IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Special Issue 2, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

Intrusion Detection Prediction Using Data Science Technique

Mrs. A. Jayanthi[1], Yuktha Sri K H[1], Sathyasree G[2], Harshitha MS[3]

Assistant Professor, Department of Computer Engineering, Velammal Engineering College, Chennai, Tamil Nadu, India

U.G. Scholar, Department of Computer Engineering, Velammal Engineering College, Chennai, Tamil Nadu, India

ABSTRACT: An intrusion is basically an activity that compromises the data security. The action of intruding is a threat to the security of the data present over the system. Intrusion detection systems are designed which are meant to safeguard security needs of enterprise networks against many cyber-attacks. Also, networks do suffer from certain limitations like it generates a high volume of low-quality alerts as notifications. The study has reviewed the state-of-the-art cyber-attack prediction based on Intrusion Alert, its models, and limitations. The ever-increasing frequency and intensity of intrusion attacks on computer networks worldwide intense research efforts towards the design of attack detection and prediction mechanisms. Although there a lot of intrusion detection systems, the prediction of intrusion events is still under process or active investigation. In the past, other means such as statistical methods have dominated the design of cyber-attack prediction methods. The analysis of dataset by supervised machine learning technique(SMLT) to capture several information's like, variable identification, univariate analysis, bivariate and multivariate analysis, missing value treatments etc. A comparative analytical study between various machine learning algorithms had been carried out, so that it can determine which of the algorithms is the most accurate in predicting the type of cyber-attacks. The results show that the effectiveness of the proposed machine learning algorithm technique can be compared with best accuracy, precision, Recall, F1 Score, Sensitivity, and Specificity.

KEYWORDS: Enterprise networks, analysis, security, intrusions, cyber-attacks, detection, prediction, mechanisms, Machine Learning, classification, NIDS, analysis, algorithms, pre-processing, deployment, visualization, anomaly detection.

I. INTRODUCTION

An Intrusion Detection System (IDS) is a device that monitors network traffic for suspicious endeavor and problems indicators when such recreation is discovered.It is a software program utility that scans a community or a gadget for the harmfulactivity or coverage breaching. Any malicious mission or violation is normallyreported both to an administrator or accrued centrally the use of a securityinformation and tournament administration (SIEM) system. A SIEM gadget integratesoutputs from more than one sources and makes use of alarm filtering strategies todifferentiate malicious pastime from false alarms. Although intrusion detection structures display networks for potentially malicious activity, they are additionally disposed to false alarms. Hence, organizationsneed to fine-tune their IDS merchandise when they first installation them. It meansproperly putting up the intrusion detection structures to understand what normaltraffic on the community appears like as in contrast to malicious activity.Intrusion prevention structures additionally reveal community packets inbound the systemto test the malicious things to do worried in it and at as soon as ship the warningnotifications.The proposed mannequin is to construct a laptop studying mannequin for anomaly detection. Anomaly detection is a vital method for recognizing fraud activities, suspicious activities, community intrusion, and different atypical events that may additionally have excellent magnitude however are tough to detect. The machine learning mannequin is constructed with the aid of making use of perfect facts science strategies like variable identification which is the structured and impartial variables. Then the pre- processing and visualisation of the records is accomplished. The mannequin is construct based totally on the previous dataset the place the algorithm research records and get skilled different algorithms are used for higher comparisons. The overall performance metrics are calculated and compared. We are imposing the laptop studying algorithm for classification purpose. More than two computer mastering algorithms are used for assessment of getting the first-rate accuracy. Deployment is finished for getting result.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

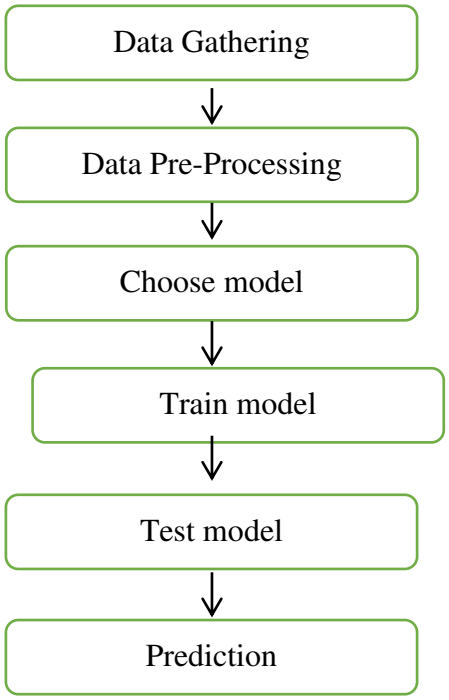
Department of CSE, Velammal Engineering College, Chennnai, India

