



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IX **Month of publication:** September 2026

DOI: <https://doi.org/10.22214/ijraset.2026.84935>

www.ijraset.com

Call: ☎ 08813907089

E-mail ID: ijraset@gmail.com

AI-Based Zero-Day Attack Detection using Graph Neural Networks

Ms. Rimzim Deshpande¹, Mr. Chetan Danav², Mr. Darshan Ganjare³, Mr. Rohit Meshram⁴, Prof. Umesh Samarth⁵

Department of Information Technology, J D College of Engineering and Management, Nagpur, India

Abstract: Zero-day attacks refer to advanced cyberattacks where there is exploitation of vulnerabilities that have not been discovered before and hence cannot be detected by signature-based and rule-based security systems. In this project, an AI-Based Zero-Day Attack Detection System Using Graph Neural Networks will be developed to detect any unusual and suspicious activity within the network. In this system, the different network entities such as the user, device, IP address, process, and network communications are modeled as nodes while the interactions between them as edges in the graph. The GNN system models learn the complex relations and normal patterns of communications within the network and detects deviations which can be seen to show the presence of new kinds of attacks. The steps in this system include data acquisition, data preprocessing, feature engineering, graph construction, GNN model training, anomaly detection, risk assessment, and security alerting. Evaluation of the system performance will be done using Accuracy, Precision, Recall, F1-Score, and False Positive Rate.

Key Terms: Zero Day Attack, Cybersecurity, Graph Neural Networks (GNNs), Artificial Intelligence, Anomaly Detection, Network Security, Intrusion Detection.

I. INTRODUCTION

Rapid evolution of computer networks, cloud computing, and web applications has made cyber attacks more complex and frequent. Modern networks produce high volumes of inter-related data, including users, devices, IP addresses, process and communication actions. Hence, one of the key issues in cybersecurity is timely identification of suspicious activity. Zero-day attacks are especially dangerous as they exploit vulnerabilities that are not known before and for which there are no patches, rules, and signatures of the attack. Signature-based intrusion detection system is limited to comparing network behavior with existing attack patterns. While this type of system can effectively detect known attacks, it may prove ineffective against attackers who implement new or altered techniques not yet added to the list of signatures [4], [5]. Machine Learning (ML) and Deep Learning (DL) methods have been widely implemented in network intrusion detection in order to overcome certain drawbacks of signature-based approach. The models including decision tree, support vector machine, random forest, and neural network have the ability to learn from the network traffic and detect abnormal behavior [4]. Nevertheless, traditional ML models often view the network information as individual features without reflecting the intricate interrelation between various network entities.

Graph Neural Networks (GNNs) are a useful method that helps in the representation and learning of interrelated data. In a graph-based representation, objects can be represented through nodes, and interactions can be represented through edges. GNNs perform node representation through the aggregation of data from neighboring nodes, helping in the capture of the structure and relation between them. GCN provides the basis of learning representations from graph-structured data [1] while GraphSAGE helps in performing inductive learning in large graphs [2]. Likewise, Graph Attention Networks (GAT) utilize attention mechanism in giving differential weights to neighbouring nodes in the process of information aggregation [3]. In the proposed AI-Based Zero-Day Attack Detection using Graph Neural Networks, the network entities such as users, devices, IP addresses, and processes are represented as nodes and interactions and communication of the entities as edges. In the system, relationships are analyzed to learn normal behaviors of the network to detect any deviation that indicates suspicious attacks or previously unknown attacks.

II. RELATED WORK

Caville et al. [6] introduced a self-supervised network intrusion detection model called Anomal-E which is a Graph Neural Network model for network intrusion detection. This method leverages information about network flow, graph topologies, and edges' features to classify network intrusions independently of any labeled attack data. The paper proves that GNN models can be effective for intrusion detection and can detect new network attacks as well.

Sun, Teixeira and Toor[7] developed a Graph Neural Network-based Intrusion Detection System called GNN-IDS. These authors noted that traditional machine learning-based IDS techniques consider network traces or logs from hosts separately, which means that they cannot discover dependencies between network elements. That is what makes the graph-based method more efficient. An ongoing study on unsupervised Graph Neural Networks for the purpose of network security anomaly detection explored the utilization of graph representation for intrusion detection using KDD Cup 1999 dataset. It was found out that the GNN algorithm was capable of capturing complex relations in network data and yielded superior results compared to several traditional classifiers.[9] Graph Neural Networks have been also studied for their ability to detect zero-day attacks in web traffic. The proposed WebWall algorithm leverages GraphSAGE to extract representations from encrypted web traffic and identify any malicious activity which cannot be detected through traditional signature-based techniques. The research utilized CICIDS2017 and CICIDS2018 datasets.

