International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 9, Issue 3, pp 275-278, March-2025
https://doi.org/10.47001/IRJIET/2025.903039

Detection of Cyber Attack in Network Using Machine Learning Networks

[1]K. Harshitha, [2]S. Ismail saheb, [3]G. Bhavana, [4]A. Asraar, [5]C. Irfan basha, [6]B. Harish

[1,3,4,5,6]UG Student, Dept. of E.C.E., Gates Institute of Technology, Gooty, Anantapur (Dist.) Andhra Pradesh, India
[2]Assistant Professor, Dept. of E.C.E., Gates Institute of Technology, Gooty, Anantapur (Dist.), Andhra Pradesh, India
E-mail: [1]harshithareddy8305@gmail.com, [2]ismail701@gmail.com, [3]bhavanaredyg1234@gmail.com, [4]asraarassu@gmail.com, [5]bashairfan2003@gmail.com, [6]harishbadri68@gmail.com

***Abstract* - Contrasted with the past, improvements in PC and correspondence innovations have given broad and propelled changes. The use of new innovations give incredible advantages to people, organizations, and governments, be that as it may, messes some up against them. For instance, the protection of significant data, security of put away information stages, accessibility of information and so forth. Contingent upon these issues, digital fear based oppression is one of the most significant issues in this day and age. Digital fear, which made a great deal of issues people and establishments, has arrived at a level that could undermine open and nation security by different gatherings, for example, criminal association, proficient people and digital activists. Along these lines, Intrusion Detection Systems (IDS) has been created to maintain a strategic distance from digital assaults. Right now, learning the bolster support vector machine (SVM) calculations were utilized to recognize port sweep endeavors dependent on the new CICIDS2017 dataset with 97.80%, 69.79% precision rates were accomplished individually. Rather than SVM we can introduce some other algorithms like random forest, CNN, ANN where these algorithms can acquire accuracies like SVM – 93.29, CNN – 63.52, Random Forest – 99.93, ANN – 99.11.**

Keywords: Cybersecurity, Cyber Attack Detection, Network Security, Machine Learning, Anomaly Detection, Classification Algorithms, Feature Extraction, Network Traffic Analysis, Supervised Learning.

I. INTRODUCTION

Contrasted with the past, improvements in PC and correspondence innovations have given broad and propelled changes. The use of new innovations give incredible advantages to people, organizations, and governments, be that as it may, messes some up against them. For instance, the protection of significant data, security of put away information stages, accessibility of information and so forth. Contingent upon these issues, digital fear based oppression is one of the most significant issues in this day and age. Digital fear, which made a great deal of issues people and establishments, has arrived at a level that could undermine open and nation security by different gatherings, for example, criminal association, proficient people and digital activists. Along these lines, Intrusion Detection Systems (IDS) has been created to maintain a strategic distance from digital assaults. Right now, learning the bolster support vector machine (SVM) calculations were utilized to recognize port sweep endeavors dependent on the new CICIDS2017 dataset with 97.80%, 69.79% precision rates were accomplished individually. Rather than SVM we can introduce some other algorithms like random forest, CNN, ANN where these algorithms can acquire accuracies like SVM – 93.29, CNN – 63.52, Random Forest – 99.93, ANN – 99.11.

II. LITERATURE REVIEW

2.1 R. Christopher, "Port scanning techniques and the defense against them," SANS Institute, 2001:

Port Scanning is one of the most popular techniques attackers use to discover services that they can exploit to break into systems. All systems that are connected to a LAN or the Internet via a modem run services that listen to well-known and not so well-known ports. By port scanning, the attacker can find the following information about the targeted systems: what services are running, what users own those services, whether anonymous logins are supported, and whether certain network services require authentication. Port scanning is accomplished by sending a message to each port, one at a time.

2.2 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:

Portscanning is a usual method in cybersecurity, both by attackers to question about mark networks and by defenders to label exposures in their own systems. Attackers usually use portscanning to decide that IP addresses and ports are active and conceivably easy, while defenders use it to evaluate safety risks. Detecting portscans is crucial for network protection, as

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 3, pp 275-278, March-2025

https://doi.org/10.47001/IRJIET/2025.903039

they frequently present image of precursors to more weighty attacks. While defenders mainly do not conceal their scans, attackers engage various secrecy methods to prevent detection. Skilled are continuous permissible and righteous debates regarding port scanning, specifically when transported outside permission.

