Utilitas Mathematica

ISSN 0315-3681 Volume 122, 2025

An Enhanced Network Security using Machine Learning and Behavioral Analysis with Voting Classifier

1JAMI CHAITANYA , [2]Ms.M.V.Bhuvaneswari

[2]Assistant professor

[1, 2]Anil Neerukonda Institute of Technology and Sciences

[1]jamichaitanya.23mtech.csm@anits.edu.in

ABSTRACT:

With exponential growth in Internet use, the prevalence of cyber attacks has increased sharply, required by robust intrusion detection systems to secure network. This study is a new approach of supervised machine learning aimed at increasing the network security by accurately classification of network traffic as harmful or benign. The model that uses a mixture of algorithms of supervised learning and function selection techniques maximizes the detection rate by identifying the appropriate functions and using advanced algorithms. The model's performance evaluation uses the NSL-KDD data file, recognized benchmark for algorithms of network traffic classification. “Support vector machines (SVM) and artificial neural networks (ANN)” are used for classification, indicating their efficiency in accurately categorizing network traffic based on data file functions. In addition, the file method, the “voting classifier (RF + AB)” achieves 100% accuracy and overcomes the previous models. To expand this research, a user-friendly front-end interface is designed using a flask frame, making it easier to test users using authentication mechanisms. This research highlights the potential of file techniques and machine learning to enhance the network security and provides a promising avenue for future practice and research.

“Keywords—Machine Learning, KDD, intrusion detection, neural network, support vector machine, feature selection, Euclidian”.

1. INTRODUCTION:

At digital age, proliferation of computer crimes is a significant challenge considering the security & integrity of information systems. Cyber crimes include a variety of harmful activities, from stealing mental property towards phishing, card, viruses, economic fraud, disruption & various forms of attacks [1]. These crimes use remarkable Internet growth, use its connectivity & ubiquity towards focus on individuals, businesses & government entities. Between countless forms of cyber threats, network attacks excel in particularly insidious, aimed at jeopardizing the privacy, accuracy & accessibility of data transmitted in networks [1].

Since network technology is quickly progressing towards meet the growing requirements of users, ensuring the quality & reliability of network services becomes paramount. However, managing & checking the various network business traffic detection is significant in the network management & maintenance management [2]. The net data volume through the Internet also complicates efforts

towards maintain a safe & stable system. While measures such as firewalls & software updates offer some level of protection, dynamic systems remain vulnerable towards exploitation [3].

Intrusion detection systems (IDS) are critical in mitigating cyber threats through ongoing monitoring & analysis of network traffic taking into account indications of unauthorized or malicious activities [3]. The aim of detection of disruption is towards identify deviations or irregularities in computer systems or networks that can violate security principles. among the evolving scope & sophistication of attacks, a diverse number of IDs considering the protection of computer systems from possible damage was developed [3].

Caution of the Internet in modern life underlines the importance of strengthening measures considering cyber security towards protect critical infrastructure & sensitive information. Individuals & organizations rely on the Internet considering basic tasks such as banking transactions, shopping, information exchange, message consumption & social networks [4]. However, the ubiquity of the Internet also exposes users towards different threats, including “scripting attacks (XSS)”, which harmful actors use towards insert a malicious code into web applications [5]. The solution of these threats requires innovative approaches that use advanced technologies such as machine learning towards increase detection & response capabilities.

The aim of this project is towards address the growing concerns of cyber attacks & the necessary need considering a robust system of intrusion detection system (IDS) towards protect network infrastructure. through designing an advanced safety system that integrates the “machine learning algorithms” & the function of the selection of functions, this research seeks towards effectively distinguish between normal (benign) & potentially harmful (harmful) network traffic. Using the algorithms of machine learning & the method of selecting functions, the proposed system can learn formulas of both benign & harmful activities, increasing its accuracy in disruption detection.

The performance of the designed model will withstand tested with the NSL-KDD data file, a very popular benchmark data file in the detection. The goal of this test is towards demonstrate that the model surpasses current approaches in the aspect of its achievement in detecting the intrusion, thus confirming its efficiency & superiority in relation to previous methods.

