An Enhanced Network Security using Machine Learning and Behavioral Analysis

SRAVANI KOKALA
PG Student
Department of IT (Data Science)
BVRIT Hyderabad College of Engineering for Women
Bachupally, Hyderabad – 500090
kokalasravani@gmail.com

Dr. MUKHTAR AHMAD SOFI
Associate Professor
Department of IT(Data Science)
BVRIT Hyderabad College of Engineering for Women
Bachupally, Hyderabad - 500090
sofimukhtar@bvrithyderabad.edu.in

***Abstract* — The recurrence of cyberattacks has developed with the quick ascent in web traffic, which underlines the prerequisite of strong intrusion detection systems (IDS) to safeguard frameworks. This paper presents a clever directed ML technique expected to definitively classify network traffic as either harmless or malevolent, consequently improving organization security. Joining many administered learning calculations with include choice strategies further develops recognition achievement rates through the recognizable proof of appropriate highlights and the sending of cutting edge calculations. Involving a notable benchmark for network traffic categorisation, the NSL-KDD dataset assists with assessing the model's presentation. Order utilizes Support Vector Machines (SVM) and Artificial Neural Networks (ANN), which show their ability to definitively group network traffic contingent upon the properties of the dataset. Besides awe-inspiring prior models, the ensemble approach in some cases alluded to as the Voting Classifier (RF + AB) arrives at 100 percent accuracy. An easy to use front-end interface fabricated utilizing the Flask framework is recommended to empower client testing with confirmation qualities, consequently propelling this review. This paper brings up how well ML and outfit approaches increment network security and suggests intriguing ways for additional examinations and valuable applications.**

***Keywords* —** *Cyber attacks, Network Security, KDD, intrusion detection, Ensemble methods, Flask Framework, neural network, support vector machine, feature selection, Voting Classifier.*

1. INTRODUCTION:

The blast of cybercrimes in the advanced time genuinely compromises data frameworks' respectability and security. From burglary of licensed innovation to phishing, checking, infections, financial fraud, interruptions, and numerous sorts of attacks, cybercrimes include a wide range of damaging ways of behaving [1]. These crimes take utilization of the astounding development of the internet by focusing on people, organizations, and government organizations both by utilizing its association and omnipresence. Among the few kinds of cyberattacks, network ones stand apart as particularly slippery as they look to think twice about classification, respectability, and accessibility of information moved by means of organizations [1].

Keeping up with the quality and reliability of organization administrations turns out to be progressively critical as quick advancing organization innovation meets developing shopper needs. In any case, overseeing and controlling different organization traffic while additionally distinguishing interruptions makes huge troubles for network tasks and upkeep the executives [2]. Keeping a protected and stable framework turns out to be significantly more testing with the gigantic measure of information passing the web. Dynamic frameworks are powerless against abuse regardless of whether intercessions like firewalls and programming updates offer some degree of safety [3].

By consistently checking and breaking down network information for indications of unlawful or threatening movement, intrusion detection systems help to counter cyber attacks [3]. Finding deviations or irregularities in PC frameworks or organizations that can think twice about security techniques is the principal objective of interruption identification. An extraordinary scope of IDS arrangements has been created to monitor PC frameworks from conceivable harm as the range and intricacy of attacks continue to create [3].

The way that the web penetrates current life stresses how critically network safety measures should be supported to safeguard delicate data and indispensable framework. For essential purposes like monetary exchanges, web based buying, data dispersion, news recovery, and long range informal communication the two individuals and organizations depend on the web [4]. In any case, the broad use of the web opens clients to various dangers, including cross-site scripting (XSS) assaults — where pernicious entertainers exploit shortcomings to embed disastrous code into online applications [5]. Battling these dangers calls for

innovative thoughts utilizing state of the art innovation including ML to reinforce recognition and response limit.

Utilizing the NSL-KDD dataset, a main benchmark in the field of interruption identification, the viability of the proposed model will be surveyed. This assessment plans to show that the model surpasses current methodologies with regards to location of interruptions, hence checking its better exhibition and predominance over past strategies.

With a particularly center around Cross-Site Scripting (XSS) attacks, this undertaking will likewise explore the utilization of specific ML strategies, similar to SVM and ANN, in the structure of organization interruption discovery. By focussing on certain cyberthreats, this work expects to show how well various calculations address centered security issues.

