Causal Neuro-Symbolic Intelligence for Attribution of Zero-Day Cyberattacks

Shambhu Sharan Srivastava[*]
Professor,
Department of Computer Science,
School of Management Sciences,
Varanasi.
shambhuss@yahoo.com

G. Gokulakrishnan
Professor, Department of CSE
Jayalakshmi Institute of Technology,
Thoppur, Dharmapuri.
gokulmaths@gmail.com

Rashmi Shekhar
Professor and Deputy Director
Amity Institute of Information Technology
Amity University Patna
Rashmi.shekhar81@gmail.com

V Sravan Kumar
Associate Professor
Department of CSE (Data Science)
MLR Institute of Technology, Hyderabad
sravan512@gmail.com

R. Naveenkumar
Dept of C.S.E
School of Engineering and Technology,
CGC University Mohali-140307,
Punjab India.
drnk1983@gmail.com
0000-0001-9033-9400

S.Sharmila
Assistant Professor
Department of Computer Science
NGM College, Pollachi-642003
mcasharmi2007@gmail.com

***Abstract*— With the advent of the zero day attack and the related vulnerabilities, new threats have cropped up for the existing cyber security solutions, which can't be detected and signature-based solutions can't be detected and attributed. The existing ML and DL based detection methods provide acceptable detection accuracy but are not explained and do not work for unseen behaviours. In this paper, an explainable approach towards the attribution of zero-day cyberattacks is proposed that is based on a Causal Neuro-Symbolic Intelligence (CNSI) approach. This framework combines the temporal cyber event graph and the hyperbolic threat representation learning with the symbolic cyber security knowledge and causal dependency discovery/counterfactual attack simulation to obtain the most probable representation of the threat actors. Data-driven learning and expert cybersecurity reasoning are combined via a neuro-symbolic fusion mechanism and causal analysis elucidating attack dependencies and the attacker's intent. Through experiments, it has been proven to outperform the traditional machine learning and graph neural network and transformer-based approaches. The proposed framework was able to correctly attribute an attack with an accuracy rate of 97.1% in five different scenarios of a zero-day attack, a precision rate of 96.4% and a recall rate of 95.9%. The results validated and reinforced the trustworthiness of the framework, its interpretability and robustness, and it proved to be useful for the cyber threat intelligence and cyber incident response processes.**

Keywords*— *Zero-Day Cyberattacks, Cyber Threat Attribution, Neuro-Symbolic Intelligence, Causal Reasoning, Counterfactual Analysis, Graph Neural Networks, Explainable Artificial Intelligence, Cybersecurity

I. INTRODUCTION

Digital infrastructure, cloud computing, and interconnections have spurred an explosion of cyberattacks in both their frequency and sophistication [1]. Of these threats, the Zero-day Cyber threat is one of the most dangerous as it utilizes yet to be known vulnerabilities prior to the patches are available [2]. Current cybersecurity solutions are mainly oriented towards detecting and preventing attacks, and typically are not adept at discovering who and why attackers are attacking [3]. Accurate attribution of cyberattacks is a critical piece of information in threat intelligence, incident response and proactive planning for defending the network [4]. But, the dynamic behavior and stealthy of the recent attacks pose significant problems in tracking attack campaigns [5]. Thus, in today's cybersecurity landscape, sophisticated attribution models which are capable of dissecting intricate attack methods and covert connections are becoming more essential.

There are various machine learning and deep learning methods to detect and attribute cyberattacks [6]. Traditional methods like Random Forests, Support Vector Machines and rule-based expert systems require predetermined signatures and features that need to be handcrafted [7]. Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTMs) networks and Transformer models enhance feature extraction and behavioral analysis skills [8]. Recently, Graph Neural Networks were developed to capture the attack relationships and interactions within a network [9]. Although these developments have been made, many of the methods currently in use are based on correlation and do not give much interpretability [10] [11].