2.3 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:

The freedom of networked plans has become a entire concern, moving individuals, activities, and governments. High-tech threats are growing briskly, with attackers steadily cleansing their strategies. High-tech disorder, conducted by criminal arrangings, specialists, and cyber activists, immediately poses a weighty risk to public and national protection. Individual of the most active defenses against these dangers is Intrusion Discovery Methods (IDS), which monitor networks for doubtful venture. Machine learning, specifically deep education and Support Vector Tool (SVM) algorithms, has demonstrated effective in IDS happening.IDS maybe anomaly-located (detecting changes from normal nature) or sign-based (equal popular attack patterns). One of the first steps in a cyberattack is inspection, place attackers scan open ports to recognize exposures.

2.4 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:

Intrusion Detection Systems (IDS) play a crucial role in network security, and feature selection significantly impacts detection accuracy. Individual feature selection methods may be unstable in different scenarios. This study proposes an ensemble-based feature selection method, treating feature selection as a two-class problem. It utilizes multiple methods such as mean decrease impurity, random forest classifier, stability selection, recursive feature elimination, and chi-square test, with a voting mechanism to determine the final feature subset. The approach is tested using Support Vector Machine (SVM), Decision Tree (DT), K-Nearest Neighbor (KNN), and Multi-Layer Perceptron (MLP) on KDDCup99, CIDDS-001, and UNSW-NB15 datasets, achieving a 99.40% classification accuracy on CIDDS-001.Since 1998, several publicly available IDS datasets have been developed, each with limitations.

III. PROPOSED SYSTEM

Proposed System for Detection of Cyber Attack in Network Using Machine Learning Techniques

Proposed System Architecture:

Data Collection: Network traffic data collected using tools like Wireshark or public datasets (e.g., NSL-KDD, CICIDS2017).

Preprocessing: Includes feature extraction, normalization, and handling missing values.

Feature Selection: Use techniques like PCA, mutual information, or recursive feature elimination.

Model Training: Apply ML algorithms like:

Decision Tree

Random Forest

Support Vector Machine (SVM)

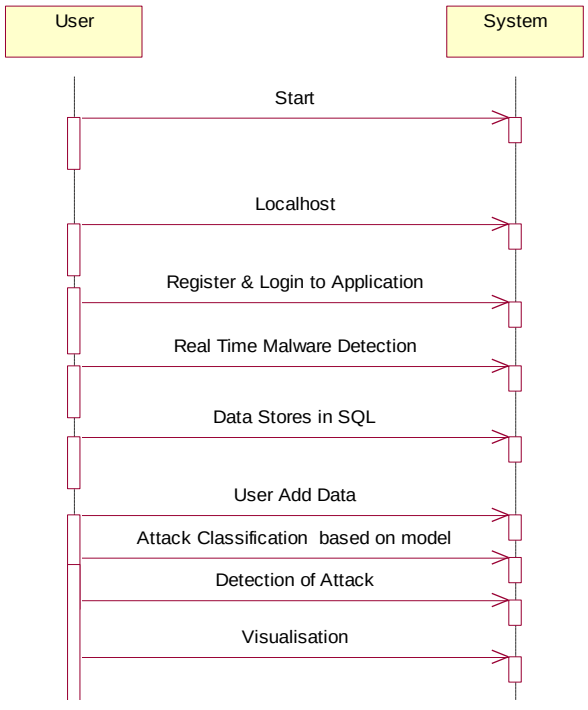
K-Nearest Neighbors (KNN)

Neural Networks

Evaluation Metrics: Accuracy, Precision, Recall, F1-score, ROC-AUC.

System Architecture

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.



