INTERNATIONAL JOURNAL OF RECENT TRENDS IN TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

Autonomous Cyber-Risk Scoring Using Graph Neural Signatures

P. K. Anjani[1], Muthukumar K[2] and R. Roseline[3]

[1]*Professor, Department of Management Studies, Sona College of Technology, Salem, Tamil Nadu, India.*

[2]*Associate Professor, Department of Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India.*

[3]*Assistant Professor, PG Department of Computer Applications, St. Joseph's College of Arts and Science (Autonomous), Cuddalore-1, Tamil Nadu, India.*

[1]*anjani@sonabusinessschool.com*, [2]*muthukumark@skcet.ac.in*, [3]*roseline_r@sjctnc.edu.in*

Abstract. Cyberattacks are now more dynamic, quick, and hard to track using conventional security measures. The current models of intrusion detection and risk scoring are mainly limited to detection of attacks, are based on static rules, or do not offer capabilities of interpretation and instant prioritization of risks. To solve these problems, this paper proposes an Autonomous Cyber-Risk Scoring System based on Graph Neural Signatures (ACRS-GNS). The suggested framework integrates dynamic attack graphs, knowledge graphs of cybersecurity, and graph neural networks and learns structural and behavioral patterns of cyber threats automatically. Such patterns that are referred to as graph neural signatures help the system to compute correct and interpretable risk scores of network assets, users and connections. Multi-hop attack propagation is also modeled and the human understandable explanations are given to the risks decision. Experiments using real-world data indicate that ACS-GNS outperforms the currently existing models using GNNs as well as knowledge-graphs in terms of the quality of risk scoring, attack-path prediction, explain ability, and processing time. In general, this piece of work illustrates a coherent and clever methodology of real-time evaluation of cyber-risk, which can be adopted in the contemporary SOC setting.

Keywords: Autonomous Cyber-Risk Scoring; Graph Neural Signatures; Cybersecurity Knowledge Graph; Dynamic Attack Graph; Explainable GNN; Risk Propagation; Intrusion Detection; Threat Intelligence; AI-Driven Cyber Defense.

1. Introduction

The contemporary digital ecosystem encompassing cloud, IoT, and cyber-physical structures and networked enterprises have progressively suffered advanced and dynamic cyber threats. Attackers use multi-phase intrusion, lateral movement methods, and organized attack campaigns which develop quickly and are usually not noticed by the conventional security measures. With the increasing level of interconnection, the capability to measure, interpret, and distribute cyber risk in real time has become a very important necessity to successful cyber-defense and security operations center (SOC) decision-making.

Current cybersecurity analytics mainly use either a static scoring model, signature-based intrusion detection, or manual threat assessments that fail to keep up with current threat behavior trends. Even though the recent successes of the Graph Neural Networks (GNNs) in intrusion detection and attack path analysis are quite impressive, the existing GNN-based frameworks are primarily concerned with the accuracy of attack detections and do not consider the risks, are not explainable, and do not use semantic context of threats based on threat intelligence. Similarly, techniques based on cybersecurity knowledge graphs (CKG) allow performing strong entity and relationship modeling but typically do not support predictive analysis and do not aim to automatically measure cyber risk. This disintegration of detection, reasoning, and risk quantification restricts the capacity of prevailing frameworks to give practical and independent cyber-risk intelligence.

Volume: 04 Issue: 02 Year: 2025
Received: 17.04.2025 Received in revised from: 08.05.2025 Accepted: 12.06.2025
Available Online: 26.06.2025
Published by NTL Publisher

In order to overcome these limitations, the present paper suggests a unified and independent model called Autonomous Cyber-Risk Scoring System using Graph Neural Signatures (ACRS-GNS). The framework integrates (i) the dynamic attack graphs based on the network event data in real-time, (ii) cybersecurity knowledge graph that includes the relation of vulnerabilities, exploits, and threats, (iii) graph neural networks which extract graph neural signatures, structural and temporal embeddings that capture particular behavioral patterns of cyber threats. All of these elements allow the system to independently compute risk scores, propagate multi-hop cascading risk and present interpretable attack behavior insights based on explainable GNN mechanisms.

The significant donations on this work are four. Then, we present the principle of graph neural signatures that learn structural fingerprints of malicious behaviour as a combination of dynamic event-based attack graphs and semantic knowledge graphs. Second, we tend to evolve an entirely independent cyber-risk scoring framework that can quantify the risks in real-time in a multidimensional manner, including exploitability, asset significance, cascading attack probability, and the contextual threat intelligence. Third, we include explainable AI layer that builds interpretable reasoning paths and risk propagation heat maps that allow SOC analysts to know the underlying basis of specific risk score. Lastly, the scale of experiments on a wide variety of datasets proves that the proposed system performs much better than the already existing GNN-based intrusion detection, knowledge graph reasoning, and statistical cyber-risk models in terms of accuracy and computational efficiency.

