International Journal of Mechanical Engineering Research and Technology

ISSN 2454-535X

Email ID: info.ijmert@gmail.com or editor@ijmert.net

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

TWO-PHASED HYBRID ENSEMBLE LEARNING AND AUTOMATIC FEATURE SELECTION FOR NETWORK INTRUSION DETECTION

KANDALA VASAVI[1], V M BHARATHI[2], T ANIL KUMAR[3], G PRATHYUSHA[4], Monisha B H [5], G.Swapna [6]

[1]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: vasavik303@gmail.com
[2]Assistant Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email:bharathisathya614@gmail.com
[3]Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: anil.thumburu@gmail.com
[4]Assistant Professor, Department of CSE, Sri Padmavathi Mahila Visvavidyalayam Tirupati, Email:prathyubmb@gmail.com
[5] Equiniti India private limited, Address: No 1/124 Block No 10 Dlf IT Park 8th Floor, Shivaji Garden, Ramapuram, Chennai - 600089 (Near L & T Manapakkam).
[6] Associate professor, Department of pharmaceutics, Apollo institute of pharmaceutical sciences, The Apollo University, Chittoor – 517127, swapnagv111@gmail.com

Abstract: A weighty NIDS is acquainted with cybersecurity. This state of the art NIDS utilizes Two-phased Hybrid Ensemble learning and Automatic Feature Selection to improve cyber threat detection. Customary NIDS battles to stay aware of digital dangers. As organization associated gadgets grow, rule-based and signature-based strategies become ineffectual, requiring modern NIDS frameworks that can deal with high-layered network information. Creative NIDS answer for interruption identification and organization security. This inventive technique utilizes Two-phased Hybrid Ensemble learning and Automatic Feature Selection. One-against One classifiers and assault class classifiers are joined in the Two-eased model to recognize interruptions in more ways than one. Likewise, a vigorous group technique utilizing Stacking and Voting Classifiers further developed the NIDS's figure accuracy. The 100 percent accurate Stacking Classifier was noteworthy. For client testing and safe access, a Flask-based front end was made to make NIDS connection simple.

Index terms *- Feature selection, feature engineering, classification, machine learning, ensemble learning, anomaly detection, intrusion detection system.*

1. INTRODUCTION

Network availability is so fundamental for our daily existences that even a couple of moments of interference might cause significant interruptions. IEEE 802.3-based wired ethernet networks have associated network-skilled gadgets for a really long time and will keep on doing so [1]. Remote organizations like IEEE 802.11 expanded gadget reception because of their convenientce [2]. Since the Internet-of-Things (IoT) has sped up remote organization extension, 29 billion organization gadgets are anticipated in the span of 10 years [3,51].

Lately, wired and remote organization security and protection have filled in notoriety [4]. An Network Intrusion Detection System (NIDS) at the center of an organization screens entry and departure parcels to

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

recognize attacks. Zarpelao et al. [5] isolated current NIDSs into particular based, signature-based, and irregularity based discovery techniques. [6], [7], and [8] have comparative scientific categorizations. A determination based NIDS banners irregularities or "assaults" when an organization digresses from its expected way of behaving. They have not many bogus up-sides since the guidelines are physically inferred. Manual rule enlistment to portray run of the mill framework conduct is a vital weakness of such frameworks, particularly in greater organizations. Signature-based NIDSs recognize known assault marks. Assuming the list of capabilities is little enough for signature creation, signature discovery for realized dangers can be exact, lessening bogus up-sides. Human blunder can make manual mark acknowledgment from high-layered network information tricky. Signature-based NIDSs just sign a matching mark to a known assault, subsequently they can't identify zero-day attacks. At last, an oddity based NIDS identifies framework inconsistencies utilizing an ML strategy[52]. This adaptation of NIDS is superior to others since it doesn't need human rule deduction. 2. It can distinguish new and unseen dangers, a much looked for normal for a contemporary NIDS. Practically all cutting edge network interruption location arrangements use ML. This exploration will likewise go under interruption recognition frameworks.

