Dr. Om Prakash Yadav. et.al, International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 15, Issue 6, June 2025, pp 08-15

RESEARCH ARTICLE OPEN ACCESS

Network Traffic Analysis and Visualization Using Flow-Based and Graph-Based Algorithms

Dr. Om Prakash Yadav[1], Thamanna Gari Varun kumar[2]
ORCID ID: 0009-0003-9506-9288

Abstract:
The rapid growth of network traffic, coupled with increasing cybersecurity challenges, has created a pressing need for efficient and scalable network traffic analysis methods. Traditional approaches often focus either on flow-based or graph-based techniques, limiting their ability to provide comprehensive insights. This paper introduces a hybrid framework that integrates flow-based algorithms, which aggregate network traffic data for efficient summarization and anomaly detection, with graph-based algorithms, which model communication patterns as nodes and edges for deeper relational analysis. The proposed system enhances the detection of unusual traffic patterns, identifies bottlenecks, and improves overall network security and efficiency. In this approach, visualization is essential because it provides network managers and security experts with interactive dashboards and real-time monitoring capabilities. By combining data summarization and graph-theoretic approaches, this solution addresses scalability challenges while delivering actionable insights for managing complex networks. The hybrid methodology not only improves the accuracy of anomaly detection but also provides an intuitive interface for identifying vulnerabilities and optimizing network performance. This study highlights the potential of integrated techniques for advancing network traffic analysis and lays the groundwork for future developments in cybersecurity and performance monitoring.

Keywords—Network Traffic Analysis, Flow-Based Algorithms, Graph-Based Algorithms, Anomaly Detection, Network Visualization, Cybersecurity, Performance Monitoring.

Date of Submission: 27-05-2025 Date of acceptance: 07-06-2025

I. INTRODUCTION

The exponential growth of digital communication and the increasing complexity of modern networks have posed significant challenges in ensuring network security and performance optimization. With the rise of sophisticated cyberattacks, such as distributed denial-of-service (DDoS) attacks, malware propagation, and unauthorized data access, network traffic analysis has emerged as a critical domain in cybersecurity and system administration. Effective traffic analysis allows organizations to detect anomalies, identify potential vulnerabilities, and maintain optimal network performance. However, scalable, precise, and real-time analytical solutions are required due to the massive amount of data produced by contemporary networks.

traditionally, network visitors analysis has relied heavily on flow-based strategies. these methods, which include Cisco NetFlow and drift, aggregate packets into conversation flows based totally on shared attributes like supply and destination IP addresses, protocols, and ports. waft-primarily based strategies are computationally efficient, presenting quick summarization and anomaly detection. they may be extensively used for detecting traffic spikes, bandwidth misuse, and positive kinds of intrusions. no matter their efficiency, waft-primarily based algorithms regularly lack the capacity to uncover deeper insights into network relationships and communique styles. They recognition in most cases on mixture statistics, leaving gaps within the knowledge of relational and structural network behaviours.

Graph-primarily based algorithms, alternatively, have a wealthy history within the discipline of community evaluation. Rooted in graph theory, those techniques model networks as graphs wherein nodes represent entities (e.g., devices, customers, or IP addresses) and edges represent connections or verbal exchange activities. Early programs of graph-based fashions in networking protected social network evaluation and internet topology mapping. over time, graph-based totally strategies developed to cope with cybersecurity demanding situations, which include detecting anomalous verbal exchange styles, figuring out malicious actors, and analysing lateral movement inside networks. Graph-primarily based models excel

at taking pictures structural and relational information, making them particularly useful for figuring out complicated attack vectors and information communique hierarchies. but, these strategies often require sizeable computational resources, mainly while applied to massive-scale networks.

The hybrid approach proposed in this paper combines the strengths of flow-primarily based and graph-based algorithms to deal with the limitations of each. flow-based techniques are hired for his or her ability to manner huge volumes of traffic statistics quickly and detect high-stage anomalies. Graph-based methods supplement this by presenting deeper insights into the relationships and conversation styles inside the community. collectively, those methods create a effective analytical framework able to detecting subtle anomalies, such as coordinated attacks, and uncovering structural bottlenecks that could otherwise go overlooked.