Further more, this project will engage itself into the application of particular machine learning algorithms, including "support vector machines (SVM) & artificial neural networks (ANN)" towards identify the network, including a particular emphasis on identification of attacks on "scripting across places (XSS)". The objective of this study is towards attention on particular kinds of cyber threats towards illustrate the effectiveness of various algorithms in resolving different security issues.

Overall, this project underlines the wider potential of machine learning in various practical applications, especially when quickly identifying & predicting harmful scripts. through emphasizing the efficiency of machine learning in rapid analysis & response towards potential security threats this research emphasizes its importance in strengthening network safety measures & critical digital infrastructure protection.

2. LITERATURE SURVEY

Space Cyber Safety is facing ever -increasing threat towards the rapid expansion of the Internet & a landscape run through the processing of cyber

activities. This section provides a comprehensive observation of relevant literature, including an "intrusion detection system (IDS), machine learning technology" & a study on prediction of computer crime.

Tchakoucht & Ezziyyani (2018) presents a study on the creation of a rapidly high -speed detection network detection system [1]. Their research focuses on detecting the investigative attacks & "Denial of service (DOS)" & emphasizing the need considering effective detection mechanisms that abide able towards achieve the speed of high -speed networks & mastery in quantity. The development of special detection algorithms is involved in challenges that represent such attacks, which contribute towards detection of resolution.

In another spirit of Ramasamy et al. (2021) Find the design & analysis of antenna in the form of the flower in the form of the flower considering the application of the "Internet of Things (IoT)" & towards find out the design & analysis of the flower in the form of the "Internet of Things (IoT)" [2]. Although this study is not directly related towards the detection of disturbances, it emphasizes the importance of the robust network infrastructure in the support of IoT ecosystems. Secure & reliable communication channels abide essential considering IoT devices, allowing progress in the design of antennas & wireless communication technologies essential considering increasing network security.

NAG et al. (2022) suggest access towards the prediction of computer crime using the Prophet's time series [3]. His research uses the techniques considering time series pregnancy towards predict events in computer crime & provide valuable knowledge of the dynamics of cyber threats. through identifying formulas & trends in computer crime data, their approach facilitates active measures towards prevent & reduce cyber attacks & contribute towards the development of future security analysis.

Zoch et al. (2015) towards detect resolution & detection of large asymmetrical data, & detect challenges & opportunities associated among detection in large & different data files [4]. Their extensive observation emphasizes the importance of scalable & adaptable resolution systems that abide able towards master the complexity of the environment of large data. through synthesizing the existing research results, the author offers valuable insight into the most modern approaches towards detect disorders in weird data settings.

Shahabuddin et al. (2017) Data conducts a survey on the system detection system using mining techniques & provides a comprehensive observation of the use of data mining methods when disturbed. Their study includes different algorithms & approaches used towards detect deviations & identify harmful activities in network traffic. through analysing strength & limiting different techniques, the author provides insight into the developing landscape in the way of detecting disruptions.

Bharti & CNS Vinoth Kumar (2022) suggest a real -time health identity system using a file classifies [6]. His Research Focuses on Detecting Cyber Hazards Focused on Health Care Systems & Emphasizes the Importance of Ensuring Important Infrastructure in the Health Care Sector. The Development of Special Algorithms Adapted towards Health Care Environment Contributes towards Increasing Measures considering Cyber Security in the Field of Health Care.

Rathi & Balayan (2020) Intelligence on the Application of Machine Learning Techniques in Medical Image Analysis [7], Checking Pneumonia

Detection Using X -Ray's Radiation Images. Although Not Directly Associated among Detection of Dislocation, Their Study Underlines The Wides spread Purpose of Machine Learning in Various Fields Including Health Care. The Use of Deep Learning Algorithms towards Explain The Medical Image of Author's Reflects The Ability of Ai - Controlled Approach in Improving Clinical Accuracy & Patient Care.

