International Journal of
HRM and Organizational Behavior

www.ijhrmob.com

editor@ijhrmob.com

HYBRID FEATURE EXTRACTION WITH MACHINE LEARNING TO IDENTIFY NETWORK ATTACKS

G VISWANATH[1], V R ABIRAMI[2] , G PRATHYUSHA[3]
[1]Associate Professor, Department of CSE(AIML), Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: viswag111@gmail.com, ORCID: https://orcid.org/0009-0001-7822-4739
[2]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: abiravi2285@gmail.com
[3]Assistant Professor, Department of CSE, Sri Padmavathi Mahila Visvavidyalayam Tirupati, Email:prathyubmb@gmail.com

Abstract: Cyber attacks are undermining network security, requiring robust Intrusion Detection Systems. This exploration uses ML and the NSL-KDD dataset to distinguish inconsistencies and further develop network security. An IDS that can rapidly and accurately distinguish network attacks continuously utilizing ML calculations learned on the NSL-KDD dataset is the undertaking's objective. It looks for proactive organization security and protection. Project preprocesses NSL-KDD dataset to separate significant qualities and trains ML models to parallel order typical way of behaving and assault ways of behaving. ML calculations are tried to track down the best interruption discovery strategy. The new IDS beats standard methodologies continuously assault discovery after broad evaluation. Intrusion detection is significantly better by ML-driven network traffic examination using the NSL-KDD dataset. This study stresses the utilization of ML and organization traffic examination in cybersecurity. The IDS shows guarantee for proactive cyber threat protection, safeguarding basic information and framework. Voting Classifier(RF + AdaBoost) and Stacking Classifier(LGBM + MLP + RF + XGB) group calculations foresee with 99% accuracy.

Index terms *- machine learning , feature selection, accuracy , intrusion detection, network attacks, binary classification.*

1. INTRODUCTION

Internet use has spread over the course of life. Internet access offers associations a few advantages. In any case, it makes serious security chances. Intruders are attracted to delicate information, making them helpless against network intrusions. Intrusion is unapproved framework access. IP addresses, working frameworks, and applications make recognizing aggressors troublesome.

Executives secure organizations to keep programmers from getting to information. Intrusion detection systems (IDS) [17] distinguish attacks on available objective frameworks. Two kinds of IDS exist. Both use inconsistencies and marks. IDS with a mark identifies known assaults. Anomaly IDS identifies unfamiliar attacks [17].

Scientists have presented ML based intrusion detection calculations to resolve this issue. ML models are supervised, unsupervised, or reinforcement learning [12, 17, 18, 19, 22].

Directed learning takes care of order issues. The model or classifier is prepared utilizing a named dataset. Grouping calculations store information and give a wide rule for ordering (mapping) new info vectors. Here, unaided learning incorporates grouping. It finds preparing information designs. The suspicion that groups will reflect instinctive example divisions is normal. Experimentation support learning is the last methodology. Here, the model might direct information activities and is compensated for smart activities and rebuffed for inaccurate ones.[24]

Each approach has advantages and disadvantages, and in our work, we take on the half and half element determination method for further developed execution and effectiveness. We train utilizing the most utilized NSL-KDD dataset [3, 5].

Preprocessing the informational index expands classifier achievement. In the wake of preparing utilizing calculation created highlights, the model is surveyed for execution.

