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

MACHINE-LEARNING-BASED CLOUD INTRUSION DETECTION

G VISWANATH[1], N MADHVIK[2], K BHASKAR[3], K SUPRIYA[4]

[1]Associate Professor, Department of CSE(AIML), Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: viswag111@gmail.com, ORCID: https://orcid.org/0009-0001-7822-4739
[2]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: madhvikroyal123@gmai.com
[3]Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: bhaskark.mca@gmail.com
[4]Assistant Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email:srisupriya05@gmail.com

Abstract: Capacity, information the executives, handling power, applications, and more are accessible on request with cloud computing. These assets are effectively available and usable. The task utilizes ML to further develop cloud security with interruption discovery. The primary objective is to screen and dissect cloud assets, administrations, and organizations to identify and forestall cyberattacks. This interruption discovery technique utilizes ML, especially the Random Forest (RF) strategy. Multi-decision tree outfit learning approach Random Forest further develops expectation accuracy. Highlight designing is essential to demonstrate advancement. It incorporates picking and advancing dataset ascribes for the ML model. Powerful element designing assists the model with perceiving patterns and attacks. The model consistently screens cloud assets, administrations, and organizations to further develop cloud security. The model purposes ML procedures to recognize odd digital assault patterns, further developing cloud foundation security. The model's exhibition is approved utilizing Bot-IoT and NSL-KDD. These datasets are interruption discovery benchmarks. Contrasted with ongoing endeavors, the model distinguishes interruptions with high exactness, recommending its value and reliability in spotting security chances. For further developed cloud discovery, the undertaking's Voting Classifier with RF + ADaBoost and Stacking Classifier with RF + MLP with LightGBM accomplished almost 100% and 100 percent accuracy for Kdd-Cup and Bot-IoT information.

Index terms *- cloud security; anomaly detection; features engineering; random forest.*

1. INTRODUCTION

Cloud innovations give more help model choices and on-request admittance to a common organization, stockpiling, and resources[1]. PaaS, SaaS, and IaaS are used in private, public, and crossover cloud arrangement models[2]. Network availability, asset sharing, quickelasticity, and quantifiable help make the cloud capability well, as per the National Institute of Standards and Technology[4].

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

As of late, cloud security issues incorporate accessibility, information classification, respectability, and control consent. Cloud servicesare gotten to over the Web, which represents a colossal risk to cloud frameworks and assets [2]. Then cloud suppliers should focus on security[5]. Firewalls, information encryption procedures, validation strategies, and others have been established to protect cloud conditions from attacks[6]. Customary strategies can't safeguard cloud administrations from different limits[7]. Interruption discovery strategies are introduced and used to recognize and obstruct undesirable action in genuine time[8, 9].

Misuse detection utilizes known attacks to distinguish interruption, though abnormality identification utilizes obscure assaults. Joining the advantages of these two techniques yields the hybridmethod[10]. Notwithstanding more answers for secure cloud conditions, late intrusion detection systems (IDSs) have critical constraints, for example, colossal measures of dissected information, continuous recognition, information quality, and others that diminish discovery model performance[8].

Today, scholarly specialists show that smart learning approaches like machine learning (ML), deep learning (DL), and group learning are successful in many fields and can get networks[14-18]. This examination proposes an abnormality discovery technique in light of random forest (RF) binary classifier and element designing in view of information perception to diminish how much highlights and carry out the recommended oddity recognition model. The model is assessed utilizing NSL-KDD and BoT-IoT datasets. The outcomes show model execution.

2. LITERATURE SURVEY

Cloud computing might convey practical, versatile, simple to-make due, and strong assets over the Web. Distributed computing expands equipment assets through ideal and shared use. The previous characteristics spur ventures and people to move applications and administrations to the cloud [1]. Cloud computing is being taken on by basic framework including power producing and appropriation units. Be that as it may, outsider cloud administrations present additional security chances. Security takes a chance with rise when client resources (information, applications, and so forth) leave regulatory control in a common climate with numerous clients. This review examines distributed computing's intrinsic security chances. The review likewise covers contemporary security arrangements in the writing. Security worries in portable distributed computing are likewise momentarily talked about [18,30]. Open subjects and future review are examined eventually.[52]

The cloud follows through on-request benefits over the Web with a ton of virtual stockpiling. This is one of the vital advantages of distributed computing: no costly PC foundation arrangement and lower costs. Distributed computing has coordinated with business and different areas lately, inspiring scientists to concentrate on new related innovations [2]. Clients and organizations move their applications, information, and administrations to the distributed storage server because of its accessibility and versatility. Remote processing has made a few security troubles and difficulties for purchasers and suppliers, regardless of its advantages. Many cloud

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

administrations are presented by dependable outsiders, making security chances. Web based cloud suppliers use different web innovations that make new security chances [1,23,5,7,19]. This article covered distributed computing essentials, security, dangers, and cures. Cloud structural system, administration and sending model, cloud advances, cloud security thoughts, dangers, and attacks are completely shrouded in the paper. Open cloud security research points are likewise shrouded in the article.[54]

