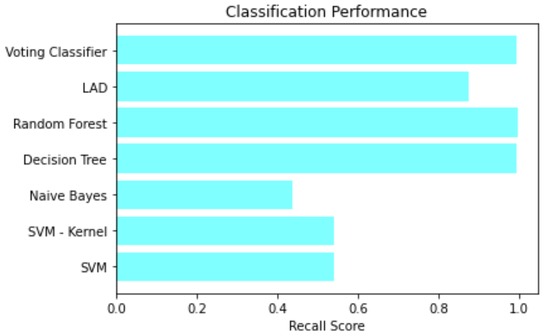
$$\text{Precision} = \frac{\textit{True Positive}}{\textit{True Positive} + \textit{False Positive}}$$



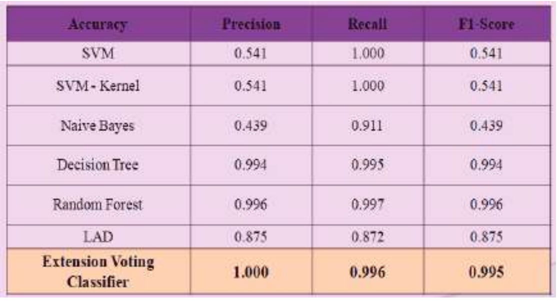
“Fig 5 Precision Comparison Graphs”

Recall: In Machine Learning, Recall Is A Statistic Measuring The Capacity Of A Model To Grasp All Relevant Moments Of A Given Input. It’s Miles The Proportion Of As It Must Be Predicted Fantastic Observations To The Total Actual Positives, Providing Data At The Efficacy Of A Version In Spotting Events Of A Given Class.

$$Recall = \frac{TP}{TP + FN}$$

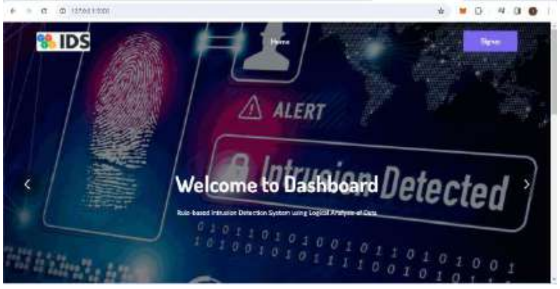


“Fig 6 Recall Comparison Graphs”



Accuracy	Precision	Recall	F1-Score
SVM	0.541	1.000	0.541
SVM - Kernel	0.541	1.000	0.541
Naive Bayes	0.439	0.911	0.439
Decision Tree	0.994	0.995	0.994
Random Forest	0.996	0.997	0.996
LAD	0.875	0.872	0.875
Extension Voting Classifier	**1.000**	**0.996**	**0.995**

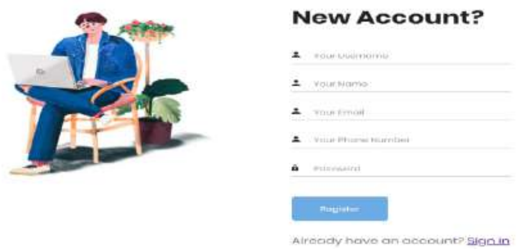
“Fig 7 Performance Evaluation Table”



Welcome to Dashboard

Rule-based Intrusion Detection System using Logical Analysis of Data

“Fig 8 Home Page”



New Account?

Your Username

Your Name

Your Email

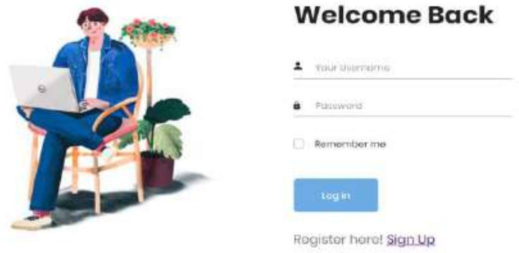
Your Phone Number

Password

Register

Already have an account? Sign in

“Fig 9 Registration Page”



