International Journal of HRM and Organizational Behavior

www.ijhrmob.com

editor@ijhrmob.com

A MACHINE LEARNING BASED CYBERATTACK DETECTOR FOR HEALTHCARE SYSTEMS IN SOFTWARE-DEFINED NETWORKING (SDN)

T ANIL KUMAR[1], *T AJITH*[2], *SYED JEELAN*[3]
[1]*Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: anil.thumburu@gmail.com*
[2]*P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: thumburuajith18@gmail.com*
[3]*Associate Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email:jee.fuzi@gmail.com*

Abstract: Software-defined networks (SDNs) give huge issues to medical care suppliers in getting delicate patient information. Digital dangers are developing more complicated, in this manner medical services applications need solid security. The venture recommends an Machine Learning-based Cyberattack Detector (MCAD). MCAD identifies and answers an assortment of medical care digital dangers utilizing ML methods. Medical care network safety is pivotal, and this drive settles it. Safeguarding patient information and ensuring medical care network versatility are vital for patient wellbeing and medical services establishment certainty. The venture intends to further develop medical services framework security and strength by decreasing digital dangers and improving organization execution. This review utilized troupe approaches like Stacking and Voting Classifiers to upgrade cyberattack identification for Medical care Frameworks using SDN and got 100 percent accuracy. Made a straightforward Flask front end with safe validation for medical services.[58]

Index Terms *- Network resilience, network management, intrusion detection system (IDS), software defined networking, healthcare, machine learning.*

1. INTRODUCTION

As of late, SDNs have been broadly utilized in a few regions because of their dependability and capacity to control and oversee networks by disaggregating control and information planes. Not at all like regular organizations, which just have application mindfulness, SDN configuration offers additional organization status data from the regulator to its applications. Following the fast headway of information and communications technologies (ICT), medical services foundations are utilizing numerous infrastructural parts of off-the-rack innovation, applications, and strategies utilized by different associations. This was anticipated since arranged or Internet associated clinical instruments further develop resource the executives, correspondences, and electronic wellbeing records, decreasing costs.Since classification and security are urgent in medical care because of the business' severe necessities, most data frameworks focus on framework and gadget security and client information privacy. In spite of the fact that emergency clinic gear costs are normal, the ongoing McAfee record noticed that arranged clinical apparatuses may uncover security holes in the clinical business' endeavor to consolidate all specialized components connected with organized foundation and functional controls.

This undertaking fosters an MCAD for programming characterized organizations to further develop medical care framework security. MCAD will be executed on the Ryu controller utilizing a L3 learning change application to survey typical and bizarre organization traffic. A definite exhibition assessment is given by assessing a few AI strategies and cyberattack situations. MCAD's solid F1-score for both typical and assault classes demonstrates steadfastness, and its ongoing throughput rate is 5,709,692 examples each second.[60]

Safeguarding touchy patient information in programming characterized networks is a central issue for medical care. Regardless of their advantages, SDNs are helpless against a few cyberattacks that undermine network respectability and patient wellbeing. This examination utilizes a layer three (L3) learning change application on the Ryu controller to develop an MCAD for medical care frameworks. MCAD's exhibition against ML calculations and assault situations will be assessed in this venture to further develop medical services information security and organization versatility.

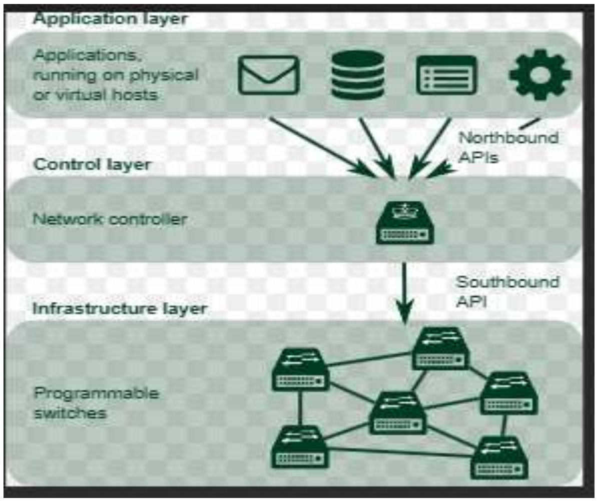


Fig 1 SDN Architecture

Notwithstanding the weakness of data in medical care organizations, the complexity, amount, and variety of instruments, eminently arranged clinical gadgets (e.g., remote pacemakers), fabricating this foundation will expand protection and security dangers [4], [5]. Assaults have fivefold ascended during the Coronavirus pandemic. Information breaks have impacted 90% of medical services suppliers [6]. As shown by ongoing ransomware occurrences [7], the medical services industry is especially powerless against cyberattacks because of classification breaks (e.g., released or contained touchy clinical records), accidental mistakes, or intentional and broad obstruction. SDN's capacity to isolate network strategy from network gadgets has driven specialists to consider using it in medical services [8].

SDNs could protect clinical organizations from malevolent attacks like denial-of-service (DoS) and examining assaults. SDN arrangements, such interruption discovery and counteraction frameworks and incorporated security draws near, don't protect information and frameworks against insider dangers [9]. For example, 92% of medical services organizations revealed insider danger gambles and required security [10]. To alleviate insider risks, utilitarian arrangements are required.[62]

2. LITERATURE SURVEY

Arising innovation have expanded medical services difficulties today. Sensors, IIoT, and large information examination can work on understanding consideration and cut medical care costs. This will give patients more secure, less expensive, and higher clinical consideration [8]. Notwithstanding asset compelled IoT, fraud, and threatening insiders, brilliant medical care in large information and computerized reasoning need edge processing administrations. We propose a SDN-based security consistence structure for brilliant medical services load movement frameworks to resolve these issues. Specialists and specialists are examining SDN-IIoT advances for continuous security assurance. Three areas with one virtual machine and various OpenFlow virtual changes make around our system [1,8,12,26,39]. This situation adjusts the area by moving medical care information from the completely stacked space to the gently stacked space, forestalling security attacks. The RYU SDN regulator recreates and assesses mininet execution after Wireshark catches OpenFlow parcels. System and calculation give secure information dealing with and 80% accuracy for all gained medical care information bundles.

Centralization, application programmability points of interaction, and quick approach execution across entire organizations are advantages of programming characterized networks. Versatility and security are superior to conventional organizations, albeit concentrated control may be defenseless against DDoS attacks. In [19], two famous SDN regulators are analyzed and the impact of inside forswearing of administration assault on the southward connection point during switch enlistment is analyzed. Regulator computer processor use and response time are contemplated during the attack.

