Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Causal AI for Predictive Cybersecurity Threat Intelligence

[1]Hamza Afzal, [2]Muhammad Ghufran
[1]Software engineer American Technology group LLC Baltimore Maryland
hafzal.student@wust.edu
[2]Data Analyst CarniTech Sterling Virginia
ghufranqureshi28@gmail.com

ARTICLE INFO

Received: 10 Jan 2025

Revised: 01 March 2025

Accepted: 18 March 2025

ABSTRACT

The rapid evolution of cyber threats makes it necessary to adopt smart and reliable cybersecurity solutions that able to detect threats and prevent them in advance. The traditional cybersecurity approaches include mainly the correlation-based algorithms that create correlations between certain events and statistic data in the past but do not reveal any reason for a particular cyber-attack. The idea of the causal AI provides a new approach that is based on researching causations in the complicated cybersecurity environment. With the help of causal inference methods like causal graphs, counterfactuals, and Structural Causal Models (SCMs), it becomes possible to reveal causality of the cyber incidents that occur due to certain weaknesses, behavior, and actions of attackers. Furthermore, the adoption of causal AI facilitates cyber-attack detection, risk evaluation, and prediction of cascades triggered by cybersecurity problems. The implementation of the causal AI also enhances the capability of conducting threat intelligence analysis using scenario-based evaluation. There are several challenges to be aware of when developing a causal AI system including data quality issues, scalability concerns, problems with interpretation of models, and integrability with other cybersecurity modules.

Keywords: Causal AI, Cyber Threat Intelligence, Predictive Cybersecurity, Causal Inference, Counterfactual Reasoning, Structural Causal Models, Threat Prediction

I. INTRODUCTION

Cybersecurity has become a major necessity in the current digitized world, whereby there is heavy reliance on cloud computing technology, internet of Things, and large-scale network usage [1][2]. With rapid digitization, the volume of sensitive data generated, transmitted, and stored has increased significantly, resulting in increased vulnerability of systems to cyber threats. Information security in terms of confidentiality, integrity, and availability is now an issue that requires guarantees in the current scenario [3]. Nevertheless, in light of the complexity involved in today's highly integrated systems, managing cybersecurity has become quite challenging, requiring advanced methods to address these threats.

As the cybersecurity framework expands, the character of cyberattacks becomes more complex than ever. For instance, today's cyberattacks such as ransomware attacks, phishing attacks, zero-day attacks, and advanced persistent threats have become highly coordinated and adaptable, using vulnerabilities, spreading through interconnected networks, and remaining undetected for a long period of time [4]. Security measures relying on traditional methodologies involving signature-based and correlation-based techniques in machine learning algorithms have failed to tackle modern cyberattacks [5]. They do not provide any predictive value when it comes to anticipating cyberattack trends because of their limited explanatory value.

In order to tackle these issues, there is a growing need for using advanced and predictive solutions in threat intelligence that would enable them to identify deeper dependencies in the context of security data [6]. In this regard, causal artificial intelligence becomes a new solution that is oriented towards transforming the existing research efforts from

Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

correlation to causality [7]. Unlike existing solutions, causal artificial intelligence is grounded on the concept of causal graphs and Structural Causal Models (SCM), which enables detecting dependencies in cyberattacks, and, hence, their mechanisms of functioning [8][9]. Apart from identifying attacks, causal artificial intelligence enables predicting future changes in attack vectors and propagation of attacks through a network. Moreover, Causal AI significantly expands possibilities for cybersecurity through its ability to provide timely detection of threats, pinpoint key vulnerabilities, model attack propagation, and conduct counterfactual analyses to estimate preventive measures' effectiveness.

A. Structure of the Paper

The structure of this paper is as follows: Section II covers cyber threat intelligence and conventional cybersecurity methods based on correlation. Section III introduces causality-based Artificial Intelligence. Section IV focuses on applications and challenges in applying causal AI to cybersecurity problems. Section V contains a literature review and research gap analysis. The final section, Section VI, offers concluding remarks.