2. LITERATURE SURVEY

Cyberattacks are turning out to be more incessant and serious. In this manner, Intrusion Detection Systems (IDSs) [17] are currently essential for the association's security foundation. Various calculations have been utilized to distinguish irregularities. AI was their significant source. Consequently, lessening misleading negatives and further developing identification are the significant objectives. In any case, handling time should be decreased. Numerous informational indexes in writing might be used for IDS learning and testing. This study plans to recognize the main properties of New Selected Learning-Knowledge Discovery in Databases Data set (NSL-KDD) [3, 5], which influence identification results. Accordingly, we will eat the risky dataset piece. We began with the Consolidated Nearest Neighbors (CNN) calculation to make our Network IDS (NIDS) [1]. A decent characterization and relapse calculation that thinks about example scattering. CNN diminishes information vector aspect, decreasing framework assets and handling time while holding recognition accuracy. Our subsequent strategy utilized a Neural Network (NN) to pre-order our learning informational index. We contrast our methods with K Nearest Neighbors (KNN) to show their proficiency. We likewise contrast our strategies with two WEKA programming techniques. Tests exhibit that our IDS procedures improve location rates, diminish missed assaults, and lessen handling time. The flood in network traffic information is an enormous security risk. Intrusion detection systems (IDSs) are ordinarily utilized correspondence network security arrangements. An IDS arranges network traffic information into ordinary and strange to distinguish assaults. The tremendous intricacy of organization traffic information makes it hard for an IDS to recognize interruptions quick and dependably. Highlight determination is critical in IDS plan to diminish intricacy and accelerate location. In this examination [2], we propose a productive element choice methodology that use the association between a subset of qualities and the conduct class name to decrease dimensionality. Both correlation-based feature selection (CFS) and symmetrical uncertainty (SU) measure include dependence on class marks and different qualities. Trial discoveries on NSL-KDD dataset [3, 5] exhibit that the recommended technique with less highlights outflanks past methodologies in preparing time, model structure time, and framework accuracy. The proposed include determination strategy is likewise tried on various order calculations, and the outcomes show that J48 classifier, with the most noteworthy exactness and accuracy values and least miss rate and deception rate values, performs better.

As cyberattacks have become more incessant, so affect society. Subsequently, research on digital protection and interruption identification as a safeguard against digital assaults is required. ML and DL are generally utilized in interruption recognition framework innovative work, and the NSL-KDD dataset is much of the time utilized in calculation examination and check. This study [3] presents a two-stage dimensionality reduction (TSDR) include determination approach demonstrated on NSL-KDD dataset. The methodology diminished dataset dimensionality and enormously further developed computation effectiveness. The KNN calculation [3] checks that the original component choice system increments calculation execution. The exactness rate is simply somewhat lower than complete component calculation.[26]Network security is a significant issue in conveyed frameworks these days. Many attacks are more earnestly to identify utilizing antivirus and firewall programming. IDSs [17] recognize network traffic inconsistencies to further develop security. Network peculiarity discovery decides whether it is unusual or genuine to approaching traffic. Well known ML strategies are utilized in mechanized rush hour gridlock abnormality location frameworks. In [4], we utilized the Data Gain-based strategy. In NSL-KDD dataset, the calculation chooses ideal element numbers. We likewise utilized the artificial bee colony algorithm and Optimization-Cuckoo Search Algorithm to advance SVM hyper boundaries for dataset characterization. The ongoing interruption dataset NSLKDD was utilized to assess the proposed approach. As indicated by tests, the recommended strategy outflanks and is more exact than other late NSLKDD techniques [3, 5].

Intrusion detection tracks down intrusions. IIDS [17] screen inbound and active traffic and recognize unusual examples that might flag a framework attack to shield organizations. A few scholastics have created IDS utilizing data mining as of late. This examination [5] assesses data mining-based ML strategies K-Means and Fuzzy C-Means clustering calculations to detect intrusion across NSL-KDD dataset for DoS, R2L, U2R, and Test attacks.

3. METHODOLOGY

i) Proposed Work:

To track down the main elements in the pre-handled NSL-KDD dataset, hybrid feature extraction is proposed [3, 5]. Our answer depends on this dataset, decided to keep up with basic data for ML network traffic analysis and anomaly identification. SVM and Naive Bayesian [11] models are prepared utilizing determined highlights. These models are thoroughly tried for network attack prediction. The best model for network security examination and execution is picked in light of accuracy and error rates. Gathering approaches incorporate Voting Classifier (Random Forest and AdaBoost) and Stacking Classifier (Random Forest , Multi-layer Perceptron with LightGBM and XGBoost) further develop expectation accuracy. This ensemble technique made close to 100% accurate forecasts, demonstrating its dependability. To empower client testing, we made a Flask-based front end with client confirmation to defend framework access. This boosts our framework's prescient capacities, client experience, and security all through testing and sending.

ii) System Architecture:

As found in Figure 1, network information is accumulated for model information. The NSL-KDD[5] network dataset gives this information. As recommended in [6], dataset highlights are pre-processed.After pre-handling the dataset, we utilize hybrid feature extraction to pick the most applicable subset. Training SVM and Naive Bayesian [11] ML models utilizing recuperated highlights learns boundaries. The models are tried on the dataset after training. The test stage expects network assaults. The outcome was shown involving a binary confusion matrix for the two models. It returns how much test dataset passages ordered appropriately and wrongly as normal and attack sets. We next assess each model's accuracy and error rate to pick the optimal binary classification model.[28]

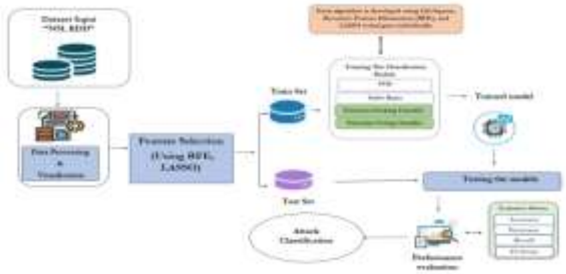
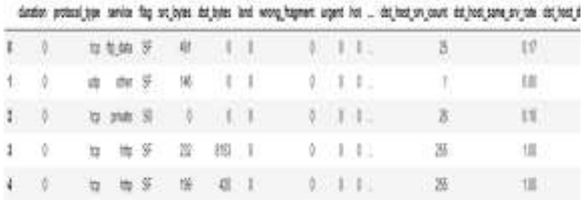


Fig 1 Proposed architecture

iii) Dataset collection:

NSL-KDD [3, 5] is a public dataset in light of KDD cup99 (Tavallaee et al., 2009). A measurable examination of the cup99 dataset uncovered imperfections that enormously influence interruption discovery accuracy and misjudge AIDS (Tavallaee and al., 2009). The enormous number of copy parcels in KDD is the key issue. Tavallaee et al. viewed that as 78% and 75% of organization parcels in KDD preparing and test sets are copied (Tavallaee et al., 2009). This enormous number of copy occurrences in the preparation set would predisposition ML frameworks toward ordinary occasions and keep them from learning unpredictable models, which are more destructive to the PC framework. Tavallaee et al. made the NSL-KDD dataset in 2009 from the KDD Cup'99 dataset to dispense with copies. The NSL-KDD train dataset has 125,973 records and the test dataset 22,544. The NSL-KDD dataset is adequately enormous to haphazardly use without testing. Different examinations have yielded comparable and equivalent outcomes. The NSL_KDD dataset has 22 training intrusion assaults and 41 elements. This dataset has 21 association qualities and 19 host-specific attributes (Tavallaee et al., 2009).



	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	...	dst_host_srv_count	dst_host_same_srv_rate	dst_host_d
0	0	tcp	ftp_data	SF	491	0	0	0	0	0	...	25	0.17	
1	0	udp	other	SF	146	0	0	0	0	0	...	1	0.00	
2	0	tcp	private	S0	0	0	0	0	0	0	...	26	0.10	
3	0	tcp	http	SF	232	8153	0	0	0	0	...	255	1.00	
4	0	tcp	http	SF	199	420	0	0	0	0	...	255	1.00	

Fig 2 NSL KDD dataset

iv) Data Processing:

Data processing transforms raw information into business-helpful data. Information researchers accumulate, sort out, clean, check, break down, and orchestrate information into diagrams or papers. Data can be handled physically, precisely, or electronically. Data ought to be more significant and decision-production simpler. Organizations might upgrade activities and settle on basic decisions quicker. PC programming improvement and other mechanized information handling innovations add to this. Big data can be transformed into significant bits of knowledge for quality administration and independent direction.

v) Feature selection:

Feature selection chooses the most steady, non-repetitive, and pertinent elements for model turn of events. As data sets extend in amount and assortment, purposefully bringing down their size is significant. The fundamental reason for feature selection is to increment prescient model execution and limit processing cost.