[10] Caville et al. illustrated that an approach to GNN-based intrusion detection under self-supervision could limit reliance on labeled traffic within the network. For instance, the Anomal-E approach relies on edge-level attributes and graph structure; this is due to the fact that network attacks are defined not just by traffic-level attributes but also by the connections between communicating nodes.[11] In addition, a 2024 review of GNNs in Intrusion Detection Systems described the evolution of GNN-based intrusion detection approaches and outlined three key areas including graph construction, GNN models creation and their deployment.

[12] An unsupervised network intrusion detection model called OPTIMAL was suggested by research in 2026, which is based on the GNN model along with graph contrastive learning. The improved GNN encoder through the application of the attention mechanism and modified message aggregation enables effective representation of network intrusion.

MaGOS-IDS is an enhancement to the OpenMax methodology that leverages Mahalanobis distance within GNN based intrusion detection schemes proposed by Nguyen and Park[13]. The particular focus of this paper lies in overcoming the inherent limitation of traditional closed set GNN intrusion detection systems that may misclassify zero-day attacks as belonging to some existing attack classes.

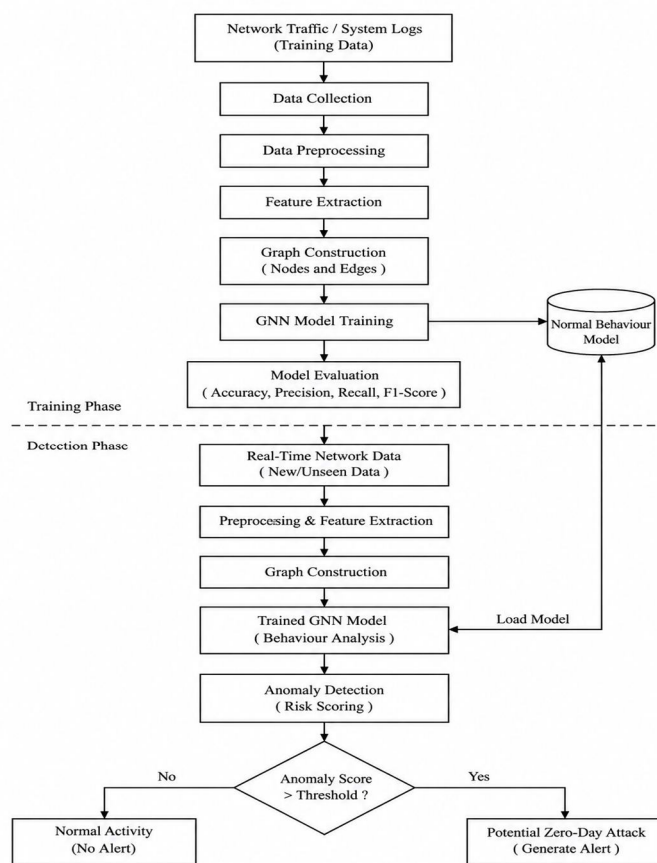


Figure 1 :Flow of model building

The figure below depicts the process of model building and the detection of zero-day attacks using Graph Neural Network (GNN). The data collection involves gathering network traffic and system logs from the system. The gathered data undergoes preprocessing and feature extraction. The extracted features form a graph where network entities are considered as nodes while their interactions constitute edges. The graph is used as input to the GNN model, which then learns the typical patterns of network communication and relationships, and the performance of the model is evaluated using performance metrics like accuracy, precision, recall, and f-score. In the detection process, new and unseen data of the network is also preprocessed and fed into the already trained GNN model for analysis of the behavioral pattern. If the anomaly or risk score produced by the model surpasses the predefined threshold, then the activity is flagged as a possible zero-day attack, hence a security alert is raised, otherwise, the activity is regarded as normal.

