Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Graph Neural Network-Based Intrusion Detection: A Comprehensive Survey of Methods, Challenges, and Future Directions

Kuppam Havya Sree
Department of Information Science and Engineering
RV Institute of Technology and Management
Bengaluru, India

Eshwar Chowdary T
Department of Information Science and Engineering
RV Institute of Technology and Management
Bengaluru, India

P. T. Bhargavi
Department of Information Science and Engineering
RV Institute of Technology and Management
Bengaluru, India

Akash K. V.
Department of Information Science and Engineering
RV Institute of Technology and Management
Bengaluru, India

Prof. Avinash N. Rao
Department of Information Science and Engineering
RV Institute of Technology and Management
Bengaluru, India

***Abstract*—In recent years,graph-oriented neural networks have shown strong potential in improving intelligent security management system by collecting detailed connections in network traffic patterns. Conventional methods of intrusion detection commonly utilize independent feature analysis, constraining their capacity to describe dynamic and structured interactions found in the current networks, particularly in internet of things and software-defined settings. A comprehensive analysis of graph-oriented neural networks for intelligent security management is presented in this paper. The survey considers different graph building algorithms and the graph neural network models, as well as their usage in different network contexts. Also, performance appraisal measures, benchmark data and issues of implementation are examined. The study focuses on analyzing and reviewing current strategies and improve areas lacking research in order to built an efficient real time intelligent security management with real time data.**

***Index Terms*—Intrusion Detection System (IDS), Graph Neural Networks (GNN), Network Security, Cybersecurity, Internet of Things (IoT), Graph Convolutional Network (GCN), Graph Attention Network (GAT), Anomaly Detection, Machine Learning, Deep Learning, Network Traffic Analysis, Real-Time Detection**

I. Introduction

Networks today are more complex as digital communication,cloud computing,and connected devices grow quickly.While these methods have improves data transfer and smart services,they are also introduced new security risks. Since attacks like malware injection,unauthorized access are getting more advanced,network security has become a key issue. Intrusion detection systems are important for watching network activity and spotting suspicious activities to keep systems and data secure.

Common intelligent security systems approaches include signature-based and anomaly-based methods.Signature-based systems depend on known attack patterns to find abnormal behavior,but the traditional systems fail to detect the abnormality in the system.Conversely, anomaly-based methods seek to identify deviations of normal behavior but can be highly false positive and lack contextual insights into behavioral patterns [10], [30]. These limitations highlight the need for more intelligent and adaptive detection mechanisms.

Over the past few years,automated learning techniques and neural network approaches helped to improve detection accuracy by learning the patterns from the dataset.However,most methods analyze traffic individually instead of finding the patterns betweens the data. In practice, the network traffic inherently creates complex structures with the nodes representing the devices or users and the edges representing the communication channels. It is necessary to capture these relationships to point out correctly coordinated and multi-stage attacks with accuracy [5], [8].

Graph-based methods are used in intrusion detection to overcome this limitation.By representing network traffic as graphs,we can study both individual features and the relationships between different entities. Graph learning models are

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

useful for analyzing graph-based information. These models combine information from nearby nodes,helping them learn both local and overall patterns in network.This feature makes it easier to find complex attacks that older methods struggle to detect.

Advanced graph-based neural methods,including graph convolutional and graph-attention networks,are widely applied in cybersecurity detection systems. They have been used in various areas like internet of things networks, software-defined networks and industrial systems, showing better accuracy and reliability. Moreover, recent works have also involved more sophisticated methods like dynamical graph modeling, heterogeneous graph representations and attention mechanisms to further improve detection abilities in dynamic network settings [9], [20], [32].

Although these have been improved, there still are some challenges. A significant portion of the existing works are concerned with particular models or datasets, and end-to-end system design is not a consideration. Scalability to large-scale networks, real-time processing needs, data imbalance, and unstandardized evaluation measures remain a challenge to real-world implementations. Moreover, the combination of these models and real-world systems and hardware platforms is an open research question [8], [17].

Hence, it is important to conduct a well-organized survey that connects various research works.This paper provides a detailed review on intrusion detection systems based on graph-based neural networks,converging graph creation,model architecture, datasets, and evaluation.The survey identifies current challenges and points out future research areas.Its goal is to offer a clear insight to help build scalable,efficient,and real-time intrusion detection systems that meet modern cybersecurity needs and requirements in practical way.