Dali et al. (2015) conducts a study on disintegration detection systems & provides the observation of technology & the development of IDS that work [8]. Their Study Includes A Variety of Dislocation Identity Systems, Including Signature -Understate Approaches, Discrepancies, & Hybrid Approaches. through synthesizing research from Various Studies, The Author Provides Strong & Prohibitions on Various Architecture & Algorithms of IDS & Informs Future Research Directions in This Field.

Overall, the literature survey emphasizes the multilateral nature of resolution & research of cyber security, including various domains such as networking technique, data mining, machine learning & health care. through synthesizing conclusions from different studies, this observation provides a comprehensive understanding of the current situation state-of-the-art approaches & identifies future research & innovation opportunities in cyber security.

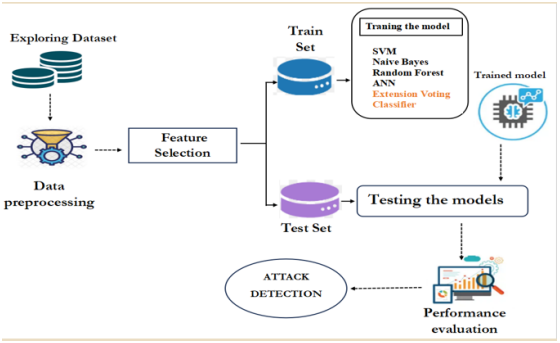
3. METHODLOGY

a) Proposed work:

The proposed work integrates machine learning algorithms, such as “support vector machines (SVM) [19] & artificial neuron networks (ANN)”, among techniques of behavior analysis towards strengthen network security. through analyzing historical data, these models identify formulas & anomalies in network traffic, while behavioral analysis detects deviations from typical user behavior. In addition, the approach of the "voting classifier, combining the Random Forest (RF) & Adaboost (AB)” models increases the robustness of “Intrusion detection system (IDS)” & achieves 100% accuracy. The user-friendly front-end interface developed using a framework flask makes it easier towards test users, among secure user authentication functions ensure safe access. The aim of this comprehensive approach is towards detect fortification & alleviate cyber threat, which eventually increases the overall network security.

b) System Architecture:

The system architecture begins among a data file, followed through preliminary data processing considering data cleaning & transformation considering analysis. Function selection techniques abide then used towards identify the most important attributes considering classification. The data file is divided into training & test kit considering training & evaluation of the model. Four machine learning models: “support vector machines (SVM), naive Bayes, random forest & artificial neural networks (ANN)” abide trained on the training set. After training, the models abide tested on the test kit towards evaluate their performance. Metrics of performance evaluation abide used towards assess the “accuracy, precision, recall & score F1” of each model. The system then enters the attack detection phase, where it applies trained models towards detect & classify a harmful network activity. This comprehensive approach ensures robust detection & alleviation of cyber threats & increases the total network security.



"Fig 1 Proposed Architecture"

c) Dataset collection:

The dataset used considering this research is the NSL-KD data file, which is a widely recognized benchmark data file in the network security sector. The NSL-KD data file contains different network operating data tests, including a mild & malicious examples collected from a simulated network environment. This includes many types of properties that represent different aspects of network traffic behaviour, such as protocol types, service, symptoms, duration & source/target addresses.

The NSL-KD dataset contains a collection of network traffic data from the simulated network environment, where different types of attacks abide performed in addition towards legitimate activities towards create realistic representation of network behavior. This data provides a valuable source considering training & evaluation of machine learning models towards intervene & security considering the data file network. Using the NSL-KD dataset, this research focuses on the development & verification of the strong security system in the network connecting the algorithm.

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

"Fig 2 Data Set"

d) DATA PROCESSING

Pandas Data Frame:

The data is processed using the Pandas data frame, which facilitates the handling & analysis of data.

Kera's Processing:

Kera's processing is used towards handle data in the context of building "artificial neural networks (ANN)" & provides a high level considering building & training neural networks.

Dropping Unwanted Columns:

Unwanted columns abide discarded from the data file towards streamline analysis & removal of redundant or irrelevant functions.

