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

A NOVEL INTRUSION DETECTION SYSTEM (IDS) FOR MULTI-CLASS CLASSIFICATION YARS-IDS

K BHASKAR[1], A R SNEHA[2], A DHANASEKHAR REDDY[3], G DAKSHAYANI[4]
[1]Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: bhaskark.mca@gmail.com
[2]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: rajamaniraja31@gmail.com
[3]Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: dhanasekhar918@gmail.com
[4]Assistant Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: gdakshayani9@gmail.com

Abstract: Intrusion Detection Systems (IDS) are urgent to digital guards in the present advanced world. Two new IDSs utilizing Deep Learning (DL) for multi-class cybersecurity arrangement are presented in this review. The primary IDS utilizes LuNet and Bi-LSTM structures, while the second purposes TCN, CNN, and Bi-LSTM. The two models are thoroughly prepared and tried utilizing benchmark datasets like NSL-KDD and UNSW-NB15, with an emphasis on the last option. Results exhibit that the recommended IDSs outflank customary Machine Learning (ML)-based approaches and a few current DL models in classification accuracy and detection rates. The basic paper's CNN utilizing Consolidated Nearest Neighbor resampling was effective, however this upgrade further develops execution utilizing ensemble draws near. Consolidating forecasts from different models, particularly CNN + BiLSTM and CNN + LSTM, expands accuracy to close to 100%. This exploration broadens IDS and shows the helpfulness of ensemble approaches in cybersecurity arrangements, recommending future examination and improvement.

Index Terms: SMOTE, IDS, CNN, Bi-LSTM, ML, DL, TCN

1. INTRODUCTION

Web and related advancements are fundamental for present day life in the present connected society. With individuals progressively involving web based contraptions and administrations for everyday undertakings, computerized resource security is a top need. In this evolving climate, digital dangers undermine basic information uprightness and privacy. In this present circumstance, Intrusion Detection Systems (IDS) become significant.[23]

An IDS is a vigilant gatekeeper against the many dangers and attacks that target computerized organizations and frameworks. An IDS's fundamental objective is to distinguish unapproved or noxious organization action and deal ideal notices to lessen hurt. IDSs match examples and information from many sources and organization information to distinguish distorted action that might show an assault.

An IDS's viability relies upon its ability to adjust to the always showing signs of change digital danger situation. Gathering huge measures of information for preparing is a significant snag to building a solid Network Intrusion Detection (NID) system. The IDS figures out how to recognize harmless organization traffic from perilous activities utilizing this information. Customary IDS advancement techniques

ISSN 2347–3657

Volume 12, Issue 3, 2024

incorporate Machine Learning (ML) and Deep Learning (DL).

The intricacy and refinement of new digital dangers have uncovered the deficiencies of exemplary ML-based IDS frameworks lately. Perceiving the constraints of ordinary procedures, DL methods are being utilized to further develop IDSs. DL gives further developed and versatile strategies for spotting network information examples and anomalies, upsetting IDS advancement.

The examination being talked about presents two special DL-based IDS models, YARS-IDS and YARS-IDS-II. These models offer better digital danger location and alleviation than standard ML-based procedures. Using state of the art DL structures, YARS-IDS and YARS-IDS-II were completely prepared and assessed on NSL-KDD and UNSW-NB15 benchmark datasets.

The appraisal discoveries show that DL-based IDS models outflank ML-based models. YARS-IDS and YARS-IDS-II are modern network safety frameworks that can deal with complicated and creating dangers with further developed classification accuracy and detection rates.

Past reproducing laid out approaches, the drive presents imaginative IDS building overhauls. YARS-IDS-II purposes a Temporal Convolutional Network (TCN) to record and assess network information transient elements. By thinking about digital dangers' transient aspect, YARS-IDS-II turns out to be more versatile and delicate to dynamic assault vectors, working on its certifiable viability.