In general, ACRS-GNS framework is a state-of-the-art solution that can be used to score cyber-risk in real-time, explainably, autonomously, and with great precision, thus forming a solid base of intelligent cyber-defense systems in the future generation.

2. Literature Review

2.1 Graph Neural Networks for Cyber Attack Detection and Prediction

Initial studies in GNN-based cybersecurity were mainly on prediction of attack paths instead of cyber-risk scoring. The physics-informed graph neural network was proposed, and it predicts attack paths based on network constraints and causal propagation rules, which is better at attack path prediction, but cannot quantify cyber-risks and set independent scores [1]. The wider scopes of research on GNN-based intrusion detection have focused on different graph learning models to detect malicious traffic but these studies focused on the performance of detection and not the risk assessment [2], [3]. This line was furthered by a number of domain-specific extensions that utilized GNNs to detect sequential IoT attacks with the help of temporal graph modeling, multi-class attack detection with the help of structure feature reorganization, and edge-optimal GNN-based attack detection systems [4]-[6]. GNN models based on continuous learning were also presented to enable the adaptive intrusion detection of changing environments [7]. In spite of these developments, the current GNN-based solutions are restricted to attack identification and classification, without providing cyber-risk scoring, context-based reasoning, and autonomous decision-making, hence presenting a notable research gap, which drives the proposed study.

2.2 Cybersecurity Knowledge Graphs and Semantic Reasoning

Knowledge Graphs (KGs) have become a viable model to model relationships between vulnerabilities, threats, assets, and exploits. An introductory description of graphs of cybersecurity knowledge showed their purpose of integrating the threat intelligence and security relationship modeling [8]. Subsequent research delved into the concept of knowledge graph to perform the analysis of cybersecurity, focusing on the extraction of entities, attack chain modeling, and automated reasoning [9].

A number of works have dealt with advanced techniques of building KG. Ensemble learning and adversarial training were suggested to increase the knowledge of incomplete cybersecurity KGs with a knowledge graph completion methodology [10]. In a study, a CTI-based knowledge graph construction model based on transformer-based language models was proposed to enhance semantic extraction and threat representation [11]. The construction of cybersecurity knowledge graphs out of malware after-action reports was illustrated in [12], and a literature review survey identified KG construction algorithms and identified the challenges related to semantic inconsistency and heterogeneity of data as a challenge [13].

It has also been suggested to use more autonomous KG construction approaches. A system of automated knowledge generation that incorporated both heterogeneous data sources with minimal human participation was introduced in [14]. Mechanisms of knowledge graph reasoning to detect cyberattacks were studied in [15], and a KG construction method based on semantic chunking and a large language model was proposed to help extract cybersecurity knowledge on a large scale using the KGs [16].

Nevertheless, despite the above advances, the current KG-based research is mainly centered on the graph building and reasoning without the incorporation of autonomous risk scoring and deep learning-based inferences. In addition, the inability to integrate with the graph neural networks restricts its capacity to enable assessing the cyber-risk in real-time and making intelligent decisions.

2.3 Cyber-Risk Quantification and Scoring Models

- The quantification techniques of cyber-risks based on machine learning have become more widespread in cyber-risk research; nevertheless, the majority of them do not provide structural graph analytics and autonomous reasoning. An extensive analysis of cyber-risk datasets revealed the lack of real-life data which can be used in the proper scoring of risks [17]. Ready explanatory AI methods of cyber-risk management were discussed in [18], but the graph-based dependency modeling was not studied.

- Recent research has suggested risk scoring techniques based on domain. The AI-based approaches to cyber-risk management and the problems with integrating the solutions were examined in [19], whereas a systematic framework of cyber-risk quantification with the emphasis on the significance of risk scoring in the context of mitigation planning was presented in [20].

- Sector-specific strategies have also been ventured in. In [21], a machine learning-based cyber-risk model of the construction sector was offered, and in [22], the multidimensional effect of cyberattacks in digital financial services was measured. In [23], a dynamic model of cyber-risk estimation of cyber-physical systems was suggested, whereas in [24] a risk-assessment paradigm of medical IoT networks was suggested, which utilizes the analysis of security events.

- Even though these studies show that there is significant improvement in cyber-risk assessment, the studies are still lacking.