III. CHALLENGES AND LIMITATIONS

There are a number of challenges involved in the development of the suggested AI-Based Zero-Day Attack Detection using Graph Neural Networks (GNNs). Firstly, there is the problem of lack of zero-day attack data due to the fact that zero-day attacks are hard to recognize and thus datasets for such attacks are hard to come by. Secondly, there is the problem related to large amounts of data produced by modern networks. Thirdly, the process of data preprocessing is also problematic since collected data is not always complete or relevant. Fourthly, there is the problem of constructing a graph from a dataset since it requires a good understanding of connections between different components of a network. In addition, the process of GNN training may require high computational capacity, especially if dealing with a big dataset. False positives, which mean that legitimate actions may be treated as attacks, and false negatives, which mean that sophisticated attacks can be missed by the system, may also occur. However, due to the constantly changing nature of attack strategies, the model should be trained and updated on a regular basis.

IV. INTERPRETATION

The proposed AI-Based Zero-Day Attack Detection using Graph Neural Network (GNNs) works on the principle of identifying any unusual activity in the network through learning the connections and communication patterns between different entities within the network. In this approach, the different network entities like users, devices, IP address, and processes are taken as nodes and the interaction between these entities are taken as edges. By analyzing such a network of graph, the GNN model can learn the usual network behavior and deviations from such behavior are detected as an anomaly. Anomaly score is calculated for any unusual activity and if it crosses certain threshold value then it is considered as a possible zero day attack and hence an alert is raised.

Table I: Models and Their Description

Model	Description
GCN (Graph Convolutional Network)	Learns node representations by aggregating information from neighbouring nodes. It is useful for analysing relationships between interconnected network entities. [1]
GraphSAGE	Learns node representations by sampling and aggregating information from neighbouring nodes. It is suitable for large and changing graphs. [2]
GAT (Graph Attention Network)	Uses an attention mechanism to assign different importance to neighbouring nodes while learning graph representations. [3]
Deep Neural Network (DNN)	Learns complex patterns from network traffic and can be used for identifying malicious or abnormal network activities. [4]
Random Forest	A traditional machine-learning approach that learns patterns from network features and can be used for intrusion detection. [4]
Support Vector Machine (SVM)	A machine-learning classification technique that can distinguish between different categories of network activities based on extracted features. [4]

V. FINDINGS

According to the study, the conventional cybersecurity models based on signatures and rules cannot adequately detect zero-day attacks because they depend on the exploitation of unknown vulnerabilities which do not have any pre-existing signatures and rules. According to the review, machine learning algorithms and deep learning algorithms can help in learning about the patterns from the data from the network and finding out the abnormalities in the network. However, since the current networks involve a high number of interconnected elements like users, devices, IP addresses, and processes, the representation of the network in terms of graph can help get more relational data. Thus, the models involving GNN like GCN, GraphSAGE, and GAT are applicable in learning about the relationships and communication in the network.

VI. FUTURE ENHANCEMENT

- 1) Applying the GNN algorithm on larger and varied cybersecurity datasets.
- 2) Improving the detection process for unidentified zero-day attacks.
- 3) Providing real-time monitoring and detection of network traffic.
- 4) Minimizing the occurrence of false positives and negatives to increase detection accuracy.
- 5) Including continuous training and updating of the model on novel attack patterns.
- 6) Enhancing risk assessment through more precise calculation of suspicious activities.
- 7) Optimizing the GNN model to ensure minimal computational and memory demands.
- 8) Designing an easy-to-use security dashboard for presenting detected attacks and their anomaly and attack information.
- 9) Comparison of efficiency of different GNN models such as GCN, GraphSAGE, and GAT.
- 10) Evaluation of the complete system through metrics like Accuracy, Precision, Recall, F1-Score, and False Positive Rate.

VII. OBJECTIVES

- 1) Create a Zero-Day Cyber Attack Detection Framework for AI-Based Systems: The first goal is to create a framework for cybersecurity that uses Artificial Intelligence and GNN. It will concentrate on the detection of unknown and unprecedented cyber threats.
- 2) Construct Graphs for Network Activities: Graphs will have network elements (users, devices, IP address, processes) as nodes and network activities as edges between nodes. Thus, this will help to detect relationships between the elements of the network.
- 3) Find Abnormal and Suspicious Activities: GNN will learn typical patterns of communication and behavior within the network. Abnormal activities that do not match these patterns may be detected by the system.
- 4) Detection of Potential Zero-Day Attack Threats and Issuance of Alerts: The system will perform analysis on the suspicious activities and calculate an anomaly score for the activities. In case the score exceeds the predefined threshold value, the system will detect a zero-day attack threat and issue an alert.
- 5) Performance Analysis of the Proposed Zero-Day Attack Detection System: The developed system will be evaluated using the following performance measures: accuracy, precision, recall, F1-Score, and False Positive Rate.