The issue of organization security is vital. Intrusion detection systems are normally used for network security. Ensemble learning has been a famous ML technique for further developing interruption identification frameworks [6]. Furthermore, preparing information quality can extensively further develop recognition. Realizing that minor thickness proportions are the best univariate classifiers. SVM outfit with highlight expansion is utilized in this article to make a successful interruption location strategy. SVM gathering was utilized to foster the interruption discovery model after logarithm peripheral thickness proportions change was applied to the first elements to obtain new and further developed preparing information. Our proposed procedure outflanks past techniques in accuracy, detection rate, false alarm rate, and training speed, as per tests. [6,24]

Distributed computing lets end clients easily connect complex administrations and applications through the Web. Giving protected and reliable distributed computing administrations is urgent. Since network interruptions can think twice about classification, accessibility, and respectability of Cloud assets and administrations, security requires more than client verification with passwords or advanced declarations and information transmission privacy [1,23,5,7,19]. Conventional firewalls are inadequate in distinguishing DoS assaults and other organization level hurtful action in Cloud. This exploration proposes a cooperative and hybrid network intrusion detection system (CH-NIDS) to screen network traffic in the Cloud to distinguish network dangers while keeping up with execution and administration quality [7]. Our NIDS design involves Grunt for signature-based identification of known dangers and Back-Engendering Brain network for network irregularity recognition. BPN just identifies obscure attacks subsequent to applying grunt before the classifier. This decreases recognizing time. To tackle BPN's sluggish intermingling and simple fall into neighborhood ideal, we propose streamlining its boundaries utilizing an advancement calculation to guarantee high recognition rate, exactness, low bogus up-sides, and low misleading negatives with low computational expense. IDSs likewise collaborate to safeguard against DoS and DDoS attacks by trading cautions in a typical log [32,47]. Subsequently, other IDSs can promptly find obscure dangers distinguished by one. This additionally brings down processing cost for different IDS interruption recognition and further develops Cloud identification rate.

Cyberattacks are developing progressively intricate, making interruption discovery harder. Without interruption counteraction, security administrations like information secrecy, uprightness, and accessibility might lose trust. The writing proposes a few interruption discovery methodologies to battle PC security chances, including Signature-based and Anomaly-based Systems (SIDS and AIDS). This

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

review study [8] gives a scientific classification of present day IDS, a total investigation of current endeavors, and an outline of assessment datasets [22,29]. It additionally analyzes assailant avoidance procedures and forthcoming exploration difficulties to defend PC frameworks.

3. METHODOLOGY

i) Proposed Work:

Strategic feature engineering and the precise and tough Random Forest ML method are utilized. This blend makes a strong cloud interruption discovery framework to help security. A powerful and reliable arrangement that further develops cloud security is accomplished by appropriately perceiving potential dangers and abnormal examples. Likewise, a Voting Classifier with Random Forest (RF) and ADaBoost accomplishes close to 100% accuracy for the Kdd-Cup dataset. Utilizing Random Forest (RF), Multi-Layer Perceptron (MLP), and LightGBM, the Stacking Classifier accomplishes 100 percent accuracy for the Bot-IoT dataset [28,29,39]. Our group models show our devotion to hearty and high-performing cloud interruption identification. The easy to use Flask framework with SQLite incorporation makes network safety application client testing simple and secure.[56]

ii) System Architecture:

After dataset revelation and preprocessing, train-test split and model preparation are basic. The fundamental engineering utilizes group draws near, like the Stacking Classifier and Voting Classifier expansions, to further develop interruption identification [24]. Model appraisals show that these classifiers are successful, with almost 100% and 100 percent accuracy. The design stresses model versatility to perceive differed datasets and viable use through an easy to understand interface empowered by the Flask framework and SQLite association. This brought together framework configuration makes the undertaking a strong and versatile ML based cloud iintrusion detection solution.

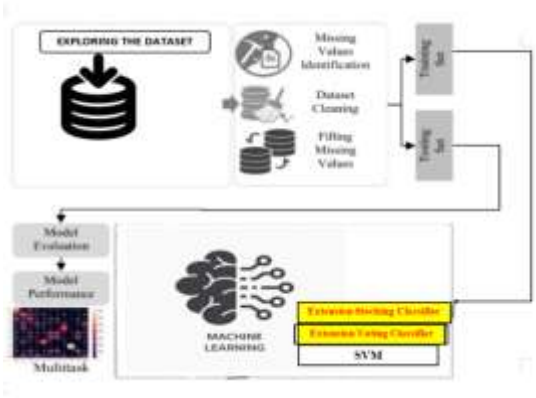


Fig 1 Proposed architecture

iii) Dataset collection:

KDD CUP DATASET

The intrusion detection system research dataset KDD-CUP [35,26] is oftentimes used. The KDD-CUP dataset is utilized to prepare and assess ML models to recognize interruptions and cyberattacks in cloud-based interruption identification. Creating models that screen network information and distinguish odd or vindictive examples is fundamental for cloud security.