Compelling ML based NIDS configuration is troublesome. Network gadgets produce huge measures of confounded, high-layered information, which characterizes large information. High dimensionality alone presents different issues. The NIDS should pick includes that perform well without overfitting the model. The scourge of dimensionality could come about because of picking such a large number of qualities in high-layered information [9,54]. Accordingly, appropriate programmed include choice is urgent for enormous scope high-layered network information as human component determination can be scary and lead to erroneous element determination or rule definition. Programmed include choice for network information is as yet being examined. Identifying new attacks is another issue while making a successful NIDS. Most new attacks are created variants of old ones. The danger scene changes intermittently with additional complex attacks [10]. The WannaCry attack contaminated around 230,000 frameworks in 150 nations, including high-profile government PCs [11]. New attacks on key framework can cause a public catastrophe if unprotected. The 2021 Provincial Pipeline attack shows this [12,53]. Accordingly, the NIDS should be powerful to these new dangers. One more NIDS trouble is the dissimilarity among wired and remote ethernet conventions. Remote organizations are accessible to anyone close by, in contrast to wired networks. This renders remote organizations powerless against new attacks not seen in conventional ethernet. NIDS originators find it trying to give a strong answer for wired and remote applications.

2. LITERATURE SURVEY

The most recent IEEE 802.11 standard changes will prompt another age of Wireless Local Area Networks (WLANs) before long. Normal guidelines incorporate IEEE 802.11aa (Hearty Sound Video Transport Web based), IEEE 802.11ac (Exceptionally high throughput at < 6 GHz), IEEE 802.11af (television

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

Blank areas), and IEEE 802.11ah (Machine-to-Machine correspondences). This review [2] covers these inventive mechanical viewpoints and the open specialized issues that will shape WLAN progress. Not at all like other IEEE 802.11 overviews, this is a utilization contextual investigation. We start with the three principal opportunities for cutting edge WLANs. We then analyze the main changes for each utilization case, zeroing in on their new elements and advancements, for example, multi-client MIMO, groupcast, dynamic channel holding, range data sets, channel detecting, power saving systems, and effective little information transmissions. We audit related work to feature significant difficulties that should be tended to. At long last, we examine new WLAN configuration patterns, zeroing in on programming characterized Macintoshes and web working with cell frameworks [13].

Mobile Network Operators are conveying 5.G remote broadband access, which has gathered consideration lately. Suddenly, 'Wi-Fi 6', the new IEEE 802.1ax norm for Remote Neighborhood with highlights for private, edge-organizations, has gotten less consideration. This examination [3] analyzes cell and Wi-Fi for fast remote Web access. The two advancements expect to further develop execution, empowering quicker remote broadband network and backing for the Internet of Things and Machine-to-Machine correspondences, making them specialized substitutes in numerous use situations. We accept both will be huge later on and contend and commend one another. We expect 5G to stay the leaned toward innovation for wide-region inclusion and Wi-Fi 6 for inside use on the grounds that to its less expensive execution costs [3, 8, 17, 36]. Be that as it may, more established cell and Wi-Fi borders are consolidating. Defenders of one innovation might guarantee that it ought to supplant the other and propose legislative measures to lean toward their innovation. We accept such drives ought to be against and that the two advancements have fundamental market liabilities relying upon differed use cases. The two innovations ought to help accomplish economical, trustworthy, and pervasive high-limit remote broadband access.

Diminishing electrical machine power utilization has added another level to keen things. Electronic devices through the Web have worked on ordinary things to deliver nearby insight and speak with the internet. IoT, another word in this field, is used to make wise things. The aggressor may essentially get to asset restriction gadgets in the IoT since they are straightforwardly associated with the hazardous Web. Public Web availability makes things presented to attacks. Inward attacks are those that taint interior hubs and get ready to go after the organization. Accordingly, IoT Intrusion Detection Systems (IDSs) are significant [17, 24, 34]. This issue is significant, yet there is no finished and thorough evaluation of its mechanics. Consequently, this work [4] presents a Systematic Literature Review (SLR) on IDSs in IoT. Then, at that point, utilizing normal elements, IoT IDSs are classified as abnormality based, signature-based, detail based, half breed, brought together, conveyed, crossover, reenactment, hypothetical, and refusal of administration assault, Sybil assault, replay assault, specific sending assault, wormhole assault, dark opening assault, sinkhole assault, sticking assault, misleading information assault. The chose components' upsides and downsides are then

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

investigated. At last, open worries and potential patterns are inspected.

IoT [26, 40] is another worldview that associates the Web and actual gadgets from home computerization, modern cycle, human wellbeing, and ecological checking. It expands the pervasiveness of Web associated contraptions in our day to day routines, presenting security gambles notwithstanding benefits. IDS [17] have safeguarded organizations and data frameworks for very nearly twenty years. Because of obliged asset gadgets, convention stacks, and guidelines, IoT is trying to apply exemplary IDS ways to deal with. In this study [5], we overview IoT IDS research [24, 34]. We look for arising patterns, unsettled concerns, and exploration open doors. We classified writing proposed IDSs by discovery method, position system, security danger, and approval approach. We likewise analyzed the various choices for each element, including concentrates on that give IoT IDS plans or construct assault recognition calculations for IoT dangers consolidated in IDSs.

