International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

2021IJIEMR.Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 17th Sept 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-09

DOI: 10.48047/IJIEMR/V10/I09/22

Title **Utilizing Machine LearningTechniques for Detection of Intrusion in a Network**

Volume 10, Issue 09, Pages: 162-170

Paper Authors

Dr.M.Jogendra Kumar, Dr. N.Raghavendra Sai, Mr.T. Ravi Kumar

International Journal for Innovative Engineering and Management Research ★

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.o

Utilizing Machine LearningTechniques for Detection of Intrusion in a Network

Dr.M.Jogendra Kumar 1 , Dr. N.Raghavendra Sai 2 , Mr.T. Ravi Kumar 3
1,2 Assoc.Professor Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India
2 Email: nallagatlaraghavendra@kluniversity.in
3Asst.Professor Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

Abstract – Growing the volume and influence of the association's assaults, compelling corporate constructions to fix the association's security arrangements to keep away from tremendous money related mishaps. Blackout identification frameworks are presumably the most basic security gadgets to guarantee the security of any association. When pondering tremendous volumes of data about the association and complex nature of blackouts, improving on the introduction of the organization interruption location framework has become an open inquiry that is acquiring and more thought by researchers in nowadays. The objective of this report is to recognize an AI estimation that gives high exactness and a nonstop casing application. This article evaluates the openness of 15 distinctive AI computations utilizing the NSL-KDD dataset dependent on the bogus exposure rate, ordinary exactness, root mean square mistake, and model form time. Initial, 5 of the 15 AI computations are chosen dependent on the most limit accuracy and minimal mistake in WEKA. Entertainment of these AI estimations is done through a ten-time cross-endorsement. From that point, the best AI estimation is picked dependent on the most extreme exactness and least edge season of the model, so it tends to be performed rapidly and logically in interruption recognition frameworks.

Keywords: **Network, WEKA,Intrusion detection, Classification**

I . Introduction

This part ought to present the article. Writers ought to present inconveniences that will be inspected all through the article. At the hour of computerization of data, the improvement of the affiliation and its inactive cutoff enables individuals to complete their all around regular tasks in the most confounding exercises from distant locales ability during the period without any difficulties. Despite the fact that the association has a ton of better ways to deal with arriving at end clients for activity plans, it additionally conveys the related threat [1]. As indicated by the examination by Kessel and Allan [2] "Each affiliation risks enduring an advanced assault". To shield against these assaults, customers and affiliations should shield themselves from disturbances. In particular terms, interruption is the capacity to enter an office and arrange its mystery, decency, and availability [3-4].

Subsequently, a PC or corporate casing is viewed as protected if it has security, reasonableness, and openness against different sorts of dangers [5-6]. To get associations and delicate data against interferences or assaults, particular protectionmost affiliations utilize the devices. Albeit the firewall istaken as a first line insurance to get against attacks/breaks from an external perspective in many affiliations, nonetheless, expecting that an interference/assault avoiding the firewall or an assault is

inner, the firewall isn't to be utilized [8]. Assault avoidance methodologies, for instance encryption, miss the mark if an aggressor utilizes an application defect, for example, a flood cushion, to create genuine security threats. The Interruption Detection System (IDS) enters the scene when the strategies referred to above emerge [9]. They take after the second line of securities in your affiliation or office.

The troublesome issue with the current IDS is the ability and precision to perceive prevents [16]. A helpful IDS ought to be adequately canny to use zero-day attacks with high precision. Lately, automated thinking systems are by and large used in network power outage ID techniques as they require less key information, liberally decline the heaviness of inspecting monstrous volumes of affiliation traffic, and give substantially more definite results. on account of a zero-day attack. An AI computation gets a gathering of areas in an informational index that contains different classes (normal and impossible to miss) as data. It implies secluding them as exactly as conceivable with the assistance of a model

The concise shows that the investigators haphazardly chose a computation from each exhibit class and contrasted them with following the best for a particular informational collection or took a gander at changed estimations from a solitary AI computation arrangement. Likewise, the best gauge is set up dependent on the figure of the gauge. Nonetheless, performing IDS in a steady environment is possible just if a distinguishing proof edge offers high forecast precision at all comprehensible time with the objective that therapeutic developments can accomplish right away.

Then, the motivation that drives the creation of this article is to choose to show the 15 most conventional AI estimations from different characterizations and select the best dependent on greatest exactness and least expected time for an IDS dependent on anomalies. This article assesses the introduction of different AI estimations in NSL-KDD informational collections.