This work stresses commonly the more extensive potential outcomes of ML in numerous helpful fields, particularly in quickly spotting and guaging antagonistic contents. This study underlines the significance of ML in supporting organization safety efforts and saving significant computerized framework by focusing on its proficiency in rapidly dissecting and responding to any security concerns.

1.1 Problem Statement:

With network attacks compromising information protection, accuracy, and accessibility, the development of cybercrimes truly tests data frameworks. Firewalls and programming redesigns are just two of the ordinary security apparatuses that generally demonstrate inadequate against perplexing and evolving dangers. Checking network traffic and spotting criminal behavior rely fundamentally upon intrusion detection systems (IDS). Viable intrusion detection is regardless becoming testing given the volume and intricacy of organization information. This work fosters a high level IDS coordinating component choice techniques and directed ML ways to deal with address these troubles. The objective is to further develop location exactness for destructive as well as harmless organization traffic. Utilizing the NSL-KDD dataset, the proposed framework will be assessed — all the more particularly, as far as distinguishing Cross-Site Scripting (XSS) assaults — for its adequacy. This study features how ML might further develop security conventions and safeguard significant foundation.

1.2 Ambition:

This task plans to resolve the developing issue of cyberattacks and the pressing need of serious areas of strong Intrusion Detection System (IDS) to defend network foundation. This study expects to effectively isolate harmless from perhaps unsafe organization traffic by proposing a superior security design including managed ML strategies and component determination methodology. By utilization of cutting edge highlight choice techniques and ML calculations, the proposed framework is expected to distinguish examples of both harmless and impeding activities, consequently upgrading its accuracy in recognizing intrusions.

1.3 Objectives :

Develop a Robust IDS: To build and use a sophisticated Intrusion Detection System (IDS) using feature selection approaches and supervised machine learning methods to improve network intrusion detection.

Enhance Detection Accuracy: Using machine learning to spot trends suggestive of both valid and malicious network data can help to increase the accuracy of separating between them.

Evaluate Using Benchmark Data: With the aim of proving its efficiency and better success rate in identifying intrusions relative to current techniques, the performance of the proposed IDS model using the NSL-KDD dataset is evaluated.

Focus on XSS Attacks: To particularly evaluate the effectiveness of many machine learning techniques in this field and specifically address and increase the detection capacities for Cross-Site Scripting (XSS) assaults.

Integrate Machine Learning Algorithms: To further network intrusion detection by looking at and using a variety of machine learning techniques including artificial neural networks (ANN) and Support Vector Machines (SVM).

1.4 Significance of the Project:

This venture is critical as a result of its response to the creating hardships of network safety in the digital era. The honesty and security of data frameworks are intensely under risk as cybercrimes

— including network attacks and high level hurtful exercises — become more normal. Focusing on people, organizations, and government offices, these dangers take utilization of the extraordinary interconnectedness of the web to think twice about security, exactness, and openness of information sent through networks. Firewalls and programming overhauls are just two instances of customary security arrangements that typically demonstrate incapable to deal with the intricacy and extent of present day cyber threats. The pertinence of this examination originates from its imaginative way to deal with further develop network security through a strong Intrusion Detection System (IDS) joining highlight choice strategies with managed ML calculations. The exploration expects to enormously build the accuracy of separating harmless from noxious organization information by utilizing these advanced innovations. The concentrate principally addresses specific sorts of attacks, similar to Cross-Site Scripting (XSS), which are notable for their ability to embed destructive code into online frameworks. The focal point of this exploration on ML fosters the area of IDS as well as offers a versatile and adaptable response to the continuously changing territory of cyber threats. Involving a notable benchmark in intrusion detection— the NSL-KDD dataset — the review means to assess the viability of the proposed IDS and show its predominance over current strategies. The pragmatic convenience and reliability of the proposed framework rely upon this approval.

2. LITERATURE SURVEY

Driven by the quick advancement of the internet and the intricacy of cybercrime tasks, the field of network safety goes up against a continuously changing peril scene. This part gives a careful outline of pertinent material covering concentrates on cybercrime forecast, ML procedures, and intrusion detection systems (IDS), including

Targeting fostering a quick IDS fit for high velocity organizations, Tchakoucht and Ezziyyani (2018) Given the extraordinary speed and measure of organization traffic in such environmental elements, their review features the need of productive discovery frameworks for examining and Denial of Service (DoS) attacks. The creators address the hardships related with these assaults by making redid recognition calculations, subsequently improving the limit of interruption identification frameworks.