Incorporating data frameworks into our life. As combination extends, framework security turns out to be more significant. These frameworks are for the most part remotely arranged because of diminished establishment and upkeep costs. We audit remote organization interruption discovery writing to distinguish holes and propose research choices. Our strategy arranges present day wireless IDS frameworks [17, 24, 34] by target remote organization, distinguishing technique, assortment system, trust model, and investigation strategy. We talk about remote interruption discovery upsides and downsides for target remote organizations like WLANs, WPANs, WSNs, impromptu organizations, versatile communication, wireless mesh networks (WMNs), and digital actual frameworks. Then, we evaluate the writing's most and least examined remote IDS procedures, distinguish research holes, and legitimize their treatment. At long last, we suggest research strategies for beneficial however understudied regions.

3. METHODOLOGY

i) Proposed Work:

The proposed approach utilizes complex Two-phased Hybrid Ensemble Learning with Automatic Feature Selection. This strategy further develops intrusion detection systems. Programmed include determination allows the framework wisely to pick the dataset's most huge properties for investigation. THE-AFS calculation advances two times. The initial step depends on multiclass characterization's One-vs-One (OVO) structure [48,56]. Stage two purposes classifiers produced using assault class blends. Together, these two stages increment the framework's organization interruption discovery and order. The result is a dependable, exact interruption discovery framework that can deal with differed assaults. In the undertaking, a hearty group strategy joins Stacking Classifier and Voting Classifier forecasts from discrete models. The Stacking Classifier further developed the Network Intrusion Detection System's expectation execution with 100 percent accuracy. [4, 5, 6, 7, 8] A simple Flask front end for NIDS association was made to permit client testing and safe access.

ii) System Architecture:

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

The proposed Network Intrusion Detection System (NIDS) [4, 5,55] purposes include designing and two-phased hybrid ensemble learning. Framework highlight designing incorporates network information arrangement, standardization, and binarization. The framework utilizes a cross breed multiclass gathering procedure with T base students prepared on irregular examples from the dataset. The two-phased hybrid ensemble learning calculation has two learning stages. The primary stage utilizes classifiers adjusted from the Onevs-One architecture [48], while the subsequent stage utilizes assault class blends. The framework additionally utilizes ML classifiers to naturally recognize the main qualities. The recommended technique outflanks past comparable exploration in attack detection on two all around referred to datasets for wired and wireless applications [13], [14], [15].

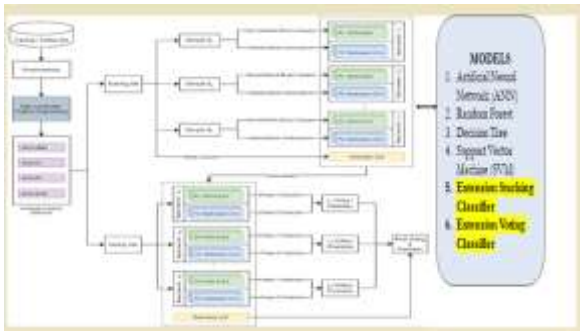

Fig 1 Proposed architecture

iii) Dataset collection:

This study utilizes NSL KDD [16] and AWIDS [17] datasets to examine their construction, content, and properties. This helps information readiness and model creation. The proposed model was evaluated utilizing every one of the four element choice methodologies. Our most memorable examinations found that 30 and 38 highlights had the most noteworthy distinguishing proof rates for AWID and NSL-KDD[58] datasets. This matches [13]. To acquire the ideal model for each dataset, model hyperparameters were iterated with each component determination approach.

Fig 2 AWIDS DATASET's

The AWIDS dataset [17] is intended to test wireless network intrusion detection systems. It records customary and attack-related wireless network traffic.

In wired network settings, the NSL-KDD [16] dataset is a famous asset for benchmarking IDS. It incorporates standard and assault network traffic measurements. The dataset has training and test sets, making it proper for testing IDS, particularly in recognizing new attacks.

