Asian Journal of Research in Computer Science

9(3): 1-12, 2021; Article no.AJRCOS.68531
ISSN: 2581-8260

Machine learning Algorithm of Intrusion Detection System

Rozin Majeed Abdullah[1*], Adnan Mohsin Abdulazeez[2] and Adel Al-Zebari[3]

[1]Department of Information Technology at Duhok Polytechnic University, Duhok, Iraq.
[2]Duhok Polytechnic University, Duhok-Kurdistan Region, Iraq.
[3]Department of Information Technology at Duhok Polytechnic University, Duhok, Iraq.

Authors' contributions

This work was carried out in collaboration among all authors. Author RMA designed the study, performed the statistical analysis, wrote the protocol and wrote the first draft of the manuscript. Author AMA managed the analyses of the study. Author AAZ managed the literature searches. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v9i330221
Editor(s):
(1) Dr. Francisco Welington de Sousa Lima, Universidade Federal do Piauí, Brazil.
Reviewers:
(1) Vidhya Sathish, SDNB Vaishnav College for Women, India.
(2) P. Sudha, Sree Saraswathi Thyagaraja College, India.
(3) K. V. N. Sunitha, BVRIT Hyderabad College of Engineering for Women, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/68531

Original Research Article

Received 21 March 2021
Accepted 01 June 2021
Published 05 June 2021

ABSTRACT

Web of thing (WoT) is a gifted answer for interface and access each gadget through the web. Consistently the gadget includes increments with huge variety fit as a fiddle, size, use and intricacy. In this paper Since WoT drives the world and changes individuals' lives with its wide scope of administrations and applications. In any case, WoT offers various types of assistance through applications, it faces serious security issues and powerless against assaults, for example, sinkhole assault, overhang dropping, forswearing of administration assaults. So on, the Interruption recognition framework is utilized to recognize such assaults when the organization's security is penetrated. Given a scale extension of Web of Things for a practical asset the executives in brilliant urban communities, a legitimate plan of an interruption recognition framework IDS is basic to protect the future organization framework from interlopers. With the development of associated things, the most broadly utilized brought together cloud-based IDS regularly suers from high inertness and organization overhead, subsequently coming about in lethargy to assaults and moderate recognition of pernicious clients.

**Corresponding author: E-mail: rozin.abdullah@dpu.edu.krd;*

Keywords: Intrusion detection system; network attack; Weka.

1. INTRODUCTION

Machine learning (ML) is used in every area of computational work where algorithms are designed and performance is increased [1]. In the last years, learning from unbalanced data sets has become a critical problem in machine learning. It is frequently found in several applications such as computer security [2], remote sensing [3], biomedicine [4,5,6], Medical Images [7,8]. Meanwhile, in the previous decade, the interconnection among people, machines, and administrations has developed Signiant, coming about into another Web of Things correspondence worldview (WoT) [9]. This worldview is relied upon to be the standard direction in the web and administration driven processing inside the current age (4G/5G) and a group of people yet to come Six generation and past networks, which will have a sign can't position in the up-and-coming age of feasible keen urban areas. With more extravagant arrangements of ecological, modern, and cultural information being traded through WoT, reasonable planning among assets and administrations in WoT-empowered savvy urban communities can be denied and upgraded [10,11], which like this, prompts supportable living and the board of the climate. The WoT has commendable utilizes cases in numerous transportation, medical, retail, industry, and schooling spaces and will ceaselessly extend across die rent bearings. This noteworthy development of associated things can be credited towards remote innovations lately as a key empowering influence. We were flawlessly associating people to actual items through telephone, tablet, and PC interfaces. Until the time of 2021, we expect that remote transmission adds to two-third of the general web information, with cell/Wi-Fi associations sharing 66% of the general web convention (IP) information [12,13].

Regular interruption recognition framework engineering is mostly engaged to give security to web the board qualities, and it slacks progressively enormous volume information streams security [14]. Fundamentally regular IDS are ordered into three kinds like situation procedure, discovery system, and approval methodology. Fig. 1 portrays the various kinds of interruption recognition frameworks in WoT. Climate. Among these three classes, discovery procedure acquires consideration, and a large portion of the frameworks are created dependent on recognition systems as it were. Mark-based IDS, Abnormality-based IDS, detail-based IDS, and Crossover IDS are the sub-classes in discovery methodologies [15,16].

Mark created IDS – It depicts the assaults and their examples and recognizes the assaults. On recognizing an assault in an organization, the signature-based location framework raises an alarm about the dubious exercises and design coordinating. In light of the likeness and contrast, the entrance or alarm gave to the client and identified the assaults successfully [18].