2. Literature Survey

At first, the possibility of the disclosure of disturbance was recognized by James in 1980 [18]. The maker has advanced a security acknowledgment model that recognizes the anomaly in the client's conduct. Lee et al. They have proposed an efficient system [19] that utilizations information mining techniques. to recognize the breaks in 1998. In 2000, Lippmann et al. introduced a relative report [20] of different portrayal computations for the disclosure of blackouts in 2000. A framework [21] that utilizations distinctive manner estimations to get ready classifiers in the informational collection of ideal and vindictive executables so they can recognize the arrangement of the new executable was made by Schultz et al. in 2001.

In 2012, Neetu proposed an IDS structure as a blend of Naïve bayes and head part assessment. The results showed that this plan can improve execution speed.It is clear from the above discussion that the makers recorded as a hard copy picked the best classifier dependent on the normal accuracy in portraying the occasions. Regardless, the time it takes to construct a model is basic to running a made blackout distinguishing proof model. Then, the expectation of this article is to plan a model that has greatest exactness and sets aside less effort to assemble the model.

3. Observational STUDY

In this report, the maker utilizes the NSL-KDD dataset to choose the plausibility of different AI computations for the area of the break and run the tests steadily. All along, the test assessment environment depends on the decision of the stage,. Right off the bat, the test assessment climate is based upon by picking the stage, programming, dataset and test alternative. Furthermore, various classifiers are browsed the distinctive arrangement classifications: Bayesian, capacities, rules and tree based methodologies.

3.1. Evaluation trial

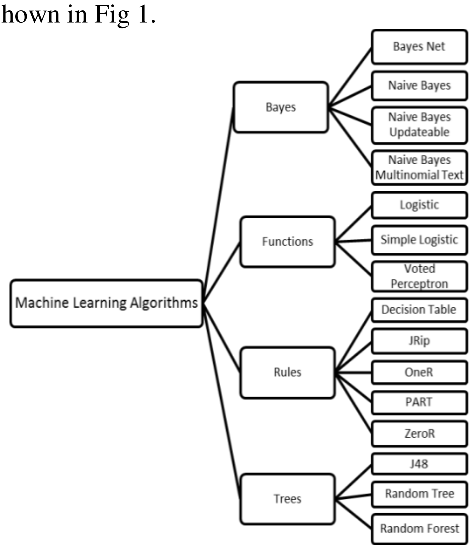
First itmaybe the most generally utilized gadget. At first it is written in C yet later it was changed to Java. WEKA incorporates different estimations to run the data extraction charges. Similarly, these are gadgets that can be utilized for the pre-handling of information,relapse, gathering, gathering, association rules, evaluator attributes and portrayal. In this record, the maker assesses a segment of the AI computations.

The NSL-KDD dataset understood that it handled a segment of the ordinary issues of KDDCUP'99. It contains meticulously picked records from an absolute educational assortment from KDDCUP'99 and moreover handles the issues constrained by Tavallaee et al. This paper surveys the NSL-KDD dataset considering the way that it will in general be viably shared and allows different analysts to consider all social occasion systems under a tantamount benchmark. With the affiliation's live traffic, analysts have attempted to complete or improve past test achieves light of how live information is never shared or given on account of abnormal inquiries. This enlightening list is used to prepare for a higher IDS. Separate affiliation traffic into 2 classes. Around the beginning it contains 125973 models and 42 properties .

This report uses a 10-wrinkle cross support to design and survey calculations, as it diminishes the appraisal collection . If a cross-underwriting event occurs, the information is isolated into 2 subsets, a subset to run the test and the other subset to insist the assessment. To decrease the, a few cycles are performed with heaps of variable size and a while later the normal is taken. Because of a 10-time cross-underwriting, the dataset is discretionally isolated into 10 regions so the class is addressed to a degree indistinguishable from that of the full dataset. The learning cycle is done on various events in various course of action sets. A regular of 10 botch speeds of 10 particular folds set out to get an overall error rate. The cross-support of 10 covers is considered considering the way that expansive assessments across various instructive assortments have found that on different occasions gives the best assessment of slip-up .From the help of the above settings, the evaluation of various arrangement assessments is performed.

3.2. Ranking calculations

Multiple classifiers can group your organization's traffic as typical or irregular. In this document, WEKA is used to classify traffic by calculations of various grouping classes, as clearly shown in Fig 1.