In this review, a Intruder Detection System (IDS) coordinated into a Artificial Neural Network (ANN) (Snort+RNA) is introduced to diminish the gamble of dynamic PC attacks on a SDN [20]. Which utilizes the Specialized College of the North Faculty of Engineering of Applied Science (FICA) server farm's hyperconverged network. The ISO/IEC 27001 PDCA model and hacking circle methods are utilized to test this thought. Snort + RNA identifies irregularities causing dynamic sort assaults on SDN, as found in cautions and traffic records. In any case, a few bundles stay on hold or dismissed, restricting examination of DoS assaults. This shows that, while the framework doesn't survey each organization bundles, it safeguards the SDN by alarming outsiders when they attempt to penetrate it with attacks that increment network traffic [12,19,26,28].

IoT is a complex correspondence and systems administration innovation for brilliant and computerized handling. With the Internet of Things being utilized in additional fundamental undertakings, no problem at all gadget availability is significant. Cyberattacks represent the most serious risk to get correspondence. Cyberattacks have gotten progressively confounded, undermining information uprightness, correspondence security, and mystery. Interruption recognition frameworks are superb for IoT gadget security since they recognize correspondence network security blemishes [21]. Nonetheless, incorporating an interruption identification framework into an IoT network is troublesome. This study audits major IoT and interruption recognition framework endeavors to survey the cutting edge, innovation, and hardships [34]. A far reaching writing investigation of 25 sources incorporates 22 examination papers and articles on danger models, IoT interruption recognition framework center issues, proposed models, execution, surveys, and assessments. The discoveries analyze the requests and best practices for coordinating AI-based interruption discovery frameworks in IoT organizations to get correspondence.[64]

Most of Internet of Things (IoT) gadgets utilize remote means, requiring various IDS frameworks to involve

802.11 header data for interruption location. Information joins, not application layers, in wired networks have remote explicit traffic qualities with significant data gain. [22] This survey looks at remote IDS sending issues in information gathering, IDS strategies, area, and traffic information handling. Absence of organization follows for preparing contemporary ML models against IoT interruptions is this paper's key outcome. In light of current information properties, the Knowledge Discovery in Databases (KDD) Cup dataset is assessed to feature remote interruption discovery configuration issues and propose various rules to future-verification remote organization traffic catch draws near. Interruption discovery, information gathering, and position techniques are investigated to begin the article. [42,44] The plan issues of remote interruption discovery frameworks are the focal point of this exploration. Wireless intrusion detection system execution is more convoluted attributable to building contrasts. This paper breaks down wired interruption location arrangement strategies, examines how they might be utilized remotely, and addresses remote plan issues. Wireless Sensor Networks (WSN), Mobile Ad Hoc Networks (MANET), and IoT are future improvements that have been focused on for attacks. Along these lines, remote organization explicit IDS engineering is fundamental.

3. METHODOLOGY

i) Proposed Work:

The task proposes an MCAD to further develop medical clinic online protection. It safeguards delicate patient information in medical services applications and organizations by distinguishing and answering an assortment of digital dangers utilizing ML methods. MCAD's dexterity, continuous reactivity, and broad danger inclusion make it a phenomenal cyberdefense and network security arrangement. Furthermore, a gathering procedure consolidates the prescient capacities of Stacking Classifier and Voting Classifier models. The two classifiers had 100 percent accuracy, showing the group approach's cyberattack discovery flexibility in Programming SDN for Medical services Systems[12,14,33]. Flask assisted us with making an easy to use front end for client testing. This connection point validates clients to safeguard the Cyberattacks Detector and work on its helpfulness in medical care settings.

ii) System Architecture:

Phase 1: In Phase 1, the model proposes a logical network topology for the medical care framework.

Phase 2: Data Collection: Information is gathered for ML model preparation and testing [19,42]. This incorporates examining assault, VNC port 5900 remote view weakness, Samba server weakness, and customary models.

Phase 3: Data Preprocessing information sets it up for ML model preparation.

Phase 4: ML Model Training and Testing: KNN, DT, RF, NB, LR, adaboost, and xgboost are utilized to prepare and assess the ML model. To track down patterns and lessen botches, the model makes an info yield planning capability. Not set in stone by precision [19,42].

Phase 5: Project deployment: The UI utilizes the learned ML model. The methodology might be conveyed progressively frameworks, further developing medical services quality.

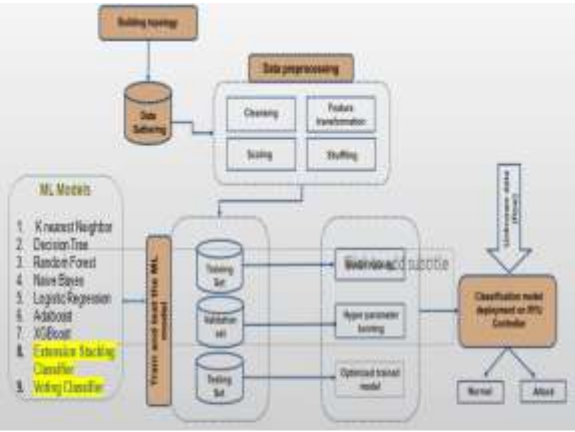
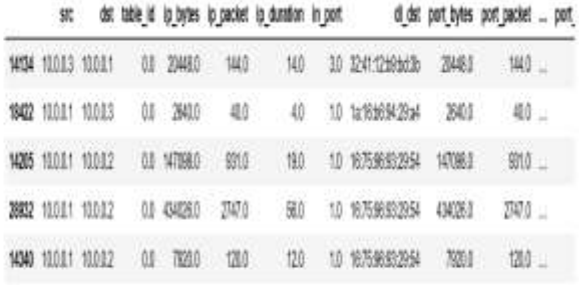


Fig 2 Proposed Architecture

iii) Dataset collection:

MCAD-SDN Dataset: The MCAD-SDN dataset may involve network traffic, security chances, and different information. This cycle includes breaking down the dataset's structure, size, and content.



	src	dst	table_id	ip_bytes	ip_packet	ip_duration	in_port	dl_dst	port_bytes	port_packet	...	port_
14134	10.0.0.3	10.0.0.1	0.0	20448.0	144.0	14.0	3.0	32:41:12:b9:bd:3b	20448.0	144.0	...	
18402	10.0.0.1	10.0.0.3	0.0	2640.0	48.0	4.0	1.0	1a:16:b6:94:29:a4	2640.0	48.0	...	
14205	10.0.0.1	10.0.0.2	0.0	147098.0	931.0	19.0	1.0	16:75:96:93:29:54	147098.0	931.0	...	
28832	10.0.0.1	10.0.0.2	0.0	434026.0	2747.0	58.0	1.0	16:75:96:93:29:54	434026.0	2747.0	...	
14340	10.0.0.1	10.0.0.2	0.0	7920.0	128.0	12.0	1.0	16:75:96:93:29:54	7920.0	128.0	...	