The review stresses the importance of IDSs in safeguarding advanced resources in an undeniably connected climate. The venture presents new DL-based IDS models and building moves up to deal with contemporary digital dangers and give an investigate the eventual fate of online protection.[25]

2. LITERATURE SURVEY

Dali, L., Bentajer, A., Abdelmajid, E., Abouelmehdi, K., Elsayed, H., Fatiha, E., and Abderahim, B. (2015) Intrusion detection system study. second World Symposium on Web Applications and Networking (WSWAN), 1-6. This study surveys Intrusion Detection Systems (IDS) in web-based applications and systems administration. The need of IDS in safeguarding computerized resources from digital assaults is talked about. The article depicts IDS innovation's turn of events and convenience in assault discovery and moderation. Signature-based, anomaly-based, and hybrid IDS are examined, alongside their advantages and disadvantages. Also, the review tends to IDS concerns such the necessity for exact and fast identification frameworks. This study gives an outline of IDS and lays out the system for future exploration.

S. Gore and A. S. Ashoor (2011). IDS significance. Global Diary of Logical and Designing Exploration 2(1):1-4. This article stresses IDS in current network protection. It features the significance of IDS in distinguishing and halting undesirable access and hurtful movement in PC organizations. The article investigates IDS administrations such continuous checking, log examination, and caution creating. It underscores the meaning of proactive protection from digital assaults. By and large, this article gives a

ISSN 2347–3657

Volume 12, Issue 3, 2024

compact outline of IDS's part in present day online protection.

Yao-X Meng (2011). Network anomaly ID utilizing ML. 2011 Global Gathering on ML and AI, 2:576-581. This study looks at ML for network anomaly intrusion detection. Carrying out ML procedures for IDS presents reasonable impediments and concerns. The review portrays IDS ML techniques such decision trees, neural networks, and support vector machines. IDS feature selection and model assessment are likewise analyzed. The concentrate additionally features ML based IDS impediments and possible methodologies. This study enlightens the items of common sense of ML ID.

Alanazi, H. O., Noor, R. M., Zaidan, B. B., and A. A. (2010). Outline of ID. This article covers IDS and online protection exhaustively. It covers ID strategies, execution strategies, and fundamental IDS standards. The concentrate likewise talks about network-based IDS (NIDS) and host-based IDS (HIDS) and its upsides and downsides. It likewise analyzes IDS's hardships perceiving and battling new dangers in unique organization settings. This archive is helpful for concentrating on IDS thoughts and strategies.

R. C. Bhagat, S. S. Patil (2015). Improved destroyed procedure for unequal large information arrangement utilizing random forest. 2015 IEEE IACC, 403-408. This work further develops SMOTE (Synthetic Minority Over-sampling Technique) to deal with class irregularity in tremendous information order difficulties. The exploration utilizes the random forest classifier and adjusted SMOTE calculation to work on uneven dataset arrangement. It depicts the methodology's execution and confirms its adequacy utilizing true information. Trial discoveries show that the altered SMOTE calculation further develops classification accuracy and diminishes class unevenness. This examination further develops lopsided enormous data classification strategies.[27]

Khan, F. A., Gumaei, Derhab, and Hussain (2019). A novel two-stage DL model for successful NID. IEEE Access 7, 30373-30385. This exploration presents a two-stage DL approach for viable NID. The model purposes CNNs and LSTM organizations to catch geological and worldly connections in network traffic information. It portrays the model's plan and execution and breaks down its presentation utilizing benchmark datasets. The exploratory discoveries show that the two-stage DL model beats existing ID techniques in exactness and misleading positive rate. Generally, this article propels DL-based NID.

In 2021, Agarwal and Sharma distributed. ML ID and exactness characterization model. Software engineering PeerJ. An ML order model for dependable ID is introduced in this paper. The order model purposes decision trees, random forests, and support vector machines, and the paper portrays its plan and execution. The model is prepared and surveyed utilizing benchmark datasets to distinguish interruptions and limit bogus up-sides. Trial discoveries show that the proposed characterization model performs ID errands with great exactness and unwavering quality. This examination propels ML based digital protection answers for PC organizations.

Toupas, P., Chamou, D., Giannoutakis, K. M., Drosou, A., and Tzovaras, D [2019]. DNN-based multi-class ID. 1253-1258, 2019 IEEE International Conference On Machine Learning And Applications (ICMLA).