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

```
data = pd.read_csv("archive/kdd_train.csv")
data.head()
```

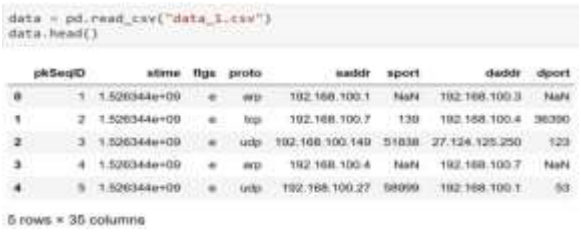
	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot
0	0	tcp	ftp_data	SF	491	0	0	0	0	0
1	0	udp	other	SF	146	0	0	0	0	0
2	0	tcp	private	S0	0	0	0	0	0	0
3	0	tcp	http	SF	232	8153	0	0	0	0
4	0	tcp	http	SF	199	420	0	0	0	0

5 rows × 42 columns

Fig 2 KDD-CUP dataset

BOT IOT DATASET

The BOT-IoT dataset practices on IoT security. In a cloud-based ntrusion detection strategy utilizing ML, the BOT-IoT dataset [46] is helpful for preparing and surveying IoT gadget and organization intrusion detection models. Cloud-based intrusion detection requires understanding and alleviating IoT-based attacks since IoT gadgets are commonly associated with cloud stages.



```
data = pd.read_csv("data_1.csv")
data.head()
```

	pkSeqID	stime	flgs	proto	saddr	sport	daddr	dport
0	1	1.526344e+09	e	arp	192.168.100.1	NaN	192.168.100.3	NaN
1	2	1.526344e+09	e	tcp	192.168.100.7	139	192.168.100.4	36390
2	3	1.526344e+09	e	udp	192.168.100.149	51838	27.124.125.250	123
3	4	1.526344e+09	e	arp	192.168.100.4	NaN	192.168.100.7	NaN
4	5	1.526344e+09	e	udp	192.168.100.27	58099	192.168.100.1	53

5 rows × 35 columns

Fig 3 BOT-IOT dataset

iv) Data Processing:

Data processing transforms crude information into business-helpful data. Data researchers accumulate, sort out, clean, check, examine, and organize information into diagrams or papers. Information can be handled physically, precisely, or electronically. Data ought to be more significant and decision-production simpler. Organizations might improve tasks and pursue basic decisions quicker. PC programming advancement and other robotized information handling innovations add to this. Big data can be transformed into applicable 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.[58]

vi) Algorithms:

Random Forest (RF), RF is an ensemble learning approach that prepares various choice trees and reports the method of their characterizations. Its accuracy, ability to endure overfitting, and tremendous list of capabilities make it astounding for intrusion detection.

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=40)

# 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)
rf_rec = recall_score(y_pred, y_test)
rf_f1 = f1_score(y_pred, y_test)
rf_auroc = roc_auc_score(y_test, rf.predict_proba(X_test)[:, 1])
rf_mcc = matthews_corrcoef(y_pred, y_test)


storeResults('Random Forest',rf_acc,rf_prec,rf_rec,rf_f1,rf_auroc,rf_mcc)
```

Fig 4 Random forest

Decision Tree (DT) DT are administered learning models that make decisions by posing inquiries about dataset properties. It makes a tree-like construction utilizing highlight values to assist with recognizing interruptions by grasping decision guidelines [28].

```
from sklearn.tree import DecisionTreeClassifier

# instantiate the model
tree = DecisionTreeClassifier(max_depth=30)

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

#predicting the target value from the model for the samples

y_pred = tree.predict(X_test)

dt_acc = accuracy_score(y_pred, y_test)
dt_prec = precision_score(y_pred, y_test)
dt_rec = recall_score(y_pred, y_test)
dt_f1 = f1_score(y_pred, y_test)
dt_auroc = roc_auc_score(y_test, tree.predict_proba(X_test)[:, 1])
dt_mcc = matthews_corrcoef(y_pred, y_test)


storeResults('Decision Tree Classifier',dt_acc,dt_prec,dt_rec,dt_f1,dt_auroc,dt_mcc)
```

Fig 5 Decision tree

Support Vector Machine (SVM) A strong managed learning strategy for characterization is SVM. A hyperplane or gathering of hyperplanes in high-layered space isolates classes. SVM handles muddled information relationships and non-linearity well, making it accommodating in intrusion detection.[60]