Fig 2 MCAD – SDN dataset

iv) Data Processing:

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

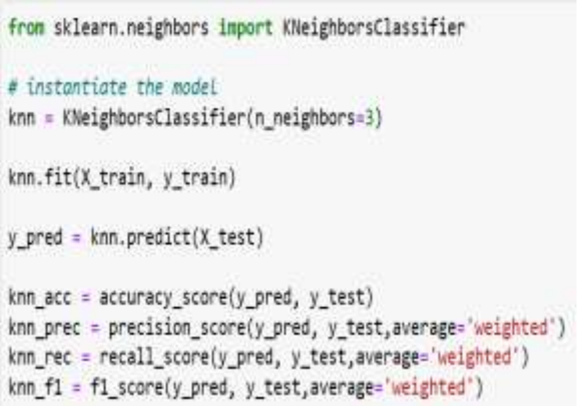
v) Feature selection:

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:

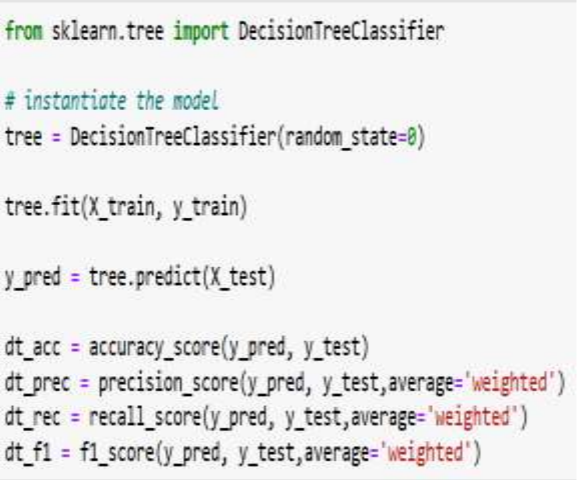
K Nearest Neighbor (KNN) regulated grouping and relapse strategy. It characterizes information by the greater part class of their k-nearest neighbors (k is client characterized), accepting similar information focuses are close in highlight space. Healthcare SDN network traffic might be characterized utilizing KNN [1,8,12]. It identifies irregular way of behaving by contrasting examples with known cases.[66]



```
from sklearn.neighbors import KNeighborsClassifier

# instantiate the model
knn = KNeighborsClassifier(n_neighbors=3)

knn.fit(X_train, y_train)

y_pred = knn.predict(X_test)

knn_acc = accuracy_score(y_pred, y_test)
knn_prec = precision_score(y_pred, y_test,average='weighted')
knn_rec = recall_score(y_pred, y_test,average='weighted')
knn_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig 3 KNN

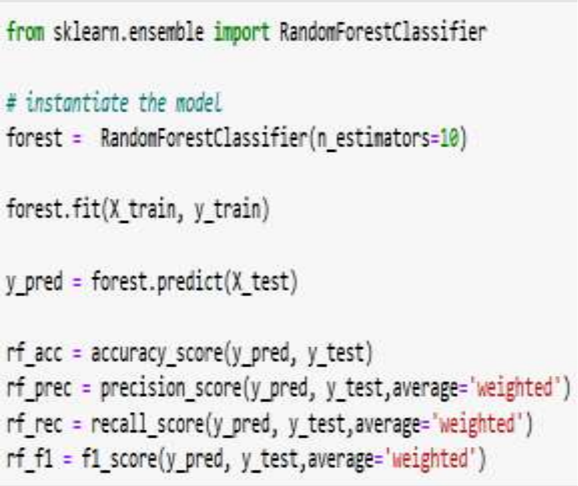
Decision trees used for relapse and grouping. Trees with hubs for include testing and branches for results. They choose by crossing root to leaves using input qualities. Network oddity location rules might be made utilizing choice trees. Decision trees assist with making sense of organization conduct since they are interpretable.



```
from sklearn.tree import DecisionTreeClassifier

# instantiate the model
tree = DecisionTreeClassifier(random_state=0)

tree.fit(X_train, y_train)

y_pred = tree.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')
```

Fig 4 Decision tree

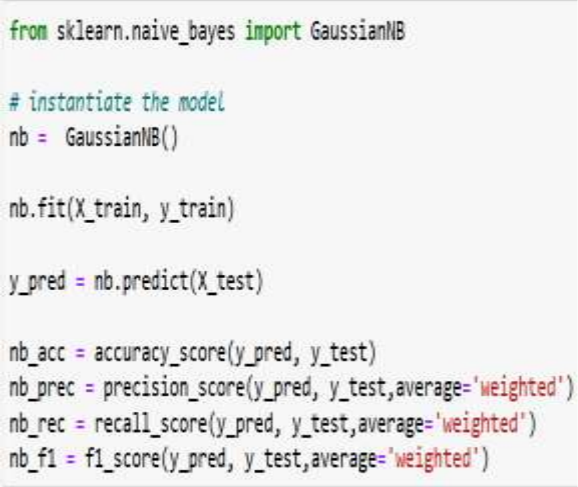
Random Forest a ensemble approach that makes a choice tree woods. Averaging or deciding on tree figures makes forecasts. Decreases overfitting and works on model accuracy. Totaling decision tree gauges with Random Forest improves cyberattack identification. Healthcare network security false positives and negatives are diminished [24], [28], and [30].