II. CONCEPT OF CAUSAL AI IN CYBERSECURITY THREAT INTELLIGENCE

Cyber Threat Intelligence (CTI) could be defined as an exercise aimed at gathering and analyzing a number of aspects associated with cyberattacks in order to figure out the manner in which they happen and their implications. CTI allows organizations to predict and prevent attacks. CTI is also known as threat intelligence, and its aim is to warn organizations about attacks using information collected and analyzed. The following factors cause data breaches: malware, insider threat, social engineering, compromised credentials, software defects, improper configurations, and human faults [10].Threat intelligence is one of the advancements in the approach towards securing the data, files, and infrastructure from any harm. With increasing sophistication in cyber-attacks, there is also an advancement in the approach to acquiring information from different sources to secure the resources of an organization. Threat intelligence plays a great role in mitigating cyberattacks.

A. Types of Threat Intelligence

Cyber Threat Intelligence (CTI) can be described as a complex concept, which can be broadly classified into four types: strategic, tactical, operational, and technical. Every type has a different objective in enhancing the cybersecurity of an organization.

1) Strategic Intelligence

Strategic intelligence gives a general idea about the threat environment, making it possible for an organization to be able to make wise decisions with respect to its operations and cybersecurity plans [11]. Strategic intelligence looks at things like:

- AI-enabled cybercrime
- The increasing prevalence of ransomware attacks targeting specific industries
- Cyber threats originating from nation-states or malicious entities

The use of strategic intelligence is most helpful to CISOs and corporate executives because it enables them to determine if the cybersecurity expenditures are appropriately spent to manage new risks.

2) Tactical Intelligence

Tactical intelligence provides details on the TTPs used by threat actors. The main focus of tactical intelligence is on security architects and cybersecurity program managers who wish to get knowledge about certain threat actors, and also on which controls are useful for defending against them [12]. If a particular threat actor uses MFA fatigue attacks rather than phishing attempts to gain credentials, such knowledge becomes very important for preventing these attacks.

3) Operational Intelligence

Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Operational intelligence offers timely information on current threat trends and cyber campaigns. The SOC team is dependent on operational intelligence to detect the actions taken by the attackers and mitigate these actions before the attackers can accomplish their goals.

B. Traditional Correlation-Based Cybersecurity Approaches

Event correlation is the method used to establish connections among security events. It creates a context between individual events and the real-time information gathered earlier while ensuring normalization of data in preparation for analysis. The purpose of alert correlation is to establish important events from security-related data through improved information quality and reduction of redundancies.

Figure 1 demonstrates that events are created based on monitoring system behavior; on the other hand, alerts/Security Events are created due to the detection of any suspicious behavior or activity such as one-step attack or multi-step attack. The Security Event correlation process assists in recognizing connections between alerts, which may be categorized as meta events/hyper alerts [13].

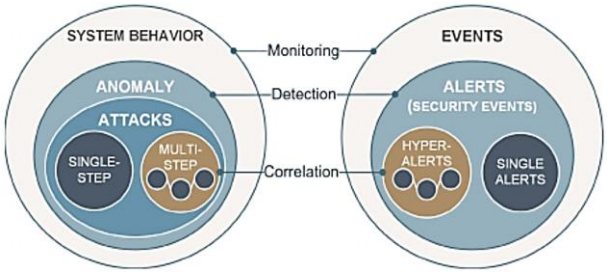

Fig. 1. Role of correlation in security event management.

Traditional correlation-based methodologies for ensuring cybersecurity have been widely applied in Security Information and Event Management (SIEM) tools where various security events from disparate sources like firewalls, IDS/IPS, endpoint devices, and servers have been collected and correlated for improved visibility of potential threats and aid security experts in identifying sophisticated attack sequences that may otherwise remain undetectable on an individual basis.

C. Limitations of Existing Predictive Security Models

Predictive security mechanisms that are currently available have shown great utility in identifying cyber-attacks and predicting risks because of their historical analysis capability [14]. However, there are several limitations associated with such predictive mechanisms that make them ineffective against complex cyber-attacks.

- **High False Positives:** Many predictive algorithms generate lots of false alarms. This creates alert fatigue and reduces efficiency.
- **Limited Adaptability:** The traditional approach might not be sufficient to deal with changing threats.
- **Dependence on Historical Data:** A majority of the strategies are highly dependent on historical attacks, making them very ineffective in dealing with any new threat.
- **Scalability Issues:** The handling of real-time and large cybersecurity data could present performance problems.
- **Data Quality Challenges:** Prediction accuracy can be negatively affected by data that is incomplete, noisy, or imbalanced.
- **Lack of Contextual Awareness:** Current models may miss out on contextual threat intelligence, which can make it hard for the accurate prioritization of threats and decision-making.