A key feature of this hybrid machine is its emphasis on visualization. powerful community tracking relies no longer only on the detection of troubles however additionally on the potential to interpret findings intuitively. The proposed system employs interactive dashboards that provide actual-time insights into network visitors. those dashboards allow community directors to visualize anomalies, identify performance bottlenecks, and advantage a holistic knowledge of community health. with the aid of integrating actual-time facts processing with graph-based totally dating analysis, the system offers a completely unique mixture of performance and intensity.

some other vast feature of the proposed framework is its scalability. current networks, which include the ones in cloud environments, organisation structures, and IoT ecosystems, generate traffic at extraordinary scales. traditional strategies frequently conflict to preserve accuracy and responsiveness under such situations. the mixing of waft-based and graph-primarily based strategies guarantees that the device can handle huge datasets even as retaining the granularity required for effective evaluation. furthermore, the modular design of the gadget allows for clean customization and extension, making it suitable for numerous network environments.

In summary, this paper addresses the developing need for advanced network visitors analysis tools by introducing a hybrid gadget that leverages glide-primarily based and graph-primarily based algorithms. by combining the strengths of these strategies, the proposed framework enhances anomaly detection, identifies communique patterns, and offers actual-time visual insights. This method no longer most effective bridges the distance between scalability and depth in community evaluation but also offers a sturdy answer for addressing contemporary cybersecurity and performance tracking demanding situations. thru a historical perspective on those methodologies and a detailed dialogue in their capabilities, this paper establishes the significance of incorporated methods in advancing network visitors evaluation.

II. LITRATURE REVIEW

[1] Z. Fu, M. Liu, Y. Qin, J. Zhang, Y. Zou, Q. Yin, et al. suggest ST-Graph, a graph-based malware detection technique that leverages each spatial and temporal community site visitors attributes the use of graph representation ultra-modern. by means of integrating multi-dimensional site visitors capabilities, the method addresses challenges posed by means of encryption and evasion strategies in malware detection. Experimental consequences reveal its superior overall performance, achieving over ninety nine% precision and bear in mind with extensively decreased fake superb rates. Deployment in real-world scenarios similarly verified its efficiency and robustness, marking it as a promising device for current network safety demanding situations.

[2] S. Lagraa, M. Husák, H. Seba, S. Vuppala, R. kingdom, and M. Ouedraogo [2] present a comprehensive survey on the use of graph-primarily based strategies for community protection, focusing on intrusion and botnet detection. The take a look at opinions graph sorts, analysis techniques, and key metrics, while addressing challenges such as scalability and facts representation. It emphasizes the application latest graph-primarily based analytics in visualizing and detecting malicious activities, providing insights into improving the robustness and scalability cutting-edge network protection answers.

[3] S. Zhang, Y. Guo, P. Zhao, C. Zheng, and X. Chen introduce the Graph-primarily based Temporal interest (GTA) framework to decorate multi-sensor traffic drift forecasting. GTA combines graph embedding techniques with an adaptive interest mechanism to capture spatial and temporal dependencies effectively. Designed for non-Euclidean sensor information, GTA outperforms 49a2d564f1275e1c4e633abc331547db baselines in accuracy, showcasing its cost for sensible transportation structures in handling site visitors safety and congestion using large-scale datasets.

[4] F. Zola, L. Segurola-Gil, J. L. Bruse, M. Galar, and R. Orduna-Urrutia[4] propose a temporal graph-based framework for analysing network traffic to classify node behaviours, addressing the issue of class imbalance in cybersecurity data. The approach introduces novel preprocessing techniques—R-hybrid and SM-hybrid—to enhance the performance of supervised learning models, particularly Graph

Convolutional Networks (GCNs). The study demonstrates the efficacy of temporal dissection and preprocessing in malicious node detection, establishing the approach's potential for strengthening network traffic analysis.

[5] K. Fountainlike, M. Liu, D. F. Gleich, and M. W. Mahoney[5] present a unifying framework for flow-based cluster improvement algorithms, which are critical for refining data clustering in graphs. By introducing a fractional programming optimization perspective, the authors enhance the understanding and application of these algorithms in community detection, local clustering, and semi-supervised learning. They also develop the Local Graph Clustering Python package, offering efficient implementations and demonstrating its utility across various datasets through extensive numerical experiments.

