IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

FALSE POSITIVE IDENTIFIERS IN XAI-BASED INTRUSION DETECTION

G VISWANATH[1], S MUNIPRATHAP[2], K BHASKAR[3], D VIDYASAGARI[4]
[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: sadhumuniprathap14@gmail.com
[3]Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: bhaskark.mca@gmail.com
[4]Assistant Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email:hkvidhyareddy@gmail.com

ABSTRACT: Utilizing eXplainable Artificial Intelligence (XAI), this study intends to lessen intrusion detection system false positives. The objective is to pursue choice making straightforward by further developing ML calculation interpretability. The methodology accepts that XAI-determined feature significance relates with intrusion detection accuracy. The exploration will test the arrangement's common sense and generalizability in genuine online protection situations utilizing the LYCOS-IDS2017 dataset. The discoveries recommend XAI combination into intrusion detection systems might be gainful. The undertaking shows the way that XAI can further develop cybersecurity false positive detection and relief thusly. This mix might further develop genuine IDS.

INDEX TERMS Intrusion detection, machine learning, explainability, XAI, false positive rate

1. INTRODUCTION:

In the present connected advanced world, PC framework security is fundamental to safeguard delicate information and keep up with tasks. Interruption location is the last line of guard against security strategy infringement and unapproved access. In network protection, ID is vital to framework respectability and wellbeing, as per Stallings and Brown [1].

IDSs recognize and stop unsafe action and strategy breaks in PC organizations and frameworks. These frameworks investigate network traffic or framework conduct to identify dangers. Signature-based detection and anomaly-based detection are the main detection methods [2].

Signature-based detection detects hurtful exercises utilizing realized assault designs. These marks, as a rule from prior assaults or weaknesses, permit the IDS to recognize and answer unsafe action designs. Signature-based detection functions admirably for known dangers, yet its foreordained marks limit its ability to identify new attacks.

Anomaly based detection recognizes framework or organization takeoffs from typical way of behaving. Irregularity based detection doesn't utilize realized assault designs like mark based location. All things being equal, they make a gauge of common way of behaving and feature flights as risks. As per Alazab et al. [3], this approach can recognize zero-day dangers. Nonetheless, oddity based recognition every now and again creates more false positives than signature-based calculations [4].

IDS battle with false positives, or misidentifying harmless action as dangers. False cautions can disappoint clients, overpower frameworks, and harm IDS certainty [5]. IDS should decrease false positives of work appropriately.

A few techniques have been created to diminish IDS false positives. High level ML or component determination can further develop identification calculation accuracy [6]. Alert sifting, copy location, and gathering related recognitions can diminish deceptions and increment framework constancy [7].

Late accentuation has zeroed in on utilizing eXplainable Artificial Intelligence (XAI) to further develop IDS interpretability and dependability. XAI creates AI models and calculations that can legitimize their decisions, settling on the choice making process more straightforward and comprehensible to people [8]. Analysts use XAI to further develop IDS' ability to recognize genuine dangers from false positives, further developing accuracy and dependability.

This examination proposes utilizing XAI to diminish IDS false positives. The framework can recognize and decrease misleading identifications by utilizing XAI methods to decide include pertinence and the calculation's certainty measures. This study utilizes genuine world datasets to exhibit the reasonableness and adequacy of this strategy, prompting intrusion detection system security and dependability upgrades.

In the accompanying segments, we will talk about false positives in intrusion detection systems, the advantages of consolidating XAI approaches, and the task's system and objectives.[28]

2. LITERATURE SURVEY

Intrusion detection shields PC frameworks and organizations from hurtful movement and unlawful access. From signature-based discovery to AI, scientists have attempted a few strategies to further develop intrusion detection systems (IDS). This writing audit analyzes contemporary ID tests, zeroing in on false positives and the potential advantages of eXplainable Artificial Intelligence (XAI).

As per Nisioti et al. [1], IDS have advanced from old strategies to additional cutting edge ones, including unsupervised learning. The creators stress aggressor attribution in ID and portray how unsupervised methods might find distorted movement without marks. This study makes sense of ID and attribution and anomaly detection issues.