Fig 2 NSL KDD dataset

iv) Data Processing:

Data processing transforms raw information into business-helpful data. Information researchers accumulate, sort out, clean, check, break down, and

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

orchestrate information into diagrams or papers. Data can be handled physically, precisely, or electronically. Data ought to be more significant and decision-production simpler. Organizations might upgrade activities and settle on basic decisions quicker. PC programming improvement and other mechanized information handling innovations add to this. Big data can be transformed into significant bits of knowledge for quality administration and independent direction.

v) Feature selection:

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

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

vi) Algorithms:

ANN

Artificial Neural Networks (ANNs) are mind motivated PC models. Interconnected hubs or neurons structure layers. These neurons utilize weighted associations and enactment capabilities to process and result information.Backpropagation is utilized to prepare ANNs by changing their inner loads to decrease yield mistakes. ANNs address confounded information designs. Since ANNs can find non-straight relationships and examples in network traffic information, they can distinguish irregularities and interruptions [35].

```
from sklearn.neural_network import MLPClassifier
# instantiate the model
clf = MLPClassifier()

# fit the model
clf.fit(X_train, y_train)

#predicting the target value from the model for the samples

y_hat = clf.predict(X_test)

ann_acc = accuracy_score(y_hat, y_test)
ann_prec = precision_score(y_hat, y_test,average='weighted')
ann_rec = recall_score(y_hat, y_test,average='weighted')
ann_f1 = f1_score(y_hat, y_test,average='weighted')
ann_fpr = 1 - ann_acc
```

Fig 3 ANN

RANDOM FOREST

Random Forest[59] is a grouping and relapse ML outfit. The preparation cycle fabricates a few decision trees and joins their results to conjecture. Different decision trees are collected in Random Forest to further develop discovery rates in uproarious or misdirecting information.

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

```
from sklearn.ensemble import RandomForestClassifier

# instantiate the model
rf = RandomForestClassifier(random_state=10)

# fit the model
rf.fit(X_train, y_train)

#predicting the target value from the model for the samples

y_pred = rf.predict(X_test)

rf_acc = accuracy_score(y_pred, y_test)
rf_prec = precision_score(y_pred, y_test,average='weighted')
rf_rec = recall_score(y_pred, y_test,average='weighted')
rf_f1 = f1_score(y_pred, y_test,average='weighted')
rf_fpr = 1 - rf_acc
```

Fig 4 Random forest

DECISION TREE

A Decision Tree is an adaptable directed ML method for order and relapse. It frames a tree with center hubs addressing highlight based decisions and leaf hubs holding results or expectations. Decision Trees are helpful in information science and ML because of their interpretability, versatility with various information sorts, and representation. Straightforward and interpretable Decision Trees are utilized. They coordinate information into various leveled choice designs to make sense of how the model arrived at an outcome. The task utilizes Decision Trees to envision the NIDS dynamic interaction [21, 34].

```
from sklearn.tree import DecisionTreeClassifier

# instantiate the model
dt = DecisionTreeClassifier(random_state=10)

# fit the model
dt.fit(X_train, y_train)

#predicting the target value from the model for the samples

y_pred = dt.predict(X_test)

dt_acc = accuracy_score(y_pred, y_test)
dt_prec = precision_score(y_pred, y_test,average='weighted')
dt_rec = recall_score(y_pred, y_test,average='weighted')
dt_f1 = f1_score(y_pred, y_test,average='weighted')
dt_fpr = 1 - dt_acc
```

Fig 5 Decision tree

SVM

Support Vector Machines (SVMs) are dependable supervised ML calculations for grouping and relapse. It finds the fitting hyperplane to segment data of interest into classes, boosting the edge between help vectors (information focuses nearest to the choice line). Portion capabilities make SVMs helpful in ML applications since they can deal with non-straight information designs. SVM finds the best hyperplane to improve the edge among normal and attack network traffic data [15].

```
from sklearn.svm import SVC

# instantiate the model
svm = SVC()

# fit the model
svm.fit(X_train, y_train)

#predicting the target value from the model for the samples

y_pred = svm.predict(X_test)

svm_acc = accuracy_score(y_pred, y_test)
svm_prec = precision_score(y_pred, y_test,average='weighted')
svm_rec = recall_score(y_pred, y_test,average='weighted')
svm_f1 = f1_score(y_pred, y_test,average='weighted')
svm_fpr = 1 - svm_acc
```

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

Fig 6 SVM

STACKING CLASSIFIER

Stacking Classifiers join the predictions of various essential classifiers, like Random Forest (RF) and Multilayer Perceptron (MLP), to make last forecasts. It involves LightGBM as a meta-classifier to join RF and MLP forecasts to make the last expectation. Stacking further develops NIDS prediction execution and flexibility by expanding base classifiers.

```
from sklearn.neural_network import MLPClassifier
from lightgbm import LGBMClassifier
from sklearn.ensemble import StackingClassifier

estimators = [('rf', forest),('mlp', MLPClassifier(random_state=1, max_iter=1000))]

clf = StackingClassifier(estimators=estimators, final_estimator=LGBMClassifier(n_estimators=1000))


clf.fit(X_train,y_train)

y_pred = clf.predict(X_train)

stac_acc = accuracy_score(y_pred, y_train)
stac_prec = precision_score(y_pred, y_train,average='weighted')
stac_rec = recall_score(y_pred, y_train,average='weighted')
stac_f1 = f1_score(y_pred, y_train,average='weighted')
```

