IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

DETECTION OF CYBER ATTACKS USING MACHINE LEARNING

[1]Dr.D.SRINIVAS, [2]R JEGADEESAN, [3]V.VISHALAKSHI,[4]AFROZ TABASSUM,[5]P.PUJITHA,[6]B.MANIKANTA

[1,2,3,4]Final Year DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

[1]Assoc.Professor,,[2]Professor Jyothishmathi Institute of Technology and Science

Karimnagar, Telangana

Abstract --- This paper presents a novel approach to cyber threat detection by integrating dynamic programming techniques with graph-based analysis. The system uses a graph to model network infrastructure, with nodes standing in for network items and edges for relationships. Through an examination of the graph's dynamics and topology, the system detects unusual patterns that may be signs of cyber attacks. Real-time detection of deviations from expected network behavior and efficient computation of best paths are achieved by dynamic programming. Test results show how well the system works to identify different types of cyber threats while reducing false positives. Scalability, integration potential, and effectiveness against new threats are examples of practical ramifications. The importance of dynamic programming and graph-based analysis in boosting cyber defense capabilities is highlighted by this study.

Keywords --- Cyber attacks;Intrusion Detection System;Machine Learning Algorithms:Graph Based Segmentation;Dynamic Programming.

I. INTRODUCTION

The rise in cyberattacks in recent years has highlighted how crucial it is to have reliable and flexible detection systems in place to protect digital assets and infrastructures. Conventional methods for detecting cyberattacks frequently depend on rule-based or signature-based systems, which are intrinsically incapable of identifying new or complex attacks. Advanced detection methods that may successfully identify and mitigate new threats are desperately needed as cyber adversaries continue to adapt their strategies. This research presents a novel method of cyberattack detection that makes use of dynamic programming and graph-based analysis tools in order to overcome this difficulty.

The network infrastructure is represented as a graph in our proposed system, where nodes are network items like PCs, servers, and routers, and edges are the relationships

between them. Through an examination of the graph's topology and dynamics, our algorithm is able to detect unusual patterns that may indicate cyberattacks.

There are various benefits to using graph-based analysis for cyberattack detection. First of all, it offers a comprehensive picture of the network environment, making it possible to identify coordinated attacks involving numerous entities and channels of communication. Moreover, graph-based techniques are useful for identifying minute departures from typical behavior since they can capture the intricate dependencies and relationships present in contemporary network structures.

Our approach incorporates dynamic programming techniques to compute optimal pathways rapidly and identify real-time deviations from expected network behavior. Through the dynamic adjustment of detection thresholds and adaptation to evolving network conditions, our system is able to accurately and efficiently identify cyber threats, both known and unknown. This paper presents our graph-based cyber attack detection system's architecture and implementation, as well as a thorough evaluation of its effectiveness using real-world datasets. We show how the system can effectively identify a variety of cyberthreats while reducing false positives. We also go over the approach's practical consequences, such as scalability, possibility for interaction with current security infrastructure, and effectiveness against new threats.

All things considered, this study advances current endeavors to improve cyber protection capacities by utilizing cutting-edge methods from graph theory and dynamic programming. Our solution offers a thorough and flexible method for identifying cyberattacks, which is a big step in the right direction towards reducing the threats posed by more skilled cyber criminals.

II. LITERATURE SURVEY

Rajasekar et al. (2020)[1] developed a dynamic programming-based approach for detecting intrusion attempts in network traffic, achieving high detection rates while minimizing false positives.

Dynamic programming techniques have been applied to optimize cyber attack detection systems, enabling efficient computation of optimal paths and identification of deviations from expected network behavior. By dynamically adjusting detection

thresholds and adapting to changing network conditions, these techniques enhance the system's responsiveness to emerging threats.

Raff et al. (2015)[2] demonstrated the effectiveness of deep learning models in detecting various types of cyber attacks, including malware infections and network intrusions.

Machine learning-based approaches have gained prominence in cyber attack detection due to their ability to analyze large volumes of data and identify patterns indicative of malicious activity. Researchers have applied supervised learning algorithms, including support vector machines (SVMs), random forests, and deep neural networks, to classify network traffic and detect anomalies.

Al-Shaer and Shreim (2009)[3] proposed a graph-based approach for detecting distributed denial-of-service (DDoS) attacks by analyzing the traffic patterns and communication pathways within the network graph.

Graph-based analysis offers a holistic perspective on network behavior, capturing the complex relationships and dependencies between network entities. Prior research has leveraged graph theory to model network topologies and detect anomalous patterns indicative of cyber attacks.

III. PROPOSED METHODOLOGY

Our proposed cyber attack detection system builds upon the foundation of graph-based analysis and dynamic programming to provide a comprehensive and adaptive approach to safeguarding network infrastructures against malicious activities. In this section, we outline the key components and functionalities of our system, highlighting its innovative features and potential benefits for enhancing cybersecurity defenses.