Independently, Ramasamy et al. (2021) take a gander at the plan and evaluation of multiband Blossom molded fix radio wires for Internet of Things (IoT) utilizes [2]. This study underscores the need of a strong organization foundation in empowering IoT gadgets regardless of whether it isn't straightforwardly associated with intrusion detection. IoT gadgets rely upon protected and reliable correspondence channels, so reinforcing network security relies upon improvements in radio wire plan and remote correspondence innovation.

Utilizing Prophet time series examination, Bother et al. (2022) present a method for assessing cybercrime [3]. < Utilizing time series anticipating strategies, their work gauges cybercrime occurrences and gives comprehension of the worldly patterns of cyberthreats. Their technique assists with propelling the field of prescient security examination by seeing patterns and examples in cybercrime information, in this manner empowering proactive measures for staying away from and taking care of cyberattacks.

Looking at the potential outcomes and troubles in such conditions, Zuech et al. (2015) investigate interruption identification inside huge and differed datasets [4]. Their intensive examination underlines the need of adaptable and adaptable IDS ready to control the intricacy of enormous information settings. The journalists give canny examination of the latest methods for recognizing attacks in different information conditions by consolidating currently distributed investigations.?

Sahasrabuddhe et al. (2017) examine how data mining approaches are utilized in IDS, in this manner offering a complete outline of how these strategies are utilized to distinguish irregularities and unfriendly movement in network traffic [5]. Their exploration takes a gander at a few data mining procedures and strategies, facing up their benefits and downsides. Through this review, the journalists give comprehension of the changing procedures and approaches in intrusion detection.

Utilizing a gathering classifier, Bharathi and C.N.S. Vinoth Kumar (2022) present an ongoing framework for distinguishing cyberattacks in medical services settings [6]. By focusing on digital perils extraordinary to this industry, their examinations help to fulfill the need major areas of strength for approaches in medical care frameworks. The creators progress online protection endeavors in this significant framework by creating explicit identification calculations for medical services conditions.

Exhibiting their use in clinical picture examination, Rathi and Balyan (2020) take a gander at the utilization of ML techniques for pneumonia identification from chest X-ray pictures [7]. However interruption discovery isn't the primary accentuation of this work, it underscores the extraordinary utilization of ML in numerous spaces, including medical care. The creators show how AI-driven approaches could further develop conclusion exactness and patient consideration by involving deep learning calculations for clinical picture translation.

Studying interruption identification frameworks, Dali et al. (2015) give an exhaustive outline of IDS innovation and strategy improvement [8]. Their examination takes a gander at a few sorts of IDS including hybrid, oddity based, and signature-based ones. Combining results from a few examinations assists the essayists with offering clever investigation of the advantages and weaknesses of different IDS structures and calculations, hence coordinating further field study.

Covering fields like organization designing, data mining, ML, and medical services, the writing study underlines the few features of interruption discovery and cybersecurity research. This study gives an exhaustive image of the latest improvements by consolidating information from a few investigations and distinguishes regions for greater cybersecurity examination and development possibilities.

3. METHODLOGY AND PROPOSED WORK

a) Proposed work:

To further develop network security, the recommended technique incorporates social examination strategies with ML calculations like artificial neural networks (ANN) and Support Vector Machines (SVM). While social examination finds deviations from run of the mill client conduct, verifiable information permits these models to find patterns and irregularities in network traffic. Besides further developing the intrusion detection system's (IDS) flexibility and it is a "Voting Classifier" group approach consolidating Random Forest (RF) and AdaBoost (AB) models to achieve 100 percent accuracy . Planned with the Flask framework, an easy to understand front-end interface makes client testing potential; highlights for client verification give safe access. This comprehensive procedure tries to improve general organization security by reinforcing the ID and relieving of cyber risks.

b) System Architecture:

Dataset investigation frames the underpinning of the framework plan; information arrangement confesses all and convert the information for study. Procedures of element determination help to track down the most appropriate qualities for categorisation. Training and testing sets separate the information for model turn of events and appraisal. Utilizing the preparation set, four ML models — SVM, NB, RF, and ANN — are trained. To survey their presentation, the trained models are next tried on a set. We assess each model utilizing measurements like accuracy, precision, recall, and F1-score. The framework then, at that point, moves into the assault location stage, utilizing trained models to distinguish and sort threatening organization exercises. This widely inclusive strategy ensures strong cyber threat detection and alleviating activity, consequently further developing network security for the most part.