Fig 7 Stacking classifier

VOTING CLASSIFIER

Voting Classifiers consolidate Random Forest (RF) and Decision Tree (DT) expectations. The result most frequently expected by RF and DT is picked by larger part voting. Because of classifier assortment, this outfit method further develops expectation accuracy and steadfastness.

```
from sklearn.ensemble import RandomForestClassifier, VotingClassifier, AdaBoostClassifier
from sklearn.tree import DecisionTreeClassifier

rfc = RandomForestClassifier()
parameters = {
    "n_estimators":[250],
    "max_depth":[200]

}

from sklearn.model_selection import GridSearchCV
forest = GridSearchCV(rfc,parameters,cv=10)

clf2 = DecisionTreeClassifier(random_state=100)

eclf1 = VotingClassifier(estimators=[('rf-parameter', forest), ('dt', clf2)], voting='soft')
eclf1.fit(X_train, y_train)
y_pred = eclf1.predict(X_test)

vot_acc = accuracy_score(y_pred, y_test)
vot_prec = precision_score(y_pred, y_test,average='weighted')
vot_rec = recall_score(y_pred, y_test,average='weighted')
vot_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig 8 Voting classifier

4. EXPERIMENTAL RESULTS

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

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

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

```
plt2.barh(y_pos, precision, align='center', alpha=0.5,color='red')
plt2.yticks(y_pos, classifier)
plt2.xlabel('Precision Score')
plt2.title('Classification Performance')
plt2.show()
```

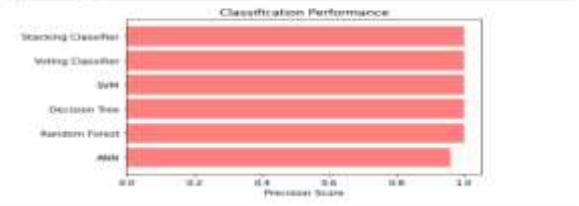

Fig 9 Precision comparison graph

Recall: ML recall measures a model's ability to catch all class occurrences. The model's ability to recognize

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

a certain type of event is measured by the percentage of precisely anticipated positive prospects that turn into real earnings.

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

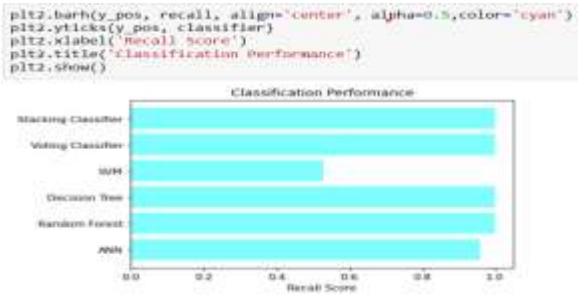

Fig 10 Recall comparison graph

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

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

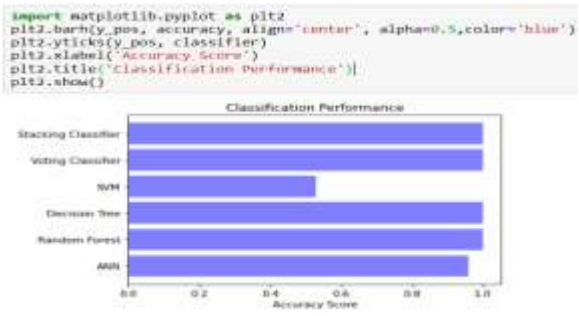

Fig 11 Accuracy graph

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

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

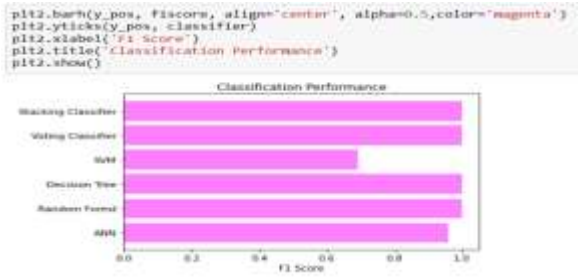

Fig 12 F1Score

ML Model	Accuracy	Precision	Recall	F1-Score	FPR
ANN	0.957	0.957	0.957	0.957	0.043
Random Forest	0.998	0.998	0.998	0.998	0.002
Decision Tree	0.998	0.998	0.998	0.998	0.002
SVM	0.529	1.000	0.529	0.691	0.471
Extension Voting Classifier	0.998	0.998	0.998	0.998	0.002
Extension Stacking Classifier	1.000	1.000	1.000	1.000	0.000

Fig 13 Performance Evaluation

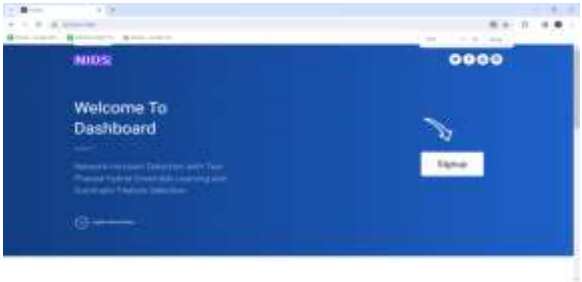

Fig 14 Home page

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

Fig 15 Signin page

Fig 16 Login page

Fig 17 User input

Fig 18 Predict result for given input

5. CONCLUSION

ML has assisted the group with making a robust Intrusion Detection System (NIDS) [4, 5, 6, 7, 8] that can identify network interruptions. Programmed

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

highlight determination and a two-phased ensemble technique have further developed identification accuracy, showing adaptability to an assortment of cyberattacks. The system's network attack detection capacities are unparalleled, as shown by thorough tests on different datasets. The drawn out group model was picked for expectation on the grounds that to its high accuracy and F-score, further developing the IDS [18, 19]. The upgraded calculation's adequacy is reinforced by the Stacking Classifier's 100 percent ensemble accuracy. This exhibition shows major areas of strength for its discovery capacities and makes it a strong arrangement, supporting NIDS[60] constancy and security. This drive reinforces network security by giving a strong insurance against expanding digital dangers.