II. Background and Motivation

The rise of connected systems,cloud computing,and the internet devices has made modern infrastructure more vulnerable to cyber attacks.With more complex and widespread networks,cyberattacks such as denial of service and unauthorized access are becoming more advanced. Conventional security systems tend to be inadequate to cope with these dynamic threats, and a huge demand exists to use smart and responsive intrusion detection systems [10], [30].

Rule-based and signature based intrusion detection systems are limited when dealing with unseen attacks.While automatic learning techniques have increased detection accuracy,most current methods fail to capture the connections between network entities. Real-world network traffic is structured and interconnected and, therefore, more sophisticated modeling methods are needed.

New techniques in intrusion detection have emerged in the recent developments in graph-based learning. Network traffic can be modeled as graphs to analyze feature information and relationships,where nodes represented as users or devices and edges are represented as connection between them. Graph neural networks have demonstrated high potential in this field, as they can learn such graph-structured data well and enhance the ability to detect complex and coordinated attacks, which are difficult to detect with other methods [7], [11].

The force behind this work is to fill in the gap between the extant research and actual implementation. Some studies demonstrate good results for graph-oriented neural intrusion detection models,but many models only focus on specific models rather than overall system. Issues like real-time processing, scaling, and integration with hardware or edge devices are yet to be thoroughly investigated. So,it is clear that we need to study existing methods carefully and work on building accurate,real time intrusion detection system which meets present cyber security needs.

III. Understanding Intrusion Detection Systems

These Systems are vital elements of an advanced cyber security infrastructure, which aims at tracking network traffic and detecting harmful actions or policy infractions. They analyze network traffic and system logs to find security issues,unauthorized access,and cyber security attacks.Based on their detection method,intrusion detection systems are classified as signature-based or anomaly-based.

Signature-based detection works by matching known attack patterns and is good at finding known suspicious attacks,but it cannot detect new attacks.Anomaly-based detection identifies unusual behavior in the network,making it useful for detecting new attacks.

As networks grow more complex because of internet of things and software-defined networks,older intrusion detection methods are less effective.Modern attacks are dynamic,distributed,and multi-stage,making them challenging to detect.

To solve these limitations,recent studies have explored advanced intelligent learning methods for intrusion detection. Specifically, the graph-based methods have become a focus of interest because they can model network traffic in terms of the interconnected structures. Graph neural networks allow analyzing both feature data and relationships among the entities of the network and enhancing the identification of sophisticated attack patterns [7], [11].

With the dynamic character of cyberthreats, real time and effective intrusion detection has gained significance. This has led to intelligent, scalable and adaptive detection systems that are capable of working well in contemporary network environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

IV. Graph-Based Network Representation and Features

The network traffic of modern computing environment may be naturally modeled as the form of structured and coupled system, in which the devices, users, or applications communicate with others via the communication links. Such interactions are well-modeled as graphs, with nodes being instances of network entities and edges being connecting or data flows between them. A representation like this is able to both describe the individual properties of objects and how they are interrelated, and can give a more detailed insight into network behavior [5], [8].

Graph based methods are effective for intrusion detection because many cyberattacks involve connections between systems,like coordinated or multi step attacks.Unlike traditional methods that treat data separately, graph based approaches capture relationships in the network,making it easier to detect complex attacks.

Graph based intrusion detection has improved a lot in recent years.Better feature engineering at node,edge and graph levels uses data like traffic patterns,connection frequency,packet details, and timing to find unusual behavior.Dynamic graph models also help track changes in network activity, making them useful in real world situations.

These graph based methods,along with improved learning models,make it easier to analyze complex network data. Graph neural network(GNN) learn from both nearby and overall connections, which helps detect malicious activities more accurately than traditional methods

However, there are still challenges such as high computation cost, scalability issues and difficulty efficient graphs. Handling large and real time data is also a problem and these issues must be solved for practical use.

V. Neural models for graph-based intrusion detection

Advanced graph learning models are widely implemented in intrusion detection because they can process connected data efficiently. Graph neural networks can be used to understand network behavior more fully, unlike the traditional learning methods where data is processed alone, data dependencies can be harnessed between network entities to give a better picture of how networks work together, as opposed to independently in the traditional methods of learning data [5], [8].