ISSN 2347–3657

Volume 12, Issue 3, 2024

An IDS utilizing DNN to order network traffic information by class is introduced in this review. The IDS design utilizes CNNs and RNNs to extricate includes and arrange network traffic into a few interruption characterizations. IDS plan, execution, and benchmark dataset execution are shrouded in the review. DNN-based IDS effectively characterizes network traffic and distinguishes interruptions across numerous arrangements, as per tests. In general, this article progresses DL-based ID in confounded network settings.

3. METHODOLOGY

a) Proposed Work:

The recommended review proposes YARS-IDS, a clever Intrusion Detection System (IDS) for multi-class online protection order. YARS-IDS utilizes LuNet[12], Bi-LSTM, TCN, and CNN, which are state of the art DL designs. This blend of creative designs further develops include portrayal and model refinement, propelling ID advances. YARS-IDS[3] can distinguish and arrange multi-class intrusion occasions with uncommon exactness and productivity by taking advantage of every engineering's abilities. The recommended IDS will advance the business and further develop network safety.

b) System Architecture:

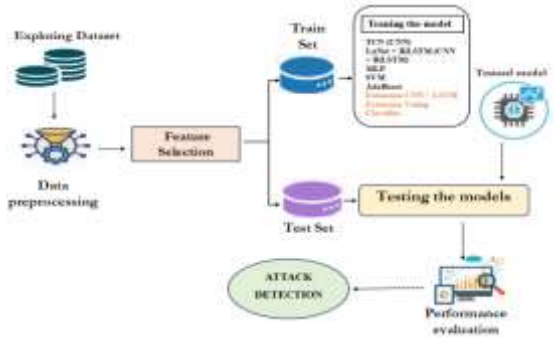


Fig1 Proposed Architecture

The system architecture gives a total establishment to creating and testing new ID models. It starts with a dataset examination to grasp its properties, laying out the preparation for additional means. Preprocessing the information cleans and standardizes it for model preparation.

Design depends on include choice to work on model productivity by finding and separating pertinent dataset qualities. This stage lessens dimensionality, working on the model's ability to recognize false organization information.

The preparation step utilizes TCN, LeNet+BiLSTM, MLP, SVM[12], and AdaBoost. These models are thoroughly prepared on a specific preparation dataset to exploit their plans. The testing step assesses model accuracy, precision, recall, and F1-score utilizing a free test dataset.[29]

At last, attack detection systems utilize prepared models to perceive and order interruption occasions progressively network information. The ID'S common sense relies upon this, ensuring fast and exact security danger reactions. Information investigation, preprocessing, model preparation, testing, and ongoing assault recognition are consistently

International Journal of Information Technology & Computer Engineering

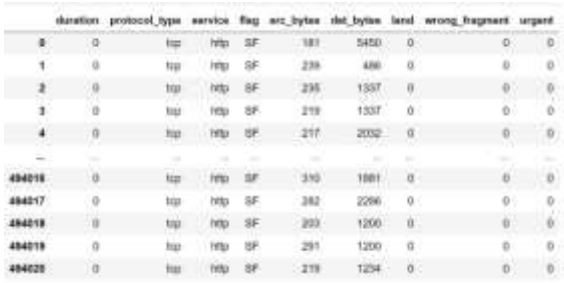
ISSN 2347–3657

Volume 12, Issue 3, 2024

coordinated in the framework engineering to foster interruption discovery innovation.

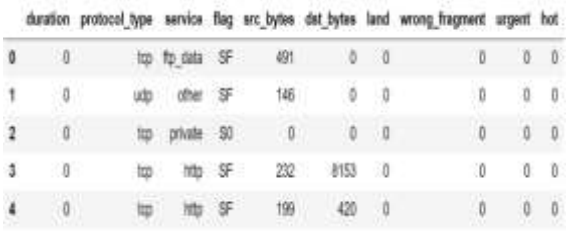
c) Dataset:

Three significant benchmarks — KDDCUP99, NSL KDD, and UNSW-NB15 — were utilized to test YARS-IDS. UNSW-NB15 covers an extensive variety of current organization dangers with two principal classifications: typical information tests and assault occasions, the last option of which has nine subcategories. The UNSW lab incorporates this dataset utilizing IXIA PerfectStorm to mimic organization traffic. Its 49 traits catch network parcel properties, making intrusion detection appraisal rich. Conversely, NSL-KDD[11] refines KDDCUP99 to dispense with overt repetitiveness. With 42 extricated qualities, it covers Dos, Test, U2R, and R2L assaults. NSL-KDD doesn't address current low-impression attacks. UNSW-NB15 has a bigger number of elements and IP addresses than NSL-KDD, giving a more complete proving ground for the model's viability against both customary and current interruption strategies.



	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent
0	0	tcp	http	SF	181	5450	0	0	0
1	0	tcp	http	SF	239	486	0	0	0
2	0	tcp	http	SF	235	1337	0	0	0
3	0	tcp	http	SF	219	1337	0	0	0
4	0	tcp	http	SF	217	2032	0	0	0
...	...	...	...	...	...	...	...	...	...
494018	0	tcp	http	SF	310	1881	0	0	0
494017	0	tcp	http	SF	282	2286	0	0	0
494019	0	tcp	http	SF	203	1200	0	0	0
494019	0	tcp	http	SF	291	1200	0	0	0
494020	0	tcp	http	SF	219	1234	0	0	0

Fig 2 KDD CUP 99 Dataset



	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 3 NSLL KDD Dataset

	id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	...	ct_dst_sport_l
0	1	0.000011	udp	-	INT	2	0	496	0	90909.0902	...	
1	2	0.000008	udp	-	INT	2	0	1762	0	125000.0003	...	
2	3	0.000005	udp	-	INT	2	0	1068	0	200000.0051	...	
3	4	0.000006	udp	-	INT	2	0	900	0	166666.6608	...	
4	5	0.000010	udp	-	INT	2	0	2126	0	100000.0025	...	

Fig 4 UNSW-NB15 Dataset

d) Data processing:

Pandas DataFrame: Data processing starts with Pandas DataFrames, adaptable designs required for even information control and examination. Pandas smoothes out dataset planning and element designing. Pandas smoothes out information purifying, change, and conglomeration, making the preparation for displaying.

Keras DataFrame: Pandas DataFrames and Keras, a solid DL tool compartment, effectively incorporate to further develop DL model data processing. Data processingand model preparation might be effectively connected with Keras DataFrames, improving on process and upgrading efficiency. Keras' undeniable level NN interface improves on information pretreatment and model creation.

Dropping Unwanted Columns: Removing unneeded columns from a dataset is vital for data processing. Dropping unnecessary sections smoothes out

ISSN 2347–3657

Volume 12, Issue 3, 2024

information by eliminating components that are irrelevant to displaying or may produce clamor. Disposing of unnecessary segments enhances the dataset for examination and model preparation, supporting execution and interpretability. Further developed input information prompts more exact and dependable model forecasts.

e) Visualization:

Seaborn and Matplotlib, two Python bundles that make wonderful and useful diagrams, empower data visualization. Seaborn's significant level connection point produces alluring and reasonable measurable visuals of information disseminations, variable cooperations, and potential examples. Matplotlib permits careful perception customisation with its adaptability and customization prospects. These libraries permit the development of useful diagrams that assist with appreciating the dataset's design and properties.[30]

f) Label Encoding:

Many ML strategies require name encoding to make an interpretation of classification marks to numbers. Utilizing Scikit-learn's LabelEncoder, straight out input is changed over completely to mathematical portrayals for model preparation. This stage works on all out factor taking care of and permits the ML pipeline to involve such information for more intensive examination and model development.

g) Feature Selection:

Model execution and interpretability rely upon feature selection. Along with Common Data Order, Scikit-learn's SelectPercentile procedure tracks down the most educational elements for model preparation. Common data scores factors' shared reliance and picks significant attributes. Just the main indicators are kept up with by picking the top percentile of factors in view of their scores, working on the model's feedback space and working on its prescient power.

h) Algorithms:

TCN (Temporal Convolutional Network): TCN, a sequential data processing deep learning framework, catches worldly connections well. TCN actually catches long-range connections utilizing convolutional layers with expanded convolutions, making it ideal for time-series information investigation. TCN assists YARS-IDS with detect intrusions by expanding the model's transient example information on network information.