III. CAUSAL AI TECHNIQUES FOR PREDICTIVE CYBERSECURITY THREAT INTELLIGENCE

Causal AI is one part of artificial intelligence that specializes in studying cause and effect relations rather than recognizing patterns or correlations performed by other machine learning methods. By using causal AI, it is easy for

Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

users to boost the validity and reliability of the AI algorithms, particularly for real-world uses such as healthcare and economics where situations become highly complex. The concept of causal inference is at the heart of Causal AI. With causal inference, the system can determine whether or not a certain cybersecurity aspect is a contributing factor in the occurrence of an attack. Unlike pattern recognition, where observations are made, causal inference measures the effects of changes in one variable on another. The elements of causal reasoning include:

- **Observational Analysis:** Analyzes past cybersecurity logs and incidents to look for patterns among attacks, vulnerabilities, and system behavior.
- **Interventional Analysis:** Considers the effects of security measures like deploying patches, making changes to the firewall, or implementing access controls.
- **Counterfactual Analysis:** Examines theoretical situations for determining what effect alternate decisions might have on cybersecurity.

A. Correlation vs Causation in Cybersecurity

The difference between correlation and causation is an important factor in cybersecurity prediction analysis. Cyber security models have been based on correlation analysis where correlation of events is established through their dependency. The correlation of events does not imply causation.

- Correlation can be defined as a statistical relation between two variables. For instance, there is usually an observed correlation between high traffic and malware within firms. However, this observation does not prove that high traffic results in malware attacks.
- Causation, on the other hand, involves establishing a cause-and-effect link between variables. In cybersecurity, causal relationships are required for understanding how vulnerabilities and attack behaviors contribute to security events.

The main differences between correlation and causation in cybersecurity can be seen in Table I below:

TABLE I. COMPARATIVE ANALYSIS OF CORRELATION AND CAUSATION IN CYBERSECURITY THREAT INTELLIGENCE

Aspect	Correlation-Based Analysis	Causation-Based Analysis
Primary Objective	Detects co-occurring patterns and relationships in cybersecurity datasets.	Explains the underlying cause-and-effect mechanisms behind cyber incidents.
Interpretation	Indicates that variables occur together but does not explain why.	Explains why a cybersecurity event occurs and identifies contributing factors.
Decision-Making Capability	Supports anomaly detection but may lead to misleading conclusions.	Enables informed intervention strategies and proactive defense planning.

Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Prediction Accuracy	Often affected by spurious relationships and false-positive alerts.	Produces more reliable and explainable cybersecurity threat predictions.
Explainability	Limited interpretability due to dependence on statistical patterns.	High interpretability through transparent causal reasoning.
Use in Threat Intelligence	Primarily used in traditional machine learning and SIEM alert systems.	Applied in predictive cyber threat intelligence, root cause analysis, and attack forecasting.

B. Counterfactual Reasoning for Threat Prediction

Counterfactual reasoning is an important characteristic of Causal AI and plays a critical role in predictive cybersecurity through hypothesis testing. Counterfactual reasoning allows for assessing other possible outcomes through studying the impact that various decisions would have had on cybersecurity events. Unlike traditional predictive algorithms based on past observations, counterfactual reasoning helps understand what might have happened under different circumstances and contributes to proactive threat intelligence [15].In the field of cybersecurity, counterfactual reasoning helps companies analyze various security scenarios. A discussion can be initiated about how early patching for vulnerabilities, immediate blocking of suspicious logins, and quick detection of ransomware could have limited the damage caused by these cyber-attacks. In this manner, the organization gets predictive insights into its potential vulnerabilities before these are exploited by attackers.

Major applications of counterfactual analysis in predictive cybersecurity include:

1) Threat Prevention

Counterfactual models assist in evaluating the possible impact that can be created by preventive security strategies on the mitigation of the risk of cyber threats. The findings that emerge through such evaluations assist firms in adopting adequate cybersecurity solutions before such threats materialize.

2) Incident Response Optimization

The cybersecurity professionals might evaluate other ways of dealing with such issues to determine if they can mitigate the effects of the attack [16]. This enables businesses to improve their strategy for response planning.