One of the vital pieces of feature engineering is picking the main attributes for machine learning algorithms. To diminish input factors, feature selection methodologies take out copy or superfluous elements and limit the assortment to those generally critical to the ML model. Rather than permitting the ML model pick the main qualities, feature selection ahead of time enjoys a few benefits.

vi) Algorithms:

Support Vector Machine (SVM): It is a sophisticated supervised ML procedure for straight or nonlinear grouping, relapse, and exception identification.Though we call it relapse challenges, it's great for characterization. The SVM technique looks for the best hyperplane in N-layered space to isolate data of interest into highlight space classes. Hyperplane expects to amplify the hole between closest places of different classes. How much attributes decides hyperplane size. For two information includes, the hyperplane is a line. The hyperplane becomes 2-D with three information attributes [14].

SVM with Chi-Square: Chi-Square tests possibility table unmitigated variable autonomy. It thinks about the noticed and anticipated frequencies of absolute factors to check whether the noticed appropriation veers off significantly from possibility. Chi-Square is utilized to pick the most useful elements by evaluating highlight target variable reliance. SVM utilizes Chi-Square feature selection to pick the most significant attributes to work on model execution. This assists the SVM with zeroing in on the main order highlights, upgrading effectiveness.

SVM with Recursive Feature Elimination (RFE): RFE chooses highlights by recursively erasing the most un-significant ones from the dataset. It involves preparing a model overall list of capabilities, positioning the elements by importance, and eliminating the most un-significant ones. The procedure is gone on until the expected number of attributes is gotten. RFE is utilized to improve ML model proficiency and interpretability by zeroing in on educational qualities. Iteratively eliminating the most un-significant elements with RFE upgrades the SVM model's presentation. This step-wise expulsion assists the SVM with finding the most helpful qualities, empowering it to recognize typical network behavior from attacks.

LASSO (Least Absolute Shrinkage and Selection Operator): Regression analysis utilizing LASSO adds a punishment term to the relapse objective capability. The punishment term is the outright coefficient size duplicated by a regularization boundary. LASSO diminishes less huge coefficients to zero to advance model sparsity. LASSO chooses a subset of the main qualities to perform variable determination and work on model interpretability. By adding a punishment term to the SVM's goal capability, LASSO chooses highlights. This advances meager capabilities, letting the model spotlight on key elements. SVM with LASSO works on model interpretability and speculation [10].

Naive Bayes : Bayes' hypothesis based probabilistic ML calculation Naive Bayes. It improves on likelihood calculation by expecting attributes are autonomous given the class mark. Naive Bayes is utilized for text classification and spam separating [11].

Naive Bayes using Chi-Square: Focusing in on the main attributes with Chi-Square feature selection develops Naive Bayes execution. This mix removes helpful qualities from network traffic information, further developing the Naive Bayes classifier.

Naive Bayes using RFE (Recursive Feature Elimination): RFE streamlines Naive Bayes by iteratively eliminating insignificant qualities. This step-wise component expulsion assists the Naive Bayes classifier with finding its most significant qualities, boosting network traffic arrangement.[30]

Naive Bayes using LASSO (Least Absolute Shrinkage and Selection Operator): LASSO and Naive Bayes cooperate to pick highlights, adding a punishment component to the goal capability. This advances sparsity in the component assortment, allowing the Naive Bayes to show center around center order qualities.

4. EXPERIMENTAL RESULTS

Precision: Precision quantifies the percentage of certain events or tests that are well characterized. To attain accuracy, use the formula:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

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

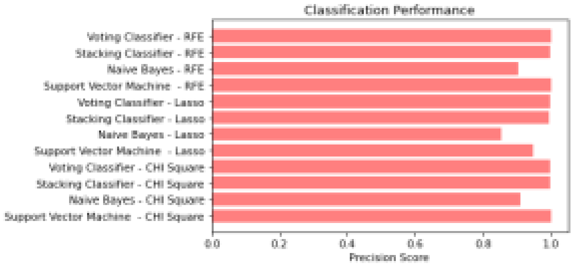


Fig 3 Precision comparison graph

Recall: ML recall measures a model's ability to catch all class occurrences. The model's ability to recognize a certain type of event is measured by the percentage of precisely anticipated positive prospects that turn into real earnings.