6. FUTURE SCOPE

Future examination might survey the structure's variation and execution on an assortment of organization datasets to uncover its flexibility. High level ML approaches can work on the structure's capacity to distinguish an assortment of organization attacks with more noteworthy precision and efficiency. Real-world applications offer an engaging method for testing the structure's adaptability and adequacy in genuine organization settings [16, 17], where it can certainly confront both existing and creating dangers. The component choice motor ought to be improved to deal with high-dimensional network data [35] and adjust to dynamic network conditions as the system advances.

REFERENCES

[1] F. Obite, E. T. Jaja, G. Ijeomah, and K. I. Jahun, ‘‘The evolution of Ethernet Passive Optical Network (EPON) and future trends,’’ Optik, vol. 167, pp. 103–120, Aug. 2018.

[2] B. Bellalta, L. Bononi, R. Bruno, and A. Kassler, ‘‘Next generation IEEE 802.11 wireless local area networks: Current status, future directions and open challenges,’’ Comput. Commun., vol. 75, pp. 1–25, Feb. 2016.

[3] E. J. Oughton, W. Lehr, K. Katsaros, I. Selinis, D. Bubley, and J. Kusuma, ‘‘Revisiting wireless internet connectivity: 5G vs Wi-Fi 6,’’ Telecommun. Policy, vol. 45, no. 5, Jun. 2021, Art. no. 102127.

[4] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, ‘‘Intrusion detection systems in the Internet of Things: A comprehensive investigation,’’ Comput. Netw., vol. 160, pp. 165–191, Sep. 2019.

[5] B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. De Alvarenga, ‘‘A survey of intrusion detection in Internet of Things,’’ J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.

[6] R. Mitchell and I.-R. Chen, ‘‘A survey of intrusion detection in wireless network applications,’’ Comput. Commun., vol. 42, no. 3, pp. 1–23, Apr. 2014.

[7] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, ‘‘Intrusion detection system: A comprehensive review,’’ J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013.

[8] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, ‘‘Deep abstraction and weighted feature selection for Wi-Fi impersonation detection,’’

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

IEEE Trans. Inf. Forensics Security, vol. 13, no. 3, pp. 621–636, Mar. 2018.

[9] G. V. Trunk, ‘‘A problem of dimensionality: A simple example,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. PAMI-1, no. 3, pp. 306–307, Jul. 1979.

[10] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, ‘‘Ransomware detection and mitigation using software-defined networking: The case of WannaCry,’’ Comput. Electr. Eng., vol. 76, pp. 111–121, Jun. 2019.

[11] C. Adams, ‘‘Learning the lessons of WannaCry,’’ Comput. Fraud Secur., vol. 2018, no. 9, pp. 6–9, Jan. 2018.

[12] A. Cooke, K. Renaud, D. Spence, and C. Tankard, ‘‘US authorities recover most of colonial pipeline ransom,’’ Netw. Secur., vol. 2021, no. 6, pp. 1–2, 2021. [Online]. Available: https://www.magonlinelibrary.com/doi/full/10.1016/S1353-4858%2821%2900057-X

[13] J. W. Mikhail, J. M. Fossaceca, and R. Iammartino, ‘‘A semi-boosted nested model with sensitivity-based weighted binarization for multi-domain network intrusion detection,’’ ACM Trans. Intell. Syst. Technol., vol. 10, no. 3, pp. 1–27, May 2019.

[14] Y. Zhou, T. A. Mazzuchi, and S. Sarkani, ‘‘M-AdaBoost-A based ensemble system for network intrusion detection,’’ Exp. Syst. Appl., vol. 162, Dec. 2020, Art. no. 113864.