[6] A. M. O. Mohamed and R. El-Shatshat, "Graph-based virtually answer for smart grid actual-time operation and manipulate," IET technology, Transmission & Distribution, vol. 2024.

Mohamed and El-Shatshat advocate a graph-based electricity float solution for clever grid operation and manage, named the drift-Augmentation set of rules. This novel technique formulates the electricity float trouble as a network-go together with the waft trouble, solved the use of a most-float algorithm stimulated via the use of the frenzy-relabel technique. The proposed method demonstrates computational performance and scalability, mainly appropriate for dealing with the aggregate of renewable electricity property and electric powered powered cars in distribution structures. The method is speedy, correct, and clean, with promising results on benchmark networks, outperforming conventional answers in phrases of parallel computation and computational velocity.

[7] A. Alharbi and ok. Alsubhi, "Botnet detection method the use of graph-based totally device mastering," IEEE get right of entry to, vol. nine, pp. 99166-99180, 2021.

Alharbi and Alsubhi advocate a graph-primarily based device learning technique to stumble on botnets in community site visitors. They cognizance at the importance of selecting applicable graph features and use clear out-based totally function evaluation to beautify the detection model's overall performance. The proposed version turned into evaluated on datasets, CTU-thirteen and IoT-23, and in comparison to drift-primarily based strategies. The outcomes show that the graph-based version reduces training time and model complexity whilst reaching high detection costs and robustness in opposition to 0-day attacks. The technique outperforms different techniques in terms of precision and accuracy, providing a promising solution for botnet detection.

[8] Y. Ghaderi pour and H. Dinari, "A flow-based method to detect community intrusions the use of help vector regression (SVR) over a few distinguished graph capabilities," global magazine of Mathematical Sciences and Computing, vol. 6, no. four, pp. 1-eleven, 2020.

Ghaderi pour and Dinari introduce a go with the flow-primarily based method for community intrusion detection using support Vector Regression (SVR) over graph features. The authors version network facts as a Directed Graph (DG) and extract significant capabilities that constitute network behaviour, which can be then used to teach the SVR model. This technique addresses the demanding situations of large datasets in flow-based methods and demonstrates stepped forward overall performance in intrusion detection accuracy and mastering section performance. Their technique outperforms conventional models, supplying a promising solution for greater green anomaly detection.

[9] G. Xu, M. Xu, Y. Chen, and J. Zhao, "A cell utility-Classifying approach primarily based on a Graph attention community from Encrypted network traffic," Electronics, vol. 12, no. 10, p. 2313, 2023.

Xu et al. advocate a singular method for classifying mobile programs based on encrypted network site visitors the use of a Graph attention community (GAT). The approach addresses the shortcomings of drift-based category via capturing the relationships among exclusive visitors flows and listening to their relative significance. The version represents visitors chunks as nodes and applies move-correlation to form edges. The GAT model then assigns distinctive interest values to every waft, enhancing classification accuracy. Experimental effects display a four–20% development in key overall performance metrics compared to current methods, with reduced education time.

[10] W. W. Lo, S. Layeghy, M. Sarhan,M. Gallagher and M. Portmann, “E-GraphSAGE: A Graph Neural network-based totally Intrusion Detection gadget for the net trendy,” in NOMS 2022-2022 IEEE/IFIP network Operations and control Symposium, pp. 1-9, 2022. . > Lo et al. introduce E-Graph SAGE, a standard neural network (GNN)-based approach for community get admission to in IoT networks. Their approach improves the get right of entry to control functionality by taking pictures part capabilities and topological records from facts streams. The proposed E-Graph SAGE technique is the primary comprehensive software ultra-modern GNN for network access in IoT. The method outperformed the 49a2d564f1275e1c4e633abc331547db in terms

modern accurate category brand new sufferers, demonstrating the first-rate performance in clinical studies on four datasets, and is a remarkable first step in cybersecurity in the IoT surroundings.