```
from sklearn.svm import SVC

# instantiate the model
svm = SVC(probability=True)

# 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)

svc_acc = accuracy_score(y_pred, y_test)
svc_prec = precision_score(y_pred, y_test)
svc_rec = recall_score(y_pred, y_test)
svc_f1 = f1_score(y_pred, y_test)
svc_auroc = roc_auc_score(y_test, svm.predict_proba(X_test)[:, 1])
svc_mcc = matthews_corrcoef(y_pred, y_test)


storeResults('Support Vector Machine',svc_acc,svc_prec,svc_rec,svc_f1,svc_auroc,svc_mcc)
```

Fig 6 SVM

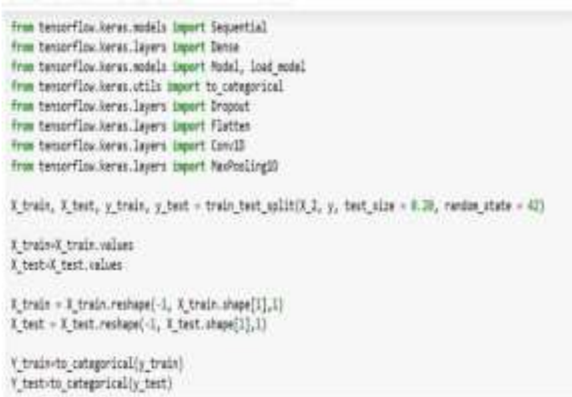
Naive Bayes Bayes' hypothesis based probabilistic order strategy NB. It infers attributes are free, which may not be valid all the time. NB is used in intrusion detection since it is basic and quick, particularly with text [28].

```
from sklearn.naive_bayes import GaussianNB

# instantiate the model
nb = GaussianNB()

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

#predicting the target value from the model for the samples

y_pred = nb.predict(X_test)

nb_acc = accuracy_score(y_pred, y_test)
nb_prec = precision_score(y_pred, y_test)
nb_rec = recall_score(y_pred, y_test)
nb_f1 = f1_score(y_pred, y_test)
nb_auroc = roc_auc_score(y_test, nb.predict_proba(X_test)[:, 1])
nb_mcc = matthews_corrcoef(y_pred, y_test)


storeResults('Naive Bayes',nb_acc,nb_prec,nb_rec,nb_f1,nb_auroc,nb_mcc)
```

Fig 7 Naïve bayes

Deep Learning (DL) Deep learning utilizes multi-layered neural networks. DL models like MLPs, CNNs, and RNNs can learn muddled information designs, making them helpful for intrusion detection with complex qualities.

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



```
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import Dense
from tensorflow.keras.models import Model, load_model
from tensorflow.keras.utils import to_categorical
from tensorflow.keras.layers import Dropout
from tensorflow.keras.layers import Flatten
from tensorflow.keras.layers import Conv1D
from tensorflow.keras.layers import MaxPooling1D

X_train, X_test, y_train, y_test = train_test_split(X_2, y, test_size = 0.20, random_state = 42)

X_train=X_train.values
X_test=X_test.values

X_train = X_train.reshape(-1, X_train.shape[1],1)
X_test = X_test.reshape(-1, X_test.shape[1],1)

Y_train=to_categorical(y_train)
Y_test=to_categorical(y_test)
```

Fig 8 Deep learning

Long Short-Term Memory (LSTM) RNNs like LSTM are intended to address groupings and time-subordinate information. LSTM can catch long term connections in arrangements of occasions or organization action, making it helpful for iintrusion detection [33].

Fig 9 LSTM

Stacking Classifier (RF + MLP with Light GBM)

The Stacking Classifier expansion predicts utilizing Random Forest (RF), Multi-Layer Perceptron (MLP), and Light Gradient Boosting Machine. RF, an ensemble of decision trees, catches convoluted designs well, though MLP with LightGBM offers fluctuated learning strategies. In cloud frameworks with differed digital dangers, the Stacking Classifier naturally mixes their results to further develop intrusion detection execution.

Fig 10 Stacking classifier

Voting Classifier (RF + AdaBoost)

The Voting Classifier addon makes serious areas of strength for an identification model utilizing Random Forest (RF) and AdaBoost. RF's choice trees catch definite examples, while AdaBoost changes loads to accentuate precise arrangement of beforehand misclassified cases. This blend makes a strong troupe model that utilizes the two classifiers to precisely and dependably identify cloud-based framework interruptions. This troupe's flexibility makes it reasonable for an assortment of digital dangers, further developing the undertaking's intrusion detection method.

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

RF + AdaBoost

```
from sklearn.ensemble import RandomForestClassifier, VotingClassifier, AdaBoostClassifier
clf1 = AdaBoostClassifier(n_estimators=100, random_state=0)
clf2 = RandomForestClassifier(n_estimators=50, random_state=1)

eclf1 = VotingClassifier(estimators=[('lr', clf1), ('rf', 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)
vot_rec = recall_score(y_pred, y_test)
vot_f1 = f1_score(y_pred, y_test)
vot_auroc = roc_auc_score(y_test, eclf1.predict_proba(X_test)[:, 1])
vot_mcc = matthews_corrcoef(y_pred, y_test)