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

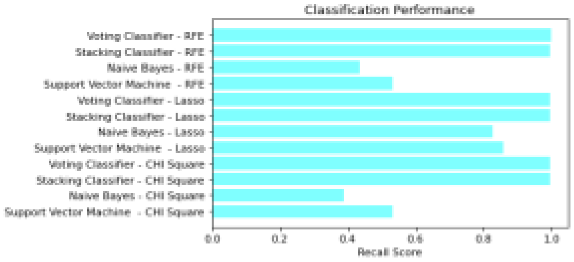


Fig 4 Recall comparison graph

Accuracy: The model's accuracy is the percentage of true predictions at a grouping position.

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

ISSN 2454 - 5015

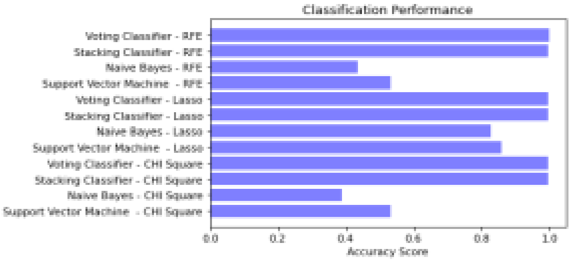


Fig 5 Accuracy graph

F1 Score: The F1 score captures both false positives and false negatives, making it a harmonized precision and validation technique for unbalanced data sets.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

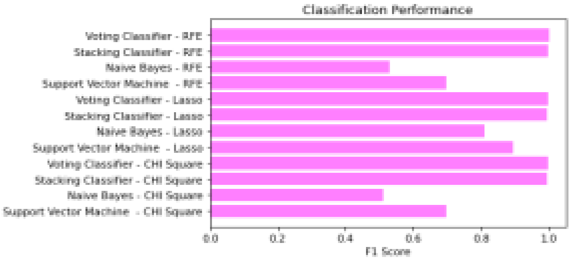
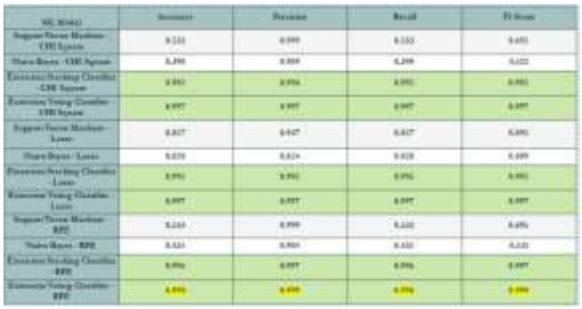


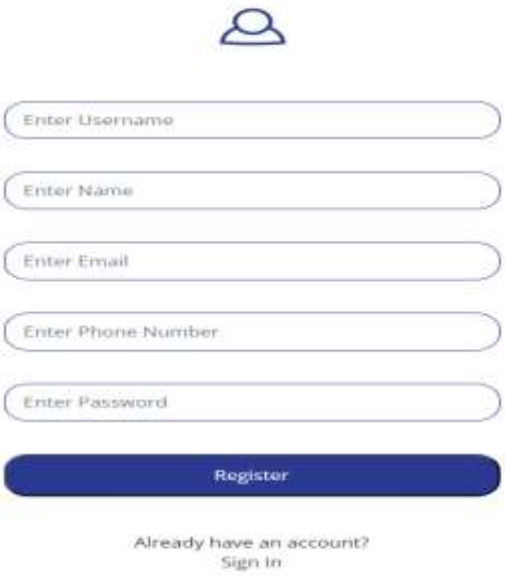
Fig 6 F1Score



ML Model	Accuracy	Precision	Recall	F1 Score
Support Vector Machine - CHI Square	0.533	0.999	0.533	0.691
Naive Bayes - CHI Square	0.390	0.909	0.390	0.522
Extension Stacking Classifier - CHI Square	0.993	0.994	0.993	0.993
Extension Voting Classifier - CHI Square	0.997	0.997	0.997	0.997
Support Vector Machine - Lasso	0.827	0.947	0.827	0.881
Naive Bayes - Lasso	0.820	0.824	0.820	0.809
Extension Stacking Classifier - Lasso	0.991	0.992	0.991	0.991
Extension Voting Classifier - Lasso	0.997	0.997	0.997	0.997
Support Vector Machine - RFE	0.533	0.999	0.533	0.696
Naive Bayes - RFE	0.433	0.969	0.433	0.522
Extension Stacking Classifier - RFE	0.996	0.997	0.996	0.997
Extension Voting Classifier - RFE	0.996	0.999	0.996	0.998