FigI Categories of Different MLAlgorithms

The classificationcategoriesare described asfollows:

a) Baye classifier

Bayesian classifiers utilize the Bayes theory to assess the likelihood of event of explicit events and store the class likelihood and the unexpected likelihood of every trademark. Subsequent to encountering another chance, the computation refreshes the probabilities put away with the instructional exercise. In this class, each of the four estimations are assessed. A short portrayal of the assessed computations is as per the following:

b) Bayes organization

A Bayesian association [37] faces a progression of components, for example, the hub of the diagram and the reliance between these factors shows up in the kind of edges. During the exhibit, a Bayesian association would need to make a few suppositions about between factor reliance and independence on the premise that, in all actuality, two variables are infrequently thoroughly free. Bayes Net models the association between the features in a straightforward manner. Nonetheless, this kind of model is incredibly awkward to make.

c) Guileless bayes

Sincere Bayes is a constrained sort of Bayes Net. To make the substantial execution of the Bayesian organization conceivable, Naïve Bayes expects the variables encompassing they are absolutely self-ruling. Artless Bayes is utilized when memory is restricted, CPU strength, and arrangement time are similarly amazingly imperative. Sincere Bayes is a PC master and can get ready with no issues. Nonetheless, it is an astoundingly straightforward portrayal that doesn't consider the rich hypothesis. Moreover, the assumption of self-sufficiency among those joined is unnecessarily persuading.

e)NaiveBayesMultinomialText

It is a particular sort of Naïve Bayes anticipated content records. Principal Naïve Bayes models a report as a lone word event and non-participation. Gullible Bayes reliant upon multinomials is used when different word events matter a ton, since you consider the amount of events. It has high computational handiness, precision for most bundling and guaging issues, regardless, the precision/exactness reduces with a subtle proportion of information.

f)NaiveBayes Updateable

It is a reliable kind of Naïve Bayes that handles every sales along these lines. It uses a section evaluator and a default precision of 0.1 to show mathematical attributes.

3.2.2 Limit classifier

They pass on the break faith plan and neuronal affiliation . In this kind of classifier, information is arranged ward on execution information. In this class the going with 3 calculations are surveyed:

a). Collaborations

The fundamental continuation recognizes that the data factors are numerical and have a Gaussian designation. In any case, you can in like manner get phenomenal results if the information isn't Gaussian. It's quick and easy to do, in any case it has an overfitting issue.

b). Direct coordinated efforts

SimpleLogistic adds a SimpleLinearRegression plan for each class. SimpleLogistic has a part elective under, for instance it quits adding SimpleLinearRegression plans when the cross endorsing blunder quits diminishing. Stay away from over-assortment of data accessibility, yet ruin learning correspondence.

c). Casted a democratic structure Perceptron

This estimation utilizes straightforwardly discernable data with gigantic edges. Easy to perform and its precision looks like Help Vector Machine (SVM). You additionally work with high-dimensional data utilizing as far as possible. In any case, this estimation requires a huge degree of breaking point..

3.2.3 . Rule classifier

For a precise assessment of the class in the midst of its immense number of qualities, the rules of association are utilized [36, 40]. They are commonly specific in nature and can be adjusted thusly. Past what can be generally anticipated with the assistance of the standard based classifier. The short portrayal of the estimations reviewed in this class is the going with:

a) Decision table

Summarizes the instructive assortment as a table of options that consolidates equivalent extents of characteristics as in the principle enlightening list. A subset of authentic properties by then pick which one uses the best first chase. By excepting the most un-contributing qualities in the arrangement of the model, this calculation takes out the hazard of overfitting and as needs be makes a little and decreased pick table. Regardless, the calculation ends up being extremely obfuscated if a couple of qualities don't know.

b)JRip

Use models from past judgment in the arranging information and make a lot of decisions that covers all individuals around there. Starting there on, continue forward to the accompanying activity until all classes have been covered. JRip develops models so they can be unscrambled with no issue. It can manage preeminent and consistent attributes similarly as high volume information. In any case, it doesn't give high sureness/exactness when the arranging set is nearly nothing.

