Review of Applied Science and Technology

Volume: 3; **Issue:** 1
Pages: 68– 105

GRAPH NEURAL NETWORK MODELS FOR PREDICTING CYBER ATTACK PATTERNS IN CRITICAL INFRASTRUCTURE SYSTEMS

Shaikat Biswas[1]; Aditya Dhanekula[2];

[1]. *Master of Science in Computer Science (Cybersecurity Concentration), Troy University; USA; Email: ethan.soikot@gmail.com*

[2]. *CloudData Technologies, Business Analyst, Wilmington, DE, USA; Email: dhanekulaaditya1@gmail.com*

Doi: 10.63125/pmnqxk63
Received: *12 January 2024;* ***Revised:*** *20 February 2024;* ***Accepted:*** *18 March 2024;* ***Published:*** *24 March 2024*

Abstract

This study addresses the growing problem of predicting coordinated cyber-attack patterns in cloud enabled critical infrastructure enterprises, where conventional intrusion detection systems struggle to exploit the graph structured nature of assets, communications, and attack paths. The purpose is to quantify how technological and organizational conditions shape the effectiveness of graph neural network (GNN) models for cyber-attack prediction. A quantitative, cross sectional, case-based design was adopted using a structured Likert five-point survey in multiple critical infrastructure cases operating cloud based and on premises enterprise environments. From 280 distributed questionnaires, 236 valid responses were retained (84.3 percent) from security and OT professionals in energy, transportation, water, and industrial organizations. Key variables included network topology visibility, security data quality and completeness, analytics and AI capability maturity, governance and policy alignment, organizational readiness for AI based security, and perceived GNN based prediction effectiveness. Analysis involved data screening, reliability assessment, descriptive statistics, Pearson correlations, hierarchical multiple regression, mediation testing, and sectoral comparisons. All scales were reliable (Cronbach's alpha 0.81–0.89), and the regression model was significant, explaining 53.2 percent of the variance in GNN effectiveness (adjusted $R^2 = 0.512$). Network topology visibility ($\beta = 0.28$, $p < .001$) and security data quality ($\beta = 0.22$, $p < .001$) were the strongest predictors, followed by analytics maturity ($\beta = 0.18$), organizational readiness ($\beta = 0.20$), and governance alignment ($\beta = 0.13$). Organizational readiness partially mediated the impact of technological capabilities, and energy sector cases reported the highest mean effectiveness ($M = 3.98$). The findings imply that successful GNN based cyber defense in critical infrastructures depends on accurate graph visibility, high quality telemetry, mature analytics pipelines, and institutionalized governance rather than model architecture alone.