Sommer and Paxson [2] inspect the constraints of mark based network ID utilizing AI. Signature-based frameworks' shut world presumption may not address genuine attacks' intricacy and assortment, the creators guarantee. They prescribe utilizing ML strategies to identify zero-day dangers to further develop IDS.

Marino et al. [3] offer an ill-disposed procedure for IDS eXplainable AI. The antagonistic structure creates threatening cases to test IDS strength and shortcomings. By annoying approaching information and watching the framework's response, specialists might comprehend the IDS's dynamic cycle and track down weaknesses. This strategy further develops interruption discovery frameworks' unwavering quality and straightforwardness.

Ribeiro et al. [4] make sense of ML classifier expectations for reply "for what reason would it be advisable for me I trust you?" The creators offer LIME (Local Interpretable Model-agnostic Explanations) to make sense of individual forecasts by approximating the classifier's conduct close to the occurrence of interest. This technique assists shoppers with grasping expectation boundaries and classifier unwavering quality. LIME makes ML models, particularly ID models, more straightforward and reliable by offering interpretable clarifications.

Shrikumar et al. [5] engender enactment contrasts to learn neural network properties. DeepLIFT (Deep Learning Important FeaTures) contrasts network enactments and without each information element to compute its commitment to yield expectation. This technique investigates muddled neural network models by recognizing fundamental viewpoints that influence direction.

The writing study underscores the need of examining IDS false positives and the potential advantages of eXplainable AI. Analysts can increment IDS interpretability, straightforwardness, and unwavering quality utilizing ML calculations and XAI approaches, further developing computer network and framework security.

3. METHODLOGY

a) Proposed work:

The proposed intrusion detection system utilizes eXplainable Artificial Intelligence (XAI) to decrease false positives. The method works on false positives detection by blending the calculation's certainty measures with XAI trait importance. This technique keeps harmless exercises from being misidentified as dangers while saving real positive detection accuracy. This joining of XAI further develops straightforwardness and interpretability, permitting buyers to trust the dynamic interaction and results [1]. This approach further develops IDS dependability and adequacy in certifiable network protection settings.[29]

b) System Architecture:

Ingestion of organization information from a dataset gives a total image of framework action in the anomaly-based IDS framework design. This information is preprocessed for consistency and ease of use. Then, a limit setting step sets okay deviations from normal way of behaving to direct anomaly identification. The component space acquires significant information from new properties extraction. Model structure trains ML calculations to find anomalies utilizing extricated features and limits. XAI is utilized to investigate model decisions to recognize false positives and distinguish genuine dangers while diminishing misleading problems. This plan guarantees straightforward and interpretable ID, fundamental for cybersecurity [1].

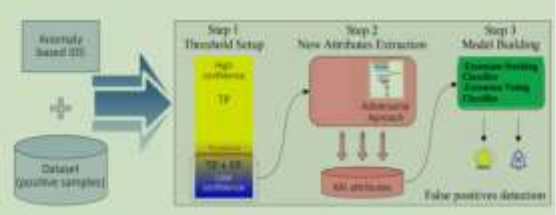
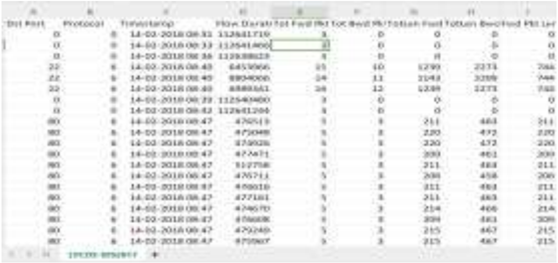


Fig 1 Proposed Architecture

c) Dataset collection:

The LYCOS-IDS2017 dataset surveys intrusion detection systems (IDS) and network safety issues. This dataset incorporates network traffic measurements from reproduced attacks and routine movement. The dataset gives a drawn out depiction of genuine organization conduct, permitting specialists to study digital risks. The LYCOS-IDS2017 dataset permits supervised learning for IDS assessment and benchmarking with labeled cases of hurtful and harmless movement. Its extensive variety of assault types and organization conventions empowers areas of strength for discovery calculation creation and testing. This dataset permits analysts to foster new organization security and digital danger moderation techniques [1].