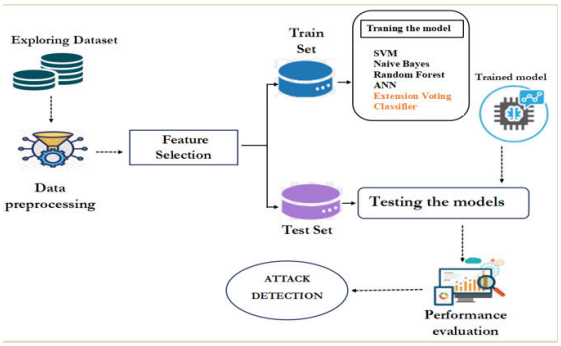

Fig 1 Architecture Diagram

c) Dataset collection:

This work applied the notable NSL-KDD dataset, a norm in network security research. Gathered from a recreated network climate, this dataset includes many organization traffic information tests — both benign and malignant. It has an extraordinary scope of qualities covering numerous features of organization traffic conduct: convention type, administration, banner, length, source/objective IP addresses.

Catching organization traffic information from reenacted situations where various assaults are done close by lawful tasks delivers a reasonable portrayal of organization conduct, subsequently creating the dataset. Training and assessment of ML models for network security and interruption location rely upon this dataset, which is accordingly rather significant. This work plans to fabricate and assess areas of strength for a security framework that mixes ML calculations and social investigation ways to deal with productively recognize and battle cyber attacks by utilizing the NSL-KDD 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 2 Data Set

d) DATA PROCESSING

Pandas DataFrame: Pandas DataFrame is used for data processing, therefore enabling data analysis and manipulation.

Keras Processing: Data is handled using keras processing in the framework of artificial neural networks (ANN), therefore offering a high-level interface for construction and training of neural networks.

Dropping Unwanted Columns: From the dataset, unwanted columns are deleted to simplify the analysis and eliminate pointless or duplicate elements.

Visualization : Seaborn and Matplotlib:

Data visualisation is done using Seaborn and Matplotlib packages, therefore enabling the development of useful graphs and charts to provide understanding of the dataset.

Label Encoding - LabelEncoder:
The LabelEncoder module performs label encoding—that is, numerical form conversion of categorical variables—to equip the data for training machine learning models.

Feature Selection- SelectPercentile using Mutual Info Classify:
SelectPercentile with Mutual Information Classify is used for feature selection to identify the most instructive characteristics for model building.

e) TRAINING AND TESTING

Training and testing comprise in various stages to ensure the productivity of the organization security framework. The dataset first comprises of two segments: the preparation set and the testing set. SVM, NB, RF, ANN, and Voting Classifier (RF + AB) among other ML models are prepared utilizing the training set. These calculations get patterns and irregularities in network traffic information all through preparing. The models are tried following training utilizing a testing set intended to evaluate their ability to accurately distinguish network traffic as harmless or threatening. Each model's presentation is learned by registering measurements like accuracy, precision, recall, and F1-score. This broad training and testing program looks to increment discovery and alleviating limit, along these lines expanding general network security against cyber attacks.

f) ALGORITHM INSIGHTS:

SVM : Applied for both grouping and relapse, Support Vector Machine (SVM) [19] is a managed learning technique. It works by deciding the best hyperplane that boosts edge between pieces of information while isolating them into many gatherings. This work utilizes SVM [19] as one of the ML models to distinguish network traffic as either harmless or threatening. SVM [19] helps with recognizing and separating among typical and perhaps perilous organization action by utilization of verifiable information examination. Its ability to sort convoluted designs and oversee high-layered information makes it a helpful instrument for improving network security.

Naive Bayes : In light of Bayes' hypothesis, gullible bayes [20] is a probabilistic ML strategy that assuming highlights are free. It utilizes contingent probabilities to learn the probability of a class name given the info data. This work utilizes Naive Bayes [20] to address characterization challenges like recognizing benign from malignant organization information. Naive Bayes finds patterns demonstrating various types of organization movement through verifiable information. Its effortlessness, speed, and capacity to deal with huge information make it a valuable instrument for traffic order based network security improvement.