c). Phenomenon

You manufacture a unique standard by differentiating each credit, along these lines, with everything taken into account you pick the standard that has the most diminished mix-up rate. That is the explanation which is also known as OneR. The WEKA, a standard that sees as far as possible number of right models is picked as the singular rule. For this, the most unpredictable class of this brand name regard is handled . If two rules have a hazy screw up rate, pick one of the norms without objective. The principles made thusly are likely not as exact instead of other machining condition calculations, anyway clear and easy to decipher. Furthermore, it detaches all of the attributes into separated ranges. This could cause an overfitting issue if consistent surveyed characteristics occur.

d). PART

This calculation spreads the word about an organized arrangement of rules as assurance plans. The new information is worked with against each standard and the thing is given out to the best coordination class with the norm. In every highlight. It is a blend of calculation of C4.5 and JRip

e) ZeroR

This assessment is follow subordinate and ignores all flags. Make a recurrent table for the target and pick its most repeating regard. Notwithstanding the way that it has no power of supposition, it is useful to evaluate the introduction of the model as a benchmark for relationship with other learning calculations. An exorbitant issue occurs.

3.2.4 Trees

They set up a tree plan for the middle focuses to go through a brand name regard test and the branch drives the test result .They are similarly eminent by the name of the picked network. The depiction of the assessments evaluated in this class in the NSL-KDD educational assortment is according to the accompanying:

a). J48

Make a joined tree and genius something different dependent upon the decision tree made by the potential gains of data planning. At whatever point a great deal of status is gifted, this evaluation sees the brand name that unquestionably withdraws by a wide margin the greater part of the occasions. It is stunning stood apart from other simulated intelligence estimations.

b)RandomTree

This computation is known as a fearless tree, as you are really planning the dataset again and again by abstractly picking a subset of highlights, this outcomes all through action of various decision trees. To appear at a last political race, each tree makes a choice. This is a kind of technique decreases the risk of overfitting. It works productively on gigantic edifying records and keeps up exactness in all conditions when there is no epic degree of data. Regardless, overlook the connection between credits.

c). RandomForest

RandomForest is a mix of different RandomTrees in an epic classifier with various randomization measures. The value of each tree relies on the enthusiastically investigated information vector. Joining the abnormality is the progress of each tree again on conceivably different lines attempted with redundancies. In specific degrees of highlights are picked by truly picking a subset of pieces. Thusly, each tree is striking and each tree votes for a specific class and the class with the most votes changes into an early class. It offers less depiction bumbles and handles clashing illuminating records well surely.

4. Execution Assessment

To assess the introduction of the 15 most regularly utilized simulated intelligence appraisals in different evaluations utilizing the NSL-KDD dataset, a wearing report is acted in this section.

4.1. Diversion climate

The responsiveness of various recreated insight assessments in the NSL-KDD dataset is surveyed with the help of WEKA. The evaluation is done in the KDDTrain+ .arff report which contains 125,973 cases with 41 properties. Cross-endorsing of 10 overlays is used as a test elective during all assessments. Examinations are run on various events and results are arranged by taking an ordinary of ten unprecedented appraisals in the KDDTrain+ .arff vault. The assessment gives a ton of computational data, for instance, model plan time, obvious sorts of bumbles, and a chaotic system. The relationship of disarray is the establishment from which past what many would consider possible can be settled. The Disorder structure consolidates 4 credits:

TP: TP shows the amount of accurately saw positive opportunities.

FP: FP shows the amount of negative opportunities that are erroneously seen as self-evident, for example, the amount of standard traffic trades with wrong names.

TN: TN shows the amount of negative cases that are perceived as negative.

FN: FN displays the amount of positive opportunities mistakenly perceived as negative.

In this record, Bogus Revelation Rate, Normal Exactness, Root Mean Square Blunder, and Model Form Time are utilized to overview the presentation of classifiers where a worth of Bogus Disclosure Rate and Normal Precision is tended to with the assistance of disarray. net.

4.2. Execution appraisal

This part presents the receptiveness association between's the 15 assessments referred to above reliant upon various assessments in the NSL-KDD enlightening assortment.