Dst Port	Protocol	Timestamp	Flow Durati	Tot Fwd Pkt	Tot Bwd Pk	TotLen Fwd	TotLen Bwd	Fwd Pkt Len
0	0	14-02-2018 08:31	112641719	3	0	0	0	0
0	0	14-02-2018 08:33	112641466	3	0	0	0	0
0	0	14-02-2018 08:36	112638623	3	0	0	0	0
22	6	14-02-2018 08:40	6453966	15	10	1239	2273	744
22	6	14-02-2018 08:40	8804066	14	11	2143	3209	744
22	6	14-02-2018 08:40	6889341	14	12	1239	2273	744
0	0	14-02-2018 08:39	112640480	3	0	0	0	0
0	0	14-02-2018 08:42	112641244	3	0	0	0	0
80	6	14-02-2018 08:47	476513	5	3	211	463	211
80	6	14-02-2018 08:47	475048	5	3	220	472	220
80	6	14-02-2018 08:47	474926	5	3	220	472	220
80	6	14-02-2018 08:47	477471	5	3	209	461	209
80	6	14-02-2018 08:47	512758	5	3	211	463	211
80	6	14-02-2018 08:47	475711	5	3	206	458	206
80	6	14-02-2018 08:47	498016	5	3	211	463	211
80	6	14-02-2018 08:47	477161	5	3	211	463	211
80	6	14-02-2018 08:47	474670	5	3	214	466	214
80	6	14-02-2018 08:47	476608	5	3	209	461	209
80	6	14-02-2018 08:47	479249	5	3	215	467	215
80	6	14-02-2018 08:47	475967	5	3	215	467	215

LYCOS-IDS2017

Fig 2 data set

d) DATA PROCESSING

The Python pandas module is utilized to successfully handle the LYCOS-IDS2017 dataset in a dataframe. In the first place, the dataset is placed into a pandasdataframe for simple altering and examination. To rearrange and accelerate computation, superfluous segments are taken out from the dataframe. This stage holds just interruption location applicable properties. Pandas assist with smoothing out information pretreatment tasks including cleaning, changing over, and sorting out. This information handling stage gives the dataset to investigation, highlight designing, and model development, empowering the production of IDS that appropriately recognize and alleviate digital dangers [1].

e) VISUALIZATION

Seaborn and Matplotlib representation instruments assist with examining the LYCOS-IDS2017 dataset. The significant level point of interaction of Seaborn makes measurable illustrations engaging, while Matplotlib takes into consideration adaptable visualisations. These bundles give representation of organization traffic, assault examples, and element relationships. Analysts might make enlightening histograms, disperse plots, heatmaps, and bar outlines with Seaborn's inherent factual visualisation calculations and Matplotlib's wide customization prospects. These perceptions help understand information structure, spot examples and abnormalities, and impact investigation and model creation. Seaborn and Matplotlib perception further develops information understanding and correspondence, empowering online protection information driven decision-production [1].

f) Feature Selection

Feature selection chooses the steadiest, 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.

g) Lable encoding

Many ML methods require name encoding utilizing LabelEncoder to make an interpretation of class marks into mathematical portrayals. For interruption discovery model preparation, classification marks like "ordinary" and "assault" should be addressed as mathematical qualities. LabelEncoder from scikit-learn does this effectively. Each mark in the dataset gets an extraordinary number, changing over unmitigated factors into a configuration ML models can comprehend and decipher. LabelEncoder improves dataset consistency and consistence with downstream examination and model advancement by encoding names consistently. Naming readies the dataset for examination and model preparation in eXplainable Artificial Intelligence (XAI) interruption discovery bogus positive recognizable proof, empowering exact and interpretable frameworks [1].

h) TRAINING AND TESTING

Utilizing eXplainable Artificial Intelligence (XAI) for ID false positive recognizable proof requires various preparation and testing processes. From the beginning, the dataset is parted into preparing and testing sets utilizing cross-approval to guarantee model strength and generalizability. ML calculations are prepared on named information utilizing XAI ways to deal with further develop dynamic interpretability and straightforwardness. SelectPercentile with Common Data Order can track down helpful elements without overfitting. In the wake of preparing, the model is tried on the testing set to recognize false positive and segregate harmless from malevolent movement. XAI approaches are then used to analyze the model's forecasts, uncovering false positive causes and further developing the intrusion detection system. This iterative strategy makes precise and interpretable intrusion detection false positive models [1].

i) ALGORITHMS:

Random Forest

Random Forest (RF) [8] is an ensemble learning approach that trains numerous decision trees and predicts class mode. RF is utilized for intrusion detection in our venture to total various decision tree expectations to further develop accuracy and flexibility while keeping away from false positives.