Random Forest : Planned as a ensemble learning strategy, Random Forest [21] creates numerous choice trees all through the preparation cycle involving the normal of expectations for relapse issues or the larger part vote in favor of grouping errands. It builds exactness and versatility by totaling the conjectures from a few trees. This work utilizes RF [21] as an ML model to sort network traffic as either benign or hostile. RF raises the accuracy and dependability of intrusion detection by consolidating the conjectures from a few decision trees, thus supporting organization safety efforts.

ANN : Planned after the structure and activity of biological neural networks, artificial neural networks (ANN) [22] are a class of ML model. Associated hubs gathered in layers — input, stowed away, and yield layers make up they. Utilizing

backpropagation — a strategy that changes the loads of associations between hubs to limit the contrast among expected and actual outcomes — ANN learns on named information. This work utilizes ANN [22] to arrange network traffic through its ability to distinguish mind boggling examples and connections inside the information. ANN assists with distinguishing and group potential risks by utilization of past organization traffic, along these lines upgrading network security.

Voting Classifier : An ensemble learning technique called Voting Classifier [23] consolidates expectations from a few separate ML models to produce an end-product. It gathers the conjectures from a few models utilizing either a weighted normal or a larger part vote. This work joins expectations from RF and AdaBoost models utilizing the Voting Classifier [23] to improve the IDS. Utilizing the advantages of a few models assists the Voting Classifier with improving summing up and grouping accuracy. Through productive location and treatment of a few sorts of cyberthreats in network traffic information, this outfit approach fundamentally upgrades network security.

4. EXPERIMENTAL RESULTS

Accuracy: The limit of a test to appropriately recognize positive (sick) and negative (healthy) cases characterizes its exactness. One should compute the proportion of true positive and true negative discoveries to the general number of cases assessed to learn the legitimacy of a test. Numerically, this is addressed as:

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

where TP stands for true positives, TN for true negatives, FP for false positives, and FN for false negatives.

Accuracy provided by Voting Classifier calculation is 1.0, Accuracy given by ANN algorithm is 0.8, Accuracy given by Random Forest algorithm is 1.0, Accuracy given by Naïve Bayes algorithm is 0.4, Accuracy given by SVM algorithm is 0.6

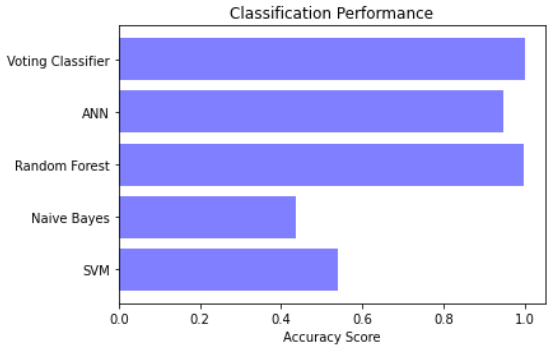

Fig 3 GRAPH COMPARING ACCURACY OF NSL-KDD DATASET

Precision: Precision is the level of appropriately found positive cases among every one of the positive cases sorted. Computation of precision follows this formula:

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

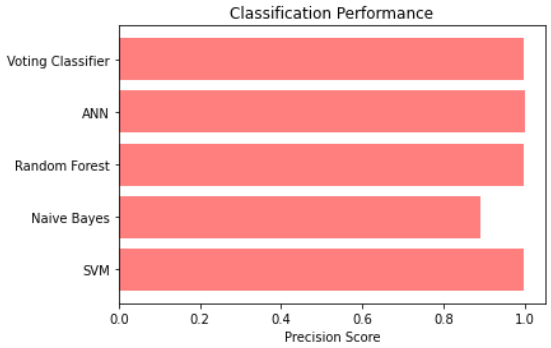

FIG 4 PRECISION COMPARISON GRAPHS OF NSL-KDD DATASET

Recall: A model's exhibition at finding everything relevant instances of a given class is estimated by review. Determined as the proportion of precisely predicted positive cases to the total actual positives, it gives data about the model's ability to comprehensively track down instances of the planned class.