Network traffic can be represented as graph ,where nodes represent devices,users or processes and edges show communication or exchange data between them. Graph neural networks work with this structure by learning with nearby nodes using the aggregated information provided by them to enable the model to learn not only local interactions but also global trends in the network. This feature is especially beneficial in finding complex attack situations like coordinated attacks, lateral movements, and distributed threats [7], [11].

Intrusion detection In intrusion detection, a number of graph neural network architectures have been investigated. Spatial graph learning methods collects the information form closely related nodes,whereas attention-based prioritize neighboring nodes differently. Inductive learning methods like GraphSAGE allow the model to be extrapolated to network nodes it has never encountered as well as large-scale networks, and it is thus applicable in real-world scenarios as well as contexts with millions of nodes and edges [7], [15].

A key benefit of neural models for graph data is their ability to use graph structure and node features to improve detection performance. This results in a higher level of anomaly detection as opposed to traditional machine learning methods. Also, recent studies have examined the dynamic and heterogeneous graph models to represent time-varying and multi-type interaction within the systems of complex networks systems [9], [20].

Although promising, GNNs have a number of obstacles in application. The complexity (high computational) of them, scalability problems, and the necessity to provide efficient graph constructions may constrain their usage in real-time systems. Moreover, managing incompleteness or the noisy network data is an issue. It is necessary to address these issues to create strong and implementable intrusion detection systems relying on graph neural networks [8], [17].

In general, graph neural networks offer an effective model of intrusion detection as they are used to effectively model the relational nature of network traffic. Their capability to extract the structural and feature-based information make them a potential solution to next-generation cybersecurity systems.

VI. Neural Architectures for graph-based Intrusion Detection

Extending the graph-based model of network traffic to graph neural networks, the performance of intrusion detection systems significantly relies on the architecture of the network under consideration. Because of the complex relationships and the dynamic interactions of the network data, it is necessary to select the network data models that can illustrate the accurate capture of both the structural and feature-based data used in network data modeling [5], [8].

Various architectures of graph neural networks have been designed to overcome different obstacles of the graph-based learning as scalability, flexibility and dynamic data handling capabilities. There is a set of advantages of each architecture due to their own peculiarities in modeling the behavior of the network and detecting anomalies.

A. Graph Convolutional Networks

The most popular architecture that has been used in detection of intrusion on graphs is known as Graph Convolutional

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Networks. These models generalize the notion of convolution of grid-based data to a graph-structured data by summing up the adjacent nodes information [7].

Graph convolutional networks provide learning of local structural patterns by aggregating features of connected nodes in intrusion detection. This assists in determining suspicious business including closely related entities, like the abnormal device communication.

B. Graph learning with Attention Mechanisms

This method add attention machinery to give neighboring nodes varying weights of importance when aggregating information. Through this the model is able to emphasize more significant relationships and minimize the effects of less important or noisy relationships [11].

In intrusion detection,attention mechanisms helps in identifying advanced attack patterns by focusing on important network connections . This gives an enhanced detection accuracy, particularly in dynamic and heterogeneous networks.

C. GraphSAGE and Inductive Learning Models

GraphSAGE is an inductive learning method which allows the graph neural networks to extrapolate to unseen nodes and network structures which change over time. Rather, it samples and aggregates features within the neighborhood of a node, and is therefore applicable to large-scale and real-time applications, unlike the full graph of the graph with many nodes [15].

This method proves to be very handy within intrusion detection systems whereby new devices and links keep on emerging. GraphSAGE lets the system change to accommodate these changes even without retraining the whole model.

D. Dynamic and Heterogeneous Graph Models

Recent developments have been on dynamic and heterogeneous graph neural networks, to more accurately capture real-world network conditions. Dynamic graph models can model time-varying interactions,and these graphs can represent many kinds of nodes and edges together [9], [20].

These techniques improve capabilities of intrusion detectors to detect multi-stage and changing attacks typical to contemporary cybercrimes.

E. Challenges in GNN Architectures

Graph neural network architectures are exposed to a number of challenges even though they are effective. Their implementation in real time systems can be constrained by high computational complexity, memory needs and scaling.