A. Project Overview

In this project, we will be working on building an AI-based Zero-Day Attack Detection System which works on Graph Neural Network (GNN). Network elements like users, devices, IP addresses, and processes are considered as nodes whereas the interaction between network entities will be taken as the edge of GNN. It learns about normal behaviors and communication within the network and analyzes any new network activity to detect abnormal behavior. Risk or anomaly scores are calculated against the suspicious activity and a security alert is triggered if the threshold limit is breached.

Table II. Overview Of Issues Approaches, Methods

Issues / Challenges	Approach	Methods / Techniques
Unknown and previously unseen attacks	Behaviour-based detection	Anomaly Detection
Large volume of network data	AI-based data analysis	Machine Learning / Deep Learning

Complex relationships between network entities	Graph-based representation	Graph Neural Networks (GNNs)
Difficulty in detecting new attack patterns	Learning normal network behaviour	GNN-based Behaviour Analysis
False positives and false negatives	Risk-based decision making	Anomaly/Risk Scoring
Changing attack patterns	Continuous model improvement	Regular Model Training and Updating
Need for quick threat identification	Automated detection and alerting	Real-Time Anomaly Detection

B. Framework Design of the Project

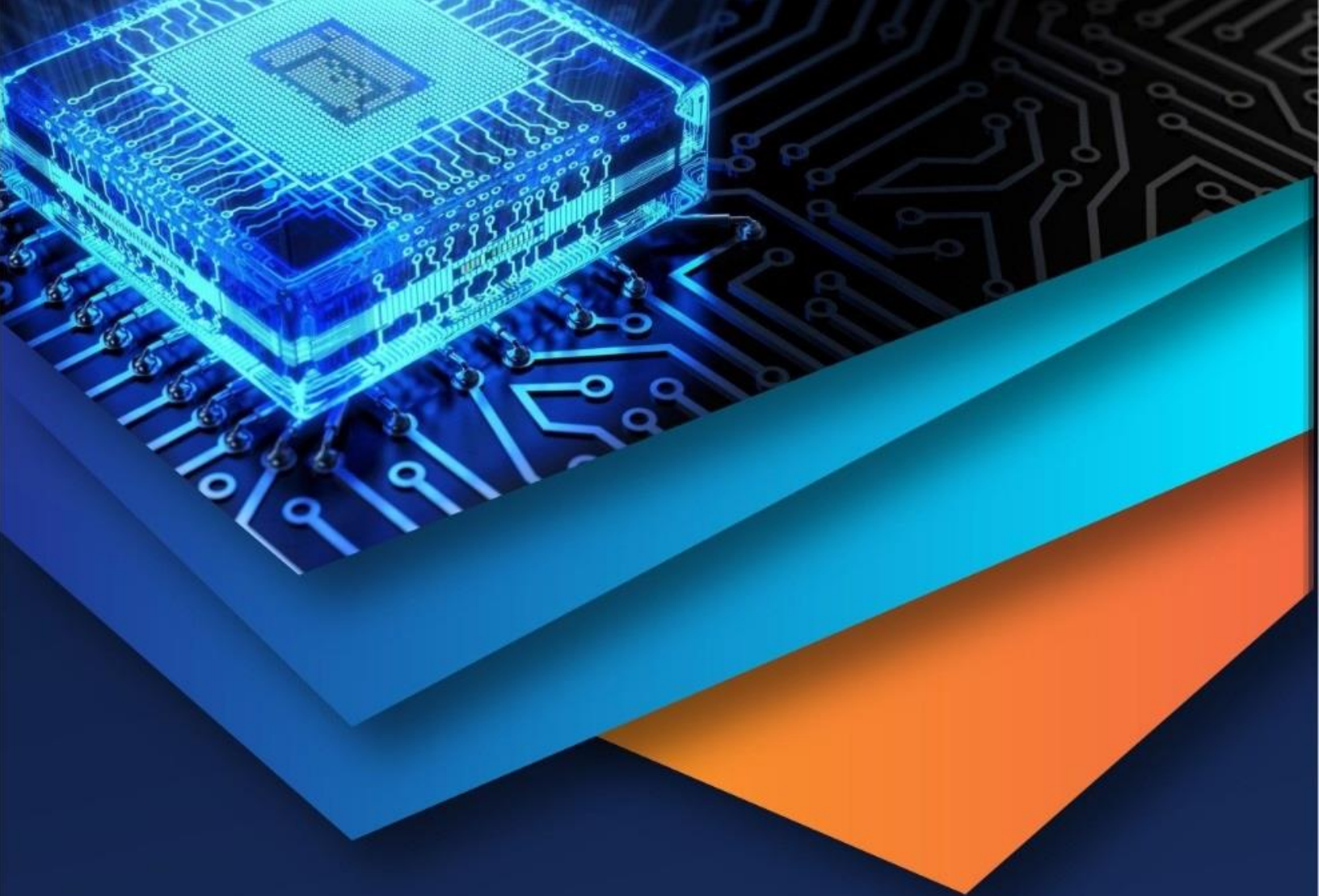
The suggested architecture has several stages that can be used to detect possible zero-day attacks. At first, the network traffic and system log data is collected and preprocessed, thus eliminating unnecessary data and extracting the useful information and features. Then, the data is mapped into graph structure where users, devices, IP addresses and processes become the graph nodes while the relationships between them become the edges of this graph. In such a way, the GNN model learns the relations and patterns of the normal behavior. While detecting zero-day attacks, the system analyses the current network behavior and identifies possible anomalies assigning them the risk/anomaly scores. If the score is higher than the specified threshold, then a zero-day attack is detected.