storeResults('RF + AdaBoost',vot_acc,vot_prec,vot_rec,vot_f1,vot_auroc,vot_mcc)
```

Fig 11 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)

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

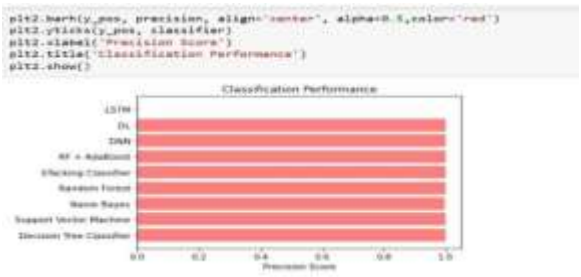


Fig 6 Precision comparison graph

Recall: ML recall measures a model's ability to catch all class occurrences. The model's ability to recognize a certain type of event is measured by the percentage of precisely anticipated positive prospects that turn into real earnings.

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

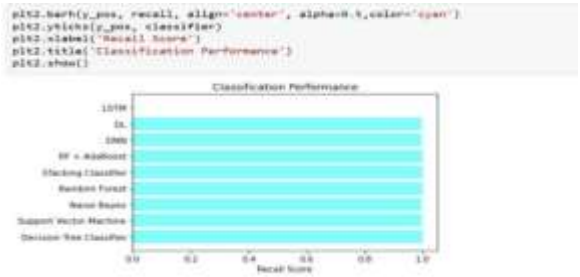


Fig 7 Recall comparison graph

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

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

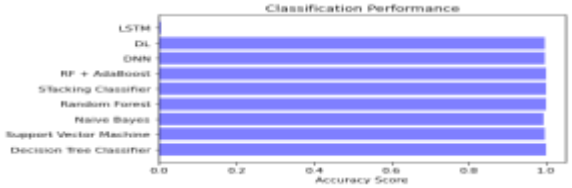


Fig 8 Accuracy graph

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

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

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

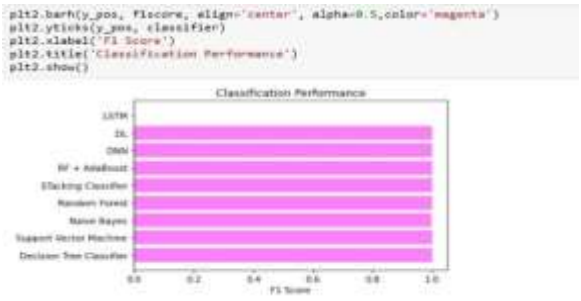


Fig 9 F1Score

ML Model	Accuracy	Precision	Recall	F1-Score
Decision Tree Classifier	1.000	1.000	1.000	1.000
Support Vector Machine	0.996	1.000	0.996	0.998
Naive Bayes	0.993	0.997	0.996	0.997
Random Forest	1.000	1.000	1.000	1.000
Extension Stacking Classifier	1.000	1.000	1.000	1.000
Extension RF + AdaBoost	1.000	1.000	1.000	1.000
DNN	0.996	1.000	0.996	0.998
DL	0.995	1.000	0.995	0.998
LSTM	0.005	0.000	0.000	0.000

Fig 10 Performance Evaluation

Fig 11 Home page

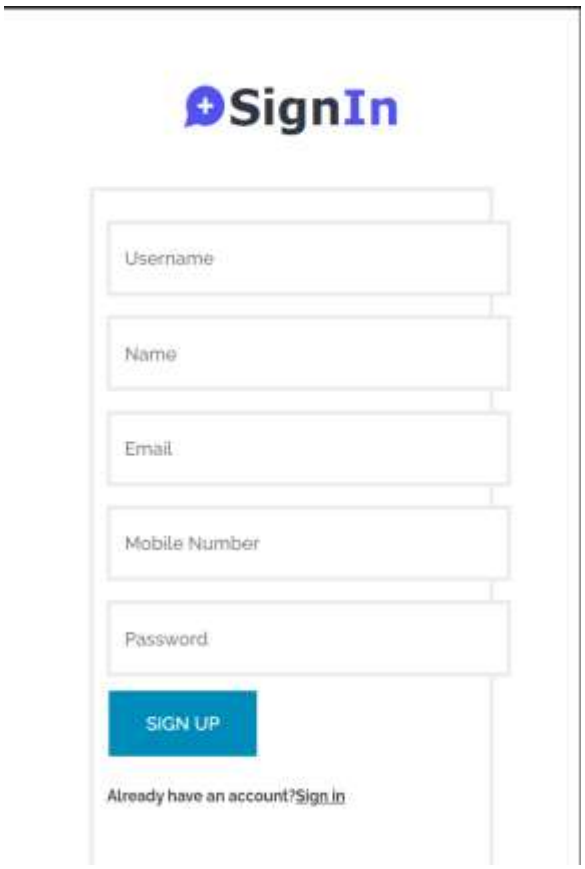


Fig 12 Signin page

Fig 13 Login page

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

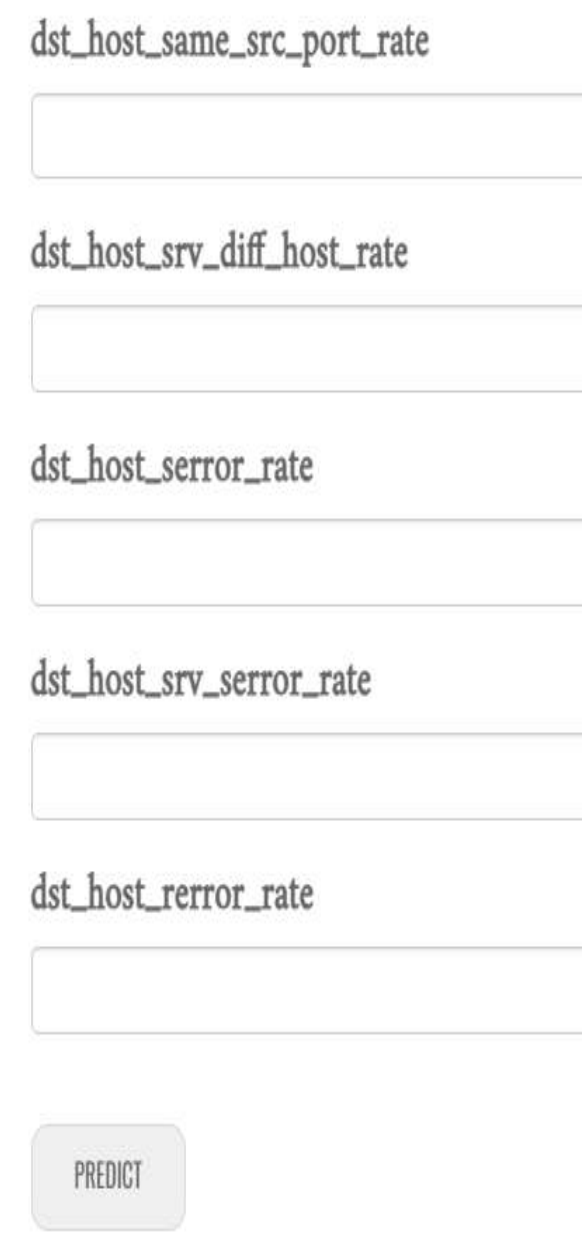


Fig 14 User input

Fig 15 Predict result for given input

5. CONCLUSION

Cloud intrusion detection using Random Forest (RF) and element designing is exact, exact, and review rich. It distinguishes atypical cloud action better compared to late endeavors. This shows the methodology's viability and trustworthiness. RF [26,29] is critical to the model's presentation. RF handles anomaly information well, making variant action distinguishing proof vigorous. Straightforward boundary setting and computerized variable importance and accuracy measurements pursue it a productive decision, further developing intrusion detection model execution. Voting Classifier and Stacking Classifier ensemble techniques further develop precision. Utilizing an easy to understand Flask interface with secure confirmation increments network safety application testing convenience.

6. FUTURE SCOPE

Deep learning (DL) and troupe learning will be utilized to further develop review, explicitly on the NSL-KDD dataset [27]. Deep learning models might further develop interruption identification by catching confounded designs. Ensemble approaches utilize many models to work on conjecture exactness and interruption recognition framework viability. Future frameworks will break down client and framework conduct. Precise peculiarity discovery and security danger ID need this procedure. Breaking down ways of behaving makes a benchmark for routine action, making security breaks easier to detect. The task will construct interruption recognition advancements that scale with cloud information intricacy and volume.

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

Improving assets for execution and cost-viability will guarantee the framework can oversee developing information load and adjust to changing cloud foundations. Joining many models utilizing group learning will further develop forecast exactness. Ensemble learning further develops the interruption location framework's exactness and dependability in perceiving cloud security chances.