3) Cyber Risk Assessment

The organization can conduct various experiments of cyber-attacks to determine how effective certain security parameters in the future. The benefits of applying counterfactual reasoning in the field of cybersecurity include the following:

- Predictive cyber threat intelligence improvement.
- Improvement of proactive security planning and mitigation techniques.
- Forensic analysis improvement after an attack.
- Evaluation of the intervention's success in cybersecurity.

Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Improved decision-making processes for threat response adaptation.

Counterfactual analysis helps improve cybersecurity by making it easier for these systems to transition from reacting to threat alerts to becoming proactive and predictive in nature.

C. Causal Graphs and Structural Causal Models

The approach of using causal graphs and SCM is seen as a useful one when it comes to representing and analyzing causality in the domain of cybersecurity. In comparison to traditional statistical techniques that mainly concentrate on correlations, causal models aid in understanding the impact of the variables related to cybersecurity on each other. A causal graph can be illustrated using a Directed Acyclic Graph (DAG). The structure includes nodes and edges indicating causal dependencies between cybersecurity variables such as authentication activity, network anomalies, vulnerabilities, malicious behaviors, and reaction of the system [17].

Figure 2 demonstrates three basic causal configurations, including: (a) common effect, in which both X and Y affect Z; (b) common cause, in which Z is causally related to both X and Y; and (c) chain (mediation), where X affects Z, which in turn affects Y.

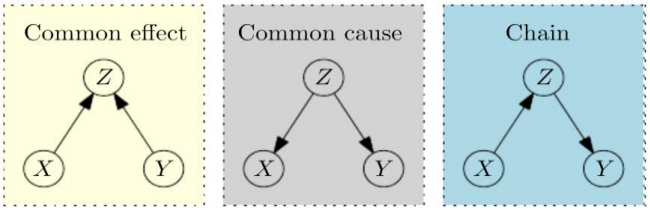

Fig. 2. Common types of structural causal models represented as DAGS

SCMs are an extension of causal graphs in that they offer a mathematical representation of relationships between different variables as well as the impact of any change in one variable on other variables [18]. They usually differentiate between two types of variables; internal system-related factors called endogenous variables and outside factors affecting cybersecurity systems referred to as exogenous variables. Furthermore, SCMs help increase transparency and interpretability of cybersecurity analytics in the sense that they reason about threats.

D. Predictive Modeling of Cyber Threats using Causal AI

Cyber threat prediction using Causal AI is a modern form of cybersecurity threat intelligence. Machine learning techniques for cyber threat prediction mainly depend upon past attack data and statistical analysis to predict the threats. Such techniques can face difficulties in dealing with the constantly changing cyber environment since they cannot provide information regarding the cause of the attacks.

The use of causal reasoning makes Causal AI an effective tool for enhancing predictive modeling in cybersecurity. The cybersecurity threat prediction process through Causal AI involves the following steps:

1) Cybersecurity Data Collection

The data collection stage entails gathering information related to cybersecurity from various sources including system logs, traffic analysis, vulnerabilities, incidents, among others. Such gathered data forms the basis for the detection of cybersecurity threats and attacks.

2) Causal Relationship Discovery

In this phase, cause-and-effect relations in cybersecurity variables are revealed using causal AI technologies. This allows one to analyze how the vulnerabilities, malicious behaviors, and system abnormalities cause cyberattacks.

3) Counterfactual Analysis

The counterfactual analysis involves studying the possibilities by examining how an alternative action on cybersecurity would affect the outcome of the threat.

4) Threat Forecasting

Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In the final stage it's all about anticipating tomorrow's cyber threats using those causal relationships plus behavioral patterns that have been observed. This then allows the orgs to reinforce their cybersecurity defenses, and to get better at being ready for threats.

IV. APPLICATIONS AND CHALLENGES OF CAUSAL AI IN CYBERSECURITY

Causal AI in cybersecurity kind of enables real-world uses like attack prediction , vulnerability analysis , cascading failure modeling, threat intelligence, and even risk prioritization, it also boosts detection accuracy and decision making, and somehow it helps with integration into existing security systems.