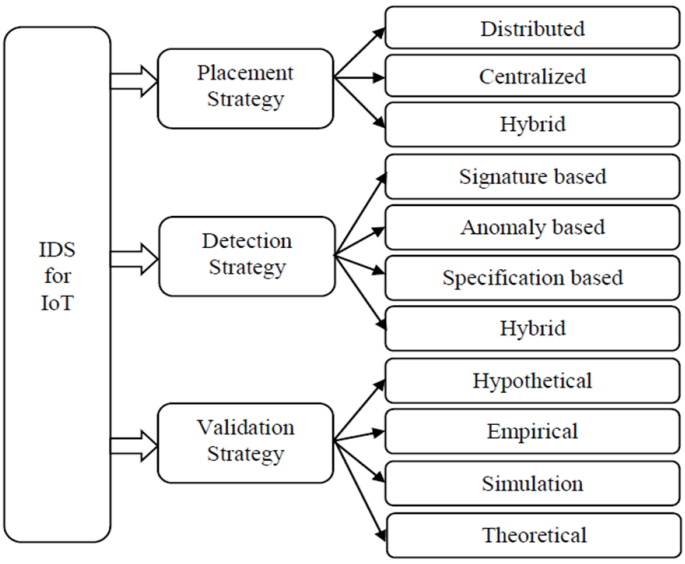

Fig. 1. Intrusion Detection Systems in Web of things [17]

Peculiarity-created IDS is an underlying stage interruption identification framework that gathers the information and recognizes the anomalies in the framework. In light of limited esteem, the typical and unusual practices are distinguished, and an alarm is raised to organize the chairman about the irregularities [19]. It identifies the obscure assaults proficiently; however, it requires huge memory to measure, and calculation costs limit the inconsistency-based interruption discovery framework [20].

Particular put together IDS – Based on the particular activity; these frameworks consistently assessed the framework tasks [21]. The organization executive characterizes the particular activity, screening the interaction consistently to approve the activity. If irregularities are recognized according to the activity, an alarm is sent to the organization head [22].

Hybris IDS – Blend of oddity and mark-based IDS considered as mixture models which gives better tradeoff between the capacity and registering cost with less bogus positive cautions [23]. As of late, a large portion of the frameworks depend on Crossbreed IDS because of its successful identification and worked on activity [24].

Security overseers customarily lean toward secret word assurance instruments, encryption methods, and access controls notwithstanding re-calls as a method for ensuring the network. In any case, these procedures are not sufficient for ensuring the framework [25,26]. Accordingly, numerous directors lean toward using Interruption Location Frameworks (IDSs) to distinguish malevolent assaults by checking network traffic, as portrayed in Fig. 2 [27].

Interruption can be defined as any unapproved movement that harms confidentiality, accessibility, or, again, the respectability of the information inside a data framework. IDSs are a profoundly favored method for identifying this kind of action [29]. IDSs can be arranged into three gatherings: Signature-based Interruption Recognition Frameworks (SIDS), Peculiarity based Interruption Recognition Frameworks (Helps), Crossbreed Frameworks [30].

SIDSs store the marks of the evil exercises in an information base and attempt to distinguish interruptions by utilizing design coordinating procedures. In the interim, AIDSs attempt to get familiar with the typical practices of the exercises and characterize the others as dubious [31]. There is no compelling reason to utilize a signature base in this sort of framework, and the framework can recognize zero-day assaults that have not been experienced already [32]. Crossbreed frameworks are formed made by the joining out of SIDS and Help to build the discovery pace of known noxious exercises by lessening the bogus positive pace of zero-day assaults [33,34,35].

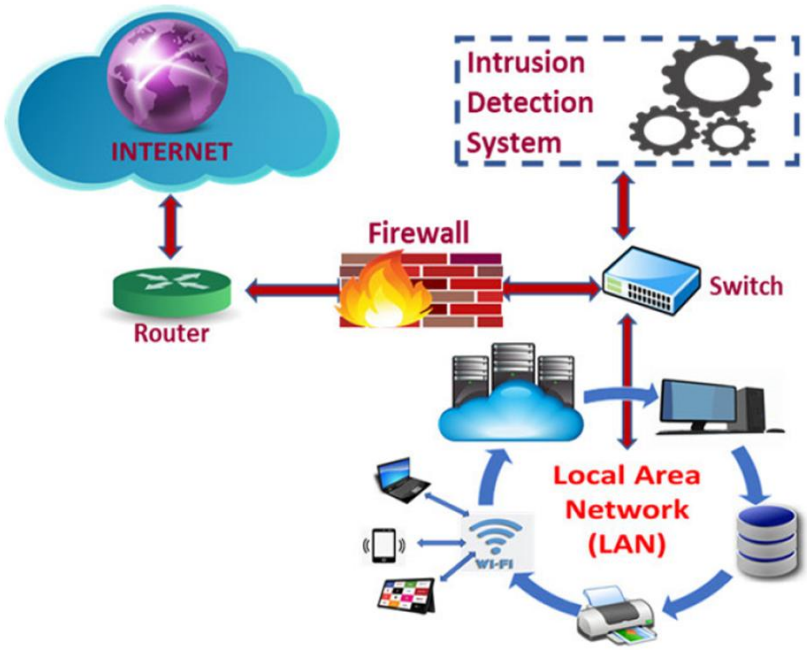

Fig. 2. Instruction detection systems and local area network [28]