This paper introduces a Causal Neuro-Symbolic Intelligence approach for explainable attribution of zero-day cyberattacks, which overcomes these limitations. The framework integrates the temporal representation of cyber events, the hyperbolic representation of a graph of these events, the infusion of symbolic cybersecurity knowledge, the discovery of causality among the events, and counterfactual reasoning in a single architecture. The proposed method does not rely on the traditional models of attribution based on mainly the similarity of the behaviour or attack signatures, but relies on causal relationships between attack stages and the assessment of attacker intent based on other attack paths. The combination of neural learning and symbolic reasoning not only improves prediction accuracy, but also increases the interpretability of the models.

This work has the following main contributions:

- A new Causal Neuro-Symbolic Intelligence model was designed for explainable attribution of zero-day

cyberattacks based on the analysis of the temporal attack graph.

- A hybrid neuro-symbolic fusion mechanism was proposed to incorporate the hyperbola graph embeddings and cyber security domain knowledge to boost the attribution results.
- The proposed framework successfully attained the high attribution accuracy of 97.1% with interpretable explanations, increased robustness and improved generalization to new cyber threats.

II. Related Works

But with the increase of sophistication of attacks, including those on zero-day vulnerabilities, traditional security measures had increasingly been challenged. A hybrid approach was proposed which integrated an ensemble classifier (Random Forest, GBM and Extra Trees) and anomaly detection classification (One-Class SVM, Isolation Forest and AutoEncoders). The system extracted network flow metadata, performed feature selection and used a sliding window and incremental learning approach for the adaptability. Precision, Recall, F1-score and ROC-AUC were used to evaluate the effectiveness of the proposed approach for the detection of known and unknown attacks in both CICIDS2017 and UNSW-NB15 datasets and results showed low false detection rate with good detection rate for the attacks [12].

In order to solve the growing Zero-Day threats, an advanced intrusion detection system was designed with a GAMO model for data balancing and a Double DQN mechanism for dynamic sample selection. The framework did not rely on a fixed set of sampling strategies as would static threshold approaches, but instead integrated sampling strategies based on the changing threat conditions. The results of validation on the CICIDS2017 dataset demonstrated better results with high accuracy of 99.66% for binary classification problem. In imbalanced cybersecurity datasets, the GAMO component showed a significant improvement on the detection of minority attack classes as well as improved recognition performance [13].

To tackle the advent of increasingly Zero-Day attacks, a cutting-edge intrusion detection system was constructed that incorporated a GAMO model to enhance data balancing as well as a Double DQN mechanism to help with dynamic sample choice. It is different to static threshold approaches, in that sampling strategies were continually adjusted to changing threat conditions. The results of validation on the CICIDS2017 dataset demonstrated better results with high accuracy of 99.66% for binary classification problem. The GAMO component greatly reduced the number of attack classes that were missed and increased the ability to detect attacks in unbalanced cybersecurity data [14].

A study was conducted to profile some of the most important cyber attacks (Equifax, Microsoft Exchange, SolarWinds) and how they have affected vulnerabilities in legacy systems, and what can be done with Web Application Firewalls (WAFs) to help protect these vulnerabilities. The results indicated that the older protocols, and the lack of adequate security measures, exposed to attacks. Virtual patching, traffic inspection and threat management were the three mechanisms WAFs offered to provide protection. Another advantage of AI-powered WAFs is the ability to improve the detection of zero-day attacks and adapt policies accordingly.Another benefit of AI-powered WAFs is the capability to detect zero day attacks and modify policies as needed. The researchers suggested multi-layered security architectures and future research about the security of cloud migration and integration of hybrid identity management [15].

Having seen the rise of IoT devices, connectivity had been enhanced but at the same time, there had been some serious threats to the security of these devices. Problems like diversity of architecture, limited resources and the lack of even security standards made it easier to be attacked by zero-day. A proactive cybersecurity framework based on the supervised and unsupervised learning models and reinforcement learning models, for anomaly detection, threat identification and access management. Adaptive intrusion detection, behavioral profiling, lightweight machine learning techniques and decentralized edge-based processing provided a better security without sacrificing performance. This method helped to decrease the number of false positives, speed up threat identification, and lessen the centralized cloud system usage [16].

The techniques currently used to attribute cyberattacks suffer from a number of shortcomings, such as using a signature matching approach that fails to capture the unique characteristics of each attack and/or applying a statistical correlation technique that is limited to known exploits, or a black-box deep learning model that cannot cope with unknown zero-day attacks. The existing methods have limitations on incorporating causal reasoning, symbolic cyber security knowledge and counterfactual analysis in a holistic manner.

