e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

ENHANCING THREAT DETECTION WITH SIEM TOOL USING GNN

Dr. J. R. Panchal*1, Anupama Rajeevan*2, Yogeshwari Bagul*3, Rutuja Bhosale*4, Susovan Bhowmik*5

*1Professor, Department Of Computer Engineering, Dr. D. Y. Patil College Of Engineering And Innovation, Varale, Talegaon Dabhade, Pune, Maharashtra, India.

*2,3,4,5Student, Department Of Computer Engineering, Dr. D. Y. Patil College Of Engineering And Innovation, Varale, Talegaon Dabhade, Pune, Maharashtra, India.

ABSTRACT

Enhancing threat detection with SIEM tool using GNN aims to enhance the threat detection system by using GNN (Graph neural network) with integration of SIEM tool. By using real-time data of security events through GNN which represents complex relationships and patterns between the data in the form of nodes and edges. The project involves integrating GNN models into existing SIEM frameworks to enhance the threat detection, optimizing them for scalability, accuracy and effectiveness. The system provides a real time alerts when suspicious activity is detected. This project highlights the effectiveness of combining GNN with SIEM tool to boost cybersecurity defenses.

Keywords: GNN, SIEM Tool, Nodes, Edges, Alerts, Threat Detection.

I. INTRODUCTION

In today's increasingly digital world, where technology is used in nearly every aspect of our life, cyber security has become more crucial than ever. Businesses, Governments and individuals relies heavily on online platform and connected devices. The threat landscape has been continuously evolving making cyber-attacks more frequent. Cyber criminals are constantly finding new ways vulnerabilities. So safe guarding sensitive information, ensuring the integrity of systems and maintaining privacy are fundamental priorities [2].

Application security is a critical concern for organizations as the threat landscape continues to evolve. Security information and event management (SIEM) tool plays a pivotal role in bolstering application security by offering real time monitoring, detection and response to security incidence across the IT environment.

SIEM is a comprehensive security management solution that aggregates, analyses and co-relates security event data from a variety of sources such as firewalls, servers, end points and application. It helps organizations detect anomalies, identify potential threats and takes action before breaches or attacks escalate. But in the rapidly evolving cyber-crimes traditional SIEM systems are often challenged by volume, complexity and interconnected nature of security event.

Here GNN presents a ground breaking solution. GNN's are designed to process and analyze graphs structured data. Security data such as network traffic, user behavior and attack paths can naturally be represented as graphs where entities like user devices or IP addresses form the node and interaction between them from the edges [1]. By using GNN in SIEM application like advanced threat detection, user-entity behavior analytics, attack path prediction can be done. System gives alerts to the admin about the threats so that the admin can take action according to the threat.

II. LITERATURE SURVEY

A. M. Thilagavathi, R.Saranyadevi, N. Vijayakumar, K.Selvi, L. Anitha, K. Sudharson "AI-Driven Fraud Detection in Financial Transactions with Graph Neural Networks and Anomaly Detection (2024)"

Framework combining Graph Neural Networks (GNNs) with anomaly detection techniques to enhance fraud detection. Transactions are represented as graphs, allowing GNNs to capture intricate fraud patterns.

B. Dingari Janhavi, Mona A, Sandeep Pulata, Sasank Sami, Bharadwaj Vakamullu, Bharathi Mohan G "Robust Hybrid Machine Learning Model for Financial Fraud Detection in Credit Card Transactions (2023)"

The majority of machine learning models used now in the field of fraud detection include Logistic Regression (LR), Decision Tree (DT), and Random Forest (RF).

C. Wasia Ashraf, Aamir Salaam Ahanger, Faheem Syeed Masoodi "Enhancing Intrusion Detection using Supervised Machine Learning Algorithms"

Creating a robust intrusion detection system (IDS) is crucial for identifying abnormalities in the network and thwarting unauthorized access to network resources, thereby ensuring the security of information.

D. Mangayarkarasi Ramaiah, C. Vanmathi, Mohammad Zubair Khan, M. Vanitha, M. Deepa "An Efficient Intrusion Detection System to Combat Cyber Threats using Deep Neural Network Model (Vol.17, No.3, 2023)"

The present research developed and intelligent NIDS system to defend against potential assaults anticipated in IoT and wireless networks.