4.2.1 FDR

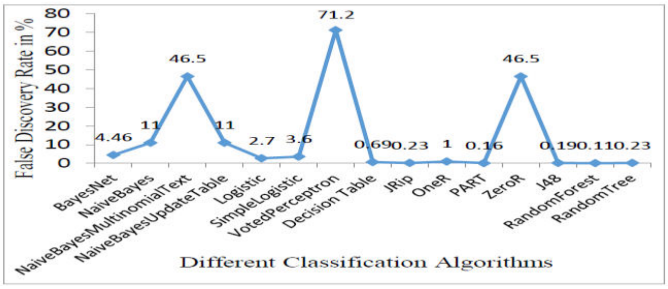


Fig2DiscoveryFalse Rate

FDR shows the level of inaccurately made positive sorts out of the full scale number of positive suppositions. It is settled with the assistance of under alluded to recipe:

FDR=FP/TP+FP *100

It ought to be fundamentally pretty much as little as practical for a pleasant strategy assessment. Figure 2 shows that RandomForest has least FDR followed by PART, J48, RandomTree and JRip.

4.2.2. Normal Exactness (AA) AA is settled as the level of reasonably gathered occasions from the absolute number of class models. It is settled with the assistance of under alluded to condition:

Conventional Precision of a depiction assessment should be on the for the most part magnificent quality. Figure 3 outlines the way that RandomForest has the most raised accuracy of 99.9% followed by RandomTree, PART, J48 and JRip with 99.8% precision.

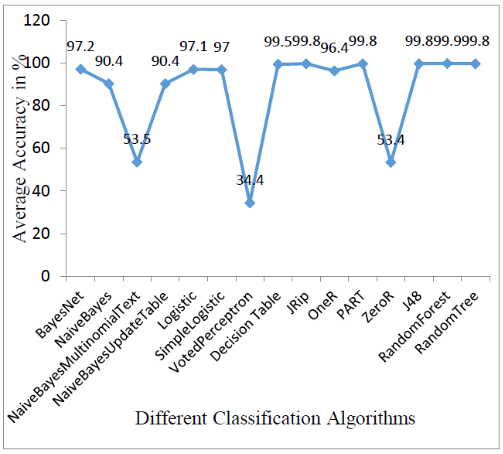


Fig 3 Average Accuracy Rate

4.2.3. RMSE:-It is a great measurement for numeric forecast. To figure RMSE, we first need to compute remaining. Remaining is contrast between genuine worth and the worth anticipated by the model. RMSE is determined with the assistance of underneath referenced recipe:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)}$$

Where, yi is the actual value, ŷi is the predicted value and n is number of predictions

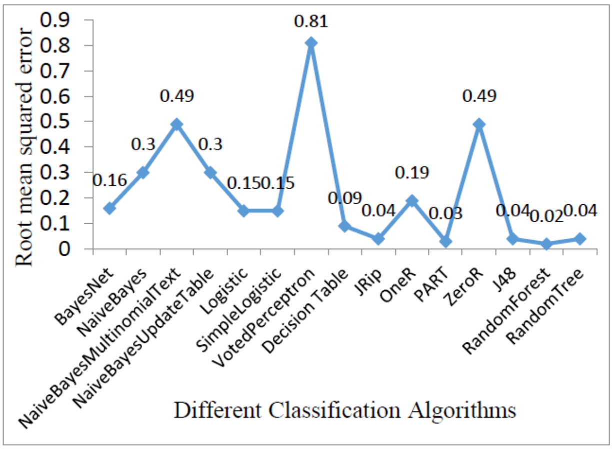


Fig 4 RMS Error

It is clear from the Figure 4 that RandomForest has least root mean squared misstep followed by PART, JRIP, J48 and RandomTree. Table 1 presents a total assessment between the

15 most notable AI estimations.

Classification Category	Algorithm	FDR	AA	RMSE
Bayes	Bayes Net	4.46%	97.17%	.16
	Naïve Bayes	11%	90.38%	.30
	Naïve Bayes Multinomial Text	46.5%	53.45%	.49
	Naïve Bayes Update Table	11%	90.38%	.30
Functions	Logistic	2.7%	97.1%	.15
	Simple Logistic	3.6%	97%	.15
	Voted Perceptron	71.2%	34.4%	.81
Rules	Decision Table	.69%	99.5%	.09
	JRip	.23%	99.8%	.04
	OneR	1.0%	96.37%	.19
	PART	.16%	99.8%	.03
	ZeroR	46.5%	53.4%	.49
Trees	J48	.19%	99.78%	.04
	Random Forest	.11%	99.9%	.02
	Random Tree	.23%	99.76%	.04

I TableComparison Performance of15 Classifiers based on various boundaries

It is obvious from the above outcomes that out of 15 arrangement calculations, 5 characterization calculations perform best as far as exactness, bogus identification rate and blunder. Table 2 portrays the exhibition correlation between best 5 AI calculations.