- **Predicting Cyber-Attacks and Vulnerabilities:** Causal AI helps with cyber-attack prediction by finding cause and effect links between vulnerability networks, network anomalies, authentication failures, and suspicious activity, kind of malicious behaviour. With causal graphs plus Structural Causal Models (SCMs) it can produce more reliable threat forecasting, and also sort the most critical weaknesses, then run counterfactual analysis to see what would happen if a preventive action is taken, in order to back proactive cybersecurity defense.

- **Cascading Effects of Cyber-Attacks:** The use of causal AI assists in the creation of models that explain the process by which cyber-attacks occur through interlinked networks. Through the application of causal graphs and SCMs, it is able to reveal attack propagation paths including privilege escalation and lateral movement despite any lack of obvious dependency factors. Intervention analysis is also made possible through causal AI.

- **Identification of High-Risk Targets:** Causal AI identifies the risky components by examining the relationships between vulnerabilities, users' activities, precise configurations of the system, and attack patterns that repeat. In simple words, this kind of approach makes it possible for businesses to identify which crucial components should be protected first. In this regard, businesses tend to become more effective with their protection efforts and eventually minimize their risks of cyberattacks.

- **Proactive Threat Intelligence Systems:** Proactive threat intelligence is made more efficient through the use of causal AI as it identifies certain causalities present in cybersecurity data. As the system analyzes various threat indicators and anomalies in addition to the behavior of the attacker, proactive measures such as risk forecasts and decision-making become easier.

- **Integration with Existing Cybersecurity Infrastructure:** Causal AI enhances existing cybersecurity architectures through the addition of conventional machine learning and rule-based methods. This technology helps provide explanations regarding attacks and vulnerabilities, which is useful for monitoring, managing incidents, and handling vulnerabilities, thus increasing efficiency.

A. Key Challenges in Real-World Deployment of Causal AI

There are many difficulties associated with the use of causal AI within the sphere of cybersecurity. This difficulty stems from the nature of cyber environments along with the availability of incomplete and noisy data.

- **Complexity of Cyber Environments:** Causal AI has difficulties modeling highly dynamic and interrelated cyber systems where the relationships between events change continually.

- **Data Quality and Availability Issues:** Insufficient, imprecise, and disorganized cybersecurity information restricts the precision of causal inference and modeling.

- **Scalability and Performance Limitations:** Application of the causality model in large-scale networks and real-time systems is a computationally intensive process.

- **Integration with Existing Systems:** The integration of causal AI and conventional rule-based or machine-learning cybersecurity solutions is often complicated and challenging.

- **Real-Time Processing Constraints:** Rapidly developing cyber threats demand an immediate reaction, which cannot be effectively provided by causal reasoning systems.

Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Interpretability and Reliability Concerns:** Causal AI is more interpretable than black-box AI systems, making it problematic to make consistent and reliable decisions within high-stakes situations.

A digital twin is considered a live view of a real-world system that monitors the state of its entities. Deeply, it is an environment that consists of a virtual and a physical machine. Each machine (model) is represented as a simulation, a mirror, or a twin of the other. So, the digital twin can list the life cycle of the physical entity which can be a human, an object, or a process [68]. Each digital twin is connected to its counterpart by a unique key, a relationship between two entities can be established [48].

A digital twin is a partition of a Cyber-Physical System (CPS), which is a set of physical systems connected to virtual cyberspace through the network [11, 49]. The communication between a physical entity and its digital twin can be represented directly by physical con-connections or indirectly via a cloud system. Also, it can be a seamless connection and con-continuous data exchange [26, 88]

V. LITERATURE REVIEW

The current studies focus on artificial intelligence-based cybersecurity, threat intelligence, anomaly detection, and causal inference. It can be seen that there is a need for more research on incorporating explainable causal reasoning into threat intelligence analysis.

S. Ramakrishna (2024) introduces an intelligence paradigm based on prediction and causality for cloud-native enterprise systems that includes AI and ML-based capabilities for interoperability, root cause analysis, and optimization. This paradigm utilizes predictive analytics, causal reasoning, and intelligent observability to manage and automate decisions in systems. Based on architectural analysis and principles of domain-driven design, the paper shows how resilient, explainable, and optimized cloud-native operations are possible for enterprises. The new paradigm presented is relevant to next-generation enterprise platforms spanning various domains including financial, healthcare, and digital systems [19].