KNN

K-Nearest Neighbors (KNN)[9] is a non-parametric classification strategy that names relevant pieces of information by their k closest neighbors' larger part class. Our ID research utilizes KNN to arrange network traffic information by surveying occurrence neighborhood likeness to track down anomalies and dangers.[30]

Decision Tree

Decision Tree [10] is a supervised learning strategy that recursively divides information by input highlight values. Our review utilizes Decision Tree for ID to order network traffic information by making a tree-like model with interior hubs addressing highlights to recognize ordinary and malevolent movement.

Naive Bayes

Naive Bayes [11] is a Bayes' hypothesis based probabilistic order method that expects feature freedom. Our ID project utilizes Naive Bayes to assess the likelihood of a given case having a place with a class, recognizing potential dangers and false positives in view of noticed information.

Neural Network

The versatile ML model Neural Network [12] depends on the human cerebrum's connected layers of neurons. Our ID project involves Neural Networks to comprehend convoluted examples and relationships in network traffic information to precisely group typical and malignant movement using high-layered feature spaces.

Voting Classifier - RF + AB

Vote Classifier [13] predicts by means of larger part vote utilizing a few classifiers. Our ID project utilizes a Voting Classifier with Random Forest and

AdaBoost classifiers to expand execution and dependability in perceiving false positives and dangers.

Stacking CLassifier - RF + MLP with LightGBM

Ensemble learning strategy Stacking Classifier [14] predicts utilizing numerous classifiers and a meta-classifier. Our ID project utilizes a Stacking Classifier with Random Forest, Multi-layer Perceptron (MLP), and LightGBM classifiers to further develop accuracy and heartiness in recognizing false positives and malevolent exercises.[32]

4. EXPERIMENTAL RESULTS

Accuracy: A test's accuracy is its ability to recognize debilitated from sound cases. To quantify test accuracy, figure the small part of true positive and true negative in completely broke down cases. Numerically, this is:

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

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

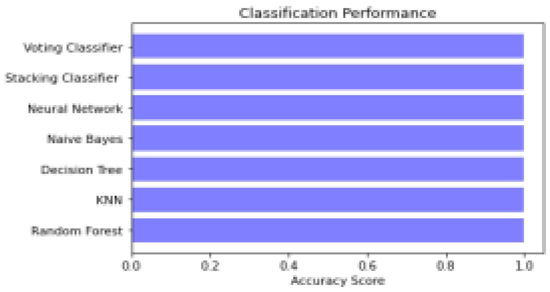


Fig 3 ACCURACY COMPARISON GRAPH

Precision: Precision estimates the level of positive cases or tests precisely sorted. Precision is determined utilizing the recipe:

$$\text{Precision} = \text{True positives/ (True positives + False positives)} = TP/(TP + FP)$$

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

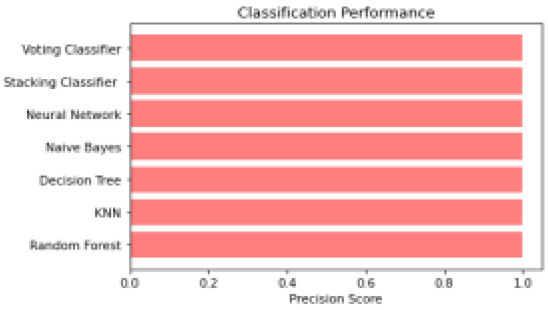


Fig 4 PRECISION COMPARISON GRAPH

Recall: Machine learning recall assesses a model's ability to perceive all significant examples of a class. It shows a model's culmination in catching occasions of a class by contrasting accurately anticipated positive perceptions with complete positives.