WEKA is a Data Mining, simulated intelligence Instrument that was first done in the School of Waikato, New Zealand, in 1997 [36]. It is an arrangement of several AI and Data Mining computations. This item is written in Java language and contains a GUI Interface to work together with data Records. It contains 49 data pre-dealing with devices, 76 gathering estimations, 15 trademark evaluators likewise, ten journey computations for feature decision [37,38,39]. It contains three computations to find connection rules. It has three Graphical UIs: "The Voyager," "The Experimenter," and "The Data Stream." The WEKA maintains data set aside in the ARFF archive plan. ARFF addresses Trademark Association Record Course of action. It similarly fuses instruments for portrayal. It has a lot of sheets that can be used to perform express tasks. WEKA enables to make and join the new artificial intelligence estimation in it. The estimations can be applied to the dataset [40].

2. LITERATURE REVIEW

As it is accessible in numerous distributions (both old and current), it is exceptionally evident that much work has been done in the space of breaking into the organization. In this segment, there are 15 In the closer view; endeavors are being made to survey the significant work of unmistakable analysts.

2.1 Related Work

Yuxin Liu et al. [41] Proposed work acquaints an interruption identification framework distinguishing the sinkhole assault utilizing RPL directing convention, which assesses the got parcels and communicated bundles proportion to acquire the interruption proportion. The framework produces an alarm to arrange executives to limit the interruption impacts on recognizing the malevolent hubs.

Snehal et al. [42] Detailed directing explicit assault in an IoT climate. Exploration works centered on wormhole assault in which the objective hub is assaulted or penetrated from two unique bearings. Distinguishing gatecrasher in an organization is troublesome and research centered on recognizing the interloper position and cautions the organization director. Recognizing the local hubs and separating the effect of danger is considered a value of this exploration work.

Rup Kumar et al. [43] Examined position assaults in an IoT climate. It is essentially a steering-based interruption that happens in a low force organization. Specific positions determine the hubs, and its qualities are refreshed at standard periods. On specific conditions, the gatecrasher adjusts the positioning cycle, so a most exceedingly terrible hub is chosen by directing interaction, decreasing the framework execution. Because of the position rule, productive geography is outlined in the examination work by staying away from customary circle detailing measure which gives better overhead.

Shailendra et al. [44] Research model. In Sybil assault, the hub has produced different characters in this way. It would create different steering conventions. Discovery calculations and ridiculing techniques are needed to distinguish such assaults. Relies on the interloper proficiency and effect of assault, Sybil assaults are arranged.

Alekha et al. [45] examined friendly diagram-based Sybil assault, which distinguishes the gatecrasher in an organization through its chart cycle. Arrangement-based identification is considered a significant area in IoT security. On the off chance that a particular hub is included to extricate all the information from its neighbor hubs, at that point, it is named as sinkhole assault.

Guangjie et al. [46] Revealed sink opening assault and its effect on the organization in his exploration work, distinguishing the malignant hubs and its directing interaction in the organization. Because of the steering cost, these kinds of assaults are distinguished in the organization.

Bin Xu et al. [47] Revealed about support reservation assault caused by duplication of hubs in the organization. Gatecrasher parts the hubs and made copy hubs for assault, and performs noxious tasks in the organization. The client is uninformed of such organizational change and the divided data. So, the interloper client the cushion space and catches different hubs in the organization.

Chen Lyu et al. [48] Announced one of the significant issues in IoT security, like refusal of administration (DoS) assault. In this cycle, interloper assaults over the hub and denies different hubs' demand information administration. This powerlessness of hub condition has alluded as a refusal of administration. At the same time, Dispersed

Refusal of Administration (DDoS) utilized various hubs for a similar cycle to make the organization unusable for the client. The proposed interruption location model recognizes the noxious client in the organization.

Mahmudul Hasan et al. [49] Revealed different systems of refusal of administration assaults as a review. Examination outline gives an outline of various avoidance components and location procedures against DoS and DDoS assaults.

Ju Ren et al. [50] Detailed the issues in IoT networks because of specific sending assaults. A malignant hub introduces itself as an essential hub for transmission and influences the organization's steering and transmission execution. In this cycle, specific messages are considered for transmission, and different messages lurk in the actual hub and square the information transmission, which influences the directing activity.

Noshina Tariq et al. [51] Interruption recognition model utilizing this examination work uses the counterfeit neural organization to distinguish such assaults in an IoT organization. Exploration work is approved with an ongoing information transmission framework that advances the control messages and squares different messages. With high discovery proportion and less calculation cost, the proposed model distinguishes the interloper in the organization.