Fig 7 Performance Evaluation

Fig 8 Home page



Enter Username

Enter Name

Enter Email

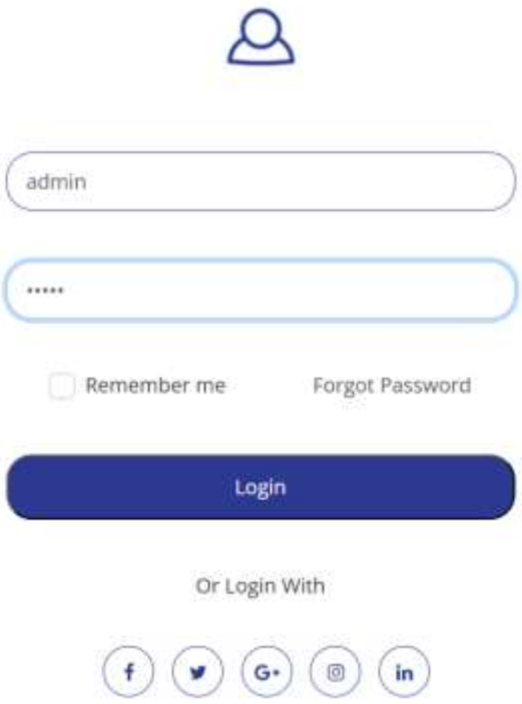
Enter Phone Number

Enter Password

Register

Already have an account?
Sign In

Fig 9 Signin page



admin

*****

Fig 10 Login page

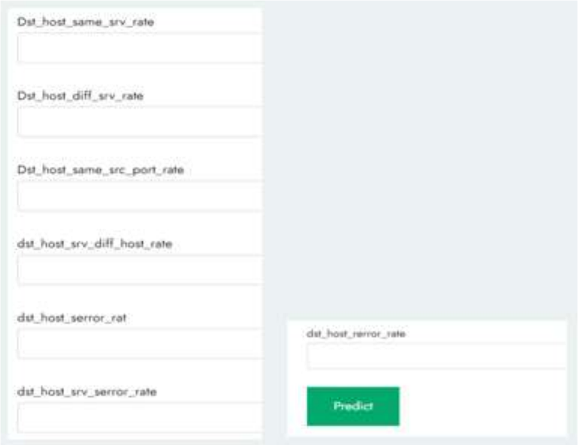
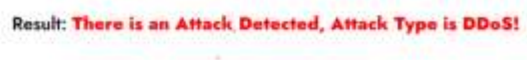


Fig 11 User input



Result: There is an Attack Detected, Attack Type is DDoS!

Fig 12 Predict result for given input

5. CONCLUSION

Hybrid feature extraction utilizing ML to distinguish network attacks was effective. The review utilized the NSL-KDD dataset [3, 5], which eliminates duplication from the 1999 KDD Cup dataset, for ML examination and abnormality recognizable proof. After cautious preprocessing and include determination, the examination trained binary classification models to precisely recognize ordinary and assault types. Voting Classifier(RF + AdaBoost) accomplishes 99% accuracy during testing and is tried in the front end interface, which permits clients to enter highlight values, showing the calculation's viability in real-world situations. Assessment estimates like accuracy and error rates showed that the better venture outflanked unique outcomes. Huge enhancements expanded effectiveness and organization assault expectation. The drive underlines network traffic examination's part in network protection from attacks. The venture advances proactive organization break counteraction with a strong Intrusion Detection System.[32]

6. FUTURE SCOPE

SVM and Naive Bayesian models are prepared on recuperated elements to learn boundaries [11, 14]. In the wake of preparing, the models are tried on a dataset for ML execution. Forecasts incorporate organization assaults during testing. This projected outcome's accuracy and error rate are inspected. The model with the most highest score is utilized for prediction accuracy analysis.