VIII. ACKNOWLEDGMENT

It is a great pleasure for us to thank We would like to thank our Project Guide, faculty members, and the Department of Information Technology, J D College of Engineering and Management, Nagpur, for their valuable guidance, inspiration, and constant support during this project. We would also like to thank our college for providing us with all the required resources and facilities for this project. At last, we would like to thank our parents, friends, and team members for their constant inspiration and support in making this project a success.

REFERENCES

- [1] T. N. Kipf and M. Welling, "Semi-Supervised Classification with Graph Convolutional Networks," *International Conference on Learning Representations (ICLR)*, 2017.
- [2] W. L. Hamilton, R. Ying, and J. Leskovec, "Inductive Representation Learning on Large Graphs," *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.
- [3] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Liò, and Y. Bengio, "Graph Attention Networks," *International Conference on Learning Representations (ICLR)*, 2018.
- [4] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.
- [5] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," *Military Communications and Information Systems Conference (MilCIS)*, 2015.
- [6] E. Caville, W. W. Lo, S. Layeghy, and M. Portmann, "Anomal-E: A Self-Supervised Network Intrusion Detection System Based on Graph Neural Networks," *Knowledge-Based Systems*, vol. 258, 2022, Art. no. 110030. DOI: 10.1016/j.knosys.2022.110030.
- [7] Z. Sun, A. M. H. Teixeira, and S. Toor, "GNN-IDS: Graph Neural Network Based Intrusion Detection System," 2024. DOI: 10.1145/3664476.3664515.
- [8] "Anomaly Detection in Network Security Using Unsupervised Graph Neural Network," 2025 International Conference on Advanced Computing Technologies (ICoACT), 2025. DOI: 10.1109/ICoACT63339.2025.11004728.
- [9] "WebWall: Zero-Day Attack Detection in Web Traffic Using Spatial Graph Neural Network," 2024 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2024. DOI: 10.1109/ANTS63515.2024.10898287.
- [10] E. Caville, W. W. Lo, S. Layeghy, and M. Portmann, "Anomal-E: A Self-Supervised Network Intrusion Detection System Based on Graph Neural Networks," *Knowledge-Based Systems*, 2022.
- [11] "A Survey on Graph Neural Networks for Intrusion Detection Systems: Methods, Trends and Challenges," *Computers & Security*, vol. 141, 2024, Art. no. 103821. DOI: 10.1016/j.cose.2024.103821.
- [12] Y. Wang, Y. Zhang, Z. Zhang, L. Gao, and H. Pang, "OPTIMAL: Unsupervised Network Intrusion Detection Model Based on Optimized Graph Neural Network and Graph Contrastive Learning," *Computer Networks*, vol. 280, 2026, Art. no. 112169. DOI: 10.1016/j.comnet.2026.112169.
- [13] T.-T. Nguyen and M. Park, "MaGOS-IDS: A Mahalanobis-Enhanced OpenMax Method for Graph Neural Network-Based Intrusion Detection," *Electronics*, vol. 15, no. 16, 2026, Art. no. 3667. DOI: 10.3390/electronics15163667



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)