Pham et al. [52] Proposed an interruption identification framework to recognize the welcome flood assault in an organization. This sort of directing convention persistently communicates hi messages in the organization and makes aggravation in network transmission. They recognized such assaults as troublesome as the interloper changes the hub position upon each transmission. The proposed location model recognizes assaults in an IoT network through the back proliferation neural organization model. The learning calculation chooses the vindictive highlights and recognizes the gatecrasher in a viable way. Alongside flooding assault, refusal of administration assault and wormhole assault are additionally recognized and broke down in the test model.

Bo Chen et al. [53] examined interruptions in IoT climate and centered the exploration work to recognize the sinkhole, replay assault, and Sybil assaults. In this replay, assault is interruption is performed at various timings to gather the fundamental information and afterward replayed by the interloper in the organization. This leads to undesirable issues in the client's local area, which faces major issues on significant transmissions. The proposed model adequately recognizes such assaults through a fluffy-based interruption location framework, which performs discovery measures through rules.

Olivier Brun et al. [54] examined sticking assault in an IoT climate in which the interloper checks the transmission medium. In this kind of assault, the interloper acquires consideration over the organization by following the control recurrence and interferes with the correspondence between the source hub and the objective hub. Exploration work proposed an interruption discovery framework utilizing a versatile fluffy neuro induction framework to recognize sticking, Sybil, and disavowal administration assaults. The calculation cost of this framework is high, which is a significant restriction.

Haythem et al. [55] proposed an interruption identification framework utilizing a profound neural organization, which successfully recognizes the dark opening assault and bogus information assault. In the dark opening assault, an interloper notices the client mentioned information bundles to acquire secret data. Noticing the properties of directing module interloper performs such assaults and gains fundamental client data that influence the organization's reliability. If there should arise bogus information assault, gatecrasher notices the organization association and design and alters the organization by embedding counterfeit answer bundles.

3. DATA SETS

This examination used of ASD assay dataset from the Division of Advanced Innovation, Manukau Establishment of Innovation, New Zealand [56]. The specialist built a screening app to check the manifestations of ASD in patients and collected the patient information, which proved useful in screening for ASD events [57], and placed it into a custom dataset. The dataset includes 11 attributes, which combine 292 cases or records. Credits or data fields incorporate age, sexual orientation, ethnicity, jaundice status, the mental imbalance between relatives, associations, country of home, screening application used, type of examination procedure, requests related to patient offer or limitation, screening outcome, and screening category. The investigation result from the screening test is

arranged into 'yes' for the patient determined to have autism spectrum disorder and 'no' for a patient without autism spectrum disorder. Because of the grouping, the dataset is arranged as a disproportionate dataset. Table 1 also shows the quality names at once, the species that are in the ASD assay dataset [58].

4. METHODOLOGY

huge information whenever coordinated with AI, empowers wellbeing professionals to anticipate the consequence of an issue all the more precisely. In Medically (ASD) it is critical to screen the Information.The main inspiration driving this examination is to take apart a lot of ASD screening data by using six order estimations to help in improving the investigation communication of ASD in clinical consideration practices. This portion shows the philosophies that we used to describe the ASD screening dataset, including the arrangement communication, characterization techniques, execution organization, and dataset drew in with this examination. Since the yield of the planning dataset is acknowledged, which is the screening class, the characterization technique is the most proper one to be used for the present circumstance. Characterization can help with improving screening association and help at lessening any potential botches achieved by fresh prosperity subject matter experts. The communication began by gathering the ASD screening dataset in two conditions, with and without missing characteristics, using six classifiers autonomously with Weka Traveler. The data credit technique was used to deal with divided data by overriding the missing characteristics with reasonable characteristics. When the results were gotten, we helped the test by running all of the six classifiers simultaneously in Weka Experimenter. The results were poor down and investigated for the two conditions.

4.1 Performance

In this paper, the precision score for every classifier is utilized as execution measure to dissect every classifier. More methodical execution. The AUC scale is additionally analyzed for all classifiers utilized in this investigation. The scale is utilized for estimating. Every classifier performs over a full scope of sensitivities and details and is unaffected by profession offs precision and particularity.

Table 1. ASD attributes

Name	Code	Description	Type
Age	Age	The kid's age	Number
Sex	Sexual orientation	The kid's sexual orientation (Male or Female)	String
Nationality	Identity	Rundown of normal identities in text design	String
Bern with jaundice	Jaundice	Regardless of whether the youngster was bom with jaundice	Boolean (indeed or no)
Relative with ASD	Mental imbalance	Regardless of whether any close relative has ASD	Boolean (yes or no)
Connection	Connection	Parent, self, guardian, clinical staff, and so forth	String
Nation of home	Country of res	Name of nations in text design	String
Utilized the application previously	App Used Before	Regardless of whether the client has utilized a screening application	Boolean (indeed or no)
Screening Strategy Type	Age-desc	The kind of screening strategies picked based cn age class (Q=todder. 1=dvkL 2= juvenile 3-grown-up)	Whole number (0.123)
Screening Scene	Result	The last score acquired dependent on the scoring calculation of the screening strategy utilized. This w3s registered in a robotized way	Whole number (0.123)
Sorting category	Class and ASD	Regardless of whether the youngster has ASD orna	Boolean (yes or no)

In information mining, exactness, determined utilizing the equation; $\frac{(TP+TN)}{(TP+FP+TN+FN)}$, indicated as a level of the aggregate of appropriately characterized information. It is determined by isolating the genuine positive aggregate and the negative absolute by the great completion positive and negative information. Affectability, review, or genuine positive rate determined utilizing the recipe; $\frac{TP}{TP+FN}$, processed the level of real positives effectively classified as, for instance, the level of patients accurately recognized as ASD.