Thus, it is necessary to optimize such architectures to be efficient, scalable and perform in real-time to enable real life intrusion detection applications.

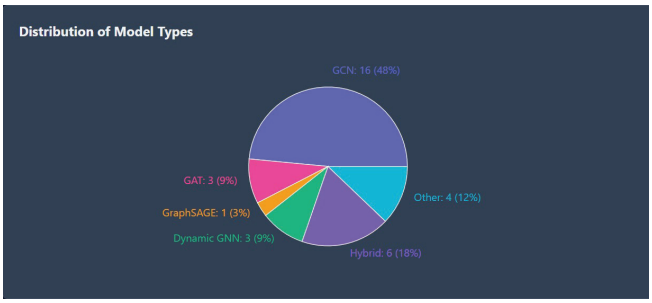

Fig. 1. Distribution of GNN model types used in intrusion detection studies

VII. Graph-Based Intrusion Detection Systems

Although an independent machine learning model can study particular characteristics of network traffic, intrusion detection in the real world is multi-layered and multi-interdependent patterns of communication. These systems model network traffic as connected graphs by applying smart methods to identify abnormal activities [5], [8].

These systems represent the network entities, which may be a device, user or application, as nodes and communication links as edges. Several characteristics such as network traffic, connection distribution, and time dynamics are used to create the picture of the entire network activity. Through this planned representation, the system is capable of building a relational behavior pattern of the network that can be studied to draw out anomalies and malicious operations.

The possibility to identify the complex interaction between network entities instead of analyzing features separately is one of the benefits that graph-based intrusion detection systems have. This makes it possible to detect better coordinated and multi-stage attacks which do not lend to easy detection by conventional methods. In addition, the system is molten with the capability of learning meaningful patterns and increased classification results through the integration of the graph neural networks [7], [11], [15].

These systems however also have a number of challenges. Graph representations of raw network data are complex to construct correctly and decipherably into easily scalable representations. Moreover, high computational cost, dynamic network behavior, and data imbalance are some of the issues that can impact performance of the system. Fluctuations in the network conditions and availability of noisy data also make consistent detection more difficult.

These challenges highlight the need for effective graph modeling methods and reliable learning methods to ensure stable and real-time performance of graph-based intrusion detection systems in real-world environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

VIII. Machine Learning Techniques in Intrusion Detection

After gathering network traffic information, data analysis and interpretation of the information collected are essential when it comes to successful intrusion detection. Network data can be extremely high-dimensional, dynamic as well as consists of intricate patterns which vary depending upon user behavior, traffic load and attacks techniques. Rule-based approaches are not effective for dealing with complex data,making advanced learning techniques necessary for pattern detection and abnormality detection [8], [30].

The relationships between malicious activities and network features can be modeled with the help of machine learning algorithms. These algorithms are able to work with labeled and unlabeled datasets to learn and determine network traffic and identify intrusions with greater accuracy.The use of advanced learning methods in intrusion detection systems has improved the detection of familiar and new attacks by supporting automatic and intelligent decision-making [5].

A. Classification Algorithms

Several intrusion detection systems are built on classification methods that identify normal and abnormal network behavior based on selected parameters

Similarity based classification methods are easy to implement on small datasets,while advanced separation models handle high-feature data efficiently and create reliable decision boundaries. Random forests and decision trees provide both interpretability and strength, which is why they are suitable to practical intrusion detection instruments.

In intrusion detection these algorithms consider features like packet size, duration of connection, type of protocol used and patterns of traffic to categorize network traffic. The major shortcoming however is that the models assume that the data are independent samples and do not provide a relationship amongst the entities in the network.

This shortcoming presents a critical lapsing research gap, in which classical machine learning models cannot be used to utilize structural and relational data. Consequently, they might perform poorly in the case of intricate and synchronized attacks.

B. Deep Learning Approaches

The deep learning approach has also led to the development of automatic extraction of features in raw network data that is used in intrusion detection. Different neural-based models,like neural networks are widely used in this fields [17], [30].

These neural models improves detection system by learning complex patterns between the data.RNNs are suitable for sequential network traffic,whereas CNNs specialize in spatial traffic analysis.

Even with these advantages, deep learning models still have some limitations.These models depend on large datasets and require significant computational resources,making them harder to implement in real-time situations.Another issue is that they don't fully capture relationships within network traffic.