LuNet + BiLSTM (CNN + BiLSTM): LuNet joins CNN and BiLSTM abilities. CNNs remove spatial elements well, while BiLSTMs gather consecutive information bidirectionally. In YARS-IDS[3], this crossover configuration further develops the model's spatial and successive example understanding in intrusion detection errands, improving execution.

MLP (Multi-Layer Perceptron): Multi-Layer Perceptron (MLP) is a feedforward neural network with numerous neurons. MLPs comprehend muddled information examples and relationships in light of the fact that every neuron associates with each neuron in the following layer. MLPs [12] might learn refined highlight connections to arrange network dangers in YARS-IDS alone or in an ensemble.

SVM (Support Vector Machine): SVM, a typical supervised learning strategy, succeeds in order. SVMs

ISSN 2347–3657

Volume 12, Issue 3, 2024

succeed at taking care of high-layered information by recognizing the best hyperplane that isolates include classes with a most extreme edge. SVMs [12] might be compelling classifiers for binary or multiclass network attack arrangement in YARS-IDS.

AdaBoost (Adaptive Boosting): Ensemble learning strategy AdaBoost utilizes feeble students to produce a strong classifier. AdaBoost[12] works on model execution by iteratively changing misclassified occasion loads to target hard-to-group pieces of information. AdaBoost might be utilized as a group approach in YARS-IDS to join feeble classifiers to further develop intrusion detection.

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:

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

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

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.

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

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

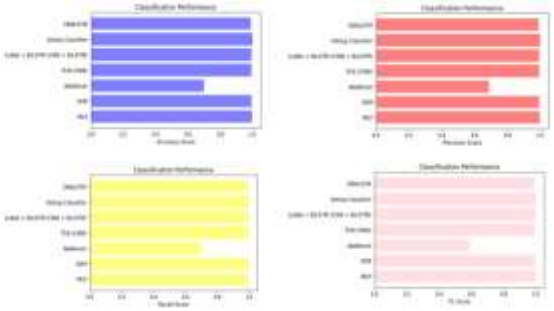
Precision: Precision estimates the level of positive cases or tests precisely sorted. Precision is determined utilizing the recipe:

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

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

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.

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



International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

Fig 5 Comparison Graphs of KDD CUP99 Dataset

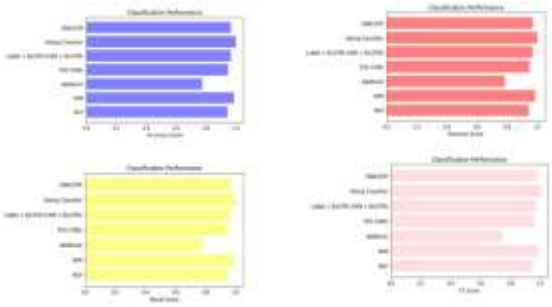


Fig 6 Comparison Graphs of NSL KDD Dataset

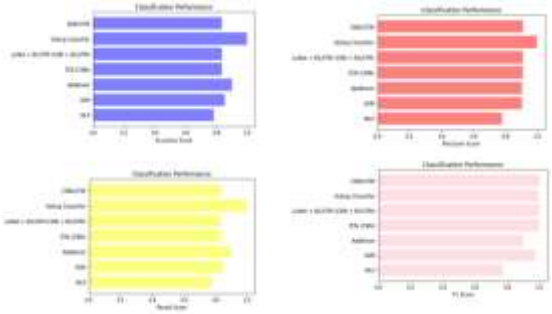


Fig 7 Comparison Graphs of UNSW-NB15 Dataset

ML Model	Accuracy	f1_score	Recall	Precision
MLP	0.999	0.999	0.999	0.999
SVM	0.995	0.995	0.995	0.995
AdaBoost	0.701	0.699	0.701	0.699
TCN (CNN)	0.995	0.995	0.995	0.995
LeNet + BiLSTM (CNN + BiLSTM)	0.995	0.996	0.995	0.996
Extension Voting Classifier	1.000	1.000	1.000	1.000
Extension CNN+LSTM	0.992	0.992	0.992	0.992