- True Positive (TP) where it is anticipated as having ASD and having ASD in genuine circumstance.
- False Negative (FN) where it is anticipated as not having ASD however having ASD in genuine circumstance.
- False Positive (FP) where it is anticipated as having ASD however not having ASD in real circumstance.
- True Negative (TN) where it is anticipated as not having ASD and not having ASD in real circumstance.

5. RESULTS

5.1 Classifier Execution Utilizing WEKA Explorer

The experiment tried six distinct classifiers which incorporate Innocent Bayes, Calculated Relapse, KNN, J48, Irregular Woods, and DNN.

In Table 2, every classifier acquired various outcomes while arranging the ASD test dataset with and without misfortune worth. When the missing qualities are disposed of, J48 and the arbitrary backwoods showed 100% execution contrasted with different classifiers as far as exactness, affectability, and explicitness. In any case, just J48 0.08 s is needed to characterize the informational index contrasted with irregular backwoods (0.76 s). In the meantime, DNN delivered the most reduced Exactness score (86.98%) In classifying a dataset with missing traits compared to (KNN) (88.35%), strategic relapse (95.20), and (98.97%). As far as the computational intricacy of building the characterization model, DNN has appeared. Most noticeably terrible execution as the model form required 28.93 seconds followed by arbitrary backwoods (0.76s), Strategic Relapse (0.51s), J 48 (0.08s), Nive Bayes (0.03.s). Albeit the quickest run time (0.0s), While grouping the dataset, KNN neglected to accurately order 11.64% of situations while disregarding the missing worth, the second most elevated after DNN. We advanced the examination by requesting the ASD screening dataset by ejection of the dataset's missing characteristics. This was motivated by using one of the attribution procedures, which is credit using mean characteristics.

In Table 3, at the point when the missing characteristics stayed supplanted with the mean qualities, equally J48 and Irregular Woodland classifiers had appeared consistent execution like when missing qualities were overlooked except the duration to fabricate the model has expanded for the two classifiers; J 48 (0.01s), Irregular Timberland (0.27s). Time spent for all classifiers to construct the model has additionally expanded with KNN creating the quickest speed to fabricate, the model (0.00s) trailed by J 48 (0.01s), Nive Bayes (0.03s), Calculated Relapse (0.11s), Arbitrary Backwoods (0.27 seconds), and (DNN) (26.29 seconds). Notwithstanding, (KNN) neglected to arrange (10.16%) of occasions effectively when contrasted with different classifiers that necessary more opportunity to group the occurrences yet can produce better precision.

In Table 4, In light of the test led utilizing WEKA Experimenter, 600 pieces of information were stacked since every classifier was assessed multiple times (10-crease cross approval increased by ten redundancies). We looked at every classifier's precision and AUC scores when tried in both WEKA Adventurer and WEKA Experimenter. The outcome shows that the J48 classifier beat different classifiers regarding its precision and AUC readings; 100% and 1.00. Then again, the precision of Credulous Bayes and Irregular Timberland diminished while Strategic Relapse, KNN, and DNN improved their precision, particularly DNN that delivered 7.5337% of progress. We advanced the test by utilizing J48 as the test base, and the outcome shows that no classifiers beat the test base, aside from Arbitrary Woodland, which created 1.00 of AUC result, likened to J48.

In Table 5, the J48 and irregular backwoods have the same 100% accuracy and a score of 1.00 AUC, it beat different exercise manuals when the missing qualities were supplanted with the middle qualities for the credits that had the missing qualities. The test showed that the strategic relapse, KNN, and DNN were essentially unique about the test base as far as of exactness.