E. Yenlik Begimbayeva,Oleksandr Gurko,Hanna Doroshenko, Serik Joldasbayev, Olena Fridman, Bakytzhan Kulambayev, Vitalina Baenko, Serhii Neronov "Detection and Classification of Threats and Vulnerabilities on Hackers Forums Based on ML(2024)"

Identifying and classifying threats and vulnerabilities with python scripts that collects text data from hacker forums. Random forest algorithms is also used.

F. Farhana Reza "DDos-Net : Classifying DDoS attacks in wireless sensor networks with hybrid deep learning (2024)" It addresses the critical issues of DDoS attacks on WSNs through the development and evaluation of DDoS-Net, of hybrid deep learning model.

G. Ghazia Qaiser, Siva Chandrasekaran, Jinchuan Zheng, Rifai Chai "A Hybrid ABNB Model for detecting malicious attacks for IIoS (2023)

The study investigates the performance of ML algorithms including Nave Bayes, Adaboost, MLP and a hybrid algorithm ABNB for detecting malicious attack.

H. Vishva Gandhi, Tirthesh Gajjar "Enhancing fraud detection in financial transactions through cyber security measures (2024)"

The intersection of cyber security and fraud detection in financial transaction represents a critical frontier in safeguarding the integrity of digital financial systems.

III. MOTIVATION AND OBJECTIVES

A. Motivation

The motivation for this project is to enhance traditional SIEM tools by integrating Graph Neural Networks (GNNs) to detect complex and hidden cyber threats that often go unnoticed. By transforming security logs into a graph structure and analyzing relationships between entities, the GNN model can identify sophisticated attack patterns in real-time, providing security analysts with advanced, accurate, and context-rich threat detection capabilities. This approach aims to improve cybersecurity by enabling quicker and more effective responses to evolving threats.

B. Objectives

1. Increase threat detection accuracy: Identify previously undetected or overlooked threats by capturing intricate patterns and dependencies among security events.
2. Enhance threat investigation efficiency: Provide actionable insights and visualizations to accelerate incident response and containment [4].
3. Detect advanced and evolving threats: Adapt to the dynamic threat landscape by effectively identifying novel attack techniques [6].
4. Improve overall security posture: Strengthen the organization's ability to protect sensitive information and systems from cyber-attacks.
5. By achieving these goals, the project will contribute to a more resilient and secure IT environment.