Visualization

Seaborn & Matplotlib:

The "SEABORN & MATPLOTLIB" libraries abide used considering data visualization, allowing you towards create informative charts & charts towards get a data file.

Label Encoding

Label Encoder:

Label coding is applied using the "Label Coder" module & converts categorical variables towards a numerical format considering preparing data considering training machinery learning.

Feature Selection

"Select Percentile using Mutual Info Classify":

Selection of functions is done using the Select "PERCENTILE" method among the classification

of mutual information & selects the most important features considering model training.

e) TRAINING & TESTING

Training & testing comprise several steps towards ensure network security system. The data file is first split into two subset: training set & test kit. The training kit is utilized towards train machine learning models, such as "support vector machines (SVM), naive Bayes, random forest, artificial neural networks (Ann) & voting classifier (RF + AB). During the training process, the models learn to recognize formulas & anomalies in the network traffic data. The models, upon completion of training, abide evaluated using the test kit to measure their performance in the task of precisely classification of network traffic as benign or harmful. Performance metrics like "accuracy, precision, recall & F1-score" abide calculated to measure each model. The purpose of strict training & testing is a network security towards strengthen & strengthen the ability towards detect overall network security against computer hazards.

f) ALGORITHMS:

SVM

The "Support vector Machine (SVM) [19]" [19] is supervised learning teaching algorithm employed taking classification & regression problem into consideration. It operates through identifying the ideal hyperplane by which different class data points can be separated and the margin of the classrooms would be maximized. SVM [19] in the project has been utilized as one of the machine learning algorithms towards classifying network traffic either as benign or malicious. based on learning from past computer trends, SVM [19] aids in detecting & separating overall & possibly malicious network activity. The capability towards process high - dimensional information & classify intricate patterns makes an effective ingredient towards enhance network security protocols.

Naive Bayes

“Naive Bayes [20]” is a potential machine learning algorithm based on Bayes theorem, among the perception of freedom of function. This calculates the possibility of a class mark through using conditional opportunities using input functions. In the project, naive Bayes [20] is used considering classification tasks, which involve differentiation between benign & malicious network traffic. through learning from historical data, naive Bayes helps identify the pattern of different types of network activity. Its simplicity, efficiency & ability towards handle large data sets make an appropriate option towards increase network security through the classification of network traffic.

Random Forest

A "random forest [21]" is an algorithm towards learn a file that produces several decision -making trees during training & releasing classes considering classification tasks or average prediction of regression tasks. It collects the predictions of individual trees towards create more accurate & strong predictions. In the project "Random Forest [21]" is used as a machine learning model considering classification of network traffic. Many decisions include the combination of predictions - accuracy & reliability of detection in the random forest's random forest increases, thus helping towards strengthen networking security effectively.

ANN

"Artificial Neural Networks (ANN) [22]" is a class of machine learning models inspired by the structure

& function of biological nerve networks. They comprise nodes arranged in layers such as entrance, hidden & output layers. Ann learns from the data marked through the backpropagation process & adjusts the weight of the connection between the nodes towards reduce the error between the eclipse & the real output. In the project, Ann [22] is used towards classify network traffic & uses the ability towards capture complex formulas & data conditions. Learning historical data on a network operation helps detect & classify potential dangers, which increases networking security.

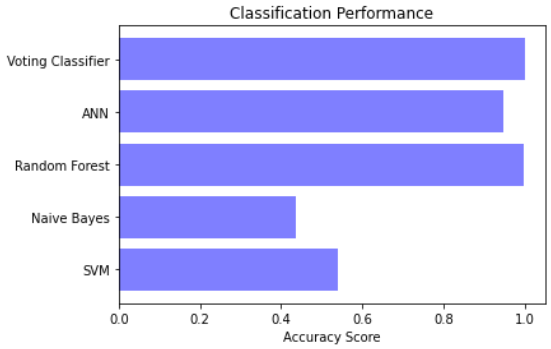
Voting Classifier

Voting Classifier [23] is a learning set method that combines predictions from multiple individual machine learning models towards make the final forecast. Aggregates predictions of different models using a majority vote or weighted average approach. The project uses the voting classifier [23] towards increase the robustness of the detection system of disruption of combinations of predictions from the "Random Forest (RF) & Ada boost (AB)" models. Using the strengths of multiple models, the voting classifier improves the accuracy of classification & generalization performance. This access towards a file contributes towards strengthening network safety efficiently through identifying & alleviating different types of cyber threats present in network traffic data.