Table 2. Normal of classifier for ASD dataset with missing qualities

Classifier	Training Runtime (s)	Acceptably characterized incidence%(accuracy)	Unacceptably characterized incidence%	Kappa Statistic
Naïve Bayes	0.03	98.97	1.02	0.97
Logistic Regression	0.51	95.20	4.79	0.90
KNN	0.00	88.35	11.64	0.76
J48	0.08	100.00	0.00	1.0
Random Forest	0.76	100.00	0.00	1.0
DNN (2- layer)	28.93	86.98	13.01	0.73

Table 2. Continue…

(TP) rate	(FP) rate	Care (Sensitivity)	Re-Call (Quality)	(ROC)	(AUC)
0.99	0.01	0.99	0.99	1.0	0.99
0.95	0.04	0.95	0.95	0.99	0.98
0.88	0.11	0.88	0.88	0.89	0.89
1.00	0.00	1.00	1.00	1.0	1.0
1.00	0.00	1.00	1.00	1.0	1.0
0.87	0.13	0.87	0.87	0.92	0.92

Table 3. Average of classifier for ASD dataset without missing values

Classifier	Training Runtime (s)	Acceptably characterized incidence%(accuracy)	Unacceptably characterized incidence%	Kappa Statistic
Naïve Bayes	0.03	98.97	1.02	0.97
Logistic Regression	0.11	95.20	4.79	0.90
KNN	0.00	89.38	10.61	0.78
J48	0.01	100.00	0.00	1.00
Random Forest	0.27	100.00	0.00	1.00
DNN (2- layer)	26.29	86.98	13.01	0.73

Table 3. Continue…

(TP) rate	(FP) rate	Care (Sensitivity)	Re-Call (Quality)	(ROC)	(AUC)
0.99	0.01	0.990	0.99	1.00	0.99
0.95	0.04	0.95	0.95	0.99	0.98
0.89	0.10	0.89	0.89	0.89	0.89
1.00	0.00	1.00	1.00	1.00	1.0
1.00	0.00	1.00	1.00	1.00	1.00
0.87	0.13	0.87	0.87	0.92	0.92

Table 4. The accuracy and AUC score were tested for all classifiers simultaneously in the WEKA experiment with Missing qualities

Classifier	Acceptably characterized incidence% (accuracy)	(AUC)
Naïve Bayes	98.84%	1.0
Logistic Regression	95.51%	0.99
(KNN)	88.42%	0.89
J48	100%	1.0
Random Forest	99.97%	1.0
(DNN)	94.52%	0.98

Table 5. The accuracy and AUC score were tested for all classifiers simultaneously in the WEKA experiment without Missing qualities

Classifier	Acceptably characterized incidence% (accuracy)	(AUC)
Naïve Bayes	98.91%	1.0
Logistic Regression	95.51%	1.0
(KNN)	89.08%	0.9
J48	100%	1.0
Random Forest	100%	1.0
(DNN)	94.52%	0.98

6. DISCUSSION

Settling on the perfect choice at the perfect time is fundamental in especially significant and related enterprises Extension for compelling and effective execution also as limiting blunders that could influence the patient's life, We compare our outcomes with past work referenced in this paper, and we tracked down that the grouping execution of the classifier was influenced by the kind of informational index just as the number of cases remembered for the analysis. In any case, a particular report is expected to test Grouping calculations to arrange other wellbeing-related informational indexes with various case sizes to research the impact.

7. CONCLUSION

Very few investigations have used order calculations to especially examine ASD assay dataset. Most of the analysts We found it through the written questionnaire used other primary data sets, for example, chest malignant growth dataset and coronary artery disease datasets, and thus there are difficulties in examining and comparing the display of classifiers that are being tried with the ASD assay dataset. This is important to help choose the best ranking strategies for screening and diagnosing a patient with autism spectrum disorder, this paper Show that the Classifies of J48 and rondom forest is the best classifiers for AUC in WEKA expirement with missing value and without missing value, We also tracked that the bulk of previous information focused on aggregating the dataset related to well-being while ignoring missing traits that might add to the critical influences on characterization outcomes and that would consequently affect existence, we have sought to seal the void in examining, ordering the ASD screening dataset by using six classifiers.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Abdulqader DM, Abdulazeez AM, Zeebaree DQ. Machine Learning Supervised Algorithms of Gene Selection: A Review. Machine Learning. 2020;62(03).
2. Abdulazeez AM, Tahir AS. Design and Implementation of Advanced Encryption Standard Security Algorithm using FPGA. Int. J. of Computers & Technology. 2013;4(9):1988-1993.
3. Abdulazeez AM, Faizi FS. Vision-Based Mobile Robot Controllers: A Scientific Review. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021;12(6):1563-1580.
4. Zeebaree DQ, Haron H, Abdulazeez AM, Zebari DA. Trainable model based on new uniform LBP feature to identify the risk of the breast cancer. In 2019 International Conference on Advanced Science and Engineering (ICOASE). 2019;106-111. IEEE.
5. Khorshid SF, Abdulazeez AM. Breast Cancer Diagnosis Based On K-Nearest Neighbors: A review. PalArch's Journal of Archaeology of Egypt/Egyptology. 2021;18(4):1927-1951.
6. Saeed JN, Abdulazeez AM. Facial Beauty Prediction and Analysis Based on Deep Convolutional Neural Network: A Review. Journal of Soft Computing and Data Mining. 2021;2(1):1-12.
7. Zeebaree DQ, Haron H, Abdulazeez AM, Zebari DA. Machine learning and region growing for breast cancer segmentation. In 2019 International Conference on Advanced Science and Engineering (ICOASE). 2019;88-93. IEEE.
8. Yahia HS, Abdulazeez AM. Medical Text Classification Based on Convolutional Neural Network: A Review. International Journal of Science and Business. 2021;5(3):27-41.
9. Bargarai F, Abdulazeez A, Tiryaki V, Zeebaree D. Management of Wireless