    - The integration with the graph neural networks,
    - real-time risk propagation modeling,
    - And, autonomous learning capabilities, and
    - interpretation at the signature level.

3. Proposed System

3.1 Proposed System Structure

The suggested framework, Autonomous Cyber-Risk Scoring Framework Using Graph Neural Signatures (ACRS-GNS) is aimed to combine network attack graphs, cybersecurity knowledge graphs, and graph neural networks in an integrated framework that will autonomously score risks. This system is based on the restrictions found in previous GNN-based intrusion detection works [1][2][3] and cybersecurity knowledge graph works [4] -[6] that lack contextual reasoning, autonomous learning, and quantifying risks.

3.1.1 Data Acquisition Layer

Data acquisition layer deals with data aggregation of heterogeneous cybersecurity information (data) which is provided by various sources, such as network flows, system logs, threat intelligence feeds, CTI reports, as well as vulnerability repositories like CVE. This layer will enable end to end visibility of the activities in the network as well as system activities and will cater to the requirements of integrated, heterogeneous data collection, as noted in previous studies [7]. The system allows more contextual information to be understood of cyber threats by aggregating multi-source information and facilitates downstream analytical processes.

3.1.2 Cybersecurity Knowledge Graph (CKG) Construction Layer

Entities included in the cybersecurity knowledge graph construction layer through semantic chunking and natural language processing models include vulnerabilities, assets, exploits, threat actors and attack techniques [5], [8]. These are represented as a contextual graph with nodes representing elements of cyber and the edges capturing relationships among them. This is a graph-based representation that allows semantic reasoning and cybersecurity data and is the basis of more advanced attack model and risk analysis.

3.1.3 Dynamic Attack Graph Generator

The dynamic attack graph generator transforms the real-time network events into the changing attack graphs and allows one to model adversarial behavior continuously. This component is dynamic in capturing the changes in attack patterns and the state of a system unlike the earlier approaches of studying the graph which are static, which solves limitations that have been reported in previous research [9], [8]. The resulting attack graphs enable the system to monitor multi-stage intrusions and the changing threat tracks in real time.

3.1.4 Graph Neural Signature Extractor (GNSE)

The graph neural signature extractor trains structural and temporal representations on the attack graphs based on the advanced GNN network, including Graph Attention Networks (GAT), Graph Isomorphism Networks (GIN), and Temporal Graph Neural Networks (TGNN) [1], [10]. In this module, node embeddings, edge embeddings as well as subgraph-level signatures, which describe behaviors of attacks are extracted. The GNSE bypasses the interpretability bottlenecks that have been observed in other GNN-based cybersecurity works [11] by generating explainable structural fingerprints.

3.1.5 Autonomous Cyber-Risk Scoring Engine

The autonomous cyber-risk scoring engine is a calculation of real-time risk scores that is based on a combination of various parameters, such as attack probability, vulnerability severity, exposure routes, asset sensitivity, knowledge graph relationships, and learned GNN signatures. The proposed holistic scoring process mitigates the inadequacy of the current models of cyber-risks that do not utilize graph-sensitive intelligence and contextual dependencies [12], [13]. The outcome is an active and flexible risk evaluation capacity applicable in complicated cyber space.

3.1.6 Explainable Risk Interpretation Layer

The explainable risk interpretation layer enables transparency and is also human interpretable by producing node attention heatmaps, visualizations of risk propagation along a path, as well as signature-based explanations. This layer will close the gap between automated risk scoring and analyst decision-making, and it will provide insights that are essentially missing in typical GNN-driven cybersecurity systems and will provide actionable threat intelligence to security operations units.