REFERENCES

[1] F. Z. Belgrana, N. Benamrane, M. A. Hamaida, A. Mohamed Chaabani and A. Taleb-Ahmed, "Network Intrusion Detection System Using Neural Network and Condensed Nearest Neighbors with Selection of NSL-

KDD Influencing Features," 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), 2021, pp. 23-29, doi: 10.1109/IoTaIS50849.2021.9359689.

[2] M. B. Shahbaz, Xianbin Wang, A. Behnad and J. Samarabandu, "On efficiency enhancement of the correlation-based feature selection for intrusion detection systems," 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON),2016,pp.1-7,doi: 10.1109/IEMCON.2016.7746286.

[3] T. Yu, Z. Liu, Y. Liu, H. Wang and N. Adilov, "A New Feature Selection Method for Intrusion Detection System Dataset – TSDR method," 2020 16th International Conference on Computational Intelligence and Security (CIS),2020,pp.362-365,doi:10.1109/CIS52066.2020.00083.

[4] Ali Hussein Shamman Al-Safi , Zaid Ibrahim Rasool Hani, , Musaddak M. Abdul Zahra,"Using A Hybrid Algorithm and Feature Selection for Network Anomaly Intrusion Detection", Journal of Mechanical Engineering Research and Developments, ISSN: 1024-1752, CODEN: JERDFO, Vol. 44, No. 4, pp. 253-262. Published Year 2021.

[5] P. S. Bhattacharjee, A. K. Md Fujail and S. A. Begum, "A Comparison of Intrusion Detection by K-Means and Fuzzy C-Means Clustering Algorithm Over the NSL-KDD Dataset," 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2017, pp. 1-6, doi: 10.1109/ICCIC.2017.8524401.

[6] Y. J. Haranwala, S. Haidri, T. S. Tricco, V. P. da Fonseca and A. Soares, "A Dashboard Tool for Mobility Data Mining Preprocessing Tasks," 2022 23rd IEEE International Conference on Mobile Data Management (MDM), 2022, pp. 278-281, doi: 10.1109/MDM55031.2022.00059.

[7] Z. Wang et al., "Image Noise Level Estimation by Employing Chi-Square Distribution," 2021 IEEE 21st International Conference on Communication Technology (ICCT), 2021, pp. 1158-1161, doi: 10.1109/ICCT52962.2021.9657946.

[8] M. S. S. Sumi and A. Narayanan, "Improving Classification Accuracy Using Combined Filter+Wrapper Feature Selection Technique," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2019, pp. 1-6, doi: 10.1109/ICECCT.2019.8869518.

[9] M. Zhu, X. Huang and H. Pham, "A Random-Field-Environment-Based Multidimensional Time-Dependent Resilience Modeling of Complex Systems," in IEEE Transactions on Computational Social Systems, vol. 8, no. 6, pp. 1427-1437, Dec. 2021, doi: 10.1109/TCSS.2021.3083515.

[10] Y. Kim, J. Hao, T. Mallavarapu, J. Park and M. Kang, "Hi-LASSO: High-Dimensional LASSO," in IEEE Access, vol. 7, pp. 44562-44573, 2019, doi: 10.1109/ACCESS.2019.2909071.

[11] N. S. Rahmi, N. W. S. Wardhani, M. B. Mitakda, R. S. Fauztina and I. Salsabila, "SMOTE Classification and Random Oversampling Naive Bayes in Imbalanced Data : (Case Study of Early Detection of Cervical Cancer in Indonesia)," 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA), 2022, pp. 1-6, doi: 10.1109/ICITDA55840.2022.9971421.

[12] L. Zeyang, "Research on Intelligent Acceleration Algorithm for Big Data Mining in Communication Network Based on Support Vector Machine," 2021 IEEE 4th International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), 2021, pp. 479-483, doi: 10.1109/AUTEEE52864.2021.9668793.

[13] G. R. Kini and C. Thrampoulidis, "Phase Transitions for One-Vs-One and One-Vs-All Linear Separability in Multiclass Gaussian Mixtures," ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2021, pp. 4020-4024, doi: 10.1109/ICASSP39728.2021.9414099

[14] J. Sewall, S. J. Pennycook, D. Jacobsen, T. Deakin and a. S. McIntosh-Smith, "Interpreting and Visualizing Performance Portability Metrics," 2020 IEEE/ACM International Workshop on Performance, Portability and Productivity in HPC (P3HPC), 2020, pp. 14-24, doi: 10.1109/P3HPC51967.2020.00007.