Because of these limitations, Graph Neural Networks (GNNs) have gained attentions they extend deep learning to data that is structured as graphs.These models provide a more combined approach to intrusion detection by bringing together feature learning and structural understanding.Overall, machine learning and deep learning have significantly improved intrusion detection systems.

However, for better efficiency, scalability, and real-time performance it is important to combine models that can capture both feature-based and relationship-based information in network data.

IX. Challenges and Limitations

While graph-focused neural architectures have shown better performance in detecting the abnormality in the pattern there are still having issues that prevent wide real-world adoption. The complexity of network data, which is highly dynamic, large-scale, and perhaps noisy, is one of the main issues. Change in traffic levels, user activities, as well as network conditions have the potential to influence model performance and cause inconsistencies in the accuracy of detection, [8], [17].

The one more major issue is the graph construction. The process of converting raw network traffic to a suitable graphical representation is non-trivial, which involves the selection of the nodes, edges, and features. Bad design of the graphs may cause the loss of important information or irrelevant relationships, which may adversely affect model performance. As well, large networks give rise to large graphs, imposing high computing and memory expenses.

Another important significant drawback is, that can arise in a system based on graph-based neural networks is scalability. many models in use are computationally expensive and they can hardly handle real time network traffic. This restricts their usefulness in fast networks and resource-constrained systems like edge devices and embedded systems.

On a system-level, the literature available today concentrates on the development of models and their evaluation based on benchmark datasets without taking into account the problem of their real-world deployment. The concern of integrating with the hardware systems, real-time data processing and continuous learning is not considered, creating the difference between the theoretical performance, on one hand, and the practical implementation, on the other hand.

Moreover, high-quality labeled datasets have not yet been available. Network datasets tend to have class imbalance,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

incomplete labeling and lack diversity, which influence the generalization of machine learning models. This may result in poor performance when it is implemented in unknown conditions [5], [9].

The challenges underscore the necessity of creating fast, scalable and dynamic intrusion detection systems that integrate effective graph models with practical systems deployment factors.

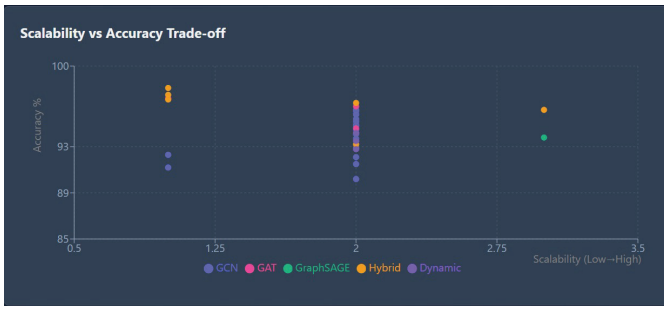

Fig. 2. Scalability–accuracy trade-off in GNN models

X. Recent Advancements

Recent developments in intrusion detection have enhanced considerably the efficiency of a graph-based method of learning in cybersecurity. The introduction of sophisticated Bidirectional graph neural network systems including attention-based and heterogeneous graph models is one of the most relevant ones, as it advances the capability to depict intricate interrelations within network traffic [7], [20].

Combining graph-focused neural methods with predictive learning methods has helped in achieving better detection performance. Graph-based networks and feature-based approaches to learn and identify known and unknown attacks can be accurately determined using graph-based models and hybrid models. Specifically, attention mechanism and dynamic graph modeling has shown enhanced potential to detect evolving and multi-stage cyberthreat in an improved manner. [9], [11], [32].

One thing that has changed recently is how graph neural networks are being used across different are as such as IoT networks, software-defined networks, and even industrial systems.This gives an idea of how flexible these graph-based intrusion detection systems can be since they are able to work across different types of network environments. At the same time, a lot of recent work has focused on making these systems faster and easier to scale.

Methods like graph sampling, distributed learning, and edge deployment are helping these models deal with large volumes of data and perform better in real-time situations. Another improvement is the use of better evaluation methods and standard benchmark datasets which makes it easier to measure performance and compare different models in a fair way.All of these improvements together are helping build intrusion detection systems that are not just more accurate, but also more practical and reliable in real-world use.