REFERENCES

[1] M. Ali, S. U. Khan, and A. V. Vasilakos, Security in cloud computing: Opportunities and challenges, Information Sciences, vol. 35, pp. 357–383, 2015.

[2] A. Singh and K. Chatterjee, Cloud security issues and challenges: A survey, Journal of Network and ComputerApplications, vol. 79, pp. 88–115, 2017.

[3] P. S. Gowr and N. Kumar, Cloud computing security: A survey, International Journal of Engineering and Technology, vol. 7, no. 2, pp. 355–357, 2018.

[4] A. Verma and S. Kaushal, Cloud computing security issues and challenges: A survey, in Proc. First International Conference on Advances in Computing and Communications, Kochi, India, 2011, pp. 445–454.

[5] H. Alloussi, F. Laila, and A. Sekkaki, L'etat de l'art de la ´ securit ´ e dans le cloud computing: Probl ´ emes et solutions ` de la securit ´ e en cloud computing, presented at Workshop ´ on Innovation and New Trends in Information Systems, Mohamadia, Maroc, 2012.

[6] J. Gu, L. Wang, H. Wang, and S. Wang, A novel approach to intrusion detection using SVM ensemble with feature augmentation, Computers and Security, vol. 86, pp. 53–62, 2019.

[7] Z. Chiba, N. Abghour, K. Moussaid, A. E. Omri, and M. Rida, A cooperative and hybrid network intrusion detection framework in cloud computing based snort and optimized back propagation neural network, Procedia Computer Science, vol. 83, pp. 1200–1206, 2016.

[8] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, Survey of intrusion detection systems: Techniques, datasets and challenges, Cybersecurity, vol. 2, p. 20, 2019.

[9] A. Guezzaz, A. Asimi, Y. Asimi, Z. Tbatou, and Y. Sadqi, A global intrusion detection system using PcapSockS sniffer and multilayer perceptron classifier, International Journal of Network Security, vol. 21, no. 3, pp. 438–450, 2019.

[10] A. Guezzaz, S. Benkirane, M. Azrour, and S. Khurram, A reliable network intrusion detection approach using decision tree with enhanced data quality, Security and Communication Networks, vol. 2021, p. 1230593, 2021.

[11] B. A. Tama and K. H. Rhee, HFSTE: Hybrid feature selections and tree-based classifiers ensemble for intrusion detection system, IEICE Trans. Inf. Syst., vol. E100.D, no. 8, pp. 1729–1737, 2017.

[12] M. Azrour, J. Mabrouki, G. Fattah, A. Guezzaz, and F. Aziz, Machine learning algorithms for efficient

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

water quality prediction, Modeling Earth Systems and Environment, vol. 8, pp. 2793–2801, 2022.

[13] M. Azrour, Y. Farhaoui, M. Ouanan, and A. Guezzaz, SPIT detection in telephony over IP using K-means algorithm, Procedia Computer Science, vol. 148, pp. 542–551, 2019.

[14] M. Azrour, M. Ouanan, Y. Farhaoui, and A. Guezzaz, Security analysis of Ye et al. authentication protocol for internet of things, in Proc. International Conference on Big Data and Smart Digital Environment, Casablanca, Morocco, 2018, pp. 67–74.

[15] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, Internet of things security: Challenges and key issues, Security and Communication Networks, vol. 2021, p. 5533843, 2021.

[16] A. Guezzaz, S. Benkirane, and M. Azrour, A novel anomaly network intrusion detection system for internet of things security, in IoT and Smart Devices for Sustainable Environment, M. Azrour, A. Irshad, and R. Chaganti, eds. Cham, Switzerland: Springer, 2022, pp. 129–138.

[17] A. Guezzaz, A. Asimi, M. Azrour, Z. Tbatou, and Y. Asimi, A multilayer perceptron classifier for monitoring network traffic, in Proc. 3rd International Conference on Big Data and Networks Technologies, Leuven, Belgium, 2019, pp. 262–270.