Communication Systems Using Artificial Intelligence-Based Software Defined Radio; 2020.
10. Li X, Chen W, Zhang Q, Wu L. Building Auto-Encoder Intrusion Detection System Based on Random Forest Feature Selection. Computers & Security; 2020.
11. Rahman MA, Asyharia AT, Leong LS, Satrya GB, Tao MH, Zolkipli MF. Scalable Machine Learning-Based Intrusion Detection System for IoT-Enabled Smart Cities. Sustainable Cities and Society; 2020.
12. Cover TM, Thomas JA. Elements of information theory. John Wiley & Sons.; 2012.
13. Younis ZA, Abdulazeez AM, Zeebaree SR, Zebari RR, Zeebaree DQ. Mobile Ad Hoc Network in Disaster Area Network Scenario: A Review on Routing Protocols. International Journal of Online & Biomedical Engineering. 2021;17(3).
14. Meryem A, Ouahidi BE. Hybrid intrusion detection system using machine learning. Network Security. 2020;2020(5):8–19.
15. Bhateja V, Peng S-L, Satapathy SC, Zhang Y-D. (Eds.). Evolution in Computational Intelligence. Advances in Intelligent Systems and Computing; 2021.
16. Abdulazeez A, Salim B, Zeebaree D, Doghramachi D. Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol; 2020.
17. Thamilarasu G, Odesile A, Hoang A. An Intrusion Detection System for Internet of Medical Things. IEEE Access; 2020.
18. Pajouh RKADHH, Javidan R, Choo KR. A two-layer dimension reduction and two-tier class cation model for anomaly-based intrusion detection in iot backbone networks, in: IEEE Transactions on Emerging Topics in Computing. 2019;7:314-323.
19. Kato K, Klyuev V. Development of a network intrusion detection system using apache Hadoop and spark. In: IEEE Conference on Dependable and Secure Computing. IEEE. 2017;416–423.
20. Gonzales H, Bauer K, Lindqvist J, McCoy D, Sicker D. Practical defenses for evil twin attacks in 802.11, in: IEEE Global Telecommunications Conference. 2010;1-6.
21. Mighan SN, Kahani M. (2020). A novel scalable intrusion detection system based on deep learning. International Journal of Information Security.
22. Beyah R, Venkataraman A. Rogue-access-point detection: Challenges, solutions, and future directions, IEEE Security Privacy. 2011;9(5):56-61.
23. Jie Y, Xin C, Xudong X, Jianxion W. HIDS-DT: An Effective Hybrid Intrusion Detection System Based on Decision Tree'. IEEE Computer Society. International Conference on Communications and Mobile Computing; 2010;1.
24. Farhat S, Abdelkader M, Meddeb-Makhlouf A, Zarai F. Comparative Study of Classification Algorithms for Cloud IDS using NSL-KDD Dataset in WEKA. International Wireless Communications and Mobile Computing (IWCMC); 2020.
25. Bambang S Supeno D Tohari A Nasrul A. Assessing centroid-based classification models for intrusion detection system using composite indicators. Procedia Computer Science. Elsevier. 2019;161(1):665-676.
26. Abdulqadir HR, Abdulazeez AM. Reinforcement Learning and Modeling Techniques: A Review. International Journal of Science and Business. 2021;5(3):174-189.
27. JM Johnson, TM Khoshgoftaar. Survey on deep learning with classimbalance," J. Big Data. 2019;6(1):27.
28. Provost F. Machine learning from imbalanced data sets 101. In Proc. AAAI Workshop Imbalanced Data Sets, Menlo Park, CA, USA: AAAI Press; 2000.
29. Kulariya M, Saraf P, Ranjan R, Gupta P. Performance analysis of network intrusion detection schemes using Apache Spark. In: 2016 International Conference on Communication and Signal Processing (ICCSP). 2016;1973–1977. IEEE.
30. Barua S, Islam MM, Yao X, Murase K. MWMOTE-majority weighted minority oversampling technique for imbalanced data set learning," IEEE Trans. Knowl. Data Eng. 2014;26(2):405-425.
31. Gao X, Shan C, Hu C, Niu Z, Liu Z. An adaptive ensemble machine learning model for intrusion detection," IEEE Access. 2019;7:8251282521.
32. Karatas G, Demir O, Sahingoz OK. Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset. IEEE Access. 2020;8:32150–32162.
33. A Ali, SM Shamsuddin, AL Ralescu. Classication with class imbalance