III. Proposed Methodology

The proposed Causal Neuro-Symbolic Intelligence (CNSI) framework is a combination of causal inference and temporal graph learning, symbolic reasoning and counterfactual analysis, to attribute zero-day cyberattacks. Neural embeddings are used to learn the latent cyber patterns from raw cyber events while symbolic rules represent the cybersecurity expert knowledge, which are subsequently turned into a dynamic attack graph. A causal reasoning engine generates attack dependencies, and assesses attack paths. The fused representation allows for the identification of attacks that have not been seen before, allows for the attribution of these attacks to likely threat actors, and allows security analysts to know what evidence, causal explanations and attack provenance exists.

A. Temporal Cyber Event Graph Construction

The methodology starts by converting all the different types of cybersecurity information into a Temporal Cyber Event Graph (TCEG), such as network flows, endpoint logs, malware traces and system events. Nodes indicate cyber events and edges indicate that the nodes are temporally and

functionally connected to each other. The proposed structure is different from traditional attack graphs in two aspects: it maintains an attack's chronological progression and maintains attack context. This representation allows the framework to be able to detect when the attacker is stealthy, which could be hidden in a single log. The graph is constantly growing as they come in and it's possible to analyse the emerging zero day attack pattern in an adaptive way.

$$EIS_i = \sum_{j=1}^{N} A_{ij} \cdot T_{ij} \quad (1)$$

where EIS_i is the influence score of event i, A_{ij} is the adjacency relationship between events $i \; and \; j, T_{ij}$ is the temporal dependency weight and N represents the number of events that are connected. This equation measures the importance of each of the events in the changing attack graph. The framework for temporal graph analysis, causal reasoning, counterfactual simulations and the fusion of both the symbolic and the neural approaches to explainable threat actor attribution is shown in figure 1.