[15] A. A. Aburomman and M. B. I. Reaz, ‘‘A novel SVM-kNN-PSO ensemble method for intrusion detection system,’’ Appl. Soft Comput., vol. 38, pp. 360–372, Jan. 2016.

[16] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, ‘‘A detailed analysis of the KDD CUP 99 data set,’’ in Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl., Jul. 2009, pp. 1–6.

[17] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, ‘‘Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,’’ IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 184–208, 1st. Quart., 2016.

[18] B. A. Tama and S. Lim, ‘‘Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation,’’ Comput. Sci. Rev., vol. 39, Feb. 2021, Art. no. 100357.

[19] G. Folino and P. Sabatino, ‘‘Ensemble based collaborative and distributed intrusion detection systems: A survey,’’ J. Netw. Comput. Appl., vol. 66, pp. 1–16, May 2016.

[20] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, ‘‘Building an efficient intrusion detection system based on feature selection and ensemble classifier,’’ Comput. Netw., vol. 174, Jun. 2020, Art. no. 107247.

[21] M. N. Adnan and M. Z. Islam, ‘‘Forest PA: Constructing a decision forest by penalizing,’’ Exp. Syst. Appl., vol. 89, pp. 389–403, Dec. 2017.

[22] N. F. Haq, A. R. Onik, and F. M. Shah, ‘‘An ensemble framework of anomaly detection using Hybridized Feature Selection Approach (HFSA),’’ in

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

Proc. SAI Intell. Syst. Conf. (IntelliSys), Nov. 2015, pp. 989–995.

[23] A. A. Aburomman and M. B. I. Reaz, ‘‘A survey of intrusion detection systems based on ensemble and hybrid classifiers,’’ Comput. Secur., vol. 65, pp. 135–152, Mar. 2017.

[24] G. Kumar, K. Thakur, and M. R. Ayyagari, ‘‘MLEsIDSs: Machine learning-based ensembles for intrusion detection systems—A review,’’ J. Supercomput., vol. 76, no. 11, pp. 8938–8971, Nov. 2020.

[25] B. A. Tama, L. Nkenyereye, S. M. R. Islam, and K. Kwak, ‘‘An enhanced anomaly detection in web traffic using a stack of classifier ensemble,’’ IEEE Access, vol. 8, pp. 24120–24134, 2020.

[26] Y. Cheng, Y. Xu, H. Zhong, and Y. Liu, ‘‘Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in IoT communication,’’ IEEE Internet Things J., vol. 8, no. 1, pp. 144–155, Jan. 2021.

[27] M. Milliken, Y. Bi, L. Galway, and G. Hawe, ‘‘Multi-objective optimization of base classifiers in StackingC by NSGA-II for intrusion detection,’’ in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Dec. 2016, pp. 1–8.

[28] Y. Wang, Y. Shen, and G. Zhang, ‘‘Research on intrusion detection model using ensemble learning methods,’’ in Proc. 7th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS), Aug. 2016, pp. 422–425.

[29] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, ‘‘Autoencoder-based feature learning for cyber security applications,’’ in Proc. Int. Joint Conf. Neural Netw. (IJCNN), May 2017, pp. 3854–3861.

[30] S. A. Ludwig, ‘‘Intrusion detection of multiple attack classes using a deep neural net ensemble,’’ in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Nov. 2017, pp. 1–7.

[31] K. Li, G. Zhou, J. Zhai, F. Li, and M. Shao, ‘‘Improved PSO_AdaBoost ensemble algorithm for imbalanced data,’’ Sensors, vol. 19, no. 6, p. 1476, Mar. 2019.

[32] J. Kennedy and R. Eberhart, ‘‘Particle swarm optimization,’’ in Proc. IEEE Int. Conf. Neural Netw., vol. 4. Nov. 1995, pp. 1942–1948.

[33] X. Li, M. Zhu, L. T. Yang, M. Xu, Z. Ma, C. Zhong, H. Li, and Y. Xiang, ‘‘Sustainable ensemble learning driving intrusion detection model,’’ IEEE Trans. Dependable Secure Comput., vol. 18, no. 4, pp. 1591–1604, Jul./Aug. 2021.