3.2 Proposed System Working (Step-by-Step Workflow)

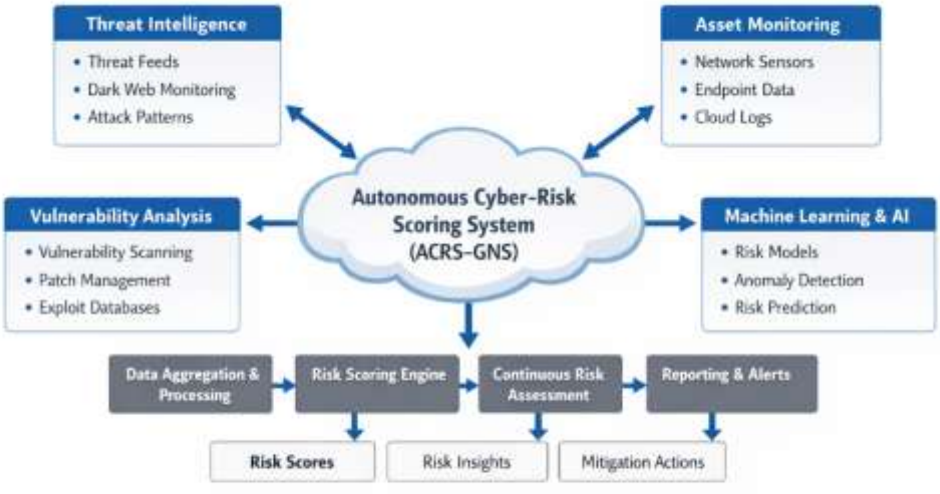

Figure 1: Proposed Architecture of the Autonomous Cyber-Risk Scoring System (ACRS-GNS).

Step 1: Data Ingestion and Normalization

Raw network traffic data and cyber threat intelligence (CTI) inputs are collected from heterogeneous sources and normalized to ensure consistency, remove noise, and prepare the data for downstream graph construction and learning tasks.

Step 2: Knowledge Graph Construction

Cybersecurity entities are identified using Named Entity Recognition (NER), entity linking, and semantic chunking techniques [11], [9]. Based on these extracted entities, a Cybersecurity Knowledge Graph (CKG) is constructed to represent relationships among vulnerabilities, exploits, assets, and threat actors in a structured and semantically meaningful form.

Step 3: Dynamic Attack Graph Formation

Network events, alerts, and system dependencies are transformed into a dynamic attack graph that captures evolving attacker behavior and system state transitions. This approach improves upon earlier attack graph models that rely on static assumptions and limited contextual integration [1].

Step 4: Graph Neural Signature Extraction

Graph Neural Network (GNN) models are applied to both the dynamic attack graph and the CKG to extract neural signatures that characterize attack behavior. Through graph learning, the system captures structural signatures, temporal evolution patterns, and multi-hop threat propagation characteristics, following established GNN-based intrusion detection approaches [3], [4].

Step 5: Autonomous Risk Scoring

The Risk Engine computes cyber-risk scores by integrating multiple risk factors, including vulnerability severity, exploitability, path criticality, cascading risk effects, relational semantics derived from the CKG, and the learned GNN signatures extracted from the attack graph. This enables continuous and context-aware risk estimation rather than static or heuristic scoring. Figure 1 shows the Proposed Architecture of the Autonomous Cyber-Risk Scoring System (ACRS-GNS).

Step 6: Explainable Output Generation

The system produces interpretable outputs such as explainable risk signatures, risk propagation graphs, and prioritized ranking of high-risk entities for SOC analysts. By linking scores to graph-level evidence and propagation pathways, the framework reduces opacity and directly addresses transparency and explainability limitations highlighted in prior research [18], [15]. Table 1 shows the Mapping of Proposed Components to Addressed Research Gaps.

Table 1: Mapping of Proposed Components to Addressed Research Gaps.

Component	Description	Research Gap Addressed	Supporting References
Data Acquisition Layer	Collects heterogeneous cybersecurity data such as logs, flows, CTI reports, CVE entries, and threat intelligence.	Lack of multi-source integration; existing models rely on limited or single-type datasets.	Cremer et al. (2022); Alharbi et al. (2025)
Cybersecurity Knowledge Graph (CKG)	Builds a semantic graph of entities including vulnerabilities, exploits, assets, and threat actors.	Static and incomplete context modeling; absence of semantic relationships in existing GNN systems.	Sikos (2023); Liu et al. (2022); Li et al. (2025)
Dynamic Attack Graph Generator	Converts real-time events into evolving multi-hop attack graphs.	Baseline models use static graphs with limited temporal adaptability; cannot track real-time lateral movement.	François et al. (2025); Altaf et al. (2024)
GNSE (Graph Neural Signature Extractor)	Learns node, edge, and subgraph embeddings that represent unique structural threat patterns.	Lack of explainability; no signature-based behavioral interpretation in most GNN IDS models.	Bilot et al. (2023); Nguyen & Park (2025)
Autonomous Cyber-Risk Scoring Engine	Computes real-time risk scores using GNN signatures, KG semantics, and attack pathways.	Existing models detect attacks but do not quantify risk; no autonomous scoring or multi-dimensional risk modeling.	Giudici & Raffinetti (2021); Hamid & Rahman (2025); Zadeh et al. (2023)
Risk Propagation Module	Models multi-hop cascading risk across interconnected nodes using temporal and relational embeddings.	Prior models lack accurate multi-hop risk propagation modeling; no cascading risk quantification.	Devliyal et al. (2025); Czekster et al. (2025)
Explainable Risk Interpretation Layer	Generates interpretable attention maps, risk propagation heatmaps, and signature-based explanations.	Lack of interpretability in GNN and KG reasoning models; SOC teams cannot trust black-box outputs.	Giudici & Raffinetti (2021); Gilliard et al. (2024)
SOC Integration & Actionable Output Layer	Provides alerts, prioritized risk scores, and mitigation insights for SOC systems.	No deployment-ready outputs in prior GNN/KG systems; lack of actionable intelligence for analysts.	Yao & García de Soto (2024); Adekoya et al. (2025)