Welcome Back

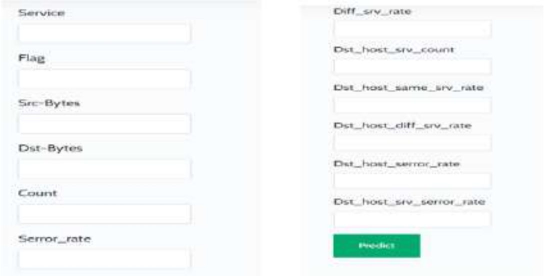
Your Username

Password

□ Remember me

Register here! Sign Up

“Fig 10 Login Page”



Service

Flag

Src-Bytes

Dst-Bytes

Count

Serror_rate

Diff_srv_rate

Dst_host_srv_count

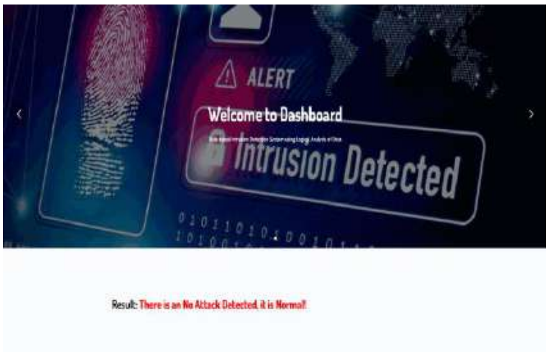
Dst_host_same_srv_rate

Dst_host_diff_srv_rate

Dst_host_serror_rate

Dst_host_srv_serror_rate

“Fig 11 Upload Input Data”



Result: There is an No Attack Detected, it is Normal!

“Fig 12 Final Outcome”

5. CONCLUSION

In End, This Research Introduces A Records-Pushed Method For Constructing An Intrusion Detection System (IDS) That Reveals More Desirable Overall Performance At The NSL-KDD Dataset. Making Use Of The Logical Analysis Of Data (LAD) Methodology, We've Effectively Developed A Rule-Based Classifier Proficient In Reliably Identifying Intrusions Inside Community Systems. Our Empirical Assessment, Juxtaposing LAD With Traditional Gadget Studying Algorithms Inclusive Of Support Vector Machine (SVM), Naive Bayes, And Random Forest (RF), And Decision Tree (DT), Underscores The Effectiveness And Dependability Of Our Counseled Method. Moreover, Our Challenge's Expansion To Include Ensemble Methods Such As The Balloting Classifier (RF+AB) Highlights Our Dedication To Enhancing Accuracy And Resilience In Intrusion Detection.

6. FUTURE SCOPE

Future Study And Development In The Field Of Intrusion Detection Has Numerous Opportunities. Initially, Extra Improvement And Optimization Of The LAD Approach May Improve Its Efficacy And Scalability In Identifying Rising Cyber Dangers. Moreover, Investigating Progressive Ensemble Strategies And Integrating Sophisticated

Feature Selection Techniques May Enhance The Accuracy And Efficiency Of IDS Systems. Furthermore, Imposing Real-Time Monitoring And Integrating Anomaly Detection Systems Helps Beautify Proactive Defenses Against Superior Cyber-Attacks. Our Study Establishes A Foundation For Further Progress In Intrusion Detection Technologies, Aiding Persevering With Projects To Protect Community Protection In A Gradually Hostile Digital Environment.

REFERENCES

[1] R. Langner, "Stuxnet: Dissecting A Cyberwarfare Weapon," IEEE Security & Privacy, Vol. 9, No. 3, Pp. 49–51, 2011.

[2] A. Hobbs, "The Colonial Pipeline Hack: Exposing Vulnerabilities In Us Cybersecurity," In SAGE Business Cases, SAGE Publications: SAGE Business Cases Originals, 2021.

[3] D. U. Case, "Analysis Of The Cyber Attack On The Ukrainian Power Grid," Electricity Information Sharing And Analysis Center (E-ISAC), Vol. 388, Pp. 1–29, 2016.

[4] M. Abrams And J. Weiss, "Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services, Australia," Tech. Rep., MITRE CORP MCLEAN VA MCLEAN, 2008.

[5] I. Abrar, Z. Ayub, F. Masoodi, And A. M. Bamhdi, "A Machine Learning Approach For Intrusion Detection System On Nsl-Kdd Dataset," In 2020 International Conference On Smart Electronics And Communication (ICOSEC), Pp. 919–924, IEEE, 2020.