Category Classification	Alg	RMSE	FDR	AA
Rules	JRip	.03	.22%	99.7%
	PART	.02	.15%	99.7%
Trees	J48	.03	.18%	99.68%
	RandomForest	.03	.10%	99.9%
	RandomTree	.04	.22%	99.75%

II Table: Comparison Performance between best 5 AI calculations based on various boundaries

Nonetheless, model structure time is a vital boundary to choose the attainability of execution of a calculation continuously network IDS. A calculation won't be reasonable if its normal exactness is exceptionally low or if its preparation time is extremely high. In this way, it is vital to decide the time needed by a calculation to assemble a model on the dataset .

4.2.4. Model Building Time : MBT is the model structure time on preparing information. Figure 5 shows that model structure time is least if there should arise an occurrence of RandomTree and most extreme for JRip out of a bunch of best 5 performing calculations

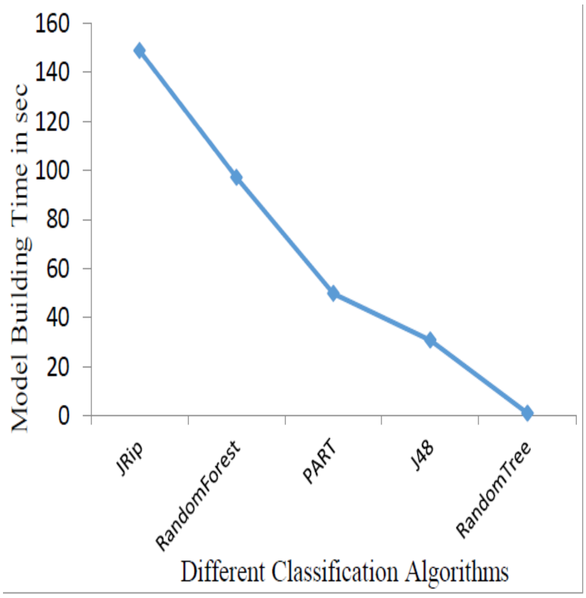


Fig 5 Model Building Time

4.3. Discussion

In the wake of investigating the presentation of 15-demand assessments, it is normal that a couple of calculations perform better contrasted with different calculations. Here, the creator investigates all of the requirements of the appraisal self-sufficiently.

A. FDR

FDR is the level of positive gauges made in screw up from irrefutably the amount of positive suspicions. It basically presents the amount of typical traffic events that are doled out inadvertently. In any case, the separation between the FDR of these calculations isn't huge, for what it's worth under 0.25% for the best 5 assessments.

B. Medium precision

All rule-based and tree-based calculations are significantly accurate, except for the ZeroR assessment. It also upholds the producer's conversation in divide 3 that ZeroR is essential to running the sort. VotedPerceptron gives a central extent of precision, followed by NaiveBayes-basedandzeroR other calculations.

C.RMS ERROR

Not in the slightest degree like Mean Supreme Mistake, RMSE scarcely excuses gigantic bungles. It is in any occasion for RandomForest followed by PART, RandomTree, J48 and JRip without or without capability..

Though the ID rate is a phenomenally gigantic part in an IDS, it is crucial to evaluate the credibility of playing out an assessment in a predictable IDS. Choosing a gathering assessment expects a basic part in improving an affiliation's IDS show. An IDS affiliation is the need of the business world, not the cognizant world. Affiliations are looking for assessments that perceive power outages with high precision and with a limited ability to focus time. Analysts ought to use significantly definite yet monotonous assessments to collect the model at their investigation office. Along these lines, it is essential to consider the hour of the development of the model.

D. Time to develop the model

It is obvious from Table 1 over that RandomForest offers the most vital discover rate and the most un-sham cautions instead of 14 distinct assessments. RandomForest saves essential exertion to amass the model as it makes various classifiers. The best calculation performed with a low ideal opportunity to gather the model is RandomTree. This model can expect an essential part for affiliations hoping to pass on an anticipated definitive IDS. This model can similarly be important for specialists wanting to improve light mining calculations.