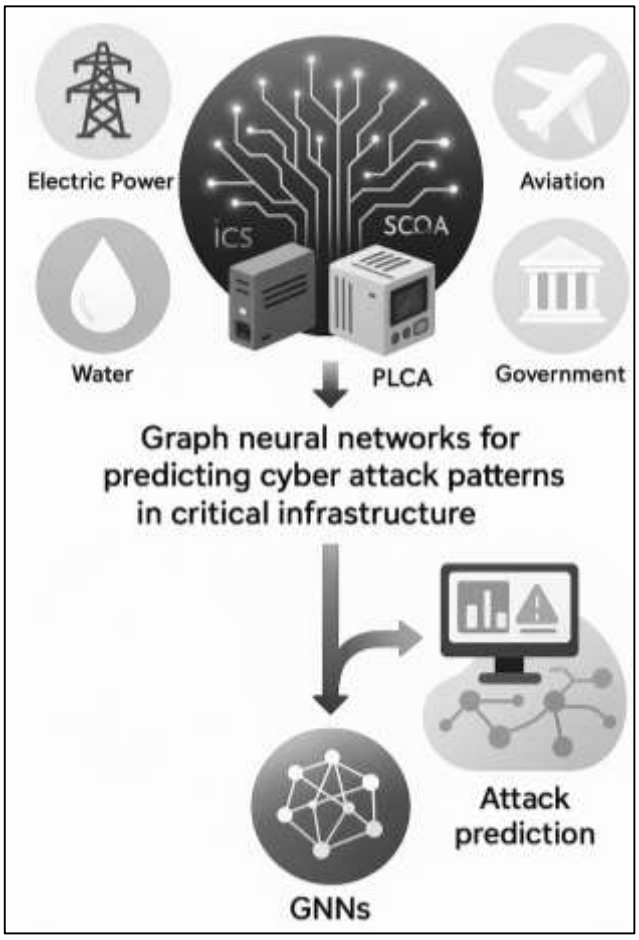
Keywords

Graph Neural Networks; Critical Infrastructure Cybersecurity; Cyber-Attack Prediction; Intrusion Detection; Technology Organization Environment Framework;

INTRODUCTION

Contemporary societies depend on intertwined critical infrastructure systems including electric power, oil and gas, transportation, telecommunications, water, and financial networks that are increasingly managed through digital information and communication technologies. "Critical information infrastructure" (CII) denotes the information systems and networks whose disruption can undermine national security, economic stability, or public welfare (Assaf, 2008). Governments and international organizations have therefore framed critical information infrastructure protection (CIIP) as a strategic policy priority, emphasizing the need for robust models that capture interdependencies and regulatory choices (Stoyanov et al., 2017). At the same time, shifts toward smart grids, intelligent transport, and industrial automation have expanded the cyber–physical attack surface, where compromises of information systems can trigger cascading physical failures (Bompard et al., 2012). In response, researchers have developed conceptual and methodological frameworks to analyze CIIP, risk management, and resilience in large-scale engineered systems (Lopez et al., 2012). Within this landscape, cyber-attacks are understood not merely as isolated events but as coordinated sequences of malicious actions that exploit technical vulnerabilities, organizational misconfigurations, and complex interconnections across infrastructures (Jarmakiewicz et al., 2017). These developments have created a demand for analytical methods capable of capturing structural relations between assets, communication paths, and threat behaviors in order to support proactive, data-driven decision-making in critical infrastructure cybersecurity.

Figure 1: Critical Infrastructure Sectors and GNN-Driven Cyber Attack Prediction Architecture



Critical infrastructure systems are increasingly realized as cyber–physical systems (CPS), where embedded sensors, programmable logic controllers (PLCs), industrial control systems (ICS), and supervisory control and data acquisition (SCADA) platforms regulate physical processes through networked computation (Mitchell & Chen, 2014). In power grids, for example, wide-area measurement

and control rely on digital communication between central operators and substations, creating rich data streams that can be monitored but also manipulated by advanced adversaries (Arfan et al., 2021; Wallace & Atkison, 2017). Similar cyber–physical couplings appear in rail signaling, water treatment, and industrial manufacturing, where safety and reliability hinge on secure operation of control protocols and field devices (Ara, 2021; Lopez et al., 2012). Empirical and conceptual studies show that ICS environments exhibit stringent real-time constraints, legacy components, and protocol heterogeneity, which limit the direct deployment of traditional IT security mechanisms and motivate customized detection and protection architectures (Bhamare et al., 2020; Jahid, 2021). Surveys of CPS security and intrusion detection underscore that attacks against such systems incorporate multi-stage strategies, including reconnaissance, lateral movement, privilege escalation, and process manipulation, often tailored to domain-specific process dynamics (Loukas et al., 2019; Akbar & Farzana, 2021). For national regulators and operators, this means that assessing cyber risk in critical infrastructures requires analytical models that integrate system topology, interdependencies, and behavior of both legitimate operations and adversarial campaigns (Assaf, 2008; Reza et al., 2021).