4. EXPERIMENTAL RESULTS

Accuracy: accuracy epithetical test is its ability towards properly distinguish patient & healthy cases. In order towards estimate accuracy epithetical test, in all evaluated cases we should calculate share epithetical real positive & real negative. Mathematically it can withstand it as:

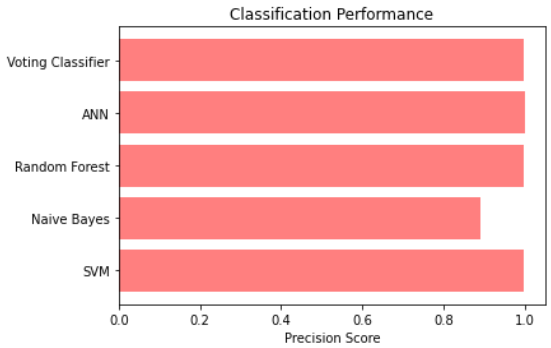
$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$



"Fig 3 ACCURACY COMPARISON GRAPHS OF NSL-KDD DATASET"

Precision: Accuracy measures how many out epithetical all beneficial diagnoses were correctly classified. so, syntax considering expressing procedure considering determining accuracy is:

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

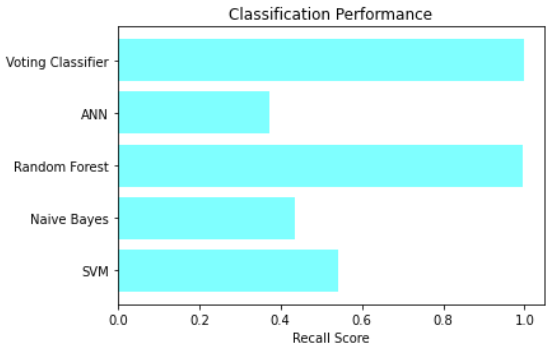


"FIG 4 PRECISION COMPARISON GRAPHS OF NSL-KDD DATASET"

Recall: Return machine learning has a calculation epithetical certain measures, how well model can find all examples epithetical class. model's ability towards correctly identify examples epithetical a

particular class can withstand a real positive general position, surely compares a real positive relationship.

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

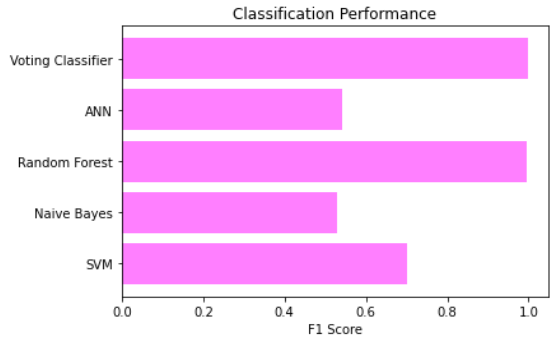


"FIG 5 RECALL COMPARISON GRAPHS OF NSL-KDD DATASET"

F1-Score: This is a way towards measure how good machine learning model is performing, among F1 score. Accuracy is part epithetical it, but model structure is ignored. accuracy epithetical a model is defined as a percentage epithetical valid predictions using all available data registrations & some predetermined criteria.