R. Kushwaha and S. Patil (2024) discuss the present-day state of AI-powered systems for threat intelligence, emphasizing their ability to detect patterns, predict potential vectors of attack, recognize anomalies, and produce alerts. The research explores the development of threat intelligence platforms, the use of artificial intelligence in threat detection/response, and the effectiveness of predictive analytics approaches like supervised learning, clustering, neural network models, and probability theory-based analytics. The paper also discusses some of the difficulties with regard to predictive threat analysis and applications of AI in cybersecurity. These difficulties include those related to poor-quality data, adversarial use of data, automation bias, poor interpretability of models, and inadequate measures of evaluating machine learning models. Overall, the importance of AI-enhanced threat intelligence solutions grows rapidly within modern cybersecurity environment, and predictive analytics plays an important role in designing robust cyber defense systems [20].

D. Levshun and I. Kotenko (2023) describe the systematization of models for security events correlation, taking into account the form of representation of such models in AI-based event monitoring systems: rule-based, semantic, graphical and machine-learning-based. The authors give the most important trends in research on the problem of security events correlation using AI-based technologies and discuss the approaches to correlation of both single events and series of events within the scenario of an attack. The possibility of hybrid correlation models is also analyzed. The conclusion describes existing problems and possible ways to solve them [21].

B. Samuel (2023) offers an extensive analysis of AI-based cyber threat detection and mitigation, covering the basics of the technology, system design, detection process, response methods, adversarial issues, ethical concerns, and future

Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

research areas. It emphasizes the importance of intelligent security systems in building more resilient networks and adopting proactive security measures [22].

Z. Jadidi, J. Hagemann, and D. Quevedo (2022) present a solution that detects the causal impact of attacks by investigating causal dependencies in ICS logs. The ICS causal anomaly detection (ICS-CAD) method consists of two phases. It initially detects attacks and identifies the ICS device generating the malicious traffic. Secondly, it analyzes causal relationships between ICS logs to diagnose the attacker's future effect. They use a causal decomposition method to discover causality relationships in ICS logs. The performance of the ICS-CAD is evaluated using two datasets collected in real-world ICS networks. The ICS-CAD provides 98% accuracy in detecting attacks and the causal impact of the detected attacks [23].

S. Sultana et al., (2022) evaluate AI technology as it improves cybersecurity elements by studying its deployment within enterprise security systems. Machine learning, deep learning, and natural language processing functions in AI technologies create autonomous systems that proactively identify security threats to prevent them. Problem prevention systems that use AI capabilities enable threat detection through pattern recognition, recasting, and time, as well as reduction in response. The research explains the benefits alongside technological difficulties and practical implementations of artificial intelligence for threat monitoring within contemporary cybersecurity designs [24].

Table II below shows some of the most significant studies that were done and their results, shortcomings, and recommendations, highlighting the fact that causality is absent in explainability, predictive intelligence, and proactive cybersecurity methods

TABLE II. RESEARCH GAP ANALYSIS OF EXISTING LITERATURE ON CAUSAL AI FOR THREAT INTELLIGENCE

Reference	Study on	Key Findings	Limitations	Recommendations
S. Ramakrishna (2024)	Predictive and causal intelligence for cloud-native enterprise platforms	Proposed an AI/ML-based framework combining predictive analytics, causal inference, and observability for proactive management and optimized operations.	Focuses on enterprise systems rather than cybersecurity threat intelligence; lacks cyberattack-specific validation.	Adapt causal intelligence frameworks for predictive cybersecurity and real-time threat management.
R. Kushwaha & S. Patil (2024)	AI-based threat intelligence systems	Showed AI methods improve anomaly detection, attack prediction, and adaptive cyber defense.	Mostly correlation-based models; limited causal explainability and standardization.	Develop hybrid causal AI-based threat intelligence systems for explainable and accurate predictions.
D. Levshun & I. Kotenko (2023)	AI-based security event correlation models	Systematized rule-based, semantic, graphical, and ML event correlation techniques.	Limited focus on causal inference and proactive attack prediction.	Explore causal event correlation models for predicting attack origins and impacts.
B. Samuel (2023)	AI-driven cyber threat detection and response	Highlighted AI's role in resilience, automated response, and proactive cybersecurity.	Focuses more on detection than causal reasoning and explainability.	Integrate causal AI for root-cause analysis and predictive threat intelligence.
Z. Jadidi, J. Hagemann & D. Quevedo (2022)	Causal anomaly detection in ICS	Proposed ICS-CAD achieving 98% accuracy in attack detection and impact diagnosis.	Limited to ICS environments and lacks broader cybersecurity applicability.	Extend causal detection methods to enterprise and network cybersecurity systems.