II. RELATED WORKS

A Prediction Model of DoS Attack's Distribution Discrete Probability et.al [1] by Wentao Zhao, Jianping Yin, Jun Long in 2008describes the clustering hassle first, and then makes use of the geneticalgorithm to put into effect the optimization of clustering methods. Based on theoptimized clustering on the pattern data, we get more than a few classes of therelation between traffics and assault amounts, and then builds up severalprediction sub-models about DoS attack. Furthermore, in accordance to theBayesian method, we deduce discrete likelihood calculation about every sub-model and then get the distribution discrete likelihood prediction mannequin forDoS (Denial of Service) attack. Adversarial Examples: Attacks and Defenses for Deep Learning et.al [2] by Xiaoyong Yuan, Pan He, Qile Zhu in 2009 reviewed current findings on adversarial examplesfor DNNs, summarize the techniques for producing adversarial examples, andpropose a taxonomy of these methods. Under the taxonomy, purposes foradversarial examples are investigated. We similarly difficult on countermeasuresfor adversarial examples. In addition, three primary challenges in adversarialexamples and the possible options are mentioned. Apriori Viterbi Model for Prior Detection of Socio-Technical Attacksin a Social Network et.al [3] by Preetish Ranjan, Abhishek Vaish in 2014 tried to locate the hiddeninformation in large social community with the aid of compressing it in small networks throughapriori algorithm and then recognized the use of viterbialgorithm to predict the mostprobable sample of dialog to be accompanied in the community and if thispattern fits with the current sample of criminals, terrorists and hijackersthen it can also be beneficial to generate some variety of alert earlier than crime.New Attack Scenario Prediction Methodology et.al [4] by SerajFayyad, CristophMeinel in 2013 proposed an actual time prediction methodology for predicting mostpossible assault steps and assault scenarios. Proposed methodologyadvantages fromattacks record in opposition to community and from assault plan supply data. It comeswithout great computation overload such as checking of assault planslibrary. It affords parallel prediction for parallel assault scenarios.

III. METHODOLOGY

Download and set up anaconda and get the most beneficial bundle for computer studying in Python. Load a dataset and recognize its shape the usage of statistical summaries and statistics visualization. Machine mastering models, pick out the fantastic and construct self-belief that the accuracy is reliable. Python is a famous and effective interpreted language. Unlike R, Pythonis a complete language and platform that you can use for both research anddevelopment and developing production systems. There are even a lot ofmodules and libraries to choose, providing many ways to do every task.Python is an interpreted high-level general-purpose programminglanguage. Its plan philosophy emphasizes code readability with its use of giant indentation.



|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

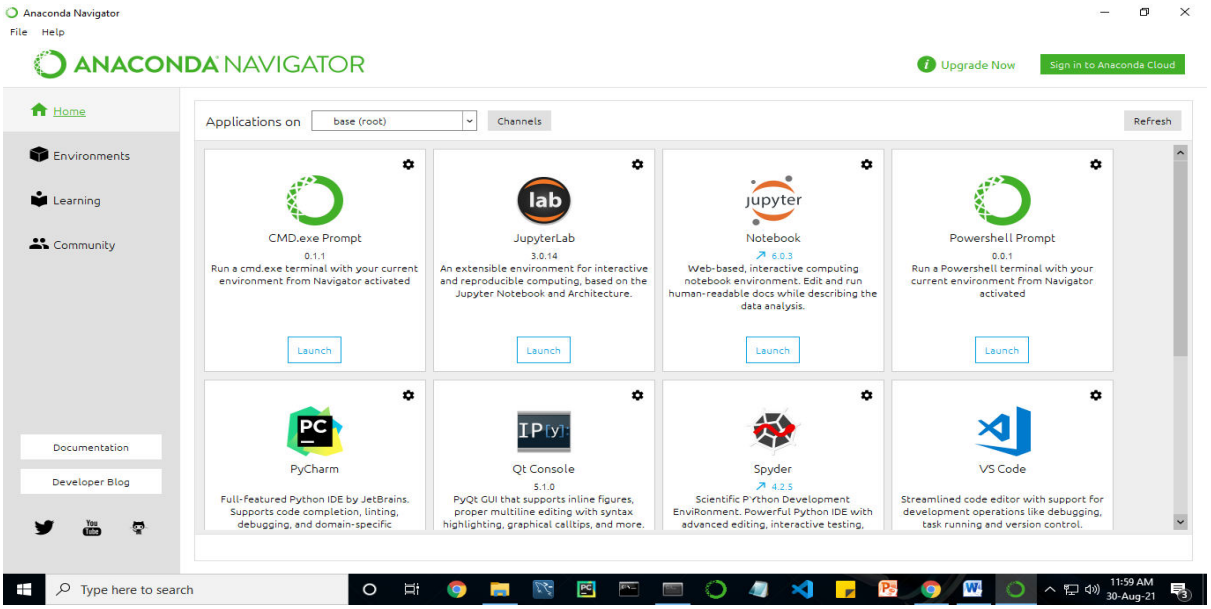
Department of CSE, Velammal Engineering College, Chennnai, India