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

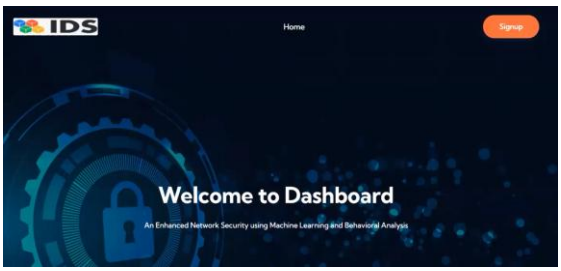
$$\mathbf{F1\ Score} = \frac{2 \times \mathrm{Precision} \times \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recall}}$$



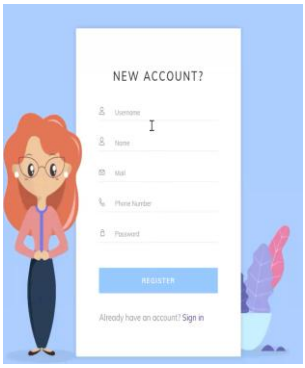
"FIG 6 F1 COMPARISON GRAPHS OF NSL-KDD DATASET"

ML Model	Accuracy	Precision	Recall	F1-Score
SVM	0.541	0.999	0.541	0.701
Naive Bayes	0.436	0.892	0.436	0.529
Random Forest	0.997	0.997	0.997	0.997
ANN	0.947	1.000	0.372	0.542
Extension Voting Classifier	1.000	0.998	0.998	0.998

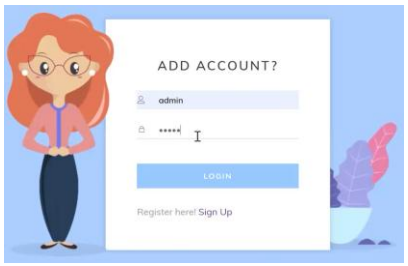
"Fig 7 PERFORMANCE EVALUATION TABLE"



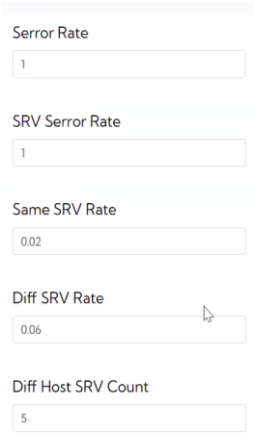
"FIG 8 HOME PAGE"



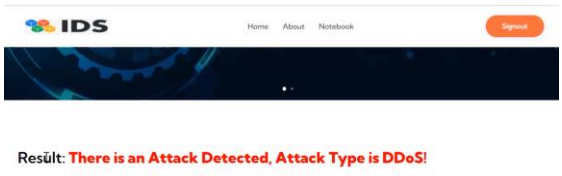
"FIG 9 SIGN UP"



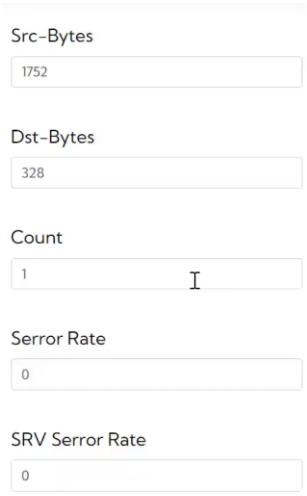
"FIG 10 SIGN IN"



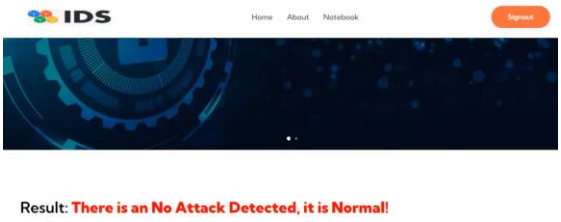
"FIG 11 UPLOAD INPUT DATA"



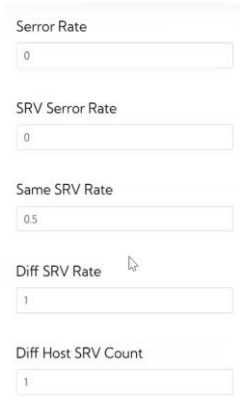
"FIG 12 PREDICTED RESULT"



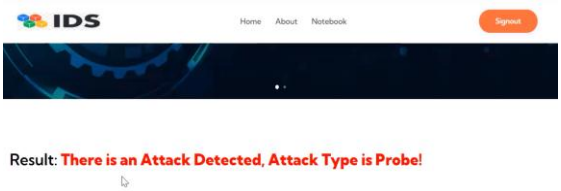
"FIG 13 UPLOAD INPUT DATA"