```
from sklearn.ensemble import RandomForestClassifier

# instantiate the model
forest =  RandomForestClassifier(n_estimators=10)

forest.fit(X_train, y_train)

y_pred = forest.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')
```

Fig 5 Random forest

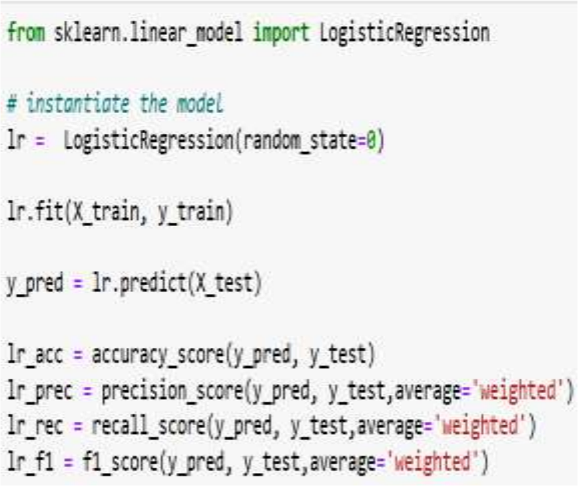
Naive Bayes utilizes Bayes' hypothesis to probabilistically characterize. Expecting restrictive freedom between qualities works with text arrangement and spam separating. Naive Bayes can order text to distinguish hurtful medical services correspondence. It can recognize odd organization literary examples [54].



```
from sklearn.naive_bayes import GaussianNB

# instantiate the model
nb =  GaussianNB()

nb.fit(X_train, y_train)

y_pred = nb.predict(X_test)

nb_acc = accuracy_score(y_pred, y_test)
nb_prec = precision_score(y_pred, y_test,average='weighted')
nb_rec = recall_score(y_pred, y_test,average='weighted')
nb_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig 6 Naïve bayes

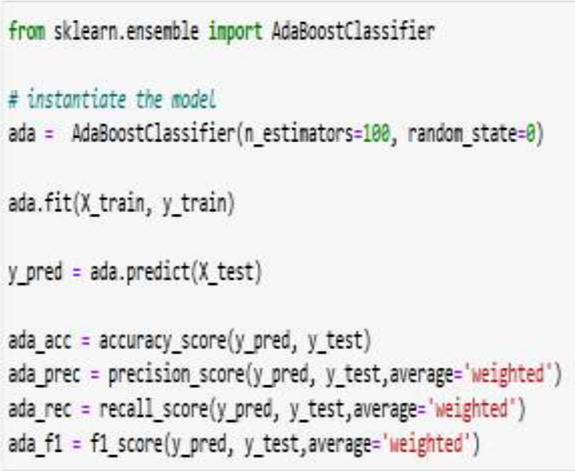
Logistic Regression is a binary characterization measurements model. It evaluates the class likelihood of an info. It demonstrates the reliant variable (binary result) and at least one autonomous factors utilizing strategic capability. Logistic regression can anticipate the opportunity of organization occasions being associated with cyberattacks, making it valuable for medical services network security binary order [55].



```
from sklearn.linear_model import LogisticRegression

# instantiate the model
lr =  LogisticRegression(random_state=0)

lr.fit(X_train, y_train)

y_pred = lr.predict(X_test)

lr_acc = accuracy_score(y_pred, y_test)
lr_prec = precision_score(y_pred, y_test,average='weighted')
lr_rec = recall_score(y_pred, y_test,average='weighted')
lr_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig 7 Logistic regression

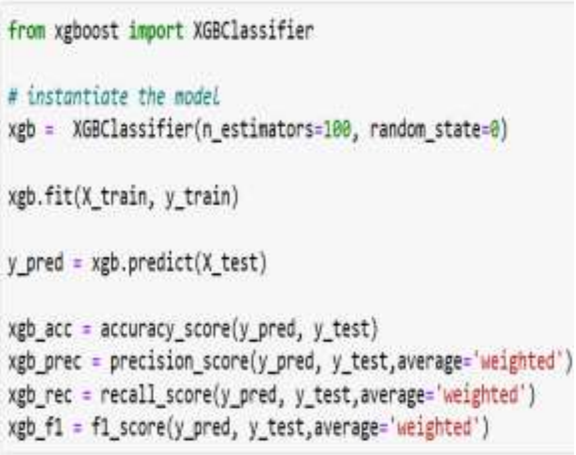
Adaboost consolidates feeble classifiers to make a strong one. It features misclassified events to assist later classifiers with fixing them. Frequently utilized for parallel classification. Adaboost works on base classifiers, improving cyberattack identification in medical services SDNs [56].



```
from sklearn.ensemble import AdaBoostClassifier

# instantiate the model
ada =  AdaBoostClassifier(n_estimators=100, random_state=0)

ada.fit(X_train, y_train)

y_pred = ada.predict(X_test)

ada_acc = accuracy_score(y_pred, y_test)
ada_prec = precision_score(y_pred, y_test,average='weighted')
ada_rec = recall_score(y_pred, y_test,average='weighted')
ada_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig 8 Adaboost

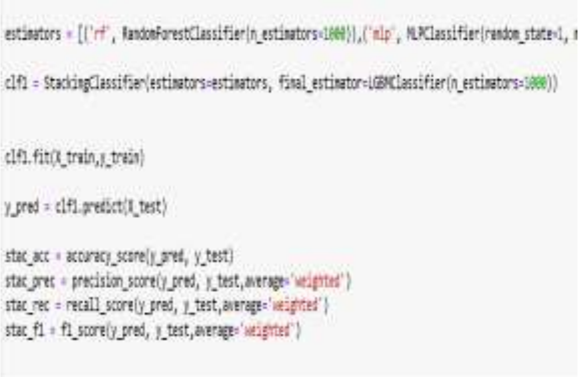
XGBoost streamlined gradient boosting calculation for directed learning with high efficiency, accuracy, regularization, missing information the executives, and equal handling. It's famous in ML challenges and applications. With its high precision, XGBoost might be used to create areas of strength for a strong cyberattack recognition model to get medical care information.



```
from xgboost import XGBClassifier

# instantiate the model
xgb =  XGBClassifier(n_estimators=100, random_state=0)

xgb.fit(X_train, y_train)

y_pred = xgb.predict(X_test)

xgb_acc = accuracy_score(y_pred, y_test)
xgb_prec = precision_score(y_pred, y_test,average='weighted')
xgb_rec = recall_score(y_pred, y_test,average='weighted')
xgb_f1 = f1_score(y_pred, y_test,average='weighted')
```