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

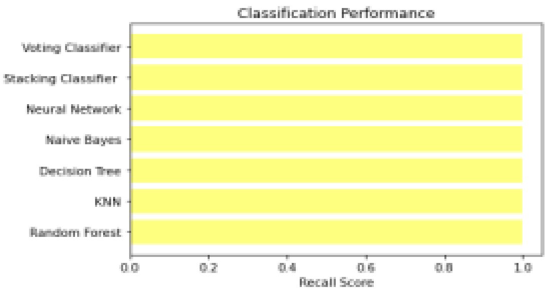


Fig 5 RECALLCOMPARISON GRAPH

F1-Score: Machine learning model accuracy is estimated by F1 score. Consolidating model precision and recall scores. The accuracy measurement estimates how frequently a model anticipated accurately all through the dataset.

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

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

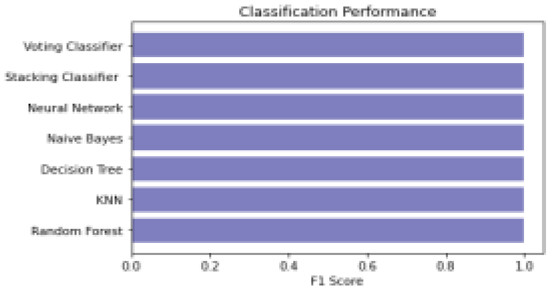
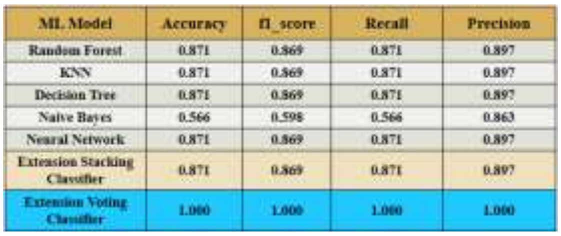


FIG 6 F1 SCORE COMPARISON GRAPH



ML Model	Accuracy	f1_score	Recall	Precision
Random Forest	0.871	0.869	0.871	0.897
KNN	0.871	0.869	0.871	0.897
Decision Tree	0.871	0.869	0.871	0.897
Naive Bayes	0.566	0.598	0.566	0.863
Neural Network	0.871	0.869	0.871	0.897
Extension Stacking Classifier	0.871	0.869	0.871	0.897
Extension Voting Classifier	1.000	1.000	1.000	1.000