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

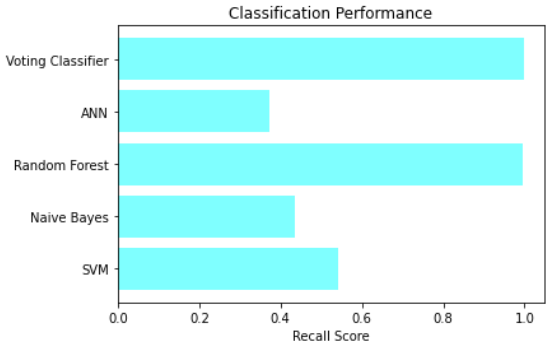

FIG 5 GRAPH COMPARING RECALL OF NSL-KDD DATASET

F1-Score: In ML, the F1 score is a measurement of appraisal that consolidates the precision and recall scores of a model to assess its accuracy. Accuracy checks all through the entire dataset the negligible portion of accurate model predictions.

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

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

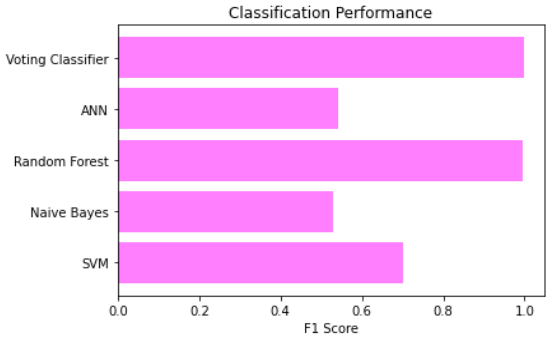

FIG 6 GRAPH COMPARING F1 SCORE OF NSL-KDD DATASET

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 ASSESSMENT TABLE

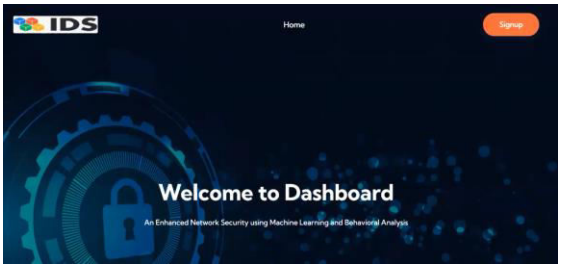

FIG 8 MAIN(HOME) PAGE

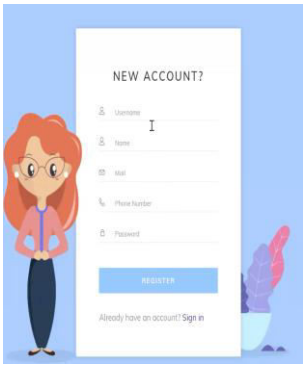

FIG 9 NEW USER - PAGE FOR SIGN UP

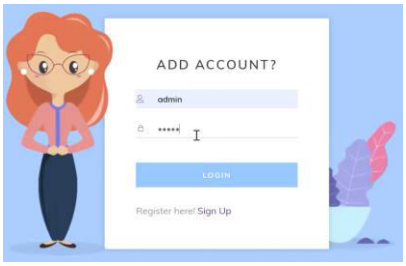

FIG 10 FOR EXISTING USER - SIGN IN

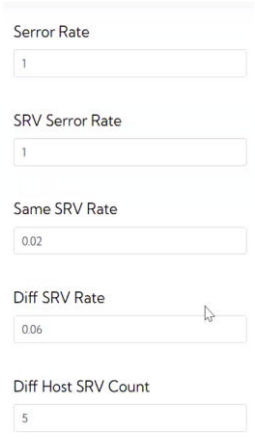

FIG 11 ENTER THE REQUESTED DATA

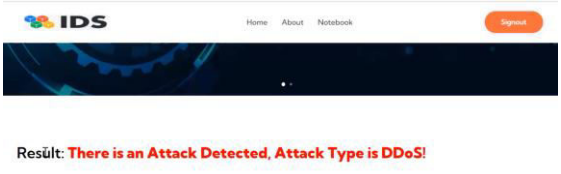

FIG 12 PREDICTED RESULT

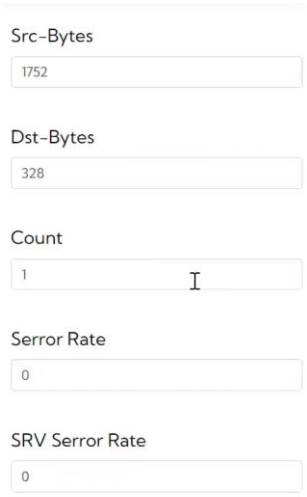

FIG 13 ENTER REQUESTED DATA

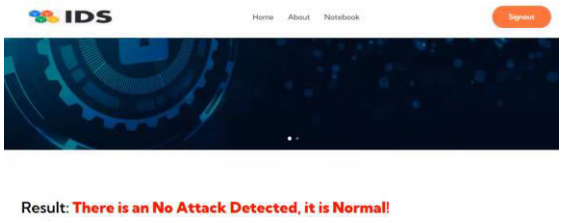

FIG 14 PREDICTED RESULT

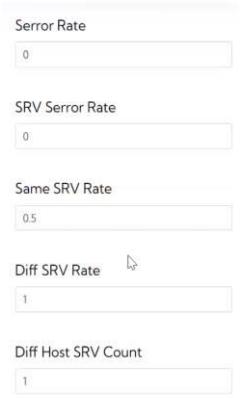

FIG 15 UPLOAD INPUT DATA

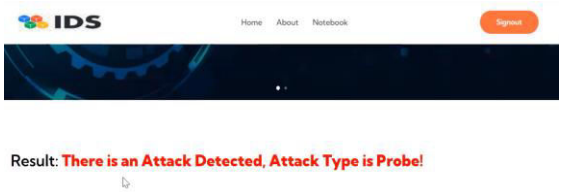

FIG 16 FORECASTED RESULT

5. CONCLUSION AND FUTURE SCOPE

At last, the proposed technique productively incorporates social examination with ML to definitively recognize network traffic as either harmless or unfriendly, thus further developing organization security. Particularly as far as intrusion detection achievement rates, a correlation investigation using the NSL-KDD dataset shows that this model beats current frameworks, consequently demonstrating its ability to perceive and appropriately handle cyber threats. The venture accentuates the prerequisite of accurate recognizable proof techniques to stay in front of changing cyberthreats and the need of vigorous safety efforts to monitor organizations. The Voting Classifier (RF + AB) among other gathering procedures assists the framework to distinguish interruptions with better accuracy. Moreover, the testing experience is improved by the blend of an easy to use Flask interface with safe validation, consequently working with information section and execution assessment. This sweeping procedure ensures client solace and information trustworthiness as well as shows how well the framework further develops network security.