Fig 9 XGBoost

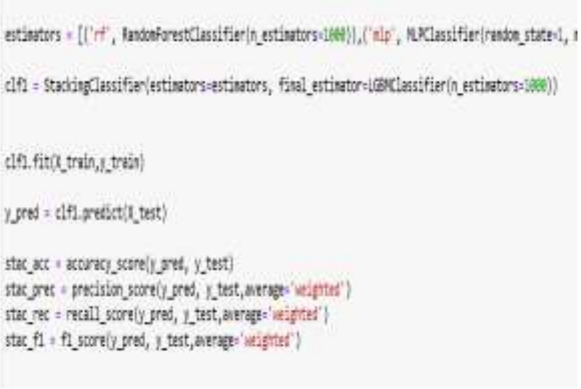
Stacking utilizes a meta-student to expect to utilize fundamental classifier results to work on prescient execution. It catches fluctuated examples to further develop precision. Stacking a few cyberattack identification models catches an extensive variety of assault ways of behaving and further develops healthcare framework security.



```
estimators = [('rf', RandomForestClassifier(n_estimators=1000)),('mlp', MLPClassifier(random_state=1, 

clf1 = StackingClassifier(estimators=estimators, final_estimator=LGBMClassifier(n_estimators=1000))


clf1.fit(X_train,y_train)

y_pred = clf1.predict(X_test)

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

Fig 10 Stacking classifier

Voting a ensemble approach that joins essential classifier expectations. Most votes are unforgiving, however class probabilities are delicate. Voting classifiers utilize a few models' assets to work on model robustness and accuracy. Utilizing a democratic classifier to incorporate different discovery models can further develop medical services network cyberattack recognition.



```
estimators = [('rf', RandomForestClassifier(n_estimators=1000)),('mlp', MLPClassifier(random_state=1, 

clf1 = StackingClassifier(estimators=estimators, final_estimator=LGBMClassifier(n_estimators=1000))


clf1.fit(X_train,y_train)

y_pred = clf1.predict(X_test)

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

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)

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

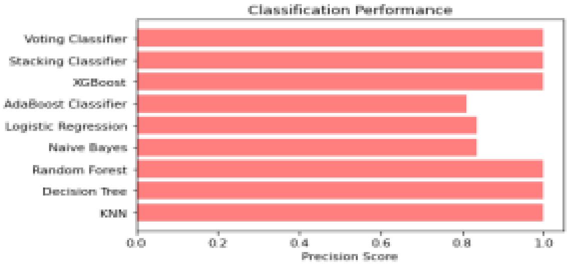


Fig 6 Precision comparison graph

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.

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

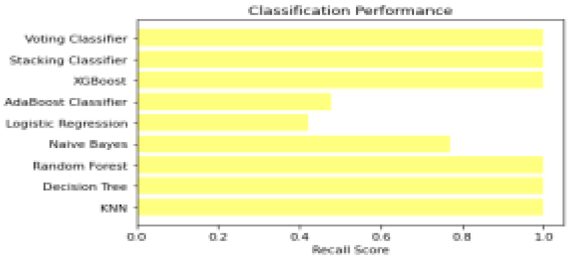


Fig 7 Recall comparison graph

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

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

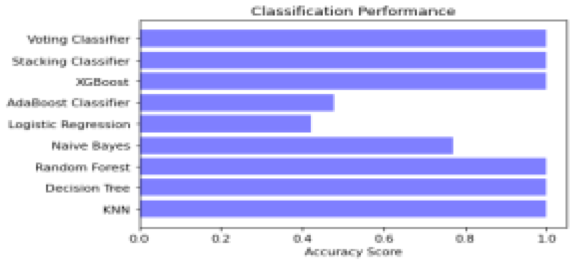


Fig 8 Accuracy graph

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

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

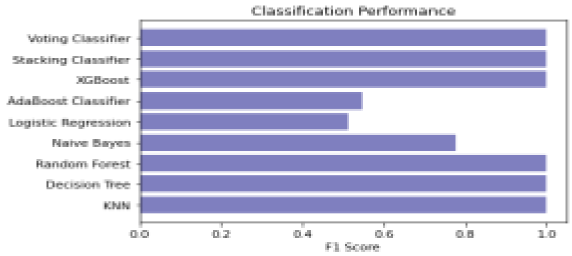
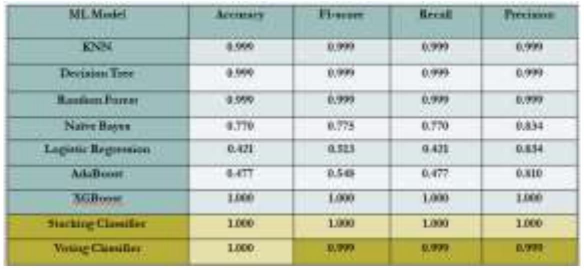


Fig 9 F1Score



ML Model	Accuracy	F1-score	Recall	Precision
KNN	0.999	0.999	0.999	0.999
Decision Tree	0.999	0.999	0.999	0.999
Random Forest	0.999	0.999	0.999	0.999
Naive Bayes	0.770	0.775	0.770	0.834
Logistic Regression	0.421	0.523	0.421	0.834
AdaBoost	0.477	0.548	0.477	0.810
XGBoost	1.000	1.000	1.000	1.000
Stacking Classifier	1.000	1.000	1.000	1.000
Voting Classifier	1.000	0.999	0.999	0.999