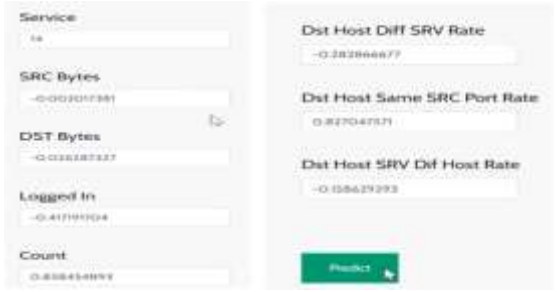
Fig 8 Performance Evaluation Table

Fig 9 Registration Page

Fig 10 Login Page

Fig 11 Main Page

Fig 12 For KDD CUP99



International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

Fig 13 Upload Input Data

Fig 14 Predicted Results

Fig 15 For NSL KDD

Fig 16 Upload Input Data

Fig 17 Final Outcome

Fig 18 For UNSW-NB15

Fig 19 Upload Input Data

Fig 20 Final Outcome

5. CONCLUSION

Contrasted with traditional ML and other DL techniques, the recommended YARS-IDS and YARS-IDS-II[3] models further develop interruption recognition. These models have shown great classification accuracy and detection rates on benchmark datasets like NSL-KDD[11] and UNSW-NB15[9], demonstrating their helpfulness in ordering network intrusions. Ensemble approaches like the Voting Classifier (RF+AB) and hybrid models like

CNN+LSTM have worked on the models' exactness and versatility, with the Voting Classifier getting 100 percent precision for the KDDCUP99 dataset. A Flask-based front connection point improves on testing and interaction, making model execution assessment simple.[32]

6. FUTURE SCOPE

The introduced models show guarantee, however further review is required. Explicit assault classes, for example, UNSW-NB15 examination and secondary passage classes and NSL-KDD U2R class, can be improved by tending to execution limitations. Future work remembers testing the models for reenacted or certifiable settings. Investigating strategies for further developing execution and versatility and further developing the UI for convenience are additionally encouraging.

REFERENCES

[1] L. Dali, A. Bentajer, E. Abdelmajid, K. Abouelmehdi, H. Elsayed, E. Fatiha, B. Abderahim, A survey of intrusion detection system, in: 2015 2nd World Symposium on Web Applications and Networking (WSWAN), 2015, pp. 1–6. doi:10.1109/WSWAN.2015.7210351.

[2] A. S. Ashoor, S. Gore, Importance of intrusion detection system (ids), International Journal of Scientific and Engineering Research 2 (1) (2011) 1–4.

[3] Y.-X. Meng, The practice on using machine learning for network anomaly intrusion detection, in: 2011 International Conference on Machine Learning and Cybernetics, Vol. 2, 2011, pp. 576–581. doi: 10.1109/ICMLC.2011.6016798.

[4] H. O. Alanazi, R. M. Noor, B. B. Zaidan, A. A. Zaidan, Intrusion detection system: Overview (2010). doi:10.48550/ARXIV.1002.4047. URL https://arxiv.org/abs/1002.4047

[5] R. C. Bhagat, S. S. Patil, Enhanced smote algorithm for classification of imbalanced big-data using random forest, in: 2015 IEEE International Advance Computing Conference (IACC), 2015, pp. 403–408. doi: 10.1109/IADCC.2015.7154739.

[6] F. A. Khan, A. Gumaei, A. Derhab, A. Hussain, A novel two-stage deep learning model for efficient network intrusion detection, IEEE Access 7 (2019) 30373–30385. doi:10.1109/ACCESS.2019.2899721.

[7] A. M. M. A. A. Agarwal A, Sharma P, Classification model for accuracy and intrusion detection using machine learning approach., PeerJ Computer Science (2021). doi:7:e437https://doi.org/10.7717/peerj-cs.437.