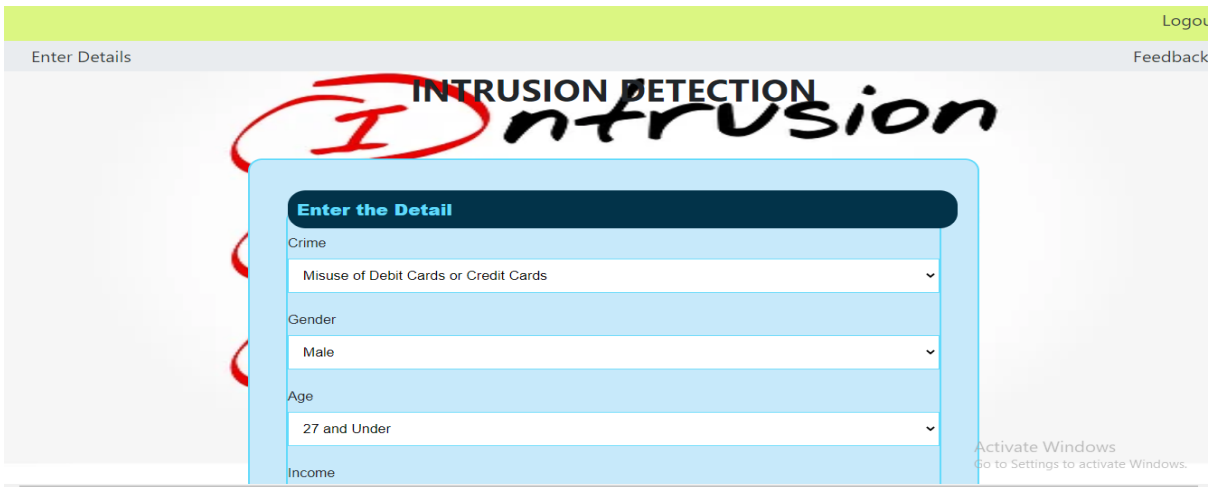
Anaconda is a free and open-source distribution of the Python and R programming languages for scientific computing (data science, laptop gaining knowledge of applications, large-scale data processing, predictive analysis, etc), that hobbies to in reality bundlemanagement and deployment. Anaconda Navigator is a laptop graphical consumer interface (GUI) includedin Anaconda distribution that permits you to launch functions and easilymanage condapackages, environments, and channels barring the use of command-linecommands.

IV. CONCLUSION

The analytical manner began from records cleansing and processing, lacking value, exploratory evaluation and eventually mannequin constructing and evaluation. The exceptional accuracy on public check set of greater accuracy rating algorithm will be discover out. The centered one is used in the utility which can help to discover the kind of intrusions. Some of the future works consist of deploying the challenge in the cloud. Also, to optimize the work to put in force in the IOT (Internet of Things) system.

V. EXPERIMENTAL RESULTS





|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

REFERENCES

[1] Abbasi, A. *et al.* (2014) "On emulation-based network intrusion detection systems," *Research in Attacks, Intrusions and Defenses*, pp. 384–404. Available at: https://doi.org/10.1007/978-3-319-11379-1_19.

[2] Ashraf, N., Ahmad, W., & Ashraf, R. (2018, January 1). A Comparative Study of Data Mining Algorithms for High Detection Rate in Intrusion Detection System. *Annals of Emerging Technologies in Computing*, *2*(1), https://doi.org/10.33166/aetic.2018.01.005 .

[3] An efficient feature selection and classification approach for an intrusion detection system using optimal neural network. (2023). https://doi.org/10.21203/rs.3.rs-1849099/v2 .

[4] Suman, C., Tripathy, S., &Saha, S. (2019). An Intrusion Detection System Using Unsupervised Feature Selection. *IEEE Region 10 Conference*. Available at: https://doi.org/10.1109/tencon.2019.8929510 .

[5] Depren, O., Topallar, M., Anarim, E., &Ciliz, M. K. (2005). An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. *Expert Systems with Applications*, *29*(4), 713–722. https://doi.org/10.1016/j.eswa.2005.05.002 .

[6] García-Teodoro, P., Díaz-Verdejo, J. E., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003 .

[7] Khan, L., Awad, M., &Thuraisingham, B. (2007). A new intrusion detection system using support vector machines and hierarchical clustering. *The Vldb Journal*, *16*(4), 507–521. https://doi.org/10.1007/s00778-006-0002-5 .

[8] Mukkamala, S., Janoski, G. I., & Sung, A. (2002). Intrusion detection using neural networks and support vector machines. *International Joint Conference on Neural Network*. https://doi.org/10.1109/ijcnn.2002.1007774 .

[9] Zhang, Y., Wang, L., Sun, W., Green, R. C., &Alam, M. S. (2011). Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. *IEEE Transactions on Smart Grid*, *2*(4), 796–808. https://doi.org/10.1109/tsg.2011.2159818 .

[10] Bahl, S., & Sharma, S. (2015). Improving Classification Accuracy of Intrusion Detection System Using Feature Subset Selection. *International Conference on Advanced Computing*. https://doi.org/10.1109/acct.2015.137 .

INNO SPACE
SJIF Scientific Journal Impact Factor

SJIF: 8.423

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details