[18] S. Benkirane, Road safety against sybil attacks based on RSU collaboration in VANET environment, in Proc. 5th International Conference on Mobile, Secure, and Programmable Networking, Mohammedia, Morocco, 2019, pp. 163–172.

[19] Q. Zhang, L. Cheng, and R. Boutaba, Cloud computing: State-of-the-art and research challenges, J. Internet Serv. Appl., vol. 1, pp. 7–18, 2010.

[20] M. K. Srinivasan, K. Sarukesi, P. Rodrigues, M. S. Manoj, and P. Revathy, State-of-the-art cloud computing security taxonomies: A classification of security challenges in the present cloud computing environment, in Proc. 2012 International Conference on Advances in Computing, Communications and Informatics, Chennai, India, 2012, pp. 470–476.

[21] A. L. Buczak and E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[22] A. Alshammari and A. Aldribi, Apply machine learning techniques to detect malicious network traffic in cloud computing, Journal of Big Data, vol. 8, p. 90, 2021.

[23] A. Geron, ´ Hands-On Machine Learning with Scikit-Learn & TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. Sebastopol, CA, USA: O'Reilly Media, Inc., 2017.

[24] N. Chand, P. Mishra, C. R. Krishna, E. S. Pilli, and M. C. Govil, A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection, in Proc. 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA), Dehradun, India, 2016, pp. 1–6.

International Journal of Mechanical Engineering Research and Technology

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

[25] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, Machine learning for cloud security: A systematic review, IEEE Access, vol. 9, pp. 20717–20735, 2021.

[26] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, A survey of deep learning-based network anomaly detection, Cluster Comput., vol. 22, pp. 949–961, 2017.

[27] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, Journal of Information Security and Applications, vol. 50, p. 102419, 2020.

[28] V. Kanimozhi and T. P. Jacob, Calibration of various optimized machine learning classifiers in network intrusion detection system on the realistic cyber dataset CSE-CICIDS2018 using cloud computing, International Journal of Engineering Applied Sciences and Technology, vol. 4, no. 6, pp. 209–213, 2019.

[29] L. Zhou, X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang, Cyber-attack classification in smart grid via deep neural network, in Proc. 2nd International Conference on Computer Science and Application Engineering, Hohhot, China, 2018, pp. 1–5.

[30] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, Deep learning approach for network intrusion detection in software defined networking, in Proc. 2016 International Conference on Wireless Networks and Mobile Communications, Fez, Morocco, 2016, pp. 258–263.

[31] L. Zhang, L. Shi, N. Kaja, and D. Ma, A two-stage deep learning approach for can intrusion detection, in Proc. 2018 Ground Vehicle Syst. Eng. Technol. Symp. (GVSETS), Novi, MI, USA, 2018, pp. 1–11.

[32] A. Mishra, B. B. Gupta, D. Perakovic, F. J. G. Penalvo, and C. H. Hsu, Classification based machine learning for detection of DDoS attack in cloud computing, in Proc. 2021 IEEE International Conference on Consumer Electronics, Las Vegas, NV, USA, 2021, pp. 1–4.

[33] F. Jiang, Y. Fu, B. B. Gupta, Y. Liang, S. Rho, F. Lou, F. Meng, and Z. Tian, Deep learning based multichannel intelligent attack detection for data security, IEEE Transactions on Sustainable Computing, vol. 5, no. 2, pp. 204–212, 2018.