Within this broader context, intrusion detection systems (IDS) remain central defensive mechanisms for identifying unauthorized access and anomalous behavior in networks and hosts. Classic taxonomies distinguish host-based and network-based IDS, and categorize detection techniques as signature-based, anomaly-based, or hybrid approaches (Glass-Vanderlan et al., 2019; Saikat, 2021). Comprehensive reviews document how IDS research has evolved from statistical profiling and expert-defined rules toward data mining, machine learning, and, more recently, deep learning methods (Buczak & Guven, 2016; Shaikh & Aditya, 2021). In critical infrastructure and CPS settings, surveys show that intrusion detection must consider specific operational constraints, domain protocols, and process semantics, leading to tailored CPS and vehicular IDS designs (Loukas et al., 2019; Kanti & Shaikat, 2021). Parallel work has explored attack graph–based analysis, where system vulnerabilities and possible exploit chains are modeled as graphs, enabling reasoning about reachability of critical states and prioritization of security controls (Shandilya et al., 2014). More recent surveys of ICS cybersecurity highlight that intrusion detection for ICS and SCADA must contend with highly imbalanced data, subtle attack manifestations, and the need for interpretable alerts that operators can map to physical consequences (Alam & Alam, 2022; Maglaras et al., 2018). Together, this literature indicates both the value of IDS as a key component of defense-in-depth and the methodological challenge of constructing detection models that reflect the graph-structured nature of critical infrastructure networks and attack paths (Ariful & Ara, 2022; Arman & Kamrul, 2022).

The emergence of graph neural networks (GNNs) provides a powerful modeling paradigm for capturing complex relational structures present in network and infrastructure data. The original graph neural network model formalized how node states can be iteratively updated through neighborhood aggregation, allowing supervised learning on graph-structured inputs (Fokhrul & Fardaus, 2022; Mesbaul & Farabe, 2022; Scarselli et al., 2009). Subsequent architectures such as graph convolutional networks (GCNs) and GraphSAGE introduced scalable neighborhood sampling and convolutional operations, enabling inductive and semi-supervised learning on large graphs (Kipf & Welling, 2017; Nahid, 2022; Hossain & Milon, 2022). A comprehensive survey of GNNs synthesizes these developments and highlights their applicability to domains where entities and relationships can be represented as nodes and edges, including social networks, knowledge graphs, recommendation systems, and physical infrastructures (Abdur & Haider, 2022; Mushfequr & Praveen, 2022; Mortuza & Rauf, 2022; Rakibul & Samia, 2022; Wu et al., 2020). In cybersecurity, this relational viewpoint aligns naturally with representations of communication flows, authentication relations, dependency graphs, and attack paths (Rony & Ashraful, 2022; Saikat, 2022; Shaikh & Sudipto, 2022; Shandilya et al., 2014). Recent studies have begun to tailor GNNs for network intrusion detection, where nodes encode hosts or flows and edges represent communication or shared attributes, and the model learns patterns of malicious activity from labeled attack datasets (Abdul, 2023; Abdulla & Zaman, 2023; Lo et al., 2022). These works demonstrate that GNN-based IDS can leverage structural information that conventional tabular deep learning or classical machine learning approaches ignore, potentially improving robustness to adversarial manipulation and generalization to new environments (Arfan et al., 2023; Ara & Onyinyechi, 2023; Liao et al., 2013).