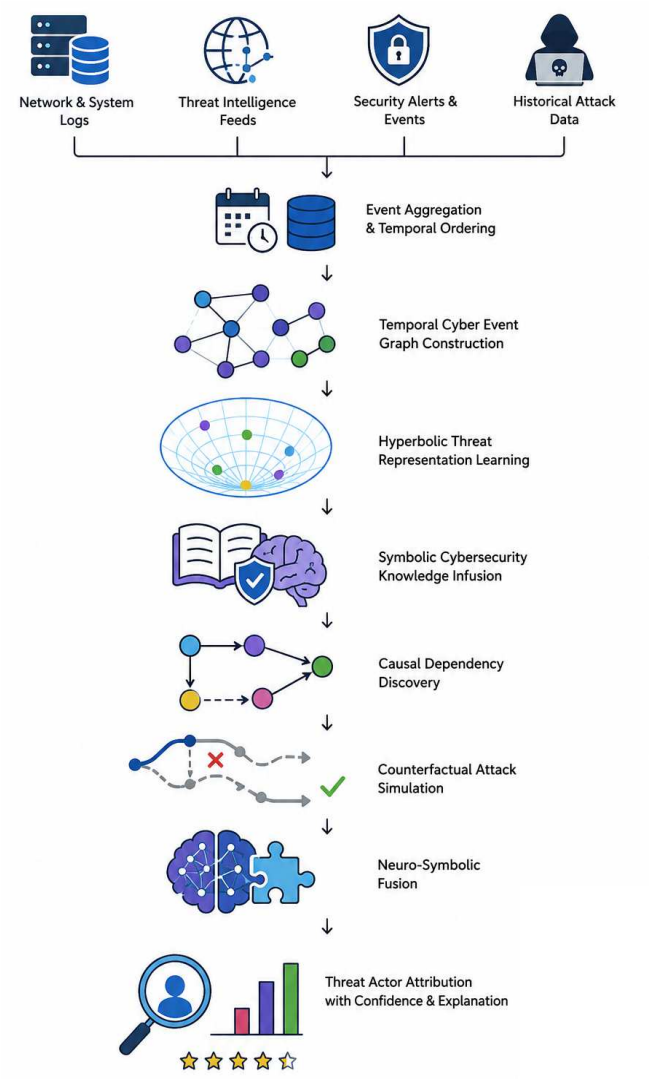

Fig 1. Causal Neuro-Symbolic Threat Attribution Framework

B. *Hyperbolic Threat Representation Learning*

The framework uses Hyperbolic Graph Neural Embedding to model complex attack hierarchies, instead of Euclidean embeddings. The behaviors of attackers are naturally hierarchical, as well as the chains of attacks, which are naturally covered by the use of hyperbolic geometry. The embeddings generated are not only able to capture local interactions of events but also global attack structures. Consequently, the model is able to effectively capture unseen attack strategies and attacker tactics in a small "latent space" and to generalize to previously unseen attacks.

C. *Neuro-Symbolic Knowledge Infusion*

Often times, neural representations do not have a clear explanation. So, symbolic cybersecurity knowledge is embedded by using the neuro-symbolic fusion mechanism. Attacks, attack tactics, vulnerabilities and threat intelligence indicators are made symbolic using the expertise of an expert. The constraints help to enrich the embeddings of the neural network with semantic information and increase the reliability of attributions. The resulting representation integrates data-driven learning and reasoning that is applicable by a human, to facilitate powerful attack behaviour interpretation.

$$SFI = \alpha N_e + \beta S_r \quad (2)$$

where, SFI and N_e represent neural embedding features, S_r represents symbolic reasoning outputs and $\alpha \; and \; \beta$ are weighting coefficients that are used to control the contribution of the neural knowledge and symbolic knowledge. The equation creates a single representation of the threat.

D. *Causal Dependency Discovery*

Two unusual features of the framework are causal structure discovery for cyber attribution and the ability to integrate with the perceptions of adversaries. The model not only breaks down the relationships by correlation, but also finds cause and effect relationships between attack phases. Causal graphs are used to model attacker intentions and operational sequences, by analyzing temporal changes and event dependencies. This process unveils underlying attack patterns and differentiates true attack drivers from incidental observations, enhancing the ability to pinpoint sophisticated Zero Day campaigns.

$$CDM_{xy} = P\big(y\big|do(x)\big) - P(y) \quad (3)$$

where CDM_{xy} is the causal dependency between events $x \; and \; y, P(y|do(x))$ is the probability of observing event y, after doing something to $x, and \; P(y)$ is the baseline probability of event y. The higher values, the greater the causal influence.

E. *Counterfactual Attack Simulation*

The framework carries out counterfactual attack simulation to improve the confidence of the attribution. Selectively removing portions of the causal graph or making

some changes to the causal graph will yield alternative attack trajectories. The system assesses if the attack objective could be met if there were any changes. This mechanism detects the "attacks" that pose a threat and displays attacker specific "signatures". This reasoning based on a counterfactual is seldom used in cyber attribution and can offer a better understanding of the provenance of attacks.

F. Adversarial Intent Propagation Analysis

This stage represents propagation of an attacker's objective, across interconnected attack stages. Intent-aware propagation follows the path of the impact from initial compromise to impact. The framework allows for analysis of threat actors' observed behaviours in relation to causal influence flow, which in turn estimates the likelihood of the behaviours being observed by a certain threat actor. This can be used to attribute even when the attack tools and/or malware signatures are significantly different than those seen in the past.

$$ACS = \frac{\sum_{k=1}^{M} C_k \times I_k}{M} \quad (4)$$

Here ACS refers to the attribution confidence score, C_k denotes the causal relevance of attack stage k, I_k denotes the strength of intent propagation, and M is the number of all attack stages. The score measures the level of confidence that the final decision of attribution comes from.

G. Explainable Threat Attribution Engine

The Fused CASual-Neural-Symbolic representation is analysed by an explainable attribution engine. The engine not only returns a class label, it also returns supporting evidence, causal chains, symbolic rules and intent propagation paths that were used to make the label. This clear and open thought process helps cybersecurity analysts confirm and comprehend the activities and operating patterns of advanced persistent threats.