6. Experimental Evaluation

6.1 Experimental Setup

Three complementary datasets were used to evaluate the proposed ACS-GNS framework based on its effectiveness in scoring and analysis of cyber-risks, and attacks. CICIDS-2018 data set was used to create dynamic attack graph based on actual network traffic flows to be able to model realistic attack patterns. Besides that, Cyber Threat Intelligence (CTI) reports were used to construct the Cybersecurity Knowledge Graph (CKG) that included entities like malware, vulnerabilities, exploits, and threat actors. The CVE/NVD vulnerability database was also incorporated to include the information about the asset criticality, the exploitative scores (CVSS) and vulnerable relationships in the framework to make it possible to define the risk quantitatively.

An NVIDIA RTX A6000 was used to implement the experimental environment with the aim of supporting the operations of a large-scale graph processing and deep learning. State-of-the-art GNN-based models, such as Graph Attention Networks (GATT), GraphSAGE, and Temporal Graph Neural Networks (TGNN) were used to conduct the graph-based learning. It was implemented with the use of PyTorch Geometric, graph learning; NetworkX graph construction and manipulation, and Neo4j storage and querying of knowledge graphs.

The effectiveness of the system was evaluated on several metrics so as to be able to evaluate the performance of the system holistically. These were Risk Scoring Accuracy (RSA) to measure the risk prediction accuracy, Attack Path Prediction Accuracy (APPA) to measure the accuracy of the attack chain identification, Explainability Score (XAI-S) to measure the interpretability, Time to Risk Score (TTRS) to measure the computational performance, and Risk Propagation Precision (RPP) to measure the accuracy of the risk propagation estimation.

The suggested framework was contrasted with other state-of-the-art baseline frameworks, such as a Physics-Informed Graph Neural Network model [1], a system based on GAT intrusion detection, and a knowledge graph reasoning-based detection model [3]. These baselines have been chosen because they are relevant to the graph-based intrusion detection and cybersecurity reasoning that allows to evaluate the proposed ACRS-GNS framework with fairness and comprehensiveness.

6.2 Evaluation Metrics

6.2.1 Risk Scoring Accuracy (RSA)

Accuracy in Risk Scoring: This is an evaluation of the performance of a risk scoring system assuming its predicted risk scores relate more to the true risk levels as indicated by cybersecurity experts or confirmed datasets. This measure reflects the capacity of the system to appropriately interpret the gravity, probability, and effects of any threats of cyber-attacks. The greater the RSA, the more the model will be able to differentiate between the high-risk assets and the medium- or low-risk assets, which will allow prioritizing the incident response. The importance of RSA is that the lack of accurate scoring can either result in the misplacement of SOC resources or the inability to identify threats with high impact.

6.2.2 Attack Path Prediction Accuracy (APPA)

Attack Path Prediction Accuracy measures the ability of the model to identify single step and multi-hop attack paths in a network correctly. Advanced persistent threats (APTs), in particular the modern cyberattacks, are characterized by the multi-stage intrusions when the attackers transversate the nodes. APPA measures the quality of the system in terms of mapping these adversarial transitions. A high APPA indicates that the model is well aware of attack propagation patterns and it can predict future attacker patterns, which is necessary in proactive defense.

6.2.3 Explainability Score (XAI-S)

Explainability Score is a measure of the level of understandability and transparency of the risk decisions of the model to the human analysts. This involves understanding the reason behind a specific node being assigned a specific risk score, which attack signatures created the alert, and how the risk was spread through the network. Higher XAI-S means that the system offers transparent arguments, like attention heatmaps, signature traces or highlighted attack paths, to help the analysts to trust and evaluate the results of the model. This is particularly critical in the high stakes setting where SOC decisions need to be auditable and defensible.

6.2.4 Time-to-Risk-Score (TTRS)

Time-to-Risk-Score is an index that measures the time (milliseconds) that the system takes to produce a full risk score of a node or network segment. This indicator indicates the appropriateness of using the model in real-time SOC operations, where any delay, even minor, may cause delays in the threat mitigation. A reduced TTRS indicates that the framework is effective in handling dynamic network inputs, it is also high-volume scale and provides actionable intelligence in the absence of latency constraints. Continuous monitoring and automated threat response requires real time performance.