Fig 10 Performance Evaluation

Fig 11 Home page

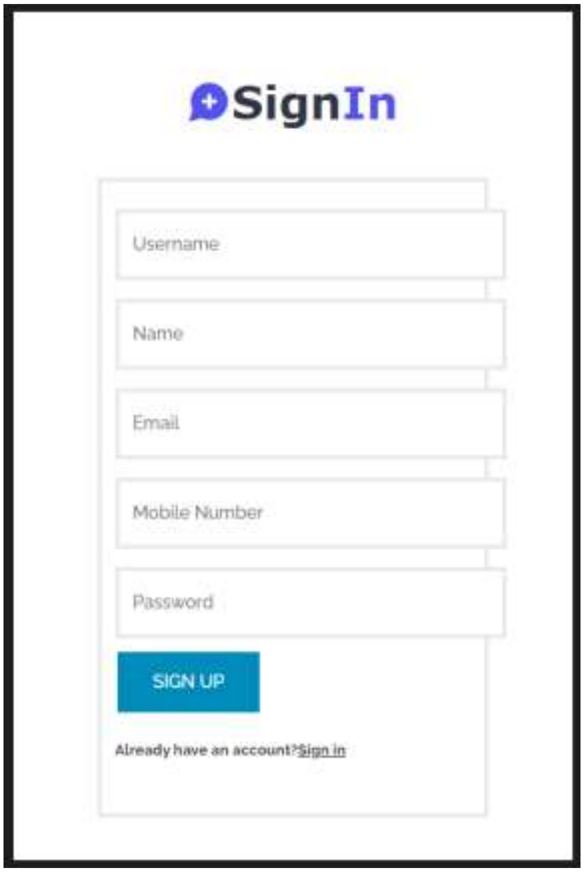
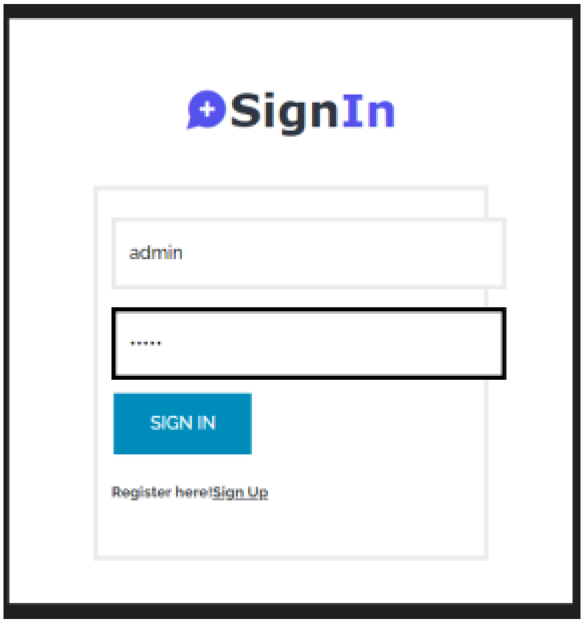


Fig 12 Signin page



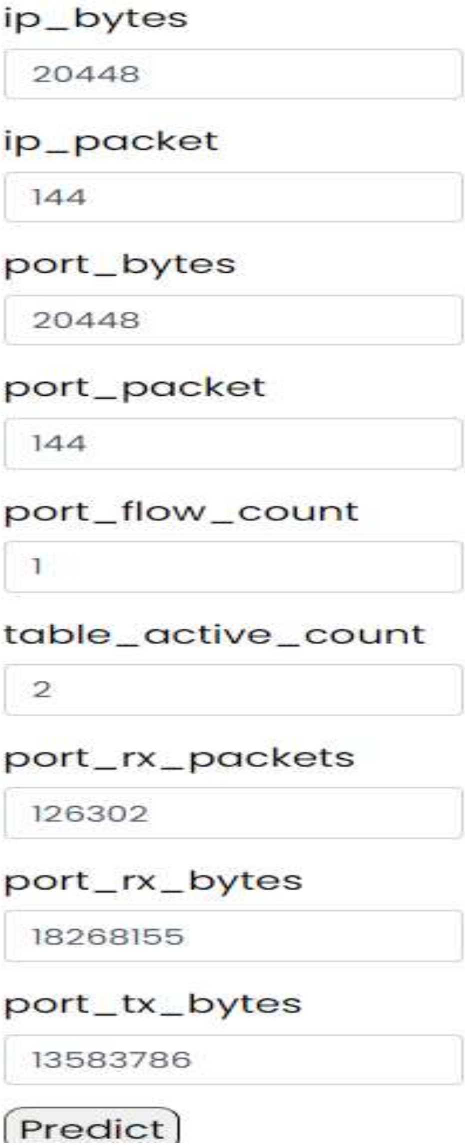
SignIn

admin

••••••

Register here!Sign Up

Fig 13 Login page



ip_bytes

20448

ip_packet

144

port_bytes

20448

port_packet

144

port_flow_count

1

table_active_count

2

port_rx_packets

126302

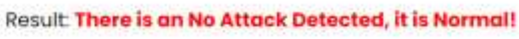
port_rx_bytes

18268155

port_tx_bytes

13583786

Fig 14 User input



Result: There is an No Attack Detected, it is Normal!

Fig 15 Predict result for given input

5. CONCLUSION

Utilizing ML, the gathering made a strong cyberattack location framework to further develop online protection. We completely investigated the MCAD-

SDN dataset, choosing and encoding elements to set it up for examination. We completely tried ML models, including troupe draws near, to find a cyberattack recognition arrangement. Among the models considered, the gathering calculation, Stacking and Voting Classifiers, with 100 percent exactness, is vigorous and successful as a high level cyberattack discovery answer for medical care SDN frameworks [37]. This drive progresses network safety and advanced danger safeguard.

6. FUTURE SCOPE

To improve cyber safety in enterprises other than medical care, like banking, transportation, and basic framework, the MCAD can be considered [35,37,42]. Test the MCAD with a greater and more broadened dataset of typical and assault traffic and other ML strategies to evaluate and improve its exhibition. The MCAD might be created to expand its ongoing abilities, versatility, and digital danger flexibility. Industry partners, network safety experts, and administrative associations might help take on and normalize the MCAD in medical care and other key enterprises.

REFERENCES

[1] M. Jarschel, T. Zinner, T. Hossfeld, P. Tran-Gia, and W. Kellerer, ‘‘Interfaces, attributes, and use cases: A compass for SDN,’’ IEEE Commun. Mag., vol. 52, no. 6, pp. 210–217, Jun. 2014.

[2] W. Meng, K.-K.-R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, ‘‘Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks,’’ IEEE Trans. Netw. Service Manage., vol. 15, no. 2, pp. 761–773, Jun. 2018.

[3] J. T. Kelly, K. L. Campbell, E. Gong, and P. Scuffham, ‘‘The Internet of Things: Impact and implications for health care delivery,’’ J. Med. Internet Res., vol. 22, p. 11, Nov. 2020.

[4] (2022). Networked Medical Devices: Security and Privacy Threats—Sym antec—[PDF Document]. [Online]. Available: https://fdocuments. net/document/networked-medical-devices-security-and-privacy-threatssymantec.html

[5] P. A. Williams and A. J. Woodward, ‘‘Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem,’’ Med. Devices, Evidence Res., vol. 8, pp. 305–316, Jul. 2015.

[6] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, ‘‘Cybersecurity risks in a pandemic,’’ J. Med. Internet Res., vol. 22, no. 9, Sep. 2020, Art. no. e23692.

[7] N. Thamer and R. Alubady, ‘‘A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,’’ in Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS), I. Babil, Ed., Apr. 2021, pp. 210–216.

[8] H. Babbar, S. Rani, and S. A. AlQahtani, ‘‘Intelligent edge load migration in SDN-IIoT for smart healthcare,’’ IEEE Trans. Ind. Informat., vol. 18, no. 11, pp. 8058–8064, Nov. 2022.

