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, Issue 8, August 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

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: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208039 |

Detection of U2R Attacks in Heterogeneous Network using KDD & ID Techniques

DR.D.J. SAMATHA NAIDU, T. Manasa

Principal, Annamacharya PG College of Computer Studies, Rajampet, India

MCA student, Department of MCA, Annamacharya PG College of Computer Studies, Rajampet, India

ABSTRACT: Currently estimates of computations for the assist vector machine, ANN, CNN, Random Forest, and deep learning based on the current CICIDS2017 dataset have been introduced significantly. Results indicate that when compared to SVM, ANN, RF, and CNN the profound learning calculation produced results that were substantially superior. We'll use port sweep operations as well as other attack kinds with AI and deep learning computations, Apache Hadoop and Sparkle technologies together based on this dataset later. All of these calculations enable us to recognize network cyber attacks. When we go back over many years, there may have been several attacks, and when these attacks are identified some datasets will be saved with the features at which values these attacks are occurring. In order to anticipate whether a cyber attack will occur or not, we will use these datasets. Four algorithms SVM, ANN, RF, and CNN are capable of performing these predictions. This study identifies the algorithm that forecasts the best accuracy rates and best outcomes to determine if cyber attacks occurred or not.

I. INTRODUCTION

Road accidents are become fairly commonplace. Road accidents are more likely to occur as people purchase cars at an increasing rate. Additionally, people nowadays are more careless than they were in the past. There is a lack of adherence to traffic regulations in larger cities, where there are numerous transportation options, the roads are getting smaller, and the population is increasing. Road accidents will therefore inevitably occur. Along with monetary loss, they also result in human loss. Therefore, regardless of the form of transportation used to travel, people need to be considerably more mindful when doing so. The rise in these incidents makes it unsafe for anyone to walk on foot. Every day, we read about incidents in the press, hear from family members, and occasionally even witness them firsthand. Over 1.35 million people die in traffic accidents each year, and an additional 20 to 50 million sustain moderate to severe non-fatal injuries, which often result in long-term impairments.

According to a World Health Organization (WHO) study on road accidents and deaths that are based on a country's financial situation, poor and middle-class persons in developing countries account for the majority of deaths from vehicle accidents When compared to the 11.3 per million persons in developed or higher-income countries, the death rate in poor countries is substantially higher at roughly 21.5 per million people. According to statistics, developing nations account for only 50% of the world's autos, however they account for over 90% of road traffic fatalities. According to statistics, 13 persons in India lose their lives in traffic accidents every hour.

However, if we consider the worst-case scenario, things could end up being far worse because the majority of accident instances are simply not recorded. Because of its low average record of 13 fatalities per hour, which leads in approximately 140,000 deaths per year, India is on the approach of supplanting the United States as the leading country in terms of traffic fatalities in the present. A victim can typically be found within the first three stages of an accident. Because approximately 10% of accident fatalities occur during this phase, the first phase of an accident is described as when the accident victim dies within a few minutes or seconds after the incident. When an accident has been in its second phase for around an hour, it has achieved its highest death rate (75% of all fatalities). preventing it by getting the victims timely assistance.

II. RELATED WORK

Different recent accomplishments in this area are presented in this segment. It should be noted that only the research that used the NSL-KDD dataset for performance benchmarking is examined in this article. Therefore, from this point on, every dataset referred to should be thought of as NSL-KDD. This process enables a more precise comparison of the

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208039 |

work with other sources of information from the writer. Another limitation is the use of information preparation for both testing and preparation in most activities. Finally, we look at a few deep learning-based approaches that have been tried before for similar kinds of tasks.

III. METHODOLOGY

A. Airport Security Scanner

Imagine your network is like an airport, and the incoming data packets are like passengers going through security. Just as security scanners detect suspicious items on passengers, machine learning algorithms act as advanced scanners that learn to identify unusual patterns in the data traffic. If a passenger (data packet) exhibits behavior that differs from regular travelers, the system raises an alert, just like the algorithm raises an alarm when it detects a potential cyber attack based on abnormal patterns.

B. Credit Card Fraud Detection

Think of your network as a bank, and the network traffic as credit card transactions. Just as banks use machine learning to identify unusual spending patterns that could indicate credit card fraud, your network's machine learning system analyzes traffic patterns to detect unusual behavior that might suggest a cyber attack. If someone suddenly starts making transactions from different countries or at odd hours, it triggers a fraud alert. Similarly, the machine learning system flags unusual network activities.