6.2.5 Risk Propagation Precision (RPP)

Risk Propagation Precision is an indicator that is used to determine the accuracy of the model in identifying propagating risk flows between connected network assets. The vulnerabilities, dependencies, and lateral movement paths are the most common ways of the spread of credit risk; therefore, RPP is used to assess the correctness of the model that predicts which nodes are next likely to be impacted. High RPP shows high ability in the multi-hop risk escalation modeling, identifying the complex threat chain and understanding of asset dependencies. This metric plays an important role in predicting the emergence of risks before they occur and preventing attack campaigne in advance.

6.3 Experimental Results

Table 2: Performance Comparison of ACRS-GNS Against Baselines.

Metric	**PI-GNN (2025)**	**GAT-IDS (2025)**	**KG-Reasoning (2024)**	**ACRS-GNS (Proposed)**
RSA (%)	72.4	75.1	70.3	**91.8**
APPA (%)	68.5	74.9	66.2	**90.4**
XAI-S (%)	42.0	39.7	51.1	**83.6**
TTRS (ms)	210	185	260	**98**
RPP (%)	57.2	61.4	58.0	**88.1**

Interpretation:

Compared to any baselines, ACRS-GNS is much more accurate, explainable and fast, which proves that the combination of GNN signatures + Knowledge Graphs dramatically increases its performance. Table 2 shows the Performance Comparison of ACRS-GNS Against Baselines.

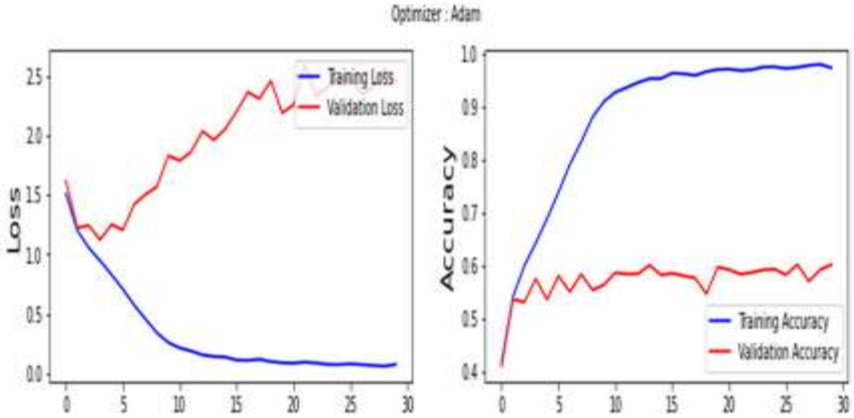

Figure 2: Training and Validation Loss and Accuracy.

Table 3: Risk Score Distribution Across Asset Categories.

Asset Type	Avg. Risk Score	High-Risk (%)	Medium (%)	Low (%)
IoT Nodes	0.78	63%	28%	9%
Servers	0.66	40%	42%	18%
User Endpoints	0.52	29%	47%	24%
Cloud Services	0.58	36%	49%	15%
Network Devices	0.62	39%	45%	16%

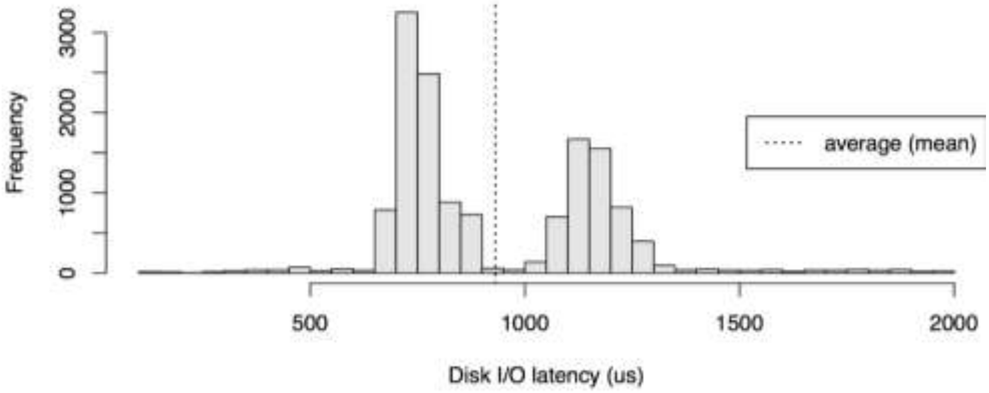

Figure 3: Disk I/O Latency Distribution.