[9] R. Hasan, S. Zawoad, S. Noor, M. M. Haque, and D. Burke, ‘‘How secure is the healthcare network from insider attacks? An audit guideline for vulnerability analysis,’’ in Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC), Jun. 2016, pp. 417–422.

[10] (Apr. 2015). 92% of Healthcare IT Admins Fear Insider Threats Thales. Accessed: Mar. 21, 2023. [Online]. Available: https://cpl.thalesgroup. com/about-us/newsroom/news-releases/92-healthcare-it-admins-fearinsider-threats

[11] D. Chaulagain, K. Pudashine, R. Paudyal, S. Mishra, and S. Shakya, ‘‘OpenFlow-based dynamic traffic distribution in software-defined networks,’’ in Mobile Computing and Sustainable Informatics. Singapore: Springer, Jul. 2021, pp. 259–272.

[12] R. Khondoker, A. Zaalouk, R. Marx, and K. Bayarou, ‘‘Feature-based comparison and selection of software defined networking (SDN) controllers,’’ in Proc. World Congr. Comput. Appl. Inf. Syst. (WCCAIS), Jan. 2014, pp. 1–7.

[13] T. Mekki, I. Jabri, A. Rachedi, and L. Chaari, ‘‘Software-defined networking in vehicular networks: A survey,’’ Trans. Emerg. Telecommun. Technol., vol. 33, no. 10, pp. 1–10, Apr. 2021, doi: 10.1002/ett.4265.

[14] Z. Ghaffar, A. Alshahrani, M. Fayaz, A. M. Alghamdi, and J. Gwak, ‘‘A topical review on machine learning, software defined networking, Internet of Things applications: Research limitations and challenges,’’ Electronics, vol. 10, no. 8, p. 880, Apr. 2021, doi: 10.3390/electronics10080880.

[15] C.-S. Li and W. Liao, ‘‘Software defined networks [guest editorial],’’ IEEE Commun. Mag., vol. 51, no. 2, p. 113, Feb. 2013.

[16] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, ‘‘Software defined networks-based smart grid communication: A comprehensive survey,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2637–2670, 3rd Quart., 2019.

[17] L. F. Eliyan and R. Di Pietro, ‘‘DoS and DDoS attacks in software defined networks: A survey of existing solutions and research challenges,’’ Future Gener. Comput. Syst., vol. 122, pp. 149–171, Sep. 2021, doi: 10.1016/j.future.2021.03.011.

[18] K. Benton, L. J. Camp, and C. Small, ‘‘OpenFlow vulnerability assessment,’’ in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw., 2013, pp. 151–152, doi: 10.1145/2491185.2491222.

[19] B. Mladenov and G. Iliev, ‘‘Studying the effect of internal DOS attacks over SDN controller during switch registration process,’’ in Proc. Int. Symp. Netw., Comput. Commun. (ISNCC), Jul. 2022, pp. 1–4.

[20] H. Domínguez-Limaico, W. N. Quilca, M. Zambrano, F. Cuzme-Rodríguez, and E. Maya-Olalla, ‘‘Intruder detection system based artificial neural network for software defined network,’’ in Proc. Int. Conf. Technol. Res. Cham, Switzerland: Springer, Aug. 2022, pp. 315–328.

[21] S. A. Mehdi and S. Z. Hussain, ‘‘Survey on intrusion detection system in IoT network,’’ in Proc. Int. Conf. Innov. Comput. Commun. Singapore: Springer, Sep. 2022, pp. 721–732.

[22] V. Ponnusamy, M. Humayun, N. Z. Jhanjhi, A. Yichiet, and M. F. Almufareh, ‘‘Intrusion detection systems in Internet of Things and mobile ad-hoc networks,’’ Comput. Syst. Sci. Eng., vol. 40, no. 3, pp. 1199–1215, 2022, doi: 10.32604/csse.2022.018518.

[23] K. Malasri and L. Wang, ‘‘Securing wireless implantable devices for healthcare: Ideas and challenges,’’ IEEE Commun. Mag., vol. 47, no. 7, pp. 74–80, Jul. 2009.

[24] D. Yin, L. Zhang, and K. Yang, ‘‘A DDoS attack detection and mitigation with software-defined Internet of Things framework,’’ IEEE Access, vol. 6, pp. 24694–24705, 2018.

[25] R. Wang, Z. Jia, and L. Ju, ‘‘An entropy-based distributed DDoS detection mechanism in software-defined networking,’’ in Proc. IEEE Trustcom/BigDataSE/ISPA, vol. 1, Aug. 2015, pp. 310–317.

[26] S. M. Mousavi and M. St-Hilaire, ‘‘Early detection of DDoS attacks against SDN controllers,’’ in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2015, pp. 77–81.

[27] S. Murtuza and K. Asawa, ‘‘Mitigation and detection of DDoS attacks in software defined networks,’’ in Proc. 11th Int. Conf. Contemp. Comput., Aug. 2018, pp. 1–3.

[28] X. You, Y. Feng, and K. Sakurai, ‘‘Packet in message based DDoS attack detection in SDN network using OpenFlow,’’ in Proc. 5th Int. Symp. Comput. Netw. (CANDAR), Nov. 2017, pp. 522–528.

[29] S. Y. Mehr and B. Ramamurthy, ‘‘An SVM based DDoS attack detection method for Ryu SDN controller,’’ in Proc. 15th Int. Conf. Emerg. Netw. Exp. Technol., New York, NY, USA, Dec. 2019, pp. 72–73, doi: 10.1145/3360468.3368183.

[30] Q. Niyaz, W. Sun, and A. Y. Javaid, ‘‘A deep learning based DDoS detection system in software-defined networking (SDN),’’ ICST Trans. Secur. Saf., vol. 4, no. 12, Dec. 2017, Art. no. 153515. [Online]. Available: https://publications.eai.eu/index.php/sesa/article/view/211

[31] G. Lucky, F. Jjunju, and A. Marshall, ‘‘A lightweight decision-tree algorithm for detecting DDoS flooding attacks,’’ in Proc. IEEE 20th Int. Conf. Softw. Quality Rel. Secur. Companion (QRS-C), Dec. 2020, pp. 382–389.

[32] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, ‘‘A DDoS attack detection method based on SVM in software defined network,’’ Secur. Commun. Netw., vol. 2018, pp. 1–8, Jan. 2018.