C. Wildlife Tracker

Consider your network as a wildlife reserve with different species of animals representing various types of network traffic. Machine learning acts like a sophisticated wildlife tracker that has learned the behaviors of different animals. If a new animal shows up or an animal starts behaving unusually, the tracker raises a red flag, indicating a potential threat. In the same way, machine learning algorithms detect new or anomalous network activities.

IV. EXPERIMENTAL RESULTS

Double-click the run button to start the project.to get the screen displayed below, run the bat file to test this application, I am using below images to store the data in decentralized form. Fig1 displays the home page of detection of cyber attack in network using machine learning techniques Fig2 displays the Data collection for Analysis. Fig3 displays the Predicting the type of attack.

Home page

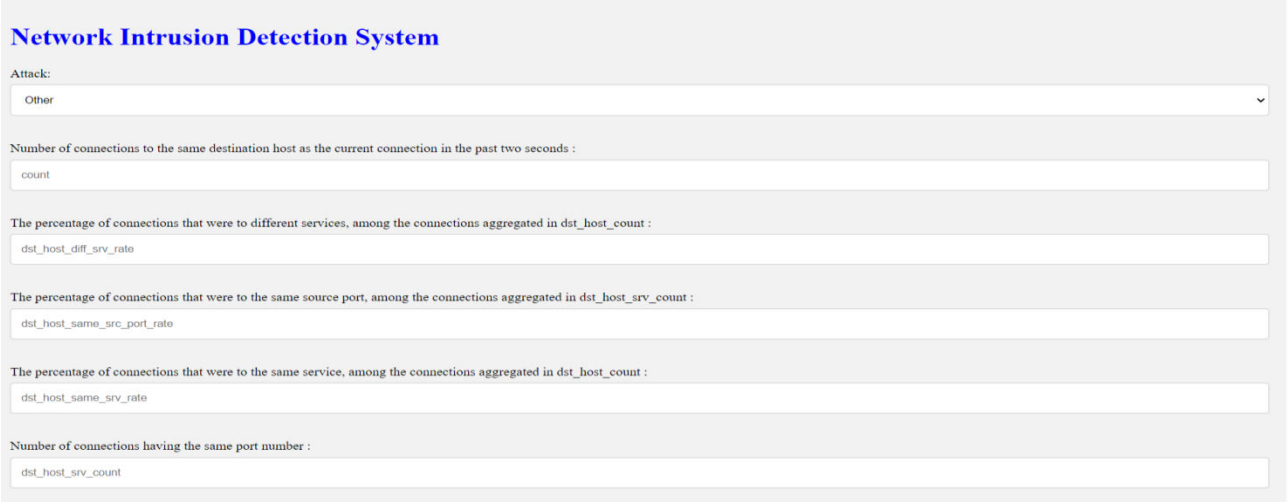

Fig1: First screen

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208039 |

Enter input data:

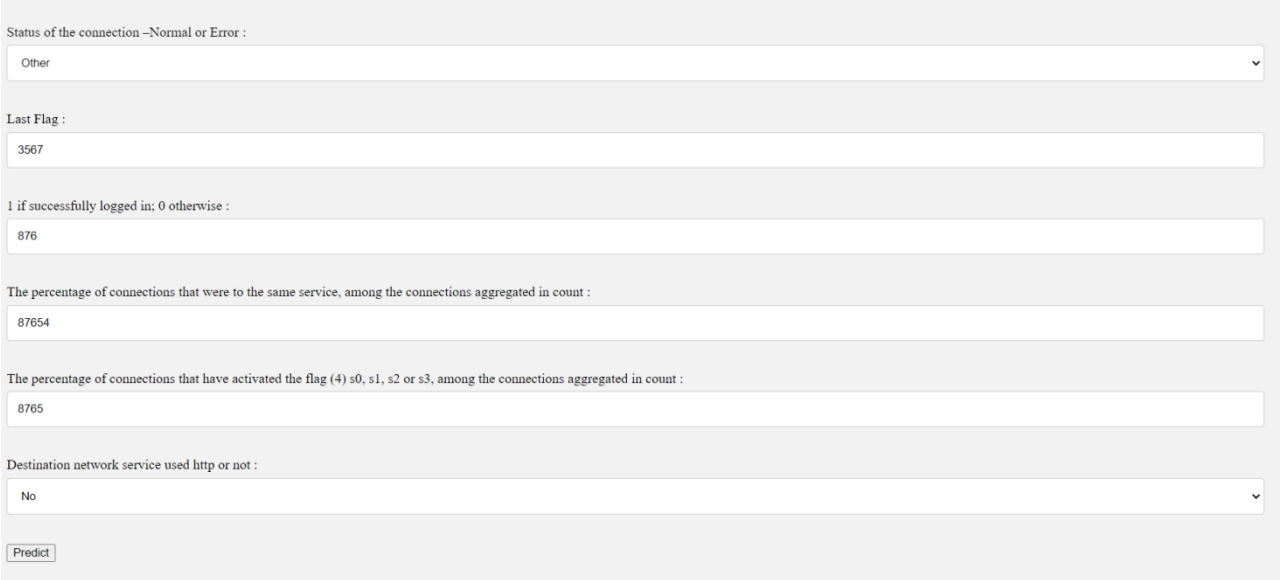

Fig 2: Data collection for Analysis

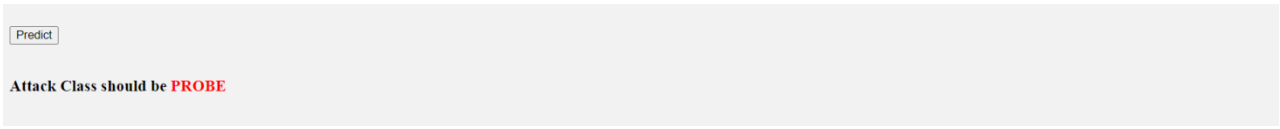

Fig 3: Predicting the type of attack

V. CONCLUSION

As of right now, estimates of computations for the assist vector machine, ANN, CNN, Random Forest, and deep learning based on the current CICIDS2017 dataset have been significantly introduced. The calculations for profound learning gave results that were noticeably better than those of SVM, ANN, RF, and CNN, according to the results. Based on this dataset, we'll eventually leverage port sweep operations, different attack types, and a combination of Apache Hadoop, Sparkle, and AI. Our ability to identify network cyberattacks is made possible by all of these calculations. Several assaults may have occurred over a long period of time, and when they are discovered, some datasets will be kept with the features whose values these attacks are occuring. For the purpose of determining whether utilise these datasets to determine whether a cyber assault will occur or not using current estimates of calculations for the assist vector machine and ANN. These predictions can be made using four algorithms: CNN, RF, SVM, and ANN. In this study, the optimal method for predicting if cyber attacks would occur and their success is identified.

REFERENCES

[1] K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.
[2] R. Christopher, “Port scanning techniques and the defense against them,” SANS Institute, 2001.
[3] M. Baykara, R. Das¸, and I. Karadogan, “Bilgi g ¨uvenli ˘gisistemlerindekullanilanarac¸larinincelenmesi,” in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013, pp. 231–239.
[4] S. Staniford, J. A. Hoagland, and J. M. McAlerney, “Practical automated detection of stealthy portscans,” Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208039 |

[5] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in high bandwidth environments," in DARPA Information Survivability Conference and Exposition, 2003.Proceedings, vol. 1. IEEE, 2003, pp. 130–138.
[6] K. Ibrahimi and M. Ouaddane, "Management of intrusion detection systems based-kdd99: Analysis with lda and pca," in Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on. IEEE, 2017, pp. 1–6.
[7] N. Moustafa and J. Slay, "The significant features of the unsw-nb15 and the kdd99 data sets for network intrusion detection systems," in Building Analysis Datasets and Gathering
Experience Returns for Security (BADGERS), 2015 4th International Workshop on. IEEE, 2015, pp. 25–31.
[8] L. Sun, T. Anthony, H. Z. Xia, J. Chen, X. Huang, and Y. Zhang, "Detection and classification of malicious patterns in network traffic using benford's law," in Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017. IEEE, 2017, pp. 864–872.
[9] S. M. Almansob and S. S. Lomte, "Addressing challenges for intrusion detection system using naive bayes and pca algorithm," in Convergence in Technology (I2CT), 2017 2nd International Conference for. IEEE, 2017, pp. 565–568.
[10] M. C. Raja and M. M. A. Rabbani, "Combined analysis of support vector machine and principle component analysis for ids," in IEEE International Conference on Communication and Electronics Systems, 2016, pp. 1–5.
[11] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," Journal of Computational Science, vol. 25, pp. 152–160, 2018.
[12] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." in ICISSP, 2018, pp. 108–116.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

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