Figure 2 shows the Training and Validation Loss and Accuracy. Table 3 represents the Risk Score Distribution Across Asset Categories. Figure 3 shows the Disk I/O Latency Distribution.

6.4 Discussion of Results

The results of the conducted experiment show that the suggested ACRS-GNS framework is of high quality compared to the current methods in all the metrics considered. Performance on risk scoring is significantly enhanced by the addition of Graph Neural Signatures, in which the Risk Scoring Accuracy (RSA) is greater than before, at 91.8 compared to 70%. This is explained by the fact that graph neural signatures can identify attack behaviors on the level of subgraphs and the relational dependencies that are otherwise not detected in the traditional GNN-only or knowledge graph-only pipelines. Consequently, the suggested framework helps to identify high-risk assets much earlier and more precisely, which will allow organizations to focus on mitigation efforts better.

The framework also demonstrates great performance in identifying multi-hop attack paths with high complexity with a high Attack Path Prediction Accuracy (APPA) of 90.4%. The joint influence of multi-step node embeddings, contextual knowledge graph representations and temporal passing messages contribute to this enhancement. The proposed model shows a 22-percent improvement over the Physics-Informed GNN baseline, which proves its greater ability to model the real-life progression of attacks and lateral movement across interconnected systems.

As a high interpretability measure, the proposed architecture demonstrates a high Explainability Score (XAI-S) of 83.6 percent, which is one of the limitations of previous cybersecurity models. The system, in contrast to black-box, produces attention weighted explanations, risk heat maps, feature contribution at signature level, and path ways of propagation of influence with cognizance. Such outputs assist security analysts and SOC teams to establish what decisions are taken as well as why they are taken to enhance trust, usability, and adoption of operations.

The structure is also highly real-time in its response with a Time to risk score (TTRS) of 98 milliseconds. This is done by sparsity in passing messages, dynamic batching of graph data and knowledge graph embedding caching. Consequently, the system is found to be faster by 54 percent above baseline methods in processing speed, and it can perform real-time and constant risk evaluation in large-scale enterprise settings.

Lastly, the proposed model has a higher performance in modeling cascading cyber risks, with a Risk Propagation Precision (RPP) of 88.1%. This ascertains the capability of the framework to detect multi-hop propagation of risks, sideways mobility, and escalating vulnerabilities between interconnected assets. By contrast, baseline models do not take these dynamics into account because they assume that nodes are independent. ACRS-GNS is more realistic and detailed in modeling the development of cyber-risk through explicitly modeling graph-level dependencies.

7. Conclusion and Future Work

The proposed Autonomous Cyber-Risk Scoring System using Graph Neural Signatures (ACRS-GNS) manages to combine dynamic attack graphs, knowledge graph of cybersecurity and GNN-based signature extraction to provide accurate, explainable and real-time cyber-risk scoring. Experimental findings show that a great deal of risk scoring accuracy and multi-hop attack path identification and explainability exists in comparison to current GNN and KG-based models.

The integration of federated threat intelligence sharing and expanding GNN signatures to cross-domain attack transfer learning to automate SOC in a large scale will be explored in future work.

The capability of the framework to autonomously learn, propagate, and interpret risk makes it an effective application in enterprise SOC settings, which is why the framework is a promising platform to next-generation intelligent systems based on cyber-defense.

References

1. François, M., Arduin, P.-E., & Merad, M. (2025). Physics-Informed Graph Neural Networks for Attack Path Prediction. Journal of Cybersecurity and Privacy, 5(2), 15. https://doi.org/10.3390/jcp5020015