Fig 7 PERFORMANCE EVALUATION TABLE

FIG8 HOME PAGE

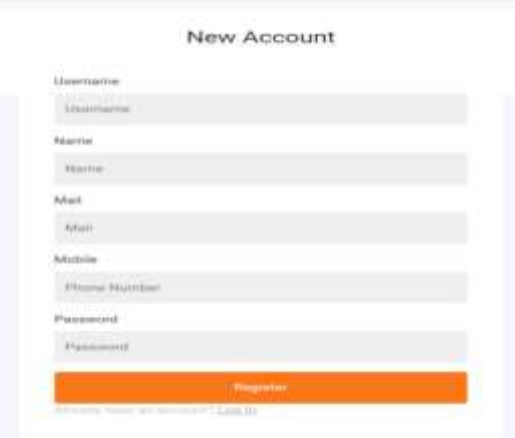


FIG 9 SIGN UP PAGE

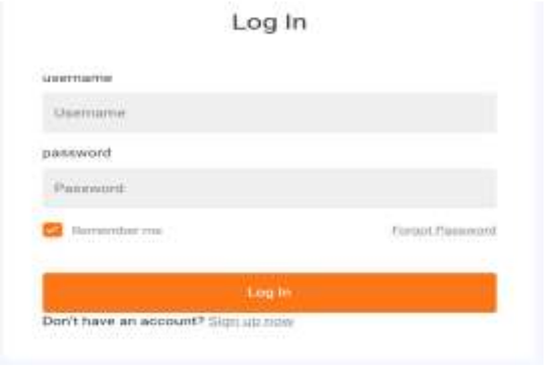


FIG 10 SIGNIN PAGE

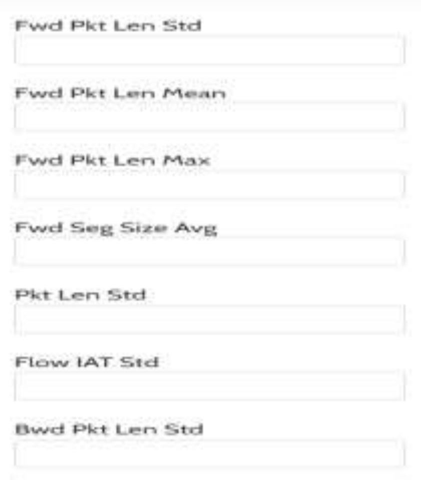


FIG11 UPLOAD INPUT DATA

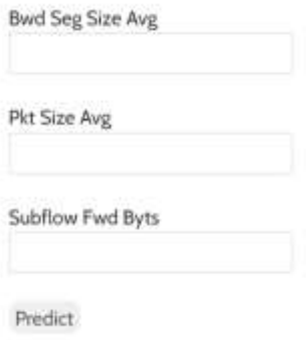
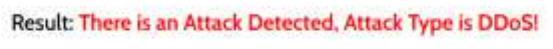
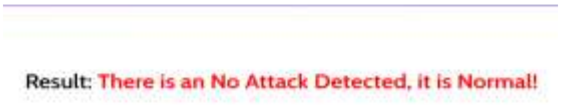


FIG 12 UPLOAD INPUT DATA



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

FIG 13 PREDICTED RESULT



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

FIG 14 PREDICTED RESULT

5. CONCLUSION

At long last, this examination stresses the need of utilizing eXplainable Artificial Intelligence (XAI) to further develop IDS. The task refines its dynamic cycle by examining false positive causes and joining property pertinence from XAI with certainty measures from the IDS calculation to more readily recognize false detections from genuine dangers.

A beneficial ML calculation further develops perception of the connection between XAI-inferred features and detection validity, permitting the IDS to calibrate its judgment limits. Testing on the LYCOS-IDS2017 dataset shows that the recommended strategy decreases bogus up-sides while saving certified positives. The venture's general objective is to further develop IDS accuracy, reliability, and ease of use to reinforce framework security past false positive decrease. The drive further develops intrusion detection and cybersecurity through these endeavors.[34]

6. FUTURE SCOPE

This venture will examine and consolidate further developed Explainable Artificial Intelligence (XAI) techniques for network traffic qualities into ID models. This will work on model interpretability and dependability, giving security examiners more framework dynamic experiences. The exploration will likewise test new ML models for ID that can comprehend complex network data examples to diminish false positives. Intrusion detection systems could involve the proposed strategy progressively, but computational effectiveness should be defeated for smooth consolidation into functional security systems. In unique organization settings, the IDS should constantly screen and update the XAI-upgraded model to answer new digital dangers.

REFERENCES

[1] A. M. Riyad, M. Ahmed, and H. Almistarihi, “A quality framework to improve ids performance through alert post-processing,” International Journal of Intelligent Engineering and Systems, 2019.

[2] R. Alshammari, S. Sonamthiang, M. Teimouri, and D. Riordan, “Using neuro-fuzzy approach to reduce false positive alerts,” in Fifth Annual Conference on Communication Networks and Services Research (CNSR’07), pp. 345–349, 2007.

[3] A. Nisioti, A. Mylonas, P. D. Yoo, and V. Katos, “From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods,”

IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 3369–3388, 2018.

[4] K. A. Scarfone and P. M. Mell, “Sp 800-94. guide to intrusion detection and prevention systems (idps),” tech. rep., National Institute of Standards & Technology, Gaithersburg, MD, USA, 2007.

[5] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in 2010 IEEE Symposium on Security and Privacy, pp. 305–316, 2010.

[6] E. K. Viegas, A. O. Santin, and L. S. Oliveira, “Toward a reliable anomaly-based intrusion detection in real-world environments,” Computer Networks, vol. 127, pp. 200–216, 2017.

[7] Internet Steering Committee project in Brazil, “Total data traffic on the brazilian internet,” 2022. https://ix.br/agregado/. Accessed on: Nov. 11, 2022.