A. Comparative Analysis of GNN Models

Table I presents a comparative analysis of various graph neural network models used in intrusion detection based on learning type, domain, accuracy, scalability, and real-time capability.

TABLE I
COMPARISON OF GNN-BASED INTRUSION DETECTION MODELS

Ref	Model	Learn	Graph	Domain	Acc (%)	F1	Scalability	Real-Time
1	GCN	Sup	Static	General	96.2	96.1	Medium	Partial
2	GCN	Sup	Static	General	94.5	94.4	Medium	Partial
3	GCN	Unsup	Static	IoT	92.1	92.1	Medium	Yes
4	GCN	Sup	Static	General	95.8	95.8	Medium	Partial
5	GAT	Sup	Static	General	97.2	97.2	Low	No
6	Hybrid	Sup	Dyn/Hetero	General	98.1	98.1	Low	No
7	Dynamic	Sup	Dynamic	IoT	93.5	93.5	Medium	Partial
8	GCN	Sup	Static	General	91.2	91.1	Low	No
9	GCN+GAT	Sup	Static	General	95.5	95.5	Medium	Partial
10	GCN	Sup	Static	General	94.8	94.8	Medium	Partial
11	GCN	Sup	Static	IoT	92.9	92.9	Medium	Yes
12	GAT	Sup	Dynamic	6G	96.5	96.5	Medium	Partial
13	GraphSAGE	Sup	Static	IoT	93.8	93.8	High	Partial
14	GCN	Sup	Static	IoT	91.5	91.5	Medium	Partial
15	GCN	Self	Static	General	90.2	90.2	Medium	Yes
16	GCN	Sup	Static	General	95.2	95.2	Medium	Partial
17	GCN	Sup	Static	IoT	92.3	92.3	Low	Yes
18	GAT	Sup	Static	IoT	94.6	94.6	Medium	Partial
19	GCN	Sup	Dynamic	SDN	95.4	95.4	Medium	Yes
20	Hybrid	Sup	Static	IoT	93.2	93.2	Medium	Partial
21	Dynamic	Semi	Dynamic	General	92.8	92.8	Medium	Partial
22	GCN	Sup	Static	General	94.1	94.1	Medium	Yes
23	GCN	Sup	Dynamic	SDN	94.9	94.9	Medium	Yes
24	GCN	Sup	Static	IoT	93.7	93.7	Medium	Yes
25	GCN	Sup	Static	IoT	96.1	96.1	Medium	Yes

XI. Future Scope and Research Directions

Going forward, research in this area should focus on building more complete systems that combine strong graph models, scalable learning methods, and real-time detection capabilities.One major issue that still needs attention is the gap between research results and real-world implementation since many of these approaches are still not widely used in real-world systems.A key direction for future work is improving efficiency and scalability.There is a need for lighter and more efficient graph neural network models that can handle large-scale network data without heavy resource usage.

Approaches like graph sampling, model compression, and distributed processing can help improve performance significantly and make these systems usable even in resource-limited environments.From a system point of view, there is increasing demand for intrusion detection systems that can run on edge devices and embedded systems.

Combining graph-based models with hardware such as microcontrollers and network monitoring devices can enable more real-time and decentralized security solutions.

Also, integrating intrusion detection systems with IoT and cloud platforms can support continuous monitoring and automated threat response along with better handling of large-scale data.Using adaptive and self-learning models can help systems respond better to changing cyberthreats.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Overall, future work should aim to balance accuracy, efficiency, scalability, and real-time performance.Finding this balance is important to make these systems practical, reliable, and actually usable in modern cybersecurity scenarios.

XII. Conclusion

The paper presents an organized and detailed overview of the use of graph-based neural networks in detecting the abnormality or intrusion for modern network environments. The article highlighted the relevance of modeling network traffic in the form of graph-structured data that allows the complex relationships and interactions undermined by conventional methods to be captured in the study [5], [8].

Different graph representation learning methods,including graph convolutional and graph attention networks,were analyzed and found to improve detection accuracy and flexibility in diverse network systems [7], [11], [15]. Moreover, the combination of graph-based neural networks with intelligent learning techniques such as Machine learning and deep learning algorithms helped to more efficiently detect known and unknown cyberthreats [9], [20].