5. CONCLUSION

The reasoning for this archive is to perceive powerful and exact AI figuring that can profitably address and control the steadily extending issue of authoritative disturbance. At first, a composed outline of the KDDCUP'99 and NSL-KDD dataset examinations is given. Therefore, a top to bottom examination was finished on the 15 most popular AI estimations alongside their benefits and burdens. Around then, WEKA is utilized to inspect the openness of the most mainstream AI estimations. The paper expects that of 15 more customary AI estimations, RandomTree has a high limitation rate and negligible model casing time, so it will in general effectively run on a steady association IDS. The decision to feature will at that point be made in the current computation so the acknowledgment precision can be additionally improved without growing the hour of the model design in the high-dimensional informational index. Besides, consistent runs of the estimation won't ever be needed to survey its achievability..

References

[1] R Daş, A Karabade, G Tuna, “Common Network Attack Types andDefenseMechanisms”,in*SignalProcessingandCommunicationsApplicationsConference(SIU)*,16-19May2015,pp.2658–266.

[2] P. Kessel, K. Allan, “Get ahead of cybercrime” in *Global InformationSecuritySurvey*,October 2014,pp.1-36.

[3] M Panda, A. Abraham, M. R. Patra, “A hybrid intelligent approach fornetworkintrusiondetection”in*InternationalConference onCommunicationTechnologyandSystemDesign*,vol.30,2012,pp.1-9.

[4] O. Can, O.K. Sahingoz, “A survey of intrusion detection systems inwirelesssensornetworks”in*6thInternationalConference oninModeling, Simulation, and Applied Optimization (ICMSAO)*, 27-29 May2015,pp.1-6.

[5] R.C.Summers,“Securecomputing:Threatsandsafe-guards”inComputers, NewYork:McGraw-Hill,2000,pp.1-688

[6] C.P.Pfleeger,S.L.Pfleeger,“SecurityinComputing”in*ComputerSecurity*,4thed., USA:PrenticeHall PTR, 2006,pp.1-845.

[7] Firewalls(2015).Firewall definition frompcmagazine encyclopedia.Retrieved from http://www.pcmag.com/encyclopedia/term/43218/firewall;accessedJune18,2015.

[8] W.Stallings,“CryptographyandNetworkSecurity:PrinciplesandPractice”5thed., USA:PrenticeHallPress, pp.1-900

[9] H.M.Imran,A.B.Abdullah,M.Hussain,S.Palaniappan,andI.Ahmad,“Intrusions detection based on optimum features subset and efficientdatasetselection”in*InternationalJournalofEngineeringandInnovativeTechnology(IJEIT)* vol. 2,no.6,2012, pp.265-270.

[10] U. Bashir, M. Chachoo, “Intrusion detection and prevention system:Challenges & opportunities” in *International Conference on Computingfor Sustainable Global Development (INDIA Com)*, 5-7 March 2014,pp.806-809.

[11] M. Baykara, R. Daş, “A Survey on Potential Applications of HoneypotTechnology in Intrusion Detection Systems”, in *International Journal ofComputer Networks and Applications (IJCNA)*, vol. 2, no. 5,October2015,pp.203-208.

[12] M.J.Ikram,J.Cazalas,“EfficientCollaborativeTechniqueusingIntrusion Detection System for Preserving Privacy in Location basedServices”,in*InternationalJournalofComputerNetworksandApplications(IJCNA),* vol. 2,no.5,October2015,pp.222-231.

[13] H.Benmoussa,A.A.Kalam,A.A.Ouahman,“Towardsanewintelligentgeneration of intrusion detection system”, in *Proceedings of the 4thEditionofNationalSecurity*

Days,12-13May2014,pp.1-5.

[14] S.Benferhat,K.Tabia,"IntegratingAnomaly-BasedApproachintoBayesian Network Classifiers" in*e-Business and Telecommunications*,2009,vol.8,eds.JoaquimFilipe,MohammadS.Obaidat,pp.127-139.

[15] J. McHugh, "Testing intrusion detection systems: A critique of the 1998and 1999 DARPA intrusion detection system evaluations as performedbyLincolnLaboratory"in*ACMTransactionsonInformationandSystemSecurity*, vol.3,no.4,2000,pp.262–294.

[16] A.Hofmann,B.Sick,"OnlineIntrusionAlertAggregationwithGenerativeDataStreamModeling,"in*IEEETransactionsonDependableandSecureComputing*,vol.8,no.2,2011,pp.282-294.

[17] O. Maimon, L. Rokach (Eds.), "Data Mining and Knowledge DiscoveryHandbook"in*DatabaseManagement&InformationRetrieval*,2nded. Springer,2010,pp.1-1285

[18] J.P.Anderson,"Computersecuritythreat monitoringand surveillance," *TechnicalReport*,FortWashington,Pennsylvania,USA,1980.