[8] P. Toupas, D. Chamou, K. M. Giannoutakis, A. Drosou, D. Tzovaras, An intrusion detection system for multi-class classification based on deep neural networks, in: 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), 2019, pp. 1253–1258. doi:10.1109/ICMLA.2019.00206.

[9] N. Moustafa, J. Slay, Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set), in: 2015 Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1–6. doi:10.1109/MilCIS.2015.7348942.

[10] IXIA Perfectstorm Tool (2017). URL http://downloads.ixiacom.com/library/user guides/IxOS/6.60 EA/ EA 6.60 Rev B/IxiaReferenceGuide/PerfectStorm.html

[11] N. Moustafa, B. Turnbull, K.-K. R. Choo, An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things, IEEE Internet of Things Journal 6 (3) (2019) 4815–4830. doi:10.1109/JIOT.2018.2871719.

[12] P. Wu, H. Guo, Lunet: A deep neural network for network intrusion detection, in: 2019 IEEE Symposium Series on Computational Intelligence (SSCI), 2019, pp. 617–624. doi:10.1109/ SSCI44817.2019.9003126.

[13] S. Wang, J. Cao, P. Yu, Deep learning for spatio-temporal data mining: A survey, IEEE Transactions on Knowledge and Data Engineering (2020) 1–1doi:10.1109/TKDE.2020.3025580.

[14] K. Pal, B. V. Patel, Data classification with k-fold cross validation and holdout accuracy estimation methods with 5 different machine learning techniques, in: 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 83–87. doi: 10.1109/ICCMC48092.2020.ICCMC-00016.

[15] F. Shakeel, A. S. Sabhitha, S. Sharma, Exploratory review on class imbalance problem: An overview, in: 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017, pp. 1–8. doi:10.1109/ICCCNT.2017.8204150.

[16] T. E. Tallo, A. Musdholifah, The implementation of genetic algorithm in smote (synthetic minority oversampling technique) for handling imbalanced dataset problem, in: 2018 4th International Conference on Science and Technology (ICST), 2018, pp. 1–4. doi:10.1109/ ICSTC.2018.8528591.

[17] W. Satriaji, R. Kusumaningrum, Effect of synthetic minority oversampling technique (smote), feature representation, and classification algorithm on imbalanced sentiment analysis, in: 2018 2nd International Conference on Informatics and Computational Sciences (ICICoS), 2018, pp. 1–5. doi:10.1109/ICICOS.2018.8621648.

[18] C. Lea, M. D. Flynn, R. Vidal, A. Reiter, G. D. Hager, Temporal convolutional networks for action segmentation and detection, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017.

[19] K. S. Rana, L.-W. Chen, L.-H. Tang, W.-T. Hong, A study on speech enhancement using deep temporal convolutional neural network, in: 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2021, pp. 1–2. doi:10.1109/ ICCE-TW52618.2021.9602920.

[20] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, M. Zhu, Hastids: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection, IEEE Access 6 (2018) 1792– 1806. doi:10.1109/ACCESS.2017.2780250.

[21] F. Z. Belgrana, N. Benamrane, M. A. Hamaida, A. Mohamed Chaabani, A. Taleb-Ahmed, Network intrusion detection system using neural network and condensed nearest neighbors with selection of nsl-kdd

influencing features, in: 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), 2021, pp. 23–29. doi:10.1109/IoTaIS50849.2021.9359689.

[22] U. S. Musa, M. Chhabra, A. Ali, M. Kaur, Intrusion detection system using machine learning techniques: A review, in: 2020 International Conference on Smart Electronics and Communication (ICOSEC), 2020, pp. 149–155. doi:10.1109/ICOSEC49089.2020.9215333.

Dataset Links:

NSL – KDD:

https://www.kaggle.com/datasets/kaggleprollc/nsl-kdd99-dataset

KDD-CUP:

https://www.kaggle.com/datasets/galaxyh/kdd-cup-1999-data

UNSW-15-NB:

https://www.kaggle.com/datasets/sweety18/unsw-nb15-training

[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,

ISSN 2347–3657

Volume 12, Issue 3, 2024

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