Nevertheless, even with these improvements, one of the major findings of this survey is the absence of emphasis on end-to-end system design. Most of the current research focuses on developing models and evaluating their performance on benchmark data and does not focus on the actual issues of the deployment of the model like scalability, real-time processing, and hardware integration. This weakness restricts the usefulness of intelligent systems based on graph-based neural networks in practice.

Performance factors analysis revealed that factors like the accuracy of the detection, the efficiency of the computation, the scalability, and the latency are essential elements in defining the effectiveness of the system. Simultaneously, such issues as the complexity of graphs construction, the size of massive data processing, and the constraint of datasets still affect the performance of the system [8], [17].

Overall, the survey shows that moving towards real time and practical detection systems is still a challenge. To achieve this, we need a complete method that combines good graph modeling, improved learning techniques and good integrated systems. Graph neural network based intrusion detection looks good because it can detect high level threats better. However, future work should focus on creating solutions that are scalable, efficient and reliable for real world network use.

In conclusion,neural methods designed for graph data are proving to be accurate for intrusion detection,especially in identifying modern and evolving threats.Nevertheless, the potential of this research can be better achieved in the future by coming up with scalable, efficient, and integrated solutions, which can be made to work reliably in a real network environment.

References

[1] G. Vijay, K. Mani, B. Rao, and D. Geethanjali, "Intrusion GNN: Graph Neural Network-Enhanced Network Intrusion Detection System," in *Proc. 10th Int. Conf. Smart Structures and Systems (ICSSS)*, 2025.
[2] M. Gorricho-Segura, X. Echeberria-Barrio, and L. Segurola-Gil, "Edge-based Analysis for Network Intrusion Detection using a GNN Approach," in *Proc. JNIC Cybersecurity Conf.*, 2023.
[3] P. Sathishkumar, S. Nikitha, R. Sruthi, and R. R. Vishwa, "Anomaly Detection in Network Security Using Unsupervised Graph Neural Network," in *Proc. Int. Conf. Advanced Computing Technologies (ICoACT)*, 2025.
[4] K. Gupta, Prachi, N. Chatterjee, and Himanshi, "A GNN-based Novel Approach to Detect Malicious Traffic in Intrusion Detection System," *Procedia Computer Science*, 2025.
[5] M. Zhong, M. Lin, C. Zhang, and Z. Xu, "A survey on graph neural networks for intrusion detection systems: Methods, trends and challenges," *Computers & Security*, 2024.
[6] S. Saxena, J. Grover, and S. Singhal, "Exploring Graph Neural Networks for Robust Network Intrusion Detection," *Procedia Computer Science*, 2025.
[7] Z. Ma, Y. Liu, Y. Chen, Z. Liu, and Y. Li, "XMF-GNN: A cross-modality dynamic fusion heterogeneous graph neural network for network intrusion detection," *Neurocomputing*, 2025.
[8] T. Bilot, N. El Madhoun, K. A. Agha, and A. Zouaoui, "Graph Neural Networks for Intrusion Detection: A Survey," *IEEE Access*, 2023.
[9] W. Villegas-Ch, J. Govea, A. Maldonado, and P. Játiva, "Intrusion Detection in IoT Networks Using Dynamic Graph Modeling and Graph-Based Neural Networks," *IEEE Access*, 2025.
[10] D. Pujol-Perich, J. Suárez-Varela, A. Cabellos-Aparicio, and P. Barlet-Ros, "Unveiling the potential of Graph Neural Networks for robust intrusion detection," *ACM SIGMETRICS*, 2021.
[11] Z. Sun, A. Teixeira, and S. Toor, "GNN-IDS: Graph Neural Network based Intrusion Detection System," in *Proc. ARES*, 2024.
[12] Z. Yang, M. Yang, and Q. Yang, "Network topology security analysis and attack detection based on graph neural networks," *Discover Internet of Things*, 2026.
[13] S. Yang et al., "Industrial Internet of Things Intrusion Detection System Based on Graph Neural Network," *Symmetry*, 2025.
[14] P. Bharathi and M. Raj, "Graph Neural Networks for Intrusion Detection in Next-Generation 6G Networks: A Cybersecurity Perspective," in *Proc. ICICV*, 2025.
[15] W. W. Lo, S. Layegheh, M. Sarhan, M. Gallagher, and M. Portmann, "E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT," in *Proc. IEEE/IFIP NOMS*, 2021.
[16] O. Bondar, "Graph Neural Network-Based Intrusion Detection for IoT: Performance and Comparative Analysis," *Grail of Science*, 2025.
[17] E. Caville, W. W. Lo, S. Layegheh, and M. Portmann, "Anomal-E: A Self-Supervised Network Intrusion Detection System based on Graph Neural Networks," *Knowledge-Based Systems*, 2022.
[18] H. D. Le and M. Park, "Enhancing Multi-Class Attack Detection in Graph Neural Network through Feature Rearrangement," *Electronics*, 2024.
[19] O. Ceran, E. Özdogan, and M. Uysal, "Leveraging Graph Neural Networks for IoT Attack Detection," *Sakarya University Journal of Computer and Information Sciences*, 2025.
[20] D. H. Tran and M. Park, "FN-GNN: A Novel Graph Embedding Approach for Enhancing Graph Neural Networks in Network Intrusion Detection Systems," *Applied Sciences*, 2024.
[21] A. S. Ahanger, S. M. Khan, F. Masoodi, and A. O. Salau, "Advanced intrusion detection in internet of things using graph attention networks," *Scientific Reports*, 2025.
[22] S. Liu, "MGF-GNN: A Multi-Granularity Graph Fusion-based Graph Neural Network Method for Network Intrusion Detection," in *Proc. GAIIS*, 2025.
[23] U. Bhoi, N. Goriya, N. Nagekar, R. Trivedi, and M. Patel, "AI Intrusion Detection System Using Graph Neural Networks for Software Defined Networks (SDN)," *International Journal of Applied Mathematics*, 2025.
[24] T. Altaf, X. Wang, W. Ni, G. Yu, and R. Liu, "A new concatenated Multigraph Neural Network for IoT intrusion detection," *Internet of Things*, 2023.
[25] G. Duan, H. Lv, H. Wang, and G. Feng, "Application of a Dynamic Line Graph Neural Network for Intrusion Detection With Semisupervised Learning," *IEEE Trans. Information Forensics and Security*, 2023.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