problem:Areview," Int. J. Adv. Soft Comput. Appl. 2015;7(3):176204.
34. Najat N, Abdulazeez AM. Gene clustering with partition around mediods algorithm based on weighted and normalized Mahalanobis distance. In 2017 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS). 2017;140-145. IEEE.
35. Hasan BMS, Abdulazeez AM. A Review of Principal Component Analysis Algorithm for Dimensionality Reduction. Journal of Soft Computing and Data Mining. 2021;2(1):20-30.
36. Sulaiman MA. Evaluating Data Mining Classification Methods Performance in Internet of Things Applications. Journal of Soft Computing and Data Mining. 2020;1(2):11-2.
37. Dash R. Selection of the Best Classifier from Diflerent Datasets Using Weka, Hert. 2013;2(3).
38. Nguyen H, Choi D. Application of Data Mining to Network Intrusion Detection: Classifier Selection Model, @Springer Verlag Berlin Heidelberg; 2008.
39. Ruggeri F, Faltin F, Kennet R. Bayesian Networks, Encyclopedia of Statistics in Quality & Reliability, Wiley & Sons; 2007.
40. Aljawarneh S, Aldwairi M, Yassein MB. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. J. Comput. Sci. 2017;25:152–160.
41. Yuxin Liu, Ming Ma, Xiao Liu, Neal N. Xiong, Anfeng Liu, Ying Zhu. Design and Analysis of Probing Route to Defense Sink-Hole Attacks for Internet of Things Security. IEEE Transactions on Network Science and Engineering. 2020;7(1):356-372.
42. Snehal Deshmukh-Bhosale, Santosh Sonavane S. A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things. Procedia Manufacturing. 2019;32:840-847.
43. Rup Kumar Deka, Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita. Active learning to detect DDoS attack using ranked features. Computer Communications. 2019;145:209-222
44. Shailendra Rathore, Jong Hyuk Park. Semi-supervised learning based distributed attack detection framework for IoT. Applied Soft Computing. 2018;72:79-89.
45. Alekha Kumar Mishra, Asis Kumar Tripathy, Deepak Puthal, Laurence Yang T. Analytical Model for Sybil Attack Phases in Internet of Things. IEEE Internet of Things Journal. 2019;6(1):379-387.
46. Guangjie Han, Xun Li, Jinfang Jiang, Lei Shu, Jaime Lloret. Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks. The Computer Journal. 2015;58(6):1280-1292,
47. Bin Xu, Weike Wang, Qiang Hao,Zhun Zhang, Pei Du, Tongsheng Xia,Hongge Li, Xiang Wang. A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device. IEEE Access. 2018;6:72862-72869.
48. Chen Lyu, Xiaomei Zhang, Zhiqiang Liu, Chi-Hung Chi (2019). Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks. IEEE Access. 7: 31068-31082.
49. Mahmudul Hasan, Md Milon Islam, Md Ishrak Islam, Zarif MMA Hashem. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things. 2019;7:1-16.
50. Ju Ren, Yaoxue Zhang, Kuan Zhang, Xuemin Shen. Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks. IEEE Transactions on Wireless Communications. 2016;15(5):3718-3731.
51. Noshina Tariq, Muhammad Asim, Zakaria Maamar M, Zubair Farooqi, Thar Baker. A Mobile Code-driven Trust Mechanism for detecting internal attacks in sensor node-powered IoT. Journal of Parallel and Distributed Computing.2019;134:198-206.
52. Thi Ngoc Diep Pham, Chai Kiat Yeo, Naoto Yanai, Toru Fujiwara. Detecting Flooding Attack and Accommodating Burst Traffic in Delay-Tolerant Networks. IEEE Transactions on Vehicular Technology. 2018;67(1):795-808.
53. Bo Chen, Daniel WC, Ho Guoqiang Hu, Li Yu. Secure Fusion Estimation for Bandwidth Constrained Cyber-Physical Systems Under Replay Attacks. IEEE Transactions on Cybernetics. 2018;48(6):1862-1876.
54. Olivier Brun, Yonghua Yin, Erol Gelenbe. Deep Learning with Dense Random Neural

Network for Detecting Attacks against IoT-connected Home Environments. Procedia Computer Science. 2018;134:458-463.
55. Haythem A, Bany Salameh, Sufyan Almajali, Moussa Ayyash, Hany Elgala. Spectrum Assignment in Cognitive Radio Networks for Internet-of-Things Delay-Sensitive Applications Under Jamming Attacks. IEEE Internet of Things Journal. 2018;5(3):1904-1913.
56. Thabtah F. An accessible and efficient autism screening method for behavioral data and predictive analyses. In Health Informatics Journal. 2019;25(4).
57. Delehanty A, Lee J, Hooker JL, Cortese J, Woods J. Exploring message framing to engage parents in earlyscreening for autism spectrum disorder. In Patient Education and Counseling; 2020.
58. Jones EJH, Gliga T, Bedford R, Charman T, Johnson MH. Developmental pathways to autism: A review of prospective studies of infants at risk. In Neuroscience & Biobehavioral Reviews. 2014;39:1–33.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/68531