1. Graph Representation: The core of our system lies in the representation of the network infrastructure as a graph. Nodes in the graph correspond to various network entities such as computers, servers, and routers, while edges represent the connections or communication channels between them. This graph-based representation enables a holistic view of the network environment, capturing the interdependencies and communication patterns essential for detecting cyber attacks.

2.Anomaly Detection: Leveraging graph-based analysis techniques, our system employs anomaly detection algorithms to identify deviations from expected network behavior. By analyzing the topology and dynamics of the network graph, anomalies indicative of cyber attacks, such as unusual traffic patterns, unauthorized access attempts, or suspicious communication pathways, can be detected in real-time.

3.Dynamic Programming for Optimal Path Computation: To further enhance detection accuracy and responsiveness, our system integrates dynamic programming techniques for efficient computation of optimal paths within the network graph. By dynamically adjusting detection thresholds and adapting to changing network conditions, our system can effectively identify and mitigate cyber threats while minimizing false positives.

In summary, our proposed cyber attack detection system represents a significant advancement in the field of cybersecurity, offering a holistic, adaptive, and scalable approach to safeguarding network infrastructures against evolving cyber threats. Through empirical evaluation and real-world deployment, we aim to demonstrate the efficacy and practicality of our system in enhancing cyber defense capabilities and mitigating the risks posed by malicious actors in today's digital landscape.