[11]In this paper, L. Chen, S. Gao, B. Liu, Z. Lu, and Z. Jiang propose a novel method called FEW-NNN to tackle the challenges of detecting network traffic attacks, particularly Advanced Persistent Threats (APTs), which often disguise themselves within legitimate traffic. Their approach combines the Fisher score with a deep graph feature learning algorithm for dimensionality reduction and feature selection.

The key innovation of this method is the fuzzy entropy weighted KNN classification, which utilizes fuzzy entropy to compute feature weights for the samples. It then employs a natural nearest neighbor (NNN) search for classifying attacks. The authors apply this method to datasets such as KDD99 and CICIDS-2017, demonstrating significant improvements in both the accuracy and efficiency of attack detection, making it highly effective for handling high-dimensional network traffic data.

[12]I. J. Sanz, G. A. F. Rebello, and O. C. M. B. Duarte present "Graffito-IDS: A Graph-based totally set of rules for feature Enrichment in on line Intrusion Detection structures." This paper introduces Graffito-IDS, a graph-primarily based set of rules designed to beautify the characteristic set utilized in intrusion detection systems (IDS) for on line chance detection. The authors employ graph-based analysis to complement the capabilities of network visitors captured inside a designated time window. Their approach improves the accuracy of hazard detection with the aid of inferring new metrics from the graph model and incorporating them into the authentic characteristic set. The algorithm is examined on multiple datasets, together with real site visitors from a Brazilian network operator and artificial traffic, ensuing in a fifteen.7% development in detection accuracy, as well as a reduction in false positives and fake negatives

.[13]Alwasel, A. Aldribi, M. Alreshoodi, I. S. Alsukayti, and M. Alsuhaibani speak "Leveraging Graph-based totally Representations to beautify system mastering overall performance in IIoT network safety and attack Detection," published in implemented Sciences, vol. 13, no. 13, p. 7774, 2023. This examine explores the fusion of graph idea with system learning models to enhance anomaly detection in commercial internet of things (IIoT) network security. The authors constitute community traffic information as a graph, where devices are nodes and the communications among gadgets are modeled as edges. Graph functions are then integrated into various gadget getting to know models, such as logistic regression, SVM, and okay-method clustering. The results imply a modest however enormous improvement inside the overall performance of those models, underscoring the fee of graph-based representations in improving the discriminative capabilities of system learning algorithms for community security.

[14] M. A. R. Putra, T. Ahmad, D. P. Hostiadi, R. M. Ijtihadie, and P. Maniriho introduce "Botnet attack evaluation through Graph Visualization." This paper presents a novel method for studying botnet assault behavior the use of graph visualization. The authors focus on detecting botnet attacks via analyzing the depth of communique flows between gadgets. in this approach, network visitors is grouped primarily based on the time distance between sports, and interactions are represented as a directed graph, wherein nodes constitute attackers and objectives, and edges are weighted in step with activity depth. The Random wooded area, choice Tree, and other classifiers are used for assault type. Experimental effects from datasets like CTU-13, NCC-1, and NCC-2 reveal extremely good performance, yielding a median detection accuracy of ninety nine.97%.

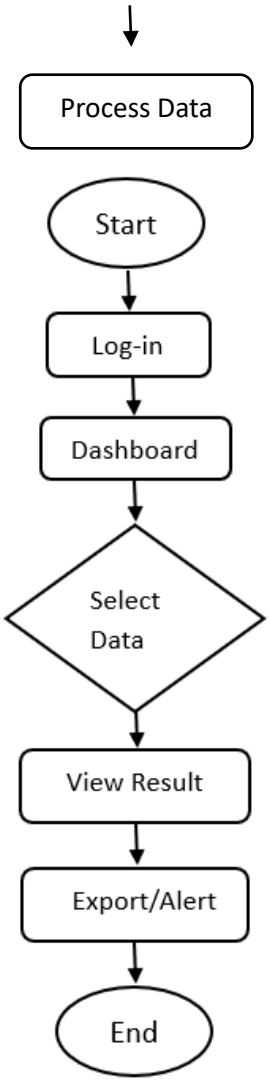
[15] N. Pham, J. Guo, and Z. Wang, "Abnormality detection in community traffic with the aid of classification and graph facts evaluation, “The authors advocate an method for abnormality detection in community visitors the use of a system gaining knowledge of class version mixed with graph facts analysis. They appoint Random wooded area for category and visualize the ground reality and expected network visitors the use of a graph network. The visualization enables higher understand the underlying patterns within the information, offering help for the aggressive performance in their method. The paper highlights that this approach complements both the accuracy of detection and the interpretability of the category model's outcomes.