Research Article

S. Sultana et al. (2022)	AI in enterprise cybersecurity systems	Demonstrated AI's effectiveness in proactive threat detection and faster response.	Limited emphasis on causal relationships and explainability.	Develop causal AI-enabled cybersecurity frameworks for transparent threat prediction.

VI. CONCLUSION AND FUTURE WORK

The introduction of causal AI in cybersecurity would result in a paradigm shift since the new technology allows moving from correlation analysis to causality-oriented analysis. The introduction of this innovation would help to increase the level of understanding not only of potential attacks but also their causes which could lead to the improvement in threat prediction capabilities. In this respect, the use of causality inference, counterfactuals, and modeling could be used in cybersecurity solutions to allow them to predict attackers' actions, identify vulnerabilities in a particular IT infrastructure, and estimate the effect of potential interventions. While this technology holds many possibilities, it still faces a number of implementation issues. The first one refers to obtaining high-quality data. On the other hand, the computational capacity required for real-time analysis of large volumes of network data must be taken into consideration. Also, it is difficult to integrate causal analysis into the existing technologies (such as SIEM) since the current ones cannot take full advantage of causal reasoning. Thus, further investigation of automated causality detection, real-time causality processing, and application of causal AI to digital twins could facilitate cyber defense processes. Causal-based approaches to cybersecurity can be seen as a promising path towards developing resilience and adaptability in threat intelligence frameworks.

REFERENCES

[1] S. Chatterjee and S. K. Malaraju, "The Role of a Highly Monitored Repository for Storing Architectures and Build Documents in the NERC Environment," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 11, no. 2, Apr. 2023, doi: 10.37082/IJIRMPS.v11.i2.232146.

[2] R. K. Gadiraju, "Cloud-Native AI Platforms for Scalable Enterprise Machine Learning: Architecture, Challenges, and Best Practices," *Int. J. Intell. Syst. Appl. Eng.*, vol. 9, no. 4, pp. 481–492, Oct. 2021, doi: 10.17762/ijisae.v9i4.8119.

[3] M. Kari, "Deep Learning-Based Fault Prediction Models for Enhanced Network Security Monitoring," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, p. 492, Jun. 2023, doi: 10.48175/IJARSCT-11600I.

[4] C. S. Kubam, "Agentic AI Microservice Framework for Deepfake and Document Fraud Detection in KYC Pipelines," *J. Inf. Syst. Eng. Manag.*, vol. 9, no. 1–12, 2024, doi: 10.5281/zenodo.18009551.

[5] G. C. Kakaraparthi, "Building a GenAI-Powered Advanced Code Generation Assistant Integrated with CI/CD Pipelines," *TIJER – Int. Res. J.*, vol. 9, no. 2, 2022.

[6] Guru Charan Kakaraparthi, "A Comparative Study of LLMs for Infrastructure-as-Code Generation and Optimization," *Comput. Fraud Secur.*, vol. 2022, no. 4, Apr. 2022, doi: 10.52710/cfs. 730.

[7] V. Sharma, "AI-Based Anomaly Detection for 5G Core and RAN Components," *Int. J. Sci. Res. Eng. Manag.*, vol. 06, no. 01, pp. 1–9, Jun. 2022, doi: 10.55041/IJSREM11453.

[8] M. Khosravi and B. T. Ladani, "Alerts Correlation and Causal Analysis for APT-Based Cyber Attack Detection," *IEEE Access*, vol. 8, pp. 162642–162656, 2020, doi: 10.1109/ACCESS.2020.3021499.

[9] P. Ma, Z. Ji, Q. Pang, and S. Wang, "NoLeaks: Differentially Private Causal Discovery Under Functional Causal Model," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 2324–2338, 2022, doi: 10.1109/TIFS.2022.3184263.