[19] W.LeeandS.J.Stolfo,"Dataminingapproachesforintrusion detection"in *Proceedings of the 7th conference on USENIX Security Symposium*,vol. 7,SanAntonio,TX,1998.

[20] N. R. Sai, G. S. C. Kumar, M. A. Safali and B. S. Chandana, "Detection System for the Network Data Security with a profound Deep learning approach," 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 1026-1031, doi: 10.1109/ICCES51350.2021.9488967.

[21] P. J. S. Kumar, P. R. Devi, N. R. Sai, S. S. Kumar and T. Benarji, "Battling Fake News: A Survey on Mitigation Techniques and Identification," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 829-835, doi: 10.1109/ICOEI51242.2021.9452829.

[22] N. Raghavendra Sai, J. Bhargav, M. Aneesh, G. Vinay Sahit and A. Nikhil, "Discovering Network Intrusion using Machine Learning and Data Analytics Approach," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 118-123, doi: 10.1109/ICICV50876.2021.9388552

[23] N. Vijaya, S.M Arifuzzaman, N. Raghavendra Sai, Ch. Manikya Rao " "Analysis Of Arrhenius Activation Energy In Electrically Conducting Casson Fluid Flow Induced Due To Permeable Elongated Sheet With Chemical Reaction And Viscous Dissipation" Frontiers in Heat and Mass Transfer (FHMT) 15 - 26 (2020) ISSN- 2151-8629,Volume -15, Dec,2020

[24] N. R. Sai, T. Cherukuri, S. B., K. R. and A. Y., "Encrypted Negative Password Identification Exploitation RSA Rule," 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2021, pp. 1-4, doi: 10.1109/ICICT50816.2021.9358713

[25] M. J. Kumar, G. V. S. R. Kumar, P. S. R. Krishna and N. R. Sai, "Secure and Efficient Data Transmission for Wireless Sensor Networks by using Optimized Leach Protocol," 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2021, pp.50-55, doi: 10.1109/ICICT50816.2021.9358729

[26] Sai N. Raghavendra1, Kumar M. Jogendra1 and Chowdary Ch. Smitha1" A Secured and Effective Load Monitoring and Scheduling Migration VM in Cloud Computing" IOP Conference Series: Materials Science and Engineering ISSN- 1757-899X, Volume-981, Dec 2020

[27] M. Jogendra Kumar1, N. Raghavendra Sai1 and Ch. Smitha Chowdary1" An Efficient Deep Learning Approach for Brain Tumor Segmentation Using CNN" IOP Conference Series: Materials Science and Engineering ISSN- 1757-899X, Volume-981, Dec 2020.

[28] A. Pavan Kumar1, Lingam Gajjela2 and N. Raghavendra Sai3" A Hybrid Hash-Stego for Secured Message Transmission Using Stegnography" IOP Conference Series: Materials Science and Engineering ISSN- 1757-899X, Volume-981, Dec 2020

[29] Ch. Smitha Chowdary1, Gayathri Edamadaka1, N. Raghavendra Sai1 and M. Jogendra Kumar1" Analogous Approach towards Performance Analysis for Software Defect Prediction and Prioritization" IOP Conference Series: Materials Science and Engineering ISSN1757-899X, Volume-981, Dec 2020

[30] Gayathri Edamadaka1, Ch. Smitha Chowdary1, M. Jogendra Kumar1 and N. Raghavendra Sai1" Hybrid Learning Method to Detect the Malicious Transactions in Network Data" IOP Conference Series: Materials Science and Engineering ISSN- 1757-899X, Volume981, Dec 2020

[31] Mohith Sai Krishna.Katakam ,Komali.Devineni, Pavana.Kanagala, DR.N.Raghavendrasai.

"ANALYSIS OF ARTIFICIAL NEURAL NETWORKS BASED INTRUSION DETECTION SYSTEM". International Journal of Advanced Science and Technology 29, no. 5s (April 4, 2020): 928 - 935. Accessed July 30, 2021. http://sersc.org/journals/index.php/IJAST/article/view/7832.

[32] N.RaghavendraSai and Dr. K.Satya Rajesh, "An Efficient Los Scheme for Network Data Analysis", Journal of Advanced Research in Dynamical and Control Systems (JARDCS) (ISSN: 1943-023X) Vol. 10,Issue 9,Aug 2018