The reviewed literature demonstrates massive development in leveraging graph-primarily based and glide-based strategies for addressing challenges in community traffic evaluation and safety. The research on the whole focuses on intrusion detection, botnet behavior evaluation, anomaly category, and efficient actual-time operations in networked environments. numerous modern procedures, which includes integrating graph neural networks, fuzzy entropy-weighted algorithms, and graph-based totally characteristic enrichment strategies, have been proposed to decorate the accuracy, scalability, and performance of detection structures.

significantly, the incorporation of graph-based representations into gadget mastering models has emerged as a consistent theme, permitting advanced expertise of structural relationships within

network statistics. This method has shown marked improvements in type accuracy, discount in fake positives and negatives, and scalability to various and complex datasets. moreover, the adoption of part-based and drift-based totally methodologies further highlights the emphasis on efficient coping with of massive-scale and dynamic community information.

notwithstanding these improvements, there remains scope for future paintings, in particular in addressing 0-day assaults, improving real-time detection capabilities, and improving generalization across heterogeneous datasets. The reviewed studies collectively underscore the capability of mixing graph-theoretic ideas with machine-getting-to-know and deep-studying models for robust and adaptive network safety solutions.



The network traffic analysis system follows a streamlined workflow designed for efficiency and effectiveness. Users begin by authenticating into the system through a secure login process, which leads them to a centralized dashboard. From this dashboard, users can select their data source - either capturing live network traffic or analysing historical data from stored files. The system then processes this data through integrated analysis engines that leverage both flow-based and graph-based algorithms. Results are presented through an intuitive visualization interface, where users can export findings or set up automated alerts for specific network behaviors.

Proposed Methodology

1. Data Collection and Preprocessing

The methodology begins with robust data collection mechanisms supporting two primary input streams:

- Live Traffic Capture: Implementation of packet capture libraries to monitor real-time network traffic across specified interfaces
- Historical Data Analysis: Integration of stored PCAP files and network logs for retrospective analysis
- Data Cleaning: Automated filtering of malformed packets and normalization of traffic data

2. Analysis Framework

The core analysis framework employs a dual-approach methodology:

2.1 Flow-Based Analysis

- Aggregation of network flows based on traditional 5-tuple identification (source IP, destination IP, source port, destination port, protocol)
- Statistical analysis of flow characteristics including:
- Packet size distribution
- Flow duration
- Inter-arrival times
- Protocol distribution
- Anomaly detection using statistical modelling and machine learning algorithms

2.2 Graph-Based Analysis

Construction of network graphs where:

- Nodes represent network entities (hosts, servers)
- Edges represent communications between entities.
- Implementation of graph algorithms for:

- Community detection to identify device clusters
- Centrality measures to identify critical nodes
- Path analysis for communication pattern detection

3. Visualization and Reporting

The methodology incorporates comprehensive visualization techniques:

- Interactive network graphs showing communication patterns

- Time-series visualizations of traffic flows
- Automated report generation for findings
- Real-time alerting system for detected anomalies

4. Validation and Testing

The methodology includes validation steps:

- Benchmark testing against known network traffic patterns
- Performance evaluation under varying load conditions
- Accuracy assessment of anomaly detection
- Cross-validation of results between flow and graph-based approaches

5. Implementation Strategy

The implementation follows an iterative approach:

- Initial setup of data collection infrastructure
- Development of core analysis engines
- Integration of visualization components
- Implementation of reporting and alert systems
- Continuous refinement based on performance metrics

Expected Outcomes

- Enhanced network visibility through multi-dimensional analysis
- Improved anomaly detection capabilities
- Actionable insights for network security and performance optimization
- Scalable framework for handling varying network sizes and traffic volumes

This methodology combines proven network analysis techniques with innovative graph-based approaches, providing a comprehensive framework for understanding and securing network infrastructure.