Empirical work at the intersection of GNNs and intrusion detection has mainly focused on general-purpose enterprise or IoT network settings, often using public benchmark datasets such as CIC-IDS2017 or UNSW-NB15. For example, Lo et al. (2022) propose E-GraphSAGE, a GNN-based IDS for IoT networks that constructs graphs from flow features and IP relationships and demonstrates competitive detection performance compared to non-graph deep learning baselines. Pujol-Perich et al. (2022) design a robust GNN-based network intrusion detector and show that modeling flows as a graph, rather than independently, can help maintain accuracy under adversarial perturbations. Parallel advances in IoT-focused intrusion detection leverage deep learning and hybrid architectures for anomaly detection in constrained environments (Amin & Mesbaul, 2023; Foysal & Aditya, 2023; Pujol-Perich et al., 2022). These studies underline that representing cyber environments as graphs and learning from those graphs can capture higher-order interaction patterns between hosts, flows, and protocols. However, much of the empirical evaluation to date has centered on generic IoT or enterprise networks rather than on high-stakes critical infrastructures such as power grids, transportation control systems, or industrial manufacturing networks, where topologies, communication patterns, and operational constraints differ substantially (Hamidur, 2023; Rashid et al., 2023; Ravi et al., 2022). This gap suggests a need for domain-specific studies that situate GNN-based intrusion detection within the operational realities, risk profiles, and data characteristics of critical infrastructure systems (Musfiqur & Kamrul, 2023; Muzahidul & Mohaiminul, 2023; Yang et al., 2022).

From a risk and governance perspective, the literature on CIIP and ICS security emphasizes that cyber threats to critical infrastructures are shaped by institutional arrangements, regulatory strategies, and engineering practices (Amin & Sai Praveen, 2023; Hasan & Ashraful, 2023; Wood et al., 2017). Models of CIIP differentiate between national security–oriented and business continuity–oriented approaches, which influence how states and operators invest in monitoring, detection, and response capabilities (Assaf, 2008; Ibne & Kamrul, 2023; Mushfequr & Ashraful, 2023). Engineering-focused work on ICS and power grid security identifies the need for architectural patterns, zoning, and defense-in-depth mechanisms specifically adapted to industrial environments (Baz, 2022; Roy & Kamrul, 2023; Saba et al., 2023). Within this frame, predictive analytics that anticipate cyber-attack patterns in critical infrastructure networks are not only technical tools but also decision-support mechanisms for prioritizing controls, allocating resources, and complying with sectoral regulations (Bridges et al., 2019; Saba & Kanti, 2023; Shaikh & Farabe, 2023). Empirical IDS research in IoT and CPS demonstrates that machine learning and deep learning–based detection can achieve high accuracy on benchmark datasets, yet the translation of these methods into CIIP contexts requires attention to data availability, interpretability, and alignment with operational security processes (Abdul & Shoeb, 2024; Dahou et al., 2022; Haider & Hozyfa, 2023). By framing critical infrastructures as graphs of interdependent nodes and edges, GNN-based models offer a way to encode both technical and organizational structures, potentially enriching the quantitative assessment of attack likelihoods, lateral movement patterns, and risk concentrations within and across infrastructures (Hozyfa & Shahrin, 2024; Husnain et al., 2022; Hasan & Shah, 2024).

In this context, the present study focuses on graph neural network models for predicting cyber-attack patterns in critical infrastructure systems, adopting a quantitative, cross-sectional, case-study–based design. Building on the CIIP and ICS security literature, the study conceptualizes critical infrastructures as graph-structured systems in which nodes represent assets such as substations, control servers, field devices, or network segments, and edges encode communication relationships or logical dependencies (Hamilton et al., 2017; Hasan & Zayadul, 2024; Muzahidul & Aditya, 2024). Drawing on prior work in GNN-based intrusion detection and deep learning for IoT and CPS security, the research models attack patterns as configurations of anomalous activity over this graph, captured through constructs such as alert frequency, anomalous communication flows, and topological risk exposure (Dat-Thinh et al., 2022). The study is grounded in survey-based data collected via Likert's five-point scales from security professionals and engineers embedded in case organizations, combined with operational security telemetry where available, enabling the use of descriptive statistics, correlation analysis, and regression modeling to test hypotheses about the relationships between GNN-based predictive capabilities, infrastructure characteristics, and cyber-attack patterns. In this way, the research aligns with calls in the CIIP and ICS literature for empirical, sector-specific studies that bridge conceptual modeling,

advanced analytics, and operational practice in critical infrastructure cybersecurity (Assaf, 2008).