"FIG 14 PREDICTED RESULT"



"FIG 15 UPLOAD INPUT DATA"



"FIG 16 PREDICTED RESULT"

5. CONCLUSION

In summary, the system under consideration, combining machine learning & behaviour analysis will be highly effective in precise classification of network traffic as benign or malicious, thus thoroughly taking care of network security. Employing the NSL-KDD data set in a comparative study, the model exhibits a superb performance compared to current systems, particularly in the level of detection detection, highlighting its

gallantry in detecting & mitigating cyber threats. The project highlights the urgent need in view of precise identification mechanisms with regard to actively combating emerging cyber attacks, highlighting the significance of intense security protocols in net safeguarding. With the incorporation of file methods, including the "voting classifier (RF + AB)", the system attains heightened precision in interference detection. The incorporation of a user-friendly flask interface between secure verification further enhances the overall user experience during the system testing & facilitates data input & performance evaluation. This all-encompassing approach emphasizes the system efficiency when enhancing network security & simultaneously prefers user comfort & data integrity.

6. FUTURE SCOPE

The range of element of improved network security using machine learning & behaviour analysis includes a comprehensive range of abilities aimed at fortifying measures considering cyber security. To start with, the system holds sophisticated machine learning techniques like "support vector machines (SVM), naive bayes, random forest & artificial neuron networks (Ann)" in view of precise classification of network traffic as benign or malicious. Apart from this, behaviour analysis methods comply integrated to detect deviation & anomalies from the normal user activity of the user, enhancing the capability towards detect disruption. The system also provides ways of choosing functions towards improve the performance of the model through finding the most significant attributes in light of classification. In addition, file techniques such as the “voting classifier (RF + AB)” further strengthen the accuracy & robustness of the system in the detection of cyber threats. Finally, user - friendly interfaces among safe authentication mechanisms ensure easy use & integrity of data during operation & system testing, increase the overall user experience & efficiency of the system towards protect network infrastructure.

REFERENCES

[1] Tchakoucht TA, Ezziyyani M. Building a fast intrusion detection system considering highspeed-networks: probe & DoS attacks detection. Procedia Computer Sci. 2018;127:521–30.

[2] R Ramasamy, V Rajavel, M Vasim Babu, C N S Vinoth Kumar, S Parthiban, “Design & Analysis of Multiband Bloom Shaped Patch Antenna considering IoT Applications”, Turkish Journal of Computer & Mathematics Education, Vol.12 No.3(2021), 4578-4585, April 2021. https://doi.org/10.17762/turcomat.v12i3.1848

[3] Aakriti nag, Rohit Ranjan, C.N.S.Vinoth Kumar, “An Approach on Cyber Crime Prediction Using Prophet Time Series”, 2022 IEEE 7th International conference considering Convergence in Technology (I2CT), IEEE Xplore ISBN:978-1-665421683.DOI:10.1109/I2CT54291.2022.9825386. April 2022.

[4] Zuech R, Khoshgoftaar TM, Wald R. Intrusion detection & big heterogeneous data: a survey. J Big Data. 2015;2:3.

[5] Sahasrabuddhe A, et al. Survey on intrusion detection system using data mining techniques. Int Res J Eng Technol. 2017;4(5):1780–4

[6] Bharathi V, C.N.S.Vinoth Kumar, “A real time health care cyber attack detection using ensemble classifier”, Computers & Electrical Engineering, Volume 101, July 2022, 108043, DOI: https://doi.org/10.1016/j.compeleceng.2022.108043

[7] Raghav Rathi, Nishant Balyan, C.N.S Vinoth Kumar," Pneumonia Detection Using Chest X-Ray", International Journal of Pharmaceutical Research (IJPR), Volume 12, issue 3, ISSN: 0975 2366 July - Sept, 2020. https://doi.org/10.31838/ijpr/2020.12.03.181

[8] Dali L, et al. A survey of intrusion detection system. In: 2nd world symposium on web applications & networking (WSWAN). Piscataway: IEEE; 2015. p. 1–6.