[8] D. L. Marino, C. S. Wickramasinghe, and M. Manic, “An adversarial approach for explainable ai in intrusion detection systems,” in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, pp. 3237–3243, 2018.

[9] S. M. Lundberg and S.-I. Lee, “A unified approach to interpreting model predictions,” in Advances in Neural Information Processing Systems 30 (I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, eds.), pp. 4765–4774, Curran Associates, Inc., 2017.

[10] L. S. Shapley, A Value for n-Person Games, pp. 307–317. Princeton University Press, 1953.

[11] M. T. Ribeiro, S. Singh, and C. Guestrin, “"why should i trust you?": Explaining the predictions of any classifier,” in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD ’16, (New York, NY, USA), p. 1135–1144, Association for Computing Machinery, 2016.

[12] A. Shrikumar, P. Greenside, A. Shcherbina, and A. Kundaje, “Not just a black box: Learning important features through propagating activation differences,” ArXiv, vol. abs/1605.01713, 2016.

[13] S. Bach, A. Binder, G. Montavon, F. Klauschen, K.-R.Müller, and W. Samek, “On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation,” PLOS ONE, vol. 10, pp. 1–46, 07 2015.

[14] MIT Lincoln Laboratory, “1999 darpa intrusion detection evaluation dataset,” 1999. https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset. Accessed on: Nov. 16, 2022.

[15] G. P. Spathoulas and S. K. Katsikas, “Reducing false positives in intrusion detection systems,” Computers & Security, vol. 29, no. 1, pp. 35–44, 2010.

[16] P. Pitre, A. Gandhi, V. Konde, R. Adhao, and V. Pachghare, “An intrusion detection system for zero-day attacks to reduce false positive rates,” in 2022 International Conference for Advancement in Technology (ICONAT), pp. 1–6, 2022.

[17] H. Kim, Y. Lee, E. Lee, and T. Lee, “Cost-effective valuable data detection based on the reliability of artificial intelligence,” IEEE Access, vol. 9, pp. 108959–108974, 2021.

[18] C. Guo, G. Pleiss, Y. Sun, and K. Q. Weinberger, “On calibration of modern neural networks,” 2017.

[19] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “A survey of network-based intrusion detection data sets,” Computers & Security, vol. 86, pp. 147–167, 2019.

[20] G. Engelen, V. Rimmer, and W. Joosen, “Troubleshooting an intrusion detection dataset: the cicids2017 case study,” in 2021 IEEE Security and Privacy Workshops (SPW), pp. 7–12, 2021.

[21] A. Rosay, E. Cheval, F. Carlier, and P. Leroux, “Network Intrusion Detection: A Comprehensive Analysis of CIC-IDS2017,” in 8th International Conference on Information Systems Security and Privacy, pp. 25–36, SCITEPRESS - Science and Technology Publications, Feb. 2022.

[22] M. Ring, A. Dallmann, D. Landes, and A. Hotho, “IP2Vec: Learning similarities between ip addresses,” in 2017 IEEE International Conference on Data Mining Workshops (ICDMW), pp. 657–666, 2017.

[23] A. Nisioti, A. Mylonas, P. D. Yoo, and V. Katos, “From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods,” IEEE Communications Surveys Tutorials, vol. 20, no. 4,pp. 3369–3388, 2018.

[24] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in 2010 IEEE Symposium on Security and Privacy, pp. 305–316, 2010.

[25] D. L. Marino, C. S. Wickramasinghe, and M. Manic, “An adversarial approach for explainable ai in intrusion detection systems,” in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, pp. 3237–3243, 2018.

[26] M. T. Ribeiro, S. Singh, and C. Guestrin, “"why should i trust you?":Explaining the predictions of any classifier,” in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD ’16, (New York, NY, USA), p. 1135–1144, Association for Computing Machinery, 2016.

[27] A. Shrikumar, P. Greenside, A. Shcherbina, and A. Kundaje, “Not just a black box: Learning important features through propagating activation differences,” ArXiv, vol. abs/1605.01713, 2016.

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

[29]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.

[30] 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.

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

[32]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.

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

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

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

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

[37] 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