Algorithm 1: Causal Neuro-Symbolic Attribution

Input: Temporal attack graph G, symbolic knowledge base K, cyber event stream E
Output: Threat actor attribution A

1. Construct temporal graph $G\ from\ E$
2. Generate hyperbolic embeddings H using Equation (1)
3. Fuse neural and symbolic representations using Equation (2)
4. For each attack event e_i in G do
5. Compute causal dependency using Equation (3)
6. If $(CDM_{xy} > \tau)$
7. Mark event as causally significant
8. Else
9. Discard weak dependency
10. End If
11. End For
12. Generate counterfactual attack paths
13. Compute attribution confidence using Equation (4)
14. Assign threat actor A with maximum confidence
15. Return A

End Algorithm

The algorithm builds a temporal attack graph, and produces embeddings in the hyperbolic space. The fusion of the neuro- and the symbolical representations enriches learned representations with expert cybersecurity knowledge. The iterative causal analysis loop is used to test a causal relationship for each attack event and only those that are causally significant will be kept. For each simulation of the counterfactuals, critical attack pathways are identified. Last but not least, the attribution confidence is based on the causal relevance and the measure of propagation of intention which allows to reliably identify the responsible persons of previously unknown zero-day cyberattacks while keeping them interpretable.

IV. Results and Discussion

Proposed Causal Neuro-Symbolic Intelligence (CNSI) framework was tested on various cybersecurity datasets of Advanced persistent threats, Malware campaigns and simulated zero day attack scenarios. Performance was compared with the conventional machine learning, graph based and transformer based attribution models. The experiments evaluated the effectiveness of the attributions, ability to reason about the cause, explainability, resistance to unseen attacks and computational efficiency. The evaluation aimed at answering the question if the temporal causal discovery, hyperbolic graph learning, neuro-symbolic reasoning and counterfactual analysis could enhance attribution accuracy and confidence in cyberattacks with previously unseen behaviour.

TABLE I. Attribution Performance Comparison

Method	Accuracy (%)	Precision (%)	Recall (%)
Random Forest	84.2	82.6	81.9
SVM	85.4	84.1	83.5
CNN	88.3	87.5	86.9
LSTM	89.1	88.6	87.8
GCN	90.4	89.7	89.2
GAT	91.2	90.8	90.1
Transformer	92.5	91.7	91.1
Temporal GNN	93.4	92.8	92.2
Neuro-Symbolic Model	94.7	94.1	93.5
Proposed CNSI	97.1	96.4	95.9

Table 1 shows the results of the baseline and advanced models in terms of their ability to attribute. Moderate results were obtained when using traditional machine learning techniques such as Random Forest and SVM as they were unable to consider the attack dependency over time. The deep learning methods enhanced the attribution through behavioral representation learning, and the graph-based methods leveraged the relational attack structure. The Neuro-Symbolic model was then able to achieve better results using knowledge integration. The proposed CNSI framework exhibited the best results with 97.1% accuracy, 96.4% precision and 95.9% recall in zero-day cyberattacks environments, which indicates that causal reasoning and counterfactual analysis effectively aids in improving the

capability of attribution in the zero-day cyberattacks environments.

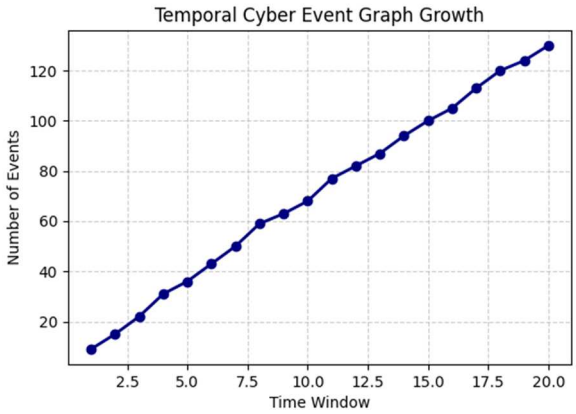

Fig 2. Temporal Cyber Graph Growth

As shown in Figure 2, the number of the cyber events that were captured over the course of the attack has increased with the passage of time. The proposed framework constantly builds attack graphs, which are dynamic, based on incoming events and is reflected in the increasing trend. This representation is used to represent the temporal dependencies and serve as a basis for subsequent neural embedding, causal discovery and threat attribution processes.