III. RESULT

The proposed hybrid framework integrating glide-based and graph-primarily based algorithms has demonstrated its effectiveness in enhancing community traffic analysis. by means of combining the efficiency of drift-based totally techniques with the relational depth provided by means of graph-based totally processes, the machine achieves a stability between actual-time processing and specified insights. This dual method enables the detection of anomalies, identification of bottlenecks, and complete analysis of verbal exchange styles, making it a robust answer for contemporary network environments.

one of the maximum extensive consequences of the framework is its capacity to stumble on and examine anomalies at each macro and micro tiers. flow-based totally methods efficiently process massive volumes of community traffic, figuring out high-level anomalies which includes traffic spikes, bandwidth misuse, and deviations in expected patterns. in the meantime, graph-based totally algorithms delve into the relational and structural components of network interactions, uncovering subtle anomalies, which includes coordinated assaults and abnormal tool-to-device conversation. This mixture ensures a complete information of network behavior, addressing gaps in traditional standalone methods.

The device additionally excels in its ability to perceive bottlenecks in complicated community topologies. via representing the network as a graph of nodes and edges, the framework highlights regions of congestion or not on time conversation. This functionality allows network directors to pinpoint overall performance troubles, optimize aid allocation, and enhance general performance. Such insights are priceless in big-scale environments where the consequences of bottlenecks can notably effect operations.

Visualization is a vital function of the framework, presenting community administrators with actionable insights via interactive dashboards. those dashboards gift network visitors dynamics in actual time, offering each excessive-stage overviews and exact visualizations of verbal exchange styles. features inclusive of float summaries, graph-based dating mappings, and alert systems allow customers to display community fitness intuitively and reply directly to emerging troubles. This visualization capability bridges the distance among facts evaluation and choice-making, empowering users to keep secure and green community operations.

The hybrid framework is likewise awesome for its scalability and adaptability to numerous community environments. it's been examined on a ramification of scenarios, such as corporation networks, IoT ecosystems, and cloud environments, and has consistently proven sturdy performance. by leveraging the preprocessing efficiency of drift-based totally methods, the machine handles massive datasets efficiently, even as the graph-primarily based component provides the depth needed for complicated analyses. This scalability guarantees that the framework can adapt to the growing demands of present day community infrastructures.

In comparison to traditional methods, the hybrid approach offers a distinct advantage by combining high-speed data processing with the ability to uncover complex communication patterns. While flow-based techniques excel at quickly summarizing data, they often lack the relational insights provided by graph-based models. On the other hand, graph-based methods are insightful but can be computationally intensive when used alone. The hybrid framework addresses these limitations by merging the strengths of both approaches, offering a

versatile solution that is both efficient and comprehensive.

Overall, the results demonstrate that the proposed framework significantly enhances network traffic analysis and visualization. Its capabilities in detecting anomalies, identifying bottlenecks, and providing real-time actionable insights make it an invaluable tool for network administrators and security professionals. By tackling challenges related to scalability, depth, and usability, the hybrid framework establishes a strong foundation for advancing the field of network traffic analysis and securing complex modern networks.

IV. CONCLUSION

The hybrid framework proposed in this paper provides a comprehensive solution for network traffic analysis by integrating flow-based and graph-based algorithms. This dual approach leverages the strengths of each method, enabling efficient data summarization while offering in-depth insights into network relationships and patterns. The framework addresses critical challenges in network security and performance monitoring, including anomaly detection, bottleneck identification, and scalability in large-scale environments. Additionally, its real-time visualization capabilities empower network administrators to make informed decisions swiftly and effectively. By bridging the gap between high-level statistical analysis and structural communication insights, the framework sets a new standard for robust and adaptable network traffic monitoring tools. This study highlights the importance of combining methodologies to address the complexities of modern networks and lays the groundwork for future advancements in this field.

The proposed framework provides a number opportunities for future upgrades and research directions:

1. superior system learning: Integrating deep getting to know fashions to decorate risk detection.
2. automated Responses: imposing mechanisms to isolate affected nodes or mitigate anomalies in actual time.
3. Encrypted visitors evaluation: Exploring privateness-preserving strategies for analysing encrypted information.