The present study is designed with a clear objective orientation that links the problem context of critical infrastructure cybersecurity with a focused empirical investigation of graph neural network–based predictive models. The overarching aim is to examine how graph-structured representations and associated analytical capabilities can be used to predict cyber-attack patterns across interconnected assets in critical infrastructure systems, and to determine which technical and organizational conditions support or hinder this predictive capacity. More specifically, the study seeks, first, to identify and operationalize key constructs that characterize GNN-oriented cyber defense in critical infrastructure environments, including network topology visibility, data quality and completeness, analytics and AI capability maturity, cybersecurity governance, and organizational readiness for AI-based security solutions. Second, the study aims to measure the perceptions and experiences of cybersecurity professionals, engineers, and managers working within selected case organizations by means of a structured questionnaire using Likert's five-point scales, allowing these constructs to be represented in a form suitable for quantitative analysis. Third, the research is directed toward estimating the strength and direction of relationships between these independent constructs and outcome variables such as perceived GNN predictive effectiveness and perceived improvement in cyber-attack detection and response, using descriptive statistics to characterize the sample, correlation analysis to explore associations, and regression modeling to test hypothesized effects. Fourth, the study seeks to contrast patterns across different critical infrastructure sectors and case organizations, thereby highlighting how sectoral context and organizational characteristics relate to the adoption and performance of GNN-based predictive approaches. Finally, the study aims to use the empirical results to refine a conceptual model that links GNN-related capabilities, infrastructure characteristics, and observable attack patterns, anchored in a cross-sectional, case-study–based design that remains grounded in the realities of operational environments. Through these interconnected objectives, the research maintains a focused, measurable, and methodologically consistent approach to examining graph neural network models for predicting cyber-attack patterns in critical infrastructure systems.

LITERATURE REVIEW

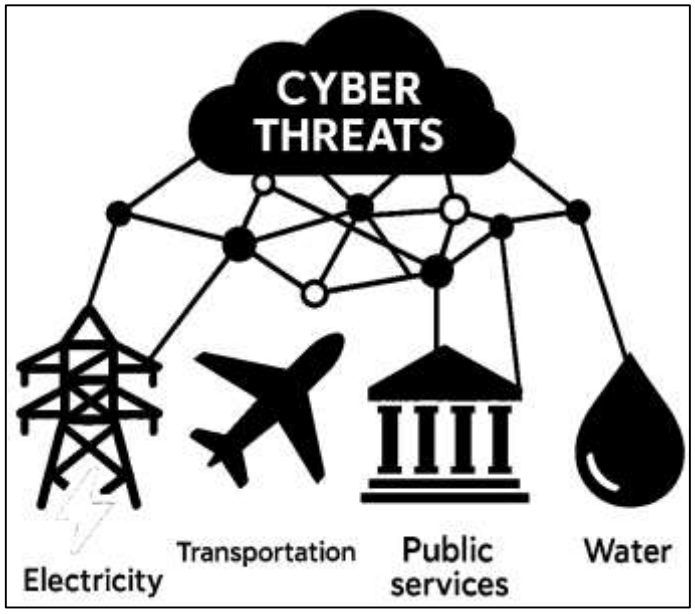
The literature on cybersecurity for critical infrastructures, cyber–physical systems (CPS), and industrial control systems (ICS) shows a steady evolution from traditional signature-based intrusion detection toward machine learning and, more recently, graph-based deep learning approaches. Early comprehensive reviews of intrusion detection techniques highlighted core taxonomies (host-based versus network-based, signature-based versus anomaly-based) and documented how statistical and rule-based techniques struggle with high-volume, heterogeneous traffic and evolving attack strategies, motivating the use of data-driven models that can learn complex patterns from observed behavior. In the ICS and CPS domain, surveys emphasize that industrial networks underpinning power grids, water treatment, transportation, and manufacturing exhibit unique timing constraints, legacy protocols, and safety-critical operations, making generic IT-oriented intrusion detection systems (IDS) insufficient and requiring solutions tailored to OT-specific characteristics, including process-aware models and specialized datasets. Parallel strands of work in machine learning–based IDS synthesize a broad range of supervised, unsupervised, and hybrid techniques from decision trees and support vector machines to deep neural networks, autoencoders, and ensemble methods demonstrating improved detection performance on benchmark datasets but also exposing challenges in feature engineering, dataset realism, class imbalance, and robustness to adversarial manipulation, particularly in high-stakes environments such as critical infrastructures. Against this backdrop, graph neural networks (GNNs) have emerged as a powerful paradigm for modeling non-Euclidean data where entities and their relationships form complex graphs; a comprehensive survey categorizes recurrent, convolutional, autoencoder, and spatio-temporal GNN architectures and documents their successful deployment in domains such as social networks, knowledge graphs, and physical infrastructure networks. Building on this foundation, recent studies explicitly apply GNNs to network intrusion detection, encoding hosts, flows, and communication links as graph-structured data so that structural patterns of normal and malicious behavior can be exploited; proposed systems such as E-GraphSAGE for IoT networks and robust GNN-based network IDS models show that leveraging graph topology and edge features can yield state-of-the-art performance and enhanced resilience against certain adversarial attacks