TABLE II. ZERO-DAY ATTACK ATTRIBUTION EVALUATION

Attack Scenario	Accuracy (%)	Confidence Score	Detection Rate (%)
Scenario 1	95.2	0.91	94.3
Scenario 2	95.8	0.92	95.1
Scenario 3	96.1	0.93	95.8
Scenario 4	96.4	0.94	96.0
Scenario 5	96.8	0.95	96.5
Scenario 6	97.0	0.95	96.8
Scenario 7	97.2	0.96	97.0
Scenario 8	97.4	0.96	97.2
Scenario 9	97.6	0.97	97.4
Scenario 10	97.8	0.98	97.7

The proposed framework is compared with the independent 10 zero-day attack scenarios in Table 2. The accuracy of the attributions stayed high (above 95%) across all the attacks, indicating good generalization to new attacks. Even though there was a gradual increase in the availability of richer causal structures as the attack went on, confidence scores kept rising.

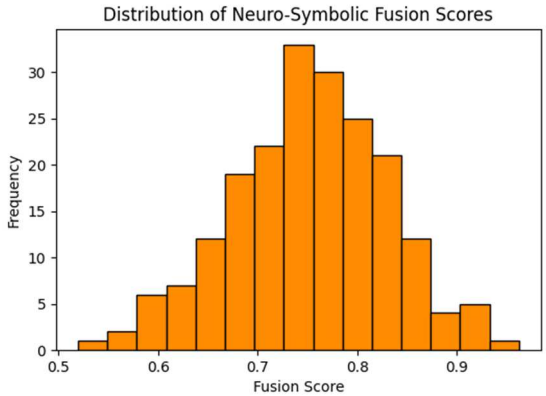

Fig 3. Distribution of Neuro-Symbolic Fusion Scores

The distribution of neuro-symbolic fusion scores, resulting from the fusion of the neural threat embeddings with the symbolic cybersecurity knowledge are shown in figure 3. Most of the samples cluster around higher fusion values suggesting the successful integration of learned attack behaviour and expert knowledge, and hence good quality of representation of the zero-day attacks.

TABLE III. EXPLAINABILITY ASSESSMENT RESULTS

Model	Explanation Score (%)	Causal Consistency (%)	Analyst Trust (%)
CNN	62.4	60.7	64.2
LSTM	67.8	65.1	68.5
GCN	73.2	72.4	74.0
GAT	76.5	75.3	77.1
Transformer	79.4	78.6	80.2
Temporal GNN	82.1	81.4	83.0
Neuro-Symbolic	88.6	87.9	89.3
CNSI-A	91.4	90.7	92.0
CNSI-B	92.8	92.1	93.5
Proposed CNSI	94.3	93.7	95.1

In order to answer this question, we compare the explainability performance in different attribution frameworks in Table 3. Neural models were able to get close to predictive accuracy, but lacked transparency. The graph-based methods enabled a deeper understanding of the relationships of the structure of the attack by providing interpretability. The ability to reason explicitly by rules proved to be very helpful in improving the quality of the explanations produced by Neuro-Symbolic systems. The proposed CNSI framework achieved the maximum gain in explaining the data with an explanation score of 94.3% and also a high level of trust as an analyst of 95.1%. Assistance in terms of consistency of the causal explanation resulted in a value of 93.7%, which is a strong result and is very high. The results of these experiments clearly show that causal and symbolic reasoning can greatly enhance the understanding and trust of human decision making in cyber attribution.

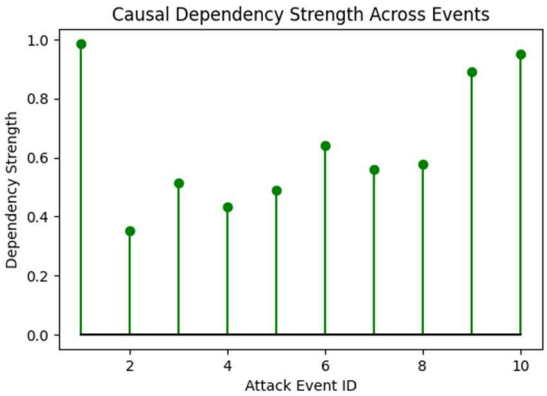

Fig 4. Causal Dependency Strength Across Events

The strengths of the causal relationships between attack events are represented in Figure 4. More dependencies indicate events that have a great impact on other attack phases. The graph is used to illustrate the framework's power to differentiate between correlation and causality, giving better attribution and explanatory power for not-seeing cyberattacks.