[15] T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," in IEEE Access, vol. 9, pp. 138432-138450, 2021, doi: 10.1109/ACCESS.2021.3118573.

[16] R. Wang, H. Jiang and G. Shi, "A Multi-Layer Hybrid Intrusion Detection Method Based on Nb And SVM," 2022 IEEE 4th International Conference on Civil Aviation Safety and Information Technology (ICCASIT), 2022, pp. 1384-1388, doi: 10.1109/ICCASIT55263.2022.9986813.

[17] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa and C. F. M. Foozy, "Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset," in IEEE Access, vol. 9, pp. 22351-22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

[18] M. Khodaskar, D. Medhane, R. Ingle, A. Buchade and A. Khodaskar, "Feature-based Intrusion Detection System with Support Vector Machine," 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 2022, pp. 1-7, doi: 10.1109/ICBDS53701.2022.9935972.

[19] K. Shashank and M. Balachandra, "Review on Network Intrusion Detection Techniques using Machine Learning," 2018 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), 2018, pp. 104-109, doi: 10.1109/DISCOVER.2018.8673974.

[20] C. Zhang, F. Ruan, L. Yin, X. Chen, L. Zhai and F. Liu, "A Deep Learning Approach for Network Intrusion Detection Based on NSL-KDD Dataset," 2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID), 2019, pp. 41-45, doi: 10.1109/ICASID.2019.8925239.

[21] J. Liu, K. Xiao, L. Luo, Y. Li and L. Chen, "An intrusion detection system integrating network-level intrusion detection and host-level intrusion detection," 2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS), 2020, pp. 122-129, doi: 10.1109/QRS51102.2020.00028.

[22] F. Yihunie, E. Abdelfattah and A. Regmi, "Applying Machine Learning to Anomaly-Based Intrusion Detection Systems," 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2019, pp. 1-5, doi: 10.1109/LISAT.2019.8817340.

[23] G.Viswanath, “Hybrid encryption framework for securing big data storage in multi-cloud environment”, Evolutionary intelligence, vol.14, 2021, pp.691-698.

[24] Viswanath Gudditi, “Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage”, Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol.12, 2021, pp.545-552.

[25] Viswanath Gudditi, “A Smart Recommendation System for Medicine using Intelligent NLP Techniques”, 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), 2022, pp.1081-1084.

[26] G.Viswanath, “Enhancing power unbiased cooperative media access control protocol in manets”, International Journal of Engineering Inventions, 2014, vol.4, pp.8-12.

[27] Viswanath G, “A Hybrid Particle Swarm Optimization and C4.5 for Network Intrusion Detection and Prevention System”, 2024, International Journal of Computing, DOI: https://doi.org/10.47839/ijc.23.1.3442, vol.23, 2024, pp.109-115.

[28] G.Viswanath, “A Real Time online Food Ording application based DJANGO Restfull Framework”, Juni Khyat, vol.13, 2023, pp.154-162.

[29] Gudditi Viswanath, “Distributed Utility-Based Energy Efficient Cooperative Medium Access Control in MANETS”, 2014, International Journal of Engineering Inventions, vol.4, pp.08-12.

[30] G.Viswanath,“ A Real-Time Video Based Vehicle Classification, Detection And Counting System”, 2023, Industrial Engineering Journal, vol.52, pp.474-480.

[31] G.Viswanath, “A Real- Time Case Scenario Based On Url Phishing Detection Through Login Urls ”, 2023, Material Science Technology, vol.22, pp.103-108.

[32] Manmohan Singh,Susheel Kumar Tiwari, G. Swapna, Kirti Verma, Vikas Prasad, Vinod Patidar, Dharmendra Sharma and Hemant Mewada, “A Drug-Target Interaction Prediction Based on Supervised Probabilistic Classification” published in Journal of Computer Science, Available at: https://pdfs.semanticscholar.org/69ac/f07f2e756b79181e4f1e75f9e0f275a56b8e.pdf