compared to conventional machine learning baselines. However, most of this graph-based intrusion detection research is carried out using generic enterprise or IoT datasets and evaluation setups, while surveys on ICS and CPS security stress that critical infrastructure networks involve domain-specific protocols, topologies, and operational constraints that affect both the feasibility and the effectiveness of advanced analytics. This divergence between the sophistication of GNN-based methods and the distinctive characteristics of critical infrastructure environments motivates a focused review of studies that link graph representation learning, intrusion detection, and the prediction of cyber-attack patterns in critical infrastructure systems, with particular attention to how technical capabilities, data requirements, and organizational factors shape their adoption and performance.

Critical Infrastructure Systems and the Cyber Threat Landscape

Critical infrastructure systems encompass those assets, networks, and services whose disruption would cause serious harm to public safety, economic stability, or national security, and they have progressively evolved into tightly coupled socio-technical systems that span local, regional, and global scales. Infrastructures such as electric power, oil and gas, transportation, water, telecommunications, and financial services are increasingly interconnected through information and communication technologies, enterprise platforms, and real-time data exchange, so that disturbances in one domain can propagate quickly to others. Early work on systemic vulnerability emphasized that these infrastructures must be understood as dynamic systems shaped by technological change, regulatory choices, and planning decisions, rather than as static collections of physical assets, and argued that vulnerability analysis should integrate both technical and institutional dimensions when evaluating risk profiles and protection strategies (Hellström, 2007).

Figure 2: Cyber Threat Pathways Across Critical Infrastructure Systems



A complementary perspective on interdependence and risk framed critical infrastructures as macro-scale engineered networks whose components are linked through physical, cyber, geographic, and logical dependencies, highlighting how disruptions can cascade across sectors via shared communication links, supply-chain relations, and control dependencies (Haimes et al., 2007). Together, these strands of research establish that any meaningful assessment of the cyber threat landscape for critical infrastructure must incorporate not only individual system vulnerabilities but also cross-sector couplings, feedback loops, and the broader context in which infrastructures are planned, operated, and modernized. Within this broader framing, the concept of critical infrastructure has expanded beyond a narrow list of sectors to include cross-cutting enabling functions such as cloud services, data centers, and communication backbones, all of which serve as crucial control and coordination layers for more traditional utilities. The result is a multi-layered infrastructure environment where failures initiated in

purely digital subsystems can have tangible physical consequences, and where cyber risk management becomes inseparable from questions of infrastructure design, governance, and long-term investment.