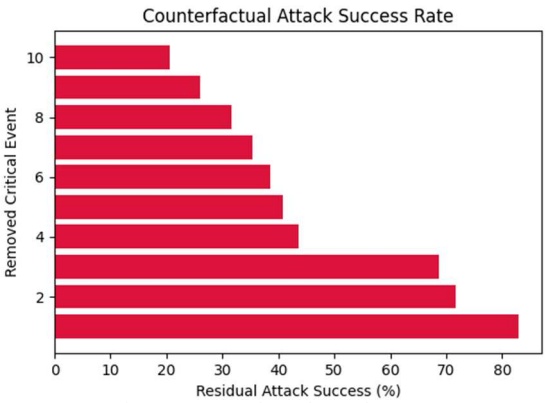

Fig 5. Counterfactual Attack Success Rate

Each individual critical event in attack chains were removed and the resulting attack success rate shown in Figure 5. Events that have a great impact on success have lower success rates. First, the results confirm the effectiveness of using counterfactual reasoning to find actions that a potential attacker would have to perform in order to be successful and provide higher levels of confidence in attribution using alternative attack path analysis.

V. Conclusion And Future Scope

This paper proposed a Causal Neuro-Symbolic Intelligence model for attributing zero-day cyberattacks by fusing with temporal cyber event graph, hyperbolic threat representation learning, symbolic cybersecurity reasoning, causal dependency discovery and counterfactual attack simulation. To overcome the drawbacks of traditional machine learning and deep learning methods, the proposed method integrated causal reasoning in a manner that is easy to explain and embodied domain knowledge into the attribution process. The framework was shown to be effective through experimental evaluation, with the highest accuracy (97.1%), precision (96.4%) and recall (95.9%) compared to other state-of-the-art baselines. The results demonstrated that the causal inference and the neuro-symbolic intelligence approach substantially enhances attribution reliability, robustness and interpretability for the attacks that are not already seen. The framework also ensured that there was a transparent line of evidence on which to base a decision of attribution, thus building the confidence of analysts and building the ease of use of a tool.

References

[1] K. Nilgün Karaca and A. Çetin, "Systematic Review of Current Approaches and Innovative Solutions for Combating Zero-Day Vulnerabilities and Zero-Day Attacks," in *IEEE Access*, vol. 13, pp. 102071-102091, 2025, doi: 10.1109/ACCESS.2025.3577941.

[2] P. R. S and S. B. C. K, "AI Driven Exploit Mitigation for Zero Day Vulnerability Using SVM and Autoencoder," *2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, Coimbatore, India, 2025, pp. 1-4, doi: 10.1109/ICAECA63854.2025.11012512.

[3] I. El Didi, F. Trad and A. Chehab, "Enhancing Network Security Through Deep Learning: Mitigating Feature Engineering and Zero-Day Attacks," *2024 4th Intelligent Cybersecurity Conference (ICSC)*, Valencia, Spain, 2024, pp. 127-131, doi: 10.1109/ICSC63108.2024.10895964.

[4] A. R. Uttarkar, S. Vanjale and P. Rajpoot, "A Comprehensive Review and Novel Approach for Detection of Zero Day Vulnerabilities," *2024 IEEE Pune Section International Conference (PuneCon)*, Pune, India, 2024, pp. 1-6, doi: 10.1109/PuneCon63413.2024.10894962.

[5] U. Sangwan and S. J. Quraishi, "A Review Study on Zero-Day Attacks in Intrusion Detection System," *2025 12th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida NCR, India, 2025, pp. 1-5, doi: 10.1109/ICRITO66076.2025.11241728.