[6] L. Lv, W. Wang, Z. Zhang, And X. Liu, "A Novel Intrusion Detection System Based On An Optimal Hybrid Kernel Extreme Learning Machine," Knowledge-Based Systems, Vol. 195, P. 105648, 2020.

[7] C. Kruegel And T. Toth, "Using Decision Trees To Improve Signature-Based Intrusion Detection," In International Workshop On Recent Advances In Intrusion Detection, Pp. 173–191, Springer, 2003.

[8] H. Alazzam, A. Sharieh, And K. E. Sabri, "A Feature Selection Algorithm For Intrusion Detection System Based On Pigeon Inspired Optimizer," Expert Systems With Applications, Vol. 148, P. 113249, 2020.

[9] D. E. Denning, "An Intrusion-Detection Model," IEEE Transactions On Software Engineering, No. 2, Pp. 222–232, 1987.

[10] T. K. Das, S. Adepu, And J. Zhou, "Anomaly Detection In Industrial Control Systems Using Logical Analysis Of Data," Computers & Security, Vol. 96, P. 101935, 2020.

[11] E. Boros, P. L. Hammer, T. Ibaraki, And A. Kogan, "Logical Analysis Of Numerical Data," Mathematical Programming, Vol. 79, No. 1, Pp. 163– 190, 1997.

[12] Y. Crama, P. L. Hammer, And T. Ibaraki, "Cause-Effect Relationships And Partially Defined Boolean Functions," Annals Of Operations Research, Vol. 16, No. 1, Pp. 299–325, 1988.

[13] P. L. Hammer, "Partially Defined Boolean Functions And Cause-Effect Relationships," In Proceedings Of The International Conference On Multiattribute Decision Making Via OR-Based Expert Systems, University Of Passau, 1986.

[14] M. Tavallaee, E. Bagheri, W. Lu, And A. A. Ghorbani, "A Detailed Analysis Of The Kdd Cup 99 Data Set," In 2009 IEEE Symposium On Computational Intelligence For Security And Defense Applications, Pp. 1– 6, IEEE, 2009.

[15] B. Ingre And A. Yadav, "Performance Analysis Of Nsl-Kdd Dataset Using Ann," In 2015 International Conference On Signal Processing And Communication Engineering Systems, Pp. 92–96, IEEE, 2015.

[16] R. Patgiri, U. Varshney, T. Akutota, And R. Kunde, "An Investigation On Intrusion Detection System Using Machine Learning," In 2018 IEEE Symposium Series On Computational Intelligence (SSCI), Pp. 1684– 1691, IEEE, 2018.

[17] S. Farhat, M. Abdelkader, A. Meddeb-Makhlouf, And F. Zarai, "Comparative Study Of Classification Algorithms For Cloud Ids Using Nsl-Kdd Dataset In Weka," In 2020 International Wireless Communications And Mobile Computing (IWCMC), Pp. 445–450, IEEE, 2020.

[18] M. Almseidin, J. Al-Sawwa, And M. Alkasassbeh, "Generating A Benchmark Cyber Multi-Step Attacks Dataset For Intrusion Detection," Journal Of Intelligent & Fuzzy Systems, No. Preprint, Pp. 1–15.

[19] S. Shakya, "Modified Gray Wolf Feature Selection And Machine Learning Classification For Wireless Sensor Network Intrusion Detection," IRO Journal On Sustainable Wireless Systems, Vol. 3, No. 2, Pp. 118–127, 2021.

[20] W. Liu, "Research On Dos Attack And Detection Programming," In 2009 Third International Symposium On Intelligent Information Technology Application, Vol. 1, Pp. 207–210, IEEE, 2009.

[21] P. G. Jeya, M. Ravichandran, And C. Ravichandran, "Efficient Classifier For R2l And U2r Attacks," International Journal Of Computer Applications, Vol. 45, No. 21, Pp. 28–32, 2012.

[22] G. Saporito, "A Deeper Dive Into The Nsl-Kdd Data Set," 2019.

[23] H. Almuallim And T. G. Dietterich, "Learning Boolean Concepts In The Presence Of Many Irrelevant Features," Artificial Intelligence, Vol. 69, No. 1-2, Pp. 279–305, 1994.

Dataset Link:

NSL – KDD:

Https://Www.Kaggle.Com/Datasets/Kaggleprollc/Nsl-Kdd99-Dataset