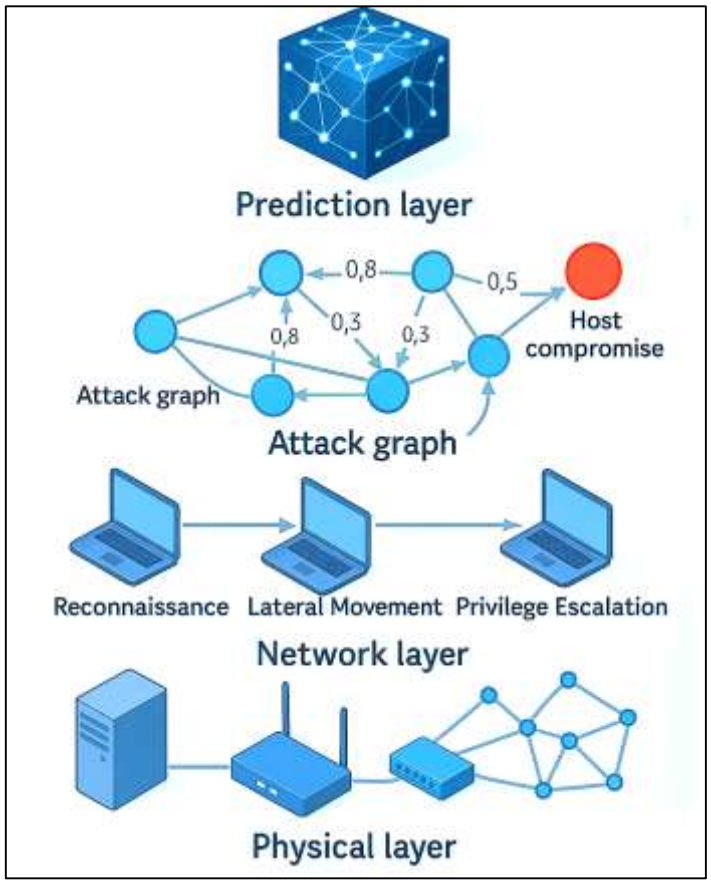
Building on these systemic views, subsequent work has paid particular attention to cyber-physical integration in power systems and other control-intensive infrastructures, where digital communication and automation have enabled new operational capabilities but simultaneously expanded the attack surface. Research on cybersecurity for critical infrastructures has shown that electric power systems, for example, rely on geographically dispersed supervisory control and data acquisition architectures, energy management systems, and substation automation platforms that interconnect field devices, control centers, and corporate networks through complex communication channels (Hasan & Rakibul, 2024; Mominul, 2024; Ten et al., 2010). Within such architectures, adversaries can exploit weaknesses in authentication, access control, or network segmentation to manipulate measurement data, interfere with protective relays, or trigger undesirable switching operations, potentially leading to wide-area outages or equipment damage. Survey studies on power grid cybersecurity further document how advanced metering infrastructure, phasor measurement units, and distribution automation increase the volume and velocity of data flows, making traditional perimeter-based defenses insufficient and motivating the deployment of intrusion detection, anomaly detection, and testbed-based evaluation environments that reflect realistic cyber-physical interactions (Mominul & Zaki, 2024; Roy & Sai Praveen, 2024; Sun et al., 2018). These developments illustrate that cyber threats are not confined to isolated penetration attempts on single hosts, but often unfold as coordinated campaigns that traverse multiple network zones and exploit both IT-facing and operational technology components. At the same time, the growing reliance on remote monitoring, vendor access channels, and standardized communication stacks means that previously air-gapped or proprietary subsystems are now part of a broader, routable infrastructure, narrowing the gap between enterprise IT threats and attacks that can directly influence physical processes. As organizations integrate renewable generation, energy storage, and responsive loads into power and industrial systems, the number of controllable endpoints increases, creating more potential vantage points for adversaries and complicating the task of maintaining situational awareness across large-scale infrastructure networks. In many sectors, this evolution has produced a situation in which operators must simultaneously manage legacy control equipment and cutting-edge digital platforms, leading to heterogeneous security postures and uneven visibility across different layers of the infrastructure stack.