The extended organization security framework utilizing ML and social investigation has an expansive scope of highlights intended to reinforce network safety measures. With its wide assortment of capacities intended to help online protection safeguards, the complex organization security framework coordinating conduct examination and ML cases To appropriately distinguish network traffic as either harmless or threatening, it utilizes progressed ML strategies including SVM, NB, RF, and ANN. The framework additionally utilizes conduct investigation to recognize odd patterns and takeoffs from normal client action, subsequently working on its ability to detect interruptions. It likewise utilizes highlight determination procedures, which focus on the main attributes for characterization, hence upgrading model execution. Counting gathering strategies like the Voting Classifier (RF + AB) assists with working on the accuracy and trustworthiness of the framework even in danger discovery. Besides, the framework has straightforward points of interaction with safe confirmation to ensure effortlessness of purpose and save information honesty, subsequently upgrading the entire client experience and the framework's ability to safeguard network foundation.

6. REFERENCES

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

[2] R Ramasamy, V Rajavel, M Vasim Babu, C N S Vinoth Kumar, S Parthiban, "Design and Analysis of Multiband Bloom Shaped Patch Antenna for IoT Applications", Turkish Journal of Computer and 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 for 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 and 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 and 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 and networking (WSWAN). Piscataway: IEEE; 2015. p. 1–6.

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

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

[11] Ferhat K, Sevcan A. Big Data: controlling fraud by 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 for 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 and mobile communication conference (IEMCON), 2016. Piscataway: IEEE. 2016; p. 1–5.

[16] Vimalkumar K, Radhika N. A big data framework for intrusion detection in smart grids using Apache Spark. In: International conference on advances in computing, communications and 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 and 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 and 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 for WSN using hop-field chaotic neural network with 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 and Deduce System", Turkish Journal of Computer and 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 And 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 and C. N. S. Vinoth Kumar, "An Approach on Cyber Threat Intelligence Using Recurrent Neural Network," ICT Infrastructure and Computing, Lecture Notes in Networks and Systems, vol 520., pp 429–439, Nov 2022, DOI: 10.1007/978-981 19-5331-6_44

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