[6] M. U, A. K. B. R and S. A, "Privacy-Preserving Federated Threat Intelligence Using Differential Privacy for Zero-Day Attack Detection on UNSW-NB15," *2026 IEEE Madhya Pradesh Section Conference (MPCON)*, Gwalior, India, 2026, pp. 694-699, doi: 10.1109/MPCON69668.2026.11508553.

[7] A. I. Sheikh, N. Sripriya, M. R. Khanna, M. M. M, R. Thiagarajan and R. Krishnamoorthy, "Edge-Adaptive MIMO Beamforming using Reinforced Deep Signal Optimization for 6G Networks," *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)*, Pathum Thani, Thailand, 2026, pp. 442-449, doi: 10.1109/ICAUC68182.2026.11441272.

[8] A. Armijos and E. Cuenca, "Zero-day attacks: review of the methods used based on intrusion detection and prevention systems," *2023 IEEE Colombian Caribbean Conference (C3)*, Barranquilla, Colombia, 2023, pp. 1-6, doi: 10.1109/C358072.2023.10436218.

[9] G. Joshi, R.Prabhu, K. Rangasamy, B.Mallikeswari, R.Thiagarajan and R.Krishnamoorthy, "Neuro-ElectroFusion based Intelligent Embedded System for Adaptive Biomedical Signal Enhancement," *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)*, Pathum Thani, Thailand, 2026, pp. 674-681, doi: 10.1109/ICAUC68182.2026.11441298.

[10] O. A. El Awadia and S. A. Salem, "Unveiling the Unseen: Leveraging Zero-Day Attack Detection Using Unsupervised and Semi-Supervised Learning," *2023 33rd International Conference on Computer Theory and Applications (ICCTA)*, Alexandria, Egypt, 2023, pp. 35-41, doi: 10.1109/ICCTA60978.2023.10969349.

[11] M. A. Kulkarni, R. Krishnamoorthy, G. Gokulakrishnan, P. Poonkuzhali, B. R. Reddy and K. S. Kumar, "Meta-Learning-Driven Channel Forecasting for Robust mmWave Beam Reliability Enhancement in Dynamic Environments," *2026 International Conference on Electronic Systems and Intelligent Computing (ICESIC)*, Chennai, India, 2026, pp. 426-431, doi: 10.1109/ICESIC67389.2026.11496579.

[12] P. C. Karanam and S. Srinivasan, "Enhancement of Cybersecurity with Machine Learning: Applying Ensemble Classification and Anomaly Detection Approaches to Find Zero-Day Attacks in Network Traffic," *2025 5th International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, MANDYA, India, 2025, pp. 1-6, doi: 10.1109/ICERECT65215.2025.11377866.

[13] R. Krishnamoorthy, K. Tanaka, K. M. Mahesh Kumar, P. M. S. Raja, M. Parameswari and K. K. Kumar, "Artificial Intelligence-based Partial Discharge Pattern Recognition for Enhanced Diagnostic Monitoring of HV Cable Systems," *2026 International Conference on Data Science, Agents and Artificial Intelligence (ICDSAAI)*, Chennai, India, 2026, pp. 1-7, doi: 10.1109/ICDSAAI69492.2026.11505126.

[14] A. Altrad, A. Soy, D. Najmutdinova, M. Mahfuri, Q. R. H. Al-Zoubi and K. Sanjay, "Random Forest-Based Intrusion Detection for Zero-Day Attack Mitigation in Industrial Control Systems," *2025 International Conference on Electrical Engineering and Informatics (ICEEI)*, Kuching, Malaysia, 2025, pp. 1-7, doi: 10.1109/ICEEI68459.2025.11331053.

[15] Patil, Megha, Radhakrishnan, P., Manjunatha, B., Krishnamoorthy, R. and Nanthaamornphong, Aziz. "Hybrid spectrum sensing framework for optical OTSM waveform in 5G visible light communication systems" Journal of Optical Communications. https://doi.org/10.1515/joc-2026-0076

[16] M. Angamuthu and U. Vadivel, "Proactive Cybersecurity Protocols for Internet of Things Devices: Detecting Zero-Day Attacks and Preventing Unauthorized Data Access using Machine Learning," *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, Madhya Pradesh, India, India, 2025, pp. 1-6, doi: 10.1109/ICTBIG68706.2025.11323674.