[33] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos, and S. Wan, ‘‘Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach,’’ IEEE Trans. Ind. Informat., vol. 18, no. 3, pp. 2041–2052, Mar. 2022.

[34] T. A. S. Srinivas and S. S. Manivannan, ‘‘Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm,’’ Comput. Commun., vol. 163, pp. 162–175, Nov. 2020.

[35] A. Kanavalli, A. Gupta, A. Pattanaik, and S. Agarwal, ‘‘Realtime DDoS detection and mitigation in software defined networks using machine learning techniques,’’ Int. J. Comput., vol. 10, pp. 353–359, Sep. 2022. [Online]. Available: https://computingonline.net/ computing/article/view/2691

[36] A. Erfan, ‘‘DDoS attack detection scheme using hybrid ensemble learning and ga algorithm for Internet of Things,’’ PalArch’s J. Archaeol. Egypt/Egyptol., vol. 18, no. 18, pp. 521–546, Jan. 2022. [Online]. Available: https://archives.palarch.nl/index.php/jae/article/view/10546

[37] Y. K. Saheed and M. O. Arowolo, ‘‘Efficient cyber attack detection on the Internet of Medical Things-smart environment based on deep recurrent neural network and machine learning algorithms,’’ IEEE Access, vol. 9, pp. 161546–161554, 2021.

[38] A. H. Celdrán, K. K. Karmakar, F. Gómez Mármol, and V. Varadharajan, ‘‘Detecting and mitigating cyberattacks using software defined networks for integrated clinical environments,’’ Peer-Peer Netw. Appl., vol. 14, no. 5, pp. 2719–2734, Sep. 2021.

[39] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, ‘‘InSDN: A novel SDN intrusion dataset,’’ IEEE Access, vol. 8, pp. 165263–165284, 2020.

[40] X. Cai, K. Shi, K. She, S. Zhong, Y. Soh, and Y. Yu, ‘‘Performance error estimation and elastic integral event triggering mechanism design for T–S fuzzy networked control system under dos attacks,’’ IEEE Trans. Fuzzy Syst., vol. 31, no. 4, pp. 1–12, Apr. 2023.

[41] X. Cai, K. Shi, K. She, S. Zhong, and Y. Tang, ‘‘Quantized sampled-data control tactic for T–S fuzzy NCS under stochastic cyber-attacks and its application to truck-trailer system,’’ IEEE Trans. Veh. Technol., vol. 71, no. 7, pp. 7023–7032, Jul. 2022.

[42] A. O. Alzahrani and M. J. F. Alenazi, ‘‘ML-IDSDN: Machine learning based intrusion detection system for software-defined network,’’ Concurrency Comput., Pract. Exper., vol. 35, no. 1, pp. 1–12, Jan. 2023.

[43] K. S. Bhosale, M. Nenova, and G. Iliev, ‘‘The distributed denial of service attacks (DDoS) prevention mechanisms on application layer,’’ in Proc. 13th Int. Conf. Adv. Technol., Syst. Services Telecommun. (TELSIKS), Oct. 2017, pp. 136–139.

[44] A. Almazyad, L. Halman, and A. Alsaeed, ‘‘Probe attack detection using an improved intrusion detection system,’’ Comput., Mater. Continua, vol. 74, no. 3, pp. 4769–4784, 2023, doi: 10.32604/cmc.2023.033382.

[45] A. Sadeghian, M. Zamani, and S. M. Abdullah, ‘‘A taxonomy of SQL injection attacks,’’ in Proc. Int. Conf. Informat. Creative Multimedia, Sep. 2013, pp. 269–273.

[46] L. Zhang-Kennedy, S. Chiasson, and R. Biddle, ‘‘Password advice shouldn’t be boring: Visualizing password guessing attacks,’’ in Proc. APWG eCrime Researchers Summit, Sep. 2013, pp. 1–11.

[47] Z. Su and G. Wassermann, ‘‘The essence of command injection attacks in web applications,’’ ACM SIGPLAN Notices, vol. 41, no. 1, pp. 372–382, Jan. 2006.

[48] M. Pivarníková, P. Sokol, and T. Bajtoš, ‘‘Early-stage detection of cyber attacks,’’ Information, vol. 11, no. 12, p. 560, Nov. 2020.

[49] K. V. A. Reddy, S. R. Ambati, Y. S. R. Reddy, and A. N. Reddy, ‘‘AdaBoost for Parkinson’s disease detection using robust scaler and SFS from acoustic

features,'' in Proc. Smart Technol., Commun. Robot. (STCR), Oct. 2021, pp. 1–6.

[50] I. T. Jolliffe and J. Cadima, ''Principal component analysis: A review and recent developments,'' Philos. Trans. Roy. Soc. A, Math., Phys. Eng. Sci., vol. 374, Apr. 2016, Art. no. 20150202, doi: 10.1098/rsta.2015.0202.

[51] P. Cunningham and S. J. Delany, ''K-nearest neighbour classifiers: 2nd edition (with Python examples),'' 2020, arXiv:2004.04523.

[52] E. H. Sussenguth, ''An algorithm for automatic design of logical cryogenic circuits,'' IEEE Trans. Electron. Comput., vol. EC-10, no. 4, pp. 623–630, Dec. 1961.

[53] P. H. Swain and H. Hauska, ''The decision tree classifier: Design and potential,'' IEEE Trans. Geosci. Electron., vol. GE-15, no. 3, pp. 142–147, Jul. 1977.

[54] Y. Ji, S. Yu, and Y. Zhang, ''A novel Naive Bayes model: Packaged hidden Naive Bayes,'' in Proc. 6th IEEE Joint Int. Inf. Technol. Artif. Intell. Conf., Aug. 2011, pp. 484–487.

[55] X. Zou, Y. Hu, Z. Tian, and K. Shen, ''Logistic regression model optimization and case analysis,'' in Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. (ICCSNT), Oct. 2019, pp. 135–139.

[56] Y. Freund and R. E. Schapire, ''A decision-theoretic generalization of on-line learning and an application to boosting,'' J. Comput. Syst. Sci., vol. 55, pp. 119–139, Aug. 1995. [Online]. Available: https://www. sciencedirect.com/science/article/pii/S002200009791504X

[57] T. Chen and C. Guestrin, ''XGBoost: A scalable tree boosting system,'' 2016, arXiv:1603.02754.

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

[59] 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.

[60] 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.

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

[62] 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.

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

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

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

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

[68] 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