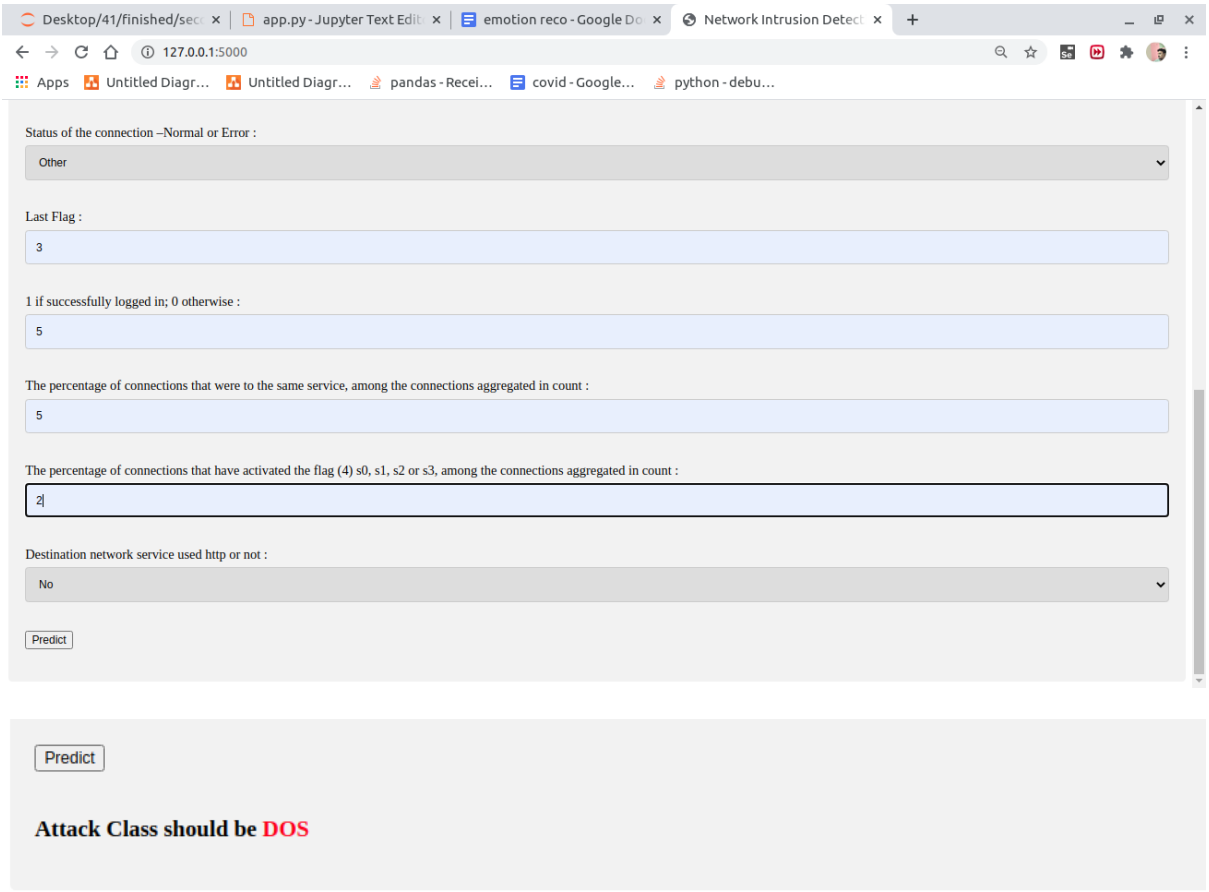
International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 3, pp 275-278, March-2025

https://doi.org/10.47001/IRJIET/2025.903039

IV. OUTPUT



V. CONCLUSION

Right now, estimations of help vector machine, ANN, CNN, Random Forest and profound learning calculations dependent on modern CICIDS2017 dataset were introduced relatively. Results show that the profound learning calculation performed fundamentally preferable outcomes over SVM, ANN, RF and CNN. We are going to utilize port sweep endeavors as well as other assault types with AI and profound learning calculations, apache Hadoop and sparkle innovations together dependent on this dataset later on. All these calculation helps us to detect the cyber attack in network. It happens in the way that when we consider long back years there may be so many attacks happened so when these attacks are recognized then the features at which values these attacks are happening will be stored in some datasets. So by using these datasets we are going to predict whether cyber attack is done or not. These predictions can be done by four algorithms like SVM, ANN, RF, CNN this paper helps to identify which algorithm predicts the best accuracy rates which helps to predict best results to identify the cyber attacks happened or not.

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. Karado ˘gan, “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.

[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.

ISSN (online): 2581-3048
Volume 9, Issue 3, pp 275-278, March-2025
https://doi.org/10.47001/IRJIET/2025.903039

[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.

[13] D. Aksu, S. Ustebay, M. A. Aydin, and T. Atmaca, "Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature selection algorithm," in International Symposium on Computer and Information Sciences. Springer, 2018, pp. 141–149.

[14] N. Marir, H. Wang, G. Feng, B. Li, and M. Jia, "Distributed abnormal behavior detection approach based on deep belief network and ensemble svm using spark," IEEE Access, 2018.

[15] P. A. A. Resende and A. C. Drummond, "Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling," Security and Privacy, vol. 1, no. 4, p. e36, 2018.

[16] C. Cortes and V. Vapnik, "Support-vector networks," Machine learning, vol. 20, no. 3, pp. 273–297, 1995.

[17] R. Shouval, O. Bondi, H. Mishan, A. Shimoni, R. Unger, and A. Nagler, "Application of machine learning algorithms for clinical predictive modeling: a data-mining approach in sct," Bone marrow transplantation, vol. 49, no. 3, p. 332, 2014.

Citation of this Article:

K. Harshitha, S. Ismail saheb, G. Bhavana, A. Asraar, C. Irfan basha, B. Harish. (2025). Detection of Cyber Attack in Network Using Machine Learning Networks. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(3), 275-278. Article DOI https://doi.org/10.47001/IRJIET/2025.903039

****