[34] M. H. L. Louk and B. A. Tama, ‘‘Dual-IDS: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system,’’ Exp. Syst. Appl., vol. 213, Mar. 2023, Art. no. 119030.

[35] M. E. Aminanto and K. Kim, ‘‘Detecting impersonation attack in WiFi networks using deep learning approach,’’ in Proc. WISA, 2016, pp. 136–147.

[36] M. E. Aminanto and K. Kim, ‘‘Improving detection of Wi-Fi impersonation by fully unsupervised deep learning,’’ in Proc. WISA, 2017, pp. 212–223.

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

[37] J. Liu and S. S. Chung, ‘‘Automatic feature extraction and selection for machine learning based intrusion detection,’’ in Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/ SCI), Aug. 2019, pp. 1400–1405.

[38] M. Lopez-Martin, A. Sanchez-Esguevillas, J. I. Arribas, and B. Carro, ‘‘Network intrusion detection based on extended RBF neural network with offline reinforcement learning,’’ IEEE Access, vol. 9, pp. 153153–153170, 2021.

[39] S. Lei, C. Xia, Z. Li, X. Li, and T. Wang, ‘‘HNN: A novel model to study the intrusion detection based on multi-feature correlation and temporalspatial analysis,’’ IEEE Trans. Netw. Sci. Eng., vol. 8, no. 4, pp. 3257–3274, Oct. 2021.

[40] R. Kumar, A. Malik, and V. Ranga, ‘‘An intellectual intrusion detection system using hybrid hunger games search and remora optimization algorithm for IoT wireless networks,’’ Knowl.-Based Syst., vol. 256, Nov. 2022, Art. no. 109762.

[41] W. Wang, S. Jian, Y. Tan, Q. Wu, and C. Huang, ‘‘Representation learningbased network intrusion detection system by capturing explicit and implicit feature interactions,’’ Comput. Secur., vol. 112, Jan. 2022, Art. no. 102537.

[42] L. Breiman, ‘‘Bagging predictors,’’ Mach. Learn., vol. 24, no. 2, pp. 123–140, 1996.

[43] Y. Freund and R. E. Schapire, ‘‘Experiments with a new boosting algorithm,’’ in Proc. 13th Int. Conf. Int. Conf. Mach. Learn., 1996, pp. 148–156.

[44] T. K. Ho, ‘‘Random decision forests,’’ in Proc. 3rd Int. Conf. Document Anal. Recognit., vol. 1, Aug. 1995, pp. 278–282.

[45] B. Quost and S. Destercke, ‘‘Classification by pairwise coupling of imprecise probabilities,’’ Pattern Recognit., vol. 77, pp. 412–425, May 2018.

[46] T. G. Dietterich and G. Bakiri, ‘‘Solving multiclass learning problems via error-correcting output codes,’’ 1995, arXiv: 9501101.

[47] J. Furnkranz, ‘‘Pairwise classification as an ensemble technique,’’ in Proc. 13th Eur. Conf. Mach. Learn., 2002, pp. 97–110.

[48] T. M. Khoshgoftaar, K. Gao, and N. H. Ibrahim, ‘‘Evaluating indirect and direct classification techniques for network intrusion detection,’’ Intell. Data Anal., vol. 9, no. 3, pp. 309–326, Jun. 2005.

[49] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, ‘‘SMOTE: Synthetic minority over-sampling technique,’’ J. Artif. Intell. Res., vol. 16, pp. 321–357, Jul. 2018.

[50] O. Y. Al-Jarrah, O. Alhussein, P. D. Yoo, S. Muhaidat, K. Taha, and K. Kim, ‘‘Data randomization and cluster-based partitioning for botnet intrusion detection,’’ IEEE Trans. Cybern., vol. 46, no. 8, pp. 1796–1806, Aug. 2016.

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 535X
http://www.ijmert.com
Vol.16 Issue 3, 2024

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

[52] 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.

[53] 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.

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

[55] 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.

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

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

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

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

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