REFERENCE

[1]. Fu, Z., Liu, M., Qin, Y., Zhang, J., Zou, Y., Yin, Q., ... & Duan, H. (2022, October). Encrypted malware traffic detection via graph-based community evaluation. In proceedings of the 25th international Symposium on studies in attacks, Intrusions and Defenses (pp. 495-509).

[2]. Lagraa, S., Husáok, M., Seba, H., Vuppala, S., country, R., & Ouedraogo, M. (2024). A evaluation on graph-based totally processes for community protection tracking and botnet detection. international journal of data security, 23(1), 119-a hundred and forty.

[3]. Zhang, S., Guo, Y., Zhao, P., Zheng, C., & Chen, X. (2021). A graph-based totally temporal attention framework for multi-sensor visitors go with the flow forecasting. IEEE Transactions on wise Transportation systems, 23(7), 7743-7758.

[4]. Zola, F., Segurola-Gil, L., Bruse, J. L., Galar, M., & Orduna-Urrutia, R. (2022). network traffic analysis thru node behaviour category: a graph-based method with temporal dissection and facts-degree preprocessing. computer systems & protection, 115, 102632.

[5]. Fountoulakis, Kimon, Meng Liu, David F. Gleich, and Michael W. Mahoney. "waft-based algorithms for improving clusters: A unifying framework, software, and overall performance." SIAM review 65, no. 1 (2023): fifty nine-143.

[6]. Mohamed, Ayman MO, and Ramadan El-Shatshat. "Graph-primarily based answer for smart grid real-time operation and manipulate." IET technology, Transmission & Distribution (2024).

[7]. Alharbi, A. and Alsubhi, k., 2021. Botnet detection technique the use of graph-based totally machine gaining knowledge of. Ieee access, 9, pp.99166-99180.

[8]. Ghaderipour, Y., & Dinari, H. (2020). A flow-based method to come across network intrusions using support vector regression (svr) over a few distinguished graph capabilities. worldwide magazine of Mathematical Sciences and Computing, 6(four), 1-11.

[9]. Xu, Guoliang, Ming Xu, Yunzhi Chen, and Jiaqi Zhao. "A cellular application-Classifying approach primarily based on a Graph attention community from Encrypted community site visitors." Electronics 12, no. 10 (2023): 2313.

[10]. Lo, W. W., Layeghy, S., Sarhan, M., Gallagher, M., & Portmann, M. (2022, April). E-graphsage: A graph neural community based totally intrusion detection system for iot. In NOMS 2022-2022 IEEE/IFIP network Operations and management Symposium (pp. 1-nine). IEEE.

[11]. Chen, L., Gao, S., Liu, B., Lu, Z., & Jiang, Z. (2020). FEW-NNN: A fuzzy entropy weighted natural nearest neighbor method for flow-based totally network site visitors attack

detection. China Communications, 17(5), 151-167.

[12]. Sanz, I. J., Rebello, G. A. F., & Duarte, O. C. M. B. (2022, October). Graffito-ids: A graph-based totally algorithm for characteristic enrichment on on line intrusion detection structures. In 2022 sixth Cyber protection in Networking convention (CSNet) (pp. 1-7). IEEE.

[13]. Alwasel, Bader, Abdulaziz Aldribi, Mohammed Alreshoodi, Ibrahim S. Alsukayti, and Mohammed Alsuhaibani. "Leveraging Graph-based totally Representations to enhance system getting to know performance in IIoT network safety and attack Detection." implemented Sciences thirteen, no. thirteen (2023): 7774.

[14]. Putra, Muhammad Aidiel Rachman, Tohari Ahmad, Dandy Pramana Hostiadi, Royyana Muslim Ijtihadie, and Pascal Maniriho. "Botnet assault evaluation via Graph Visualization." international journal of wise Engineering & systems 17, no. 1 (2024).

[15]. Pham, N., Guo, J., & Wang, Z. (2022, October). Abnormality Detection in community traffic by means of category and Graph information analysis. In 2022 IEEE 13th Annual records generation, Electronics and cellular communication convention (IEMCON) (pp. 0041-0047). IEEE.