[10] W. Zhiqun, A. David, and A. Akinrayo, "Summary of Cyber Threat Intelligence," *Int. J. Innov. Res. Multidiscip. F.*, vol. 8, pp. 32–42, 2023, doi: 10.2015/IJIRMF/202203006.

[11] S. Chatterjee, "A Data Governance Framework for Big Data Pipelines: Integrating Privacy, Security, and Quality

Research Article

in Multitenant Cloud Environments," *Tech. Int. J. Eng. Res.*, vol. 10, no. 5, 2023, doi: 10.56975/tijer.v10i5.158181.

[12] I. A. Khan, N. Moustafa, D. Pi, K. M. Sallam, A. Y. Zomaya, and B. Li, "A new explainable deep learning framework for cyber threat discovery in industrial IoT networks," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 11604–11613, 2021.

[13] I. Kotenko, D. Gaifulina, and I. Zelichenok, "Systematic Literature Review of Security Event Correlation Methods," *IEEE Access*, vol. 10, pp. 43387–43420, 2022, doi: 10.1109/ACCESS.2022.3168976.

[14] P. Tubío Figueira, C. López Bravo, and J. L. Rivas López, "Improving information security risk analysis by including threat-occurrence predictive models," *Comput. Secur.*, vol. 88, p. 101609, Jan. 2020, doi: 10.1016/j.cose.2019.101609.

[15] S. Chatterjee, "Understanding the Risk of Implementing A.I. for Managing NERC BCSI Data Repository and Security Baseline to Secure the BCSI Data," *J. Inf. Syst. Eng. Manag.*, vol. 9, no. 4, pp. 1–14, 2024, doi: 10.52783/jisem.v9i4.19.

[16] S. K. Malaraju and R. Bondalapati, "Least Outstanding Requests (LOR) Algorithm in Application Load Balancer," *Int. J. Sci. Technol.*, vol. 14, no. 3, p. 7, 2023, doi: 10.71097/ijsat.v14.i3.3171.

[17] Y. Cao, B. Li, Q. Li, A. Stokes, D. Ingram, and A. Kiprakis, "Reasoning Operational Decisions for Robots via Time Series Causal Inference," in *2021 IEEE International Conference on Robotics and Automation (ICRA)*, IEEE, May 2021, pp. 6124–6131. doi: 10.1109/ICRA48506.2021.9561659.

[18] S. Bongers, P. Forré, J. Peters, and J. Mooij, "Foundations of structural causal models with cycles and latent variables," *Ann. Stat.*, vol. 49, 2021, doi: 10.1214/21-AOS2064.

[19] S. Ramakrishna, "Predictive and Causal Intelligence in Cloud-Native Enterprise Platforms through AI and ML Driven Interoperability Root-Cause Analysis and Performance Optimization," *Int. J. Res. Publ. Eng. Technol. Manag.*, vol. 7, no. 3, pp. 10504–10510, 2024, doi: 10.15662/IJRPETM.2024.0703007.

[20] R. Kushwaha and S. Patil, "AI-Driven Threat Intelligence: A Comprehensive Review of Predictive Analytics for Modern Cyber Défense," *Int. J. Eng. Sci. \& Humanit.*, vol. 14, no. 3, pp. 50–61, 2024.

[21] D. Levshun and I. Kotenko, "A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 56, no. 8, pp. 8547–8590, Aug. 2023, doi: 10.1007/s10462-022-10381-4.

[22] B. Samuel, "AI-Driven Cyber Threat Detection and Response," *Int. J. Emerg. Res. Eng. Technol.*, vol. 4, no. 1, pp. 153–157, Mar. 2023, doi: 10.63282/3050-922X.IJERET-V4I1P116.

[23] Z. Jadidi, J. Hagemann, and D. Quevedo, "Multi-step attack detection in industrial control systems using causal analysis," *Comput. Ind.*, vol. 142, p. 103741, Nov. 2022, doi: 10.1016/j.compind.2022.103741.

[24] S. Sultana, M. M. Rahman, M. S. Hossain, M. N. Gony, and A. Rafy, "AI-powered threat detection in modern cybersecurity systems: Enhancing real-time response in enterprise environments," *World J. Adv. Eng. Technol. Sci.*, vol. 6, no. 2, pp. 136–146, Aug. 2022, doi: 10.30574/wjaets.2022.6.2.0079.