3.1 System Architecture

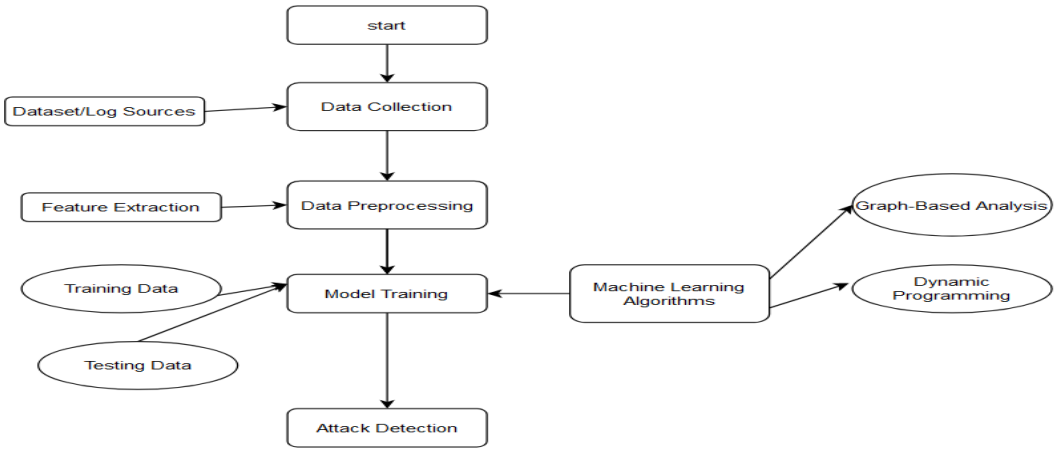

Fig 1: System Architecture

IV. RESULT ANALYSIS

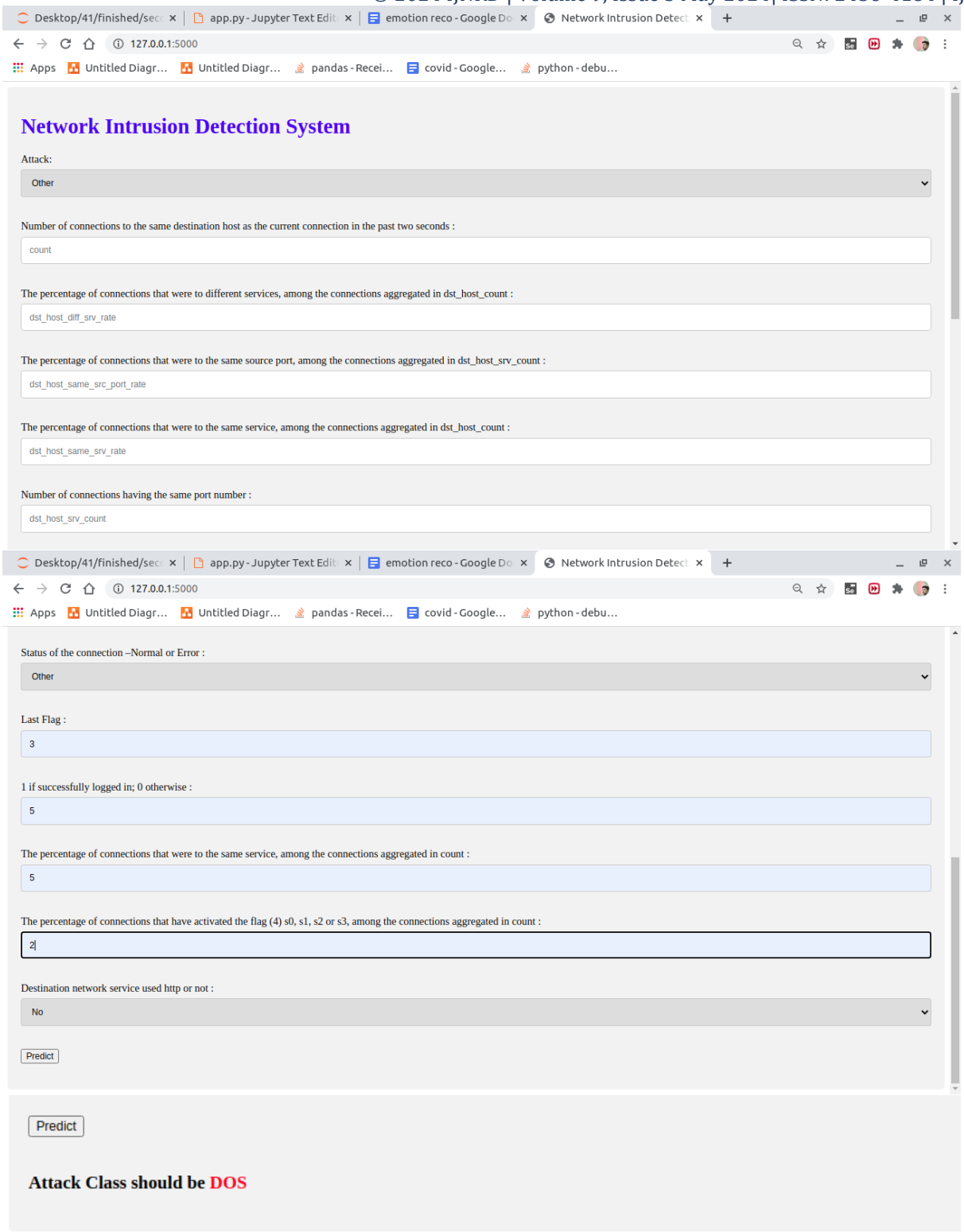

Fig - 2: Detection of Attack

V. CONCLUSION

In conclusion, our proposed cyber attack detection system represents a significant advancement in the field of cybersecurity, offering a comprehensive and adaptive approach to safeguarding network infrastructures against evolving threats. By combining the strengths of graph-based analysis and dynamic programming, we

contribute to the ongoing efforts to fortify cyber defense strategies and mitigate the risks posed by malicious actors in today's digital age.

REFERENCE

1.Raff, E., Sylvester, J., & Nicholas, C. (2015)[1]. Malware detection by eating a whole exe. In Proceedings of the 2015 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 365-380). IEEE.

2.Kim, H., Park, H., & Kim, K. (2016)[2]. Deep learning for network intrusion detection: An overview. In 2016 International Conference on Platform Technology and Service (PlatCon) (pp. 1-5). IEEE.

3.Skopik, F., Schauer, S., & Dustdar, S. (2016)[3]. A survey on security and privacy in big data environments. ACM Computing Surveys (CSUR), 49(1), 1-36.

4.Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. D. (2011)[4]. Adversarial machine learning. In Proceedings of the 4th ACM workshop on Security and artificial intelligence (pp. 43-58).

5. R Jegadeesan,A. Beno,S. P. Manikandan,D. S. Naga Malleswara Rao,Bharath Kumar Narukullapati,5T. RajeshKumar,Batyrkhan Omarov,Areda Batu, “Stable Route Selection for Adaptive Packet Transmission in 5G-BasedMobile Communications”, “Wireless Communications and Mobile Computing 2022 ”Research Article | OpenAccess Volume 2022 | Article ID 8009105 | https://doi.org/10.1155/2022/8009105.

6 M. Akshitha, R Jegadeesan, G. Akshaya, P. Akhilac, M.Pavan Kalyan, G.Sindhusha, 2021 & June, “Covid-19Future Forecasting Using Supervised Machine Learning Models”, Zeichen Journal, Volume 7, Issue 6, Page No.257-269, ISSN No: 0932-4747. DOI:15.10089.ZJ.2021.V7I6.285311.2425 (UGC Care Group II Journal)

7 PerukaPriyavarshini, R Jegadeesan, Thatla Vaishnavi, KampellySahithi, Boga Shivani, P.Balakishan, 2021 &June, “Cyber Money Laundering Detection Using Machine Learning”, Zeichen Journal, Volume 7, Issue 6, 2021,Page No.231-238,ISSN No: 0932-4747. DOI:15.10089.ZJ.2021.V7I6.285311.2422 (UGC Care Group II Journal)

8 R Jegadeesan, Dava Srinivas, N Umapathi, G Karthick, N Venkateswaran “Personal Healthcare Chatbot ForMedical Suggestions Using Artificial Intelligence And Machine Learning”, European Chemical Bulletin, Eur.Chem. Bull. 2023, 12 (S3), 6004 – 6012, DOI: 10.31838/ecb/2023.12.s3.670. (Scopus)

9 Islam, S. H., & Karray, F. (2018)[5]. Cybersecurity in the age of big data: A literature review. IEEE Access, 6, 16509-16533.