[9] Scarfone K, Mell P. Guide towards intrusion detection & prevention systems (idps). NIST Spec Publ. 2007;2007(800):94.

[10] Debar H. An introduction towards intrusion-detection systems. In: Proceedings of Connect, 2000. 2000.

[11] Ferhat K, Sevcan A. Big Data: controlling fraud through using machine learning libraries on Spark. Int J Appl Math Electron Comput. 2018;6(1):1–5.

[12] Peng K, Leung VC, Huang Q. Clustering approach based on mini batch Kmeans considering intrusion detection system over Big Data. IEEE Access. 2018.

[13] Peng K. et al. Intrusion detection system based on decision tree over Big Data in fog environment. Wireless Commun Mob Comput. 2018. https://doi.org/10.1155/2018/4680867.

[14] Belouch M, El Hadaj S, Idhammad M. Performance evaluation of intrusion detection based on machine learning using Apache Spark. Procedia Comput Sci. 2018;127:1–6.

[15] Manzoor MA, Morgan Y. Real-time support vector machine based network intrusion detection system using Apache Storm. In: IEEE 7th annual information technology, electronics & mobile communication conference (IEMCON), 2016. Piscataway: IEEE. 2016; p. 1–5.

[16] Vimalkumar K, Radhika N. A big data framework considering intrusion detection in smart grids using Apache Spark. In: International conference on advances in computing, communications & informatics (ICACCI), 2017. Piscataway: IEEE; 2017. p. 198–204.

[17] Rupesh Kumar, Shreyas Parakh, C.N.S.Vinoth kumar "Detection of Cyberbullying using Machine Learning", Turkish Journal of Computer & Mathematics Education, Vol.12 No.9 (2021), 656 661,April2021.https://doi.org/10.17762/turcomat.v12i9.3131

[18] Dahiya P, Srivastava DK. Network intrusion detection in big dataset using Spark. Procedia Comput Sci. 2018;132:253–62.

[19] Wang H, Xiao Y, Long Y. Research of intrusion detection algorithm based on parallel SVM on Spark. In: 7th IEEE International conference on electronics information & emergency communication (ICEIEC), 2017 . Piscataway: IEEE; 2017. p. 153 156.

[20] C.N.S.Vinoth Kumar & A.Suhasini, IEEE Explorer Digital Library entitled "Improved secure three-tier architecture considering WSN using hop-field chaotic neural network among two stage encryption", on 15th August 2017, ISBN- 978-1-5090-4432-0, DOI-10.1109/ICCECE.2016.8009540

[21] Seethal Sasikumar, Abhay K S, C.N.S.Vinoth kumar "Network Intrusion Detection & Deduce System", Turkish Journal of Computer & Mathematics Education, Vol.12 No.9 (2021), 404 - 410,April2021.https://doi.org/10.17762/turcomat.v12i9.3094

[22] Dharmendra Yadav, Dhananjay Umrao, Mohammad Manzoor Hussain, Anitha S, Janvee Garg, "An Empirical analysing the Critical Determinants of Implementing Blockchain Technology in Enhancing the Health Care Services using Management Activities", Bulletin Of Environment, Pharmacology & Life Sciences, Bull. Env. Pharmacol. Life Sci., Special Issue [1]2022, Volume (1), pp.no. 676-683, Online ISSN 2277-1808, April 2022. (WOS-Web of Science)

[23] U. Sakthivelu & C. N. S. Vinoth Kumar, "An Approach on Cyber Threat Intelligence Using Recurrent Neural Network," ICT Infrastructure & Computing, Lecture Notes in Networks & Systems, vol 520., pp 429–439, Nov 2022, DOI: 10.1007/978-981 19-5331-6_44

[24] Anitha S, Saravanan S, & Chandrasekar A, "Data Transmission among Improving Lifetime of Cluster Network", Turkish Journal of Computer & Mathematics Education, Vol.12 No.2 (2021), 420 428, April 2021.

Dataset link

Kdd-cup :

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