IV. ARCHITECTURE

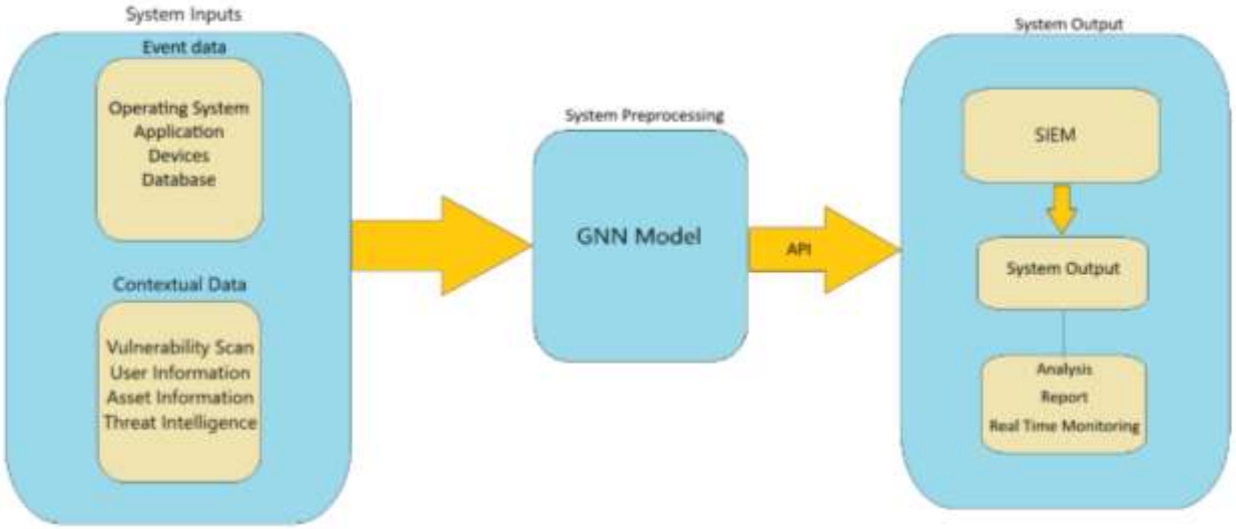

Fig 1: Architecture of SIEM tool using GNN

V. FEASIBILITY AND SCOPE

A. Feasibility

1. GNNs can be applied to a wide range of threat detection tasks, including anomaly detection, intrusion detection, and malware analysis.
2. Using real-time data sets can significantly improve the accuracy and timeliness of threat detection.
3. The benefits of GNNs and real-time data can be significant for organizations facing advanced and sophisticated cyber threats.
4. As GNN models can be trained and deployed within the SIEM environment, we can integrate GNN with existing SIEM tool.

B. Scope

1. Improved Pattern Recognition: GNNs enhance the ability of SIEM tools to recognize patterns in security data by leveraging advanced analytics methods. For instance, GNNs can detect relationships and patterns indicative of vulnerabilities and potential exploitation attempts, aiding in the identification of zero-day exploits and other advanced threats. Through the integration, SIEM tools can benefit from GNNs' ability to analyze data in real-time and provide actionable insights.
2. Risk Management: The risk management process involves identifying and addressing potential risks that could impact the development, deployment, and operational success of integrating Graph Neural Networks (GNNs) into SIEM systems for enhanced threat detection.

VI. CONCLUSION

In conclusion, integrating Graph Neural Networks (GNNs) with Security Information and Event Management (SIEM) tools is a significant step forward in cybersecurity. This project addresses the limitations of traditional SIEM systems in detecting complex and evolving threats. By leveraging GNNs' ability to analyze intricate relationships within security data, the project enhances threat detection accuracy, reduces false positives, and improves the overall efficiency of security operations. This advancement bridges the gap between cutting edge research and practical application, offering a robust solution to the increasing challenges in cybersecurity.

VII. REFERENCES

[1] M. Thilagavathi , R. Saranyadevi , N. Vijayakumar, K. Selvi , L. Anitha, K. Sudharson: "AI-Driven Fraud Detection in Financial Transactions with Graph Neural Networks and Anomaly Detection". (2024)

[2] Vishva Gandhi, Tirthesh Gajjar: "Enhancing fraud detection in financial transactions through cyber security measures". (2024)

[3] Farhana Reza: "DDos-Net : Classifying DDoS attacks in wireless sensor networks with hybrid deep learning". (2024).

[4] Yenlik Begimbayeva, Oleksandr Gurko, Hanna Doroshenko, Serik Joldasbayev, Olena Fridman, Bakytzhan Kulambayev, Vitalina Baenko, Serhii Neronov: "Detection and Classification of Threats and Vulnerabilities on Hackers Forums Based on ML". (2024)

[5] Sudarshan Gaikar, Ajay Bichukale, Deep Barvekar: "Cyber Attack Detection with QR (Vol. 9, 4 April 2024)".

[6] Dingari Janhavi , Mona A, Sandeep Pulata, Sasank Sami, Bharadwaj Vakamullu, Bharathi Mohan G: "Robust Hybrid Machine Learning Model for Financial Fraud Detection in Credit Card Transactions". (2023)

[7] Mangayarkarasi Ramaiah, C. Vanmathi, Mohammad Zubair Khan, M. Vanitha, M. Deepa: "An Efficient Intrusion Detection System to Combat Cyber Threats using Deep Neural Network Model (Vol.17,No.3, 2023)".

[8] Wasia Ashraf, Aamir Salaam Ahanger, Faheem Syeed Masoodi: "Enhancing Intrusion Detection using Supervised Machine Learning Algorithms".

[9] Ghazia Qaiser, Siva Chandrasekaran, Jinchuan Zheng, Rifai Chai: "A Hybrid ABNB Model for detecting malicious attacks for IIoS". (2023)

[10] Talla Yashwanth, K. Ashwini, Gandla Shiva Chaithanya, Arshiya Tabassum: "Network Intrusion Detection using Auto-encoder Neural Networks and MLP". (2023)