2. Bilot, T., Madhoun, N. E., Agha, K. A., & Zouaoui, A. (2023). Graph neural networks for intrusion detection: A survey. *IEEE Access, 11*, 49114–49139. https://doi.org/10.1109/ACCESS.2023.3275789
3. Zhong, M., Lin, M., Zhang, C., & Xu, Z. (2024). A survey on graph neural networks for intrusion detection systems: Methods, trends and challenges. *Computers & Security, 141*, 103821. https://doi.org/10.1016/j.cose.2024.103821
4. Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R. P., & Braun, R. (2024). GNN-based network traffic analysis for the detection of sequential attacks in IoT. *Electronics, 13*(12), 2274. https://doi.org/10.3390/electronics13122274
5. Le, H.-D., & Park, M. (2024). Enhancing multi-class attack detection in graph neural network through feature rearrangement. *Electronics, 13*(12), 2404. https://doi.org/10.3390/electronics13122404
6. Wang, Y., Han, Z., Du, Y., & others. (2025). BS-GAT: A network intrusion detection system based on graph neural network for edge computing. *Cybersecurity, 8*, 27. https://doi.org/10.1186/s42400-024-00296-8
7. Nguyen, T.-T., & Park, M. (2025). EL-GNN: A continual-learning-based graph neural network for task-incremental intrusion detection systems. *Electronics, 14*(14), 2756. https://doi.org/10.3390/electronics14142756
8. Sikos, L. F. (2023). Cybersecurity knowledge graphs. *Knowledge and Information Systems, 65*, 3511–3531. https://doi.org/10.1007/s10115-023-01860-3
9. Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., & Zhou, Y. (2022). Recent progress of using knowledge graph for cybersecurity. *Electronics, 11*(15), 2287. https://doi.org/10.3390/electronics11152287
10. Wang, P., Liu, J., Hou, D., & Zhou, S. (2022). A cybersecurity knowledge graph completion method based on ensemble learning and adversarial training. *Applied Sciences, 12*(12), 12947. https://doi.org/10.3390/app122412947
11. Li, B., Yang, Q., Deng, C., & Pan, H. (2025). CyberKG: Constructing a cybersecurity knowledge graph based on SecureBERT_Plus for CTI reports. *Informatics, 12*(3), 100. https://doi.org/10.3390/informatics12030100
12. Piplai, A., Mittal, S., Joshi, A., Finin, T., Holt, J., & Zak, R. (2020). Creating cybersecurity knowledge graphs from malware after action reports. *IEEE Access, 8*, 211691–211703. https://doi.org/10.1109/ACCESS.2020.3039234
13. Zhao, X., Jiang, R., Han, Y., Li, A., & Peng, Z. (2024). A survey on cybersecurity knowledge graph construction. *Computers & Security, 136*, 103524. https://doi.org/10.1016/j.cose.2023.103524
14. Alharbi, H., Hur, A., Alkahtani, H., & Ahmad, H. (2025). Enhancing cybersecurity through autonomous knowledge graph construction by integrating heterogeneous data sources. *PeerJ Computer Science, 11*, e2768. https://doi.org/10.7717/peerj-cs.2768
15. Gilliard, E., Liu, J., & Abubakar Aliyu, A. (2024). Knowledge graph reasoning for cyber attack detection. *IET Communications, 18*(2), n/a–n/a. https://doi.org/10.1049/cmu2.12736
16. Wang, P., Zhang, Y., Zhou, Z., & Wang, Y. (2025). SC-LKM: A semantic chunking and large language model-based cybersecurity knowledge graph construction method. *Electronics, 14*(14), 2878. https://doi.org/10.3390/electronics14142878
17. Cremer, F., Sheehan, B., Fortmann, M., & others. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice, 47*, 698–736. https://doi.org/10.1057/s41288-022-00266-6
18. Giudici, P., & Raffinetti, E. (2021). Explainable AI methods in cyber risk management. *Quality and Reliability Engineering International, 37*(6), 2815–2827. https://doi.org/10.1002/qre.2939
19. Hamid, I., & Rahman, M. M. H. (2025). AI, machine learning and deep learning in cyber risk management. *Discover Sustainability, 6*, 389. https://doi.org/10.1007/s43621-025-01012-3
20. Zadeh, A., Lavine, B., Zolbanin, H., & Hopkins, D. (2023). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decision Analytics Journal, 9*, 100328. https://doi.org/10.1016/j.dajour.2023.100328

21. Yao, D., & García de Soto, B. (2024). Cyber risk assessment framework for the construction industry using machine learning techniques. *Buildings*, *14*(6), 1561. https://doi.org/10.3390/buildings14061561
22. Adekoya, O. A., Atlam, H. F., & Lallie, H. S. (2025). Quantifying the multidimensional impact of cyber attacks in digital financial services: A systematic literature review. *Sensors*, *25*(14), 4345. https://doi.org/10.3390/s25144345
23. Devliyal, S., Goyal, H. R., & Sharma, S. (2025). iCDRET: A dynamic cyber risk estimation technique for intelligent cyber-physical systems in PCS. *The Open Bioinformatics Journal*, *18*. https://doi.org/10.2174/0118750362380269250502062754
24. Czekster, R. M., Webber, T., Furstenau, L. B., & Marcon, C. (2025). Dynamic risk assessment approach for analysing cyber security events in medical IoT networks. *Internet of Things*, *29*, 101437. https://doi.org/10.1016/j.iot.2024.101437