[34] A. N. Khan, M. Y. Fan, A. Malik, and R. A. Memon, Learning from privacy preserved encrypted data on cloud through supervised and unsupervised machine learning, in Proc. 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies, Sukkur, Pakistan, 2019, pp. 1–5.

[35] S. Potluri and C. Diedrich, Accelerated deep neural networks for enhanced intrusion detection system, in Proc. 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation, Berlin, Germany, 2016, pp. 1–8.

[36] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, Long short term memory recurrent neural network classifier for intrusion detection, in Proc. 2016 International Conference on Plateform Technology and Service, Jeju, Republic of Korea, 2016, pp. 1–5.

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

[37] J. Zhang, Anomaly detecting and ranking of the cloud computing platform by multi-view learning, Multimedia Tools and Applications, vol. 78, pp. 30923–30942, 2019.

[38] F. B. Ahmad, A. Nawaz, T. Ali, A. A. Kiani, and G. Mustafa, Securing cloud data: A machine learning based data categorization approach for cloud computing, http://doi.org/ 10.21203/rs.3.rs-1315357/v1, 2022.

[39] A. Mubarakali, K. Srinivasan, R. Mukhalid, S. C. Jaganathan, and N. Marina, Security challenges in Internet of things: Distributed denial of service attack detection using support vector machine-based expert systems, Computational Intelligence, vol. 36, no. 4, pp. 1580–1592, 2020.

[40] N. M. Abdulkareem and A. M. Abdulazeez, Machine learning classification based on radom forest algorithm: A review, International Journal of Science and Business, vol. 5, no. 2, pp. 128–142, 2021.

[41] L. Breiman, Random forests, Machine Learning, vol. 45, pp. 5–32, 2001.

[42] I. Reis, D. Baron, and S. Shahaf, Probabilistic random forest: A machine learning algorithm for noisy data sets, The Astronomical Journal, vol. 157, no. 1, p. 16, 2018.

[43] J. Ali, R. Khan, N. Ahmad, and I. Maqsood, Random forests and decision trees, IJCSI International Journal of Computer Science Issues, vol. 9, no. 5, pp. 272–278, 2012.

[44] B. O. Yigin, O. Algin, and G. Saygili, Comparison of morphometric parameters in prediction of hydrocephalus using random forests, Computers in Biology and Medicine, vol. 116, p. 103547, 2020.

[45] A. Sarica, A. Cerasa, and A. Quattrone, Random forest algorithm for the classification of neuroimaging data in alzheimer's disease: A systematic review, Frontiers in Aging Neuroscience, vol. 9, p. 329, 2017.

[46] A. Devarakonda, N. Sharma, P. Saha, and S. Ramya, Network intrusion detection: A comparative study of four classifiers using the NSL-KDD and KDD'99 datasets, Journal of Physics: Conference Series, vol. 2161, p. 012043, 2022.

[47] M. Zeeshan, Q. Riaz, M. A. Bilal, M. K. Shahzad, H. Jabeen, S. A. Haider, and A. Rahim, Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSWNB15 and Bot-IoT data-sets, IEEE Access, vol.10, pp. 2269– 2283, 2021.

[48] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, CorrAUC: A malicious Bot-IoT traffic detection method in IoT network using machine-learning techniques, IEEE Internet Things J., vol. 8, no. 5, pp. 3242–3254, 2021.

[49] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, Selection of effective machine learning algorithm and BotIoT attacks traffic identification for Internet of things in smart city, Future Generation Computer Systems, vol. 107, pp. 433–442, 2020.

[50] M. Hossin and M. N. Sulaiman, A review on evaluation metrics for data classification evaluations, International Journal of Data Mining & Knowledge Management Process, doi: 10.5121/ijdkp.2015.5201.

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