[26] S. Saidane, F. Telch, K. Shahin, and F. Granelli, "Deep GraphSAGE enhancements for intrusion detection: Analyzing attention mechanisms and GCN integration," *Journal of Information Security and Applications*, 2025.

[27] K. V. Krishna, K. Akarsh, B. Harsha, P. Vamshi, and E. S. Reddy, "Secure GNNs: Defending Graph Data Privacy with Randomized Edge Perturbations," *Journal of Science Engineering Technology and Management Sciences*, 2025.

[28] R. Vinayakumar, K. Soman, and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," in *Proc. ICACCI*, 2017.

[29] M. A. Jahin, S. S. Souddeep, M. F. Mridha, R. Kabir, and M. R. Islam, "CAGN-GAT Fusion: A Hybrid Contrastive Attentive Graph Neural Network for Network Intrusion Detection," in *Proc. Int. Conf. Industrial Engineering and Applied Intelligent Systems*, 2025.

[30] R. Vinayakumar, M. Alazab, I. K. P. S. (Senior Member), P. Poornachandran, and A. Al-Nemrat, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, 2019.

[31] C. Thumma, D. V. Patil, S. Dash, M. Balakrishnan, and S. Aluvala, "AI-Driven Intrusion Detection in Software-Defined Networks Using GNNs," in *Proc. Int. Conf. Computational Intelligence and Network Systems (CINS)*, 2025.

[32] T. Ngo, J. Yin, Y. Ge, and H. Wang, "Optimizing IoT Intrusion Detection - A Graph Neural Network Approach with Attribute-Based Graph Construction," *Information Sciences*, 2025.

[33] M. K. Devnath, "GCNIDS: Graph Convolutional Network-Based Intrusion Detection System for CAN Bus," *arXiv*, 2023.

[34] I. E. Boukari, I. Abderrahmane, S. Bouzefrane, L. Hamdad, and S. N. Bahloul, "StrucTemp-GNN: An Intrusion Detection Framework in IoT Networks Using Dynamic Heterogeneous Graph Neural Networks," in *Proc. Int. Conf. Mobile, Secure and Programmable Networking*, 2023.