More recent investigations emphasize that industrial control systems in critical infrastructures remain exposed to sophisticated hardware and software exploitation techniques, even as operators adopt modern platforms and standardized communication technologies. Studies of specific vulnerability classes illustrate how low-level memory faults in widely deployed hardware components can be turned into practical attack vectors against controllers and programmable logic devices, challenging assumptions that industrial systems are protected simply by network segmentation or proprietary protocols (Aydın & Sertbaş, 2022). These findings reinforce the view that the cyber threat landscape facing critical infrastructures is characterized by adversaries capable of targeting every layer of the technology stack from hardware and firmware to operating systems, middleware, and application logic while leveraging knowledge of process semantics and operational constraints to maximize disruptive impact. In parallel, the growing digitization of monitoring, maintenance, and asset management functions means that historically isolated subsystems are now reachable via remote access channels, cloud-based services, and third-party integration interfaces, further increasing the pathways through which attackers can move laterally across infrastructure environments. In practice, this results in a threat environment where a vulnerability in a single field device, engineering workstation, or remote maintenance tunnel may provide an entry point into core operational networks, and where detection of early-stage compromise requires close observation of subtle deviations in communication patterns and process behavior. Against this background, the need emerges for analytical and predictive approaches that can capture not only isolated vulnerabilities, but also the graph-structured relationships among infrastructure components, communication links, and potential attack paths, laying the conceptual foundation for graph-based cyber-attack modeling and graph neural network–driven prediction in later sections of the literature review.

Cyber Attack Patterns, Attack Graphs, and Network Topology

Cyber-attack patterns in enterprise and critical infrastructure networks are rarely isolated, single-step events; instead, they typically unfold as sequences of reconnaissance, privilege escalation, lateral movement, and impact actions that traverse multiple hosts, applications, and network segments. To capture this multi-stage structure, security researchers introduced attack graphs as a formalism that encodes how individual vulnerabilities, misconfigurations, and trust relationships can be chained together to reach an attacker's goal (Rony & Hozyfa, 2024; Saba & Hasan, 2024). An attack graph represents states of the system (such as a host compromise or credential acquisition) as nodes and possible exploits or transitions as edges, enabling analysts to reason about feasible attack paths rather than only local weaknesses (Shaikat & Zaman, 2024; Sudipto & Hasan, 2024). Early work in this area treated attack graphs primarily as qualitative tools for scenario exploration, but subsequent studies incorporated probabilistic information so that each path could be assigned an estimated likelihood of successful exploitation, allowing the overall security posture of a configuration to be expressed in quantitative terms. For example, probabilistic attack graphs can model how different combinations of vulnerability exploitability, attacker skill, and network reachability influence the probability that an adversary reaches a critical asset, and can then aggregate these probabilities to produce security metrics that are more informative than simple vulnerability counts (Gao et al., 2018; Kanti & Saba, 2024; Tonoy Kanti & Sai Praveen, 2024; Wang et al., 2008). In combination, such probabilistic extensions demonstrate that attack patterns in complex infrastructures can be characterized not just by their logical structure but also by their probability distribution over alternative paths, laying a foundation for data-driven prediction and optimization in network defense and offering a bridge between qualitative threat modeling and quantitative risk assessment (Zamal Haider & Sai Praveen, 2024; Zulqarnain & Zayadul, 2024).

Figure 3: Layered Model of Physical Infrastructure



As attack graphs became more widely used for vulnerability assessment and defensive planning, questions emerged about how best to configure and visualize them so that human decision makers can

accurately perceive and interpret complex attack patterns. One strand of empirical work investigated how practitioners with different backgrounds such as security analysts, engineers, and students respond to variations in attack graph layout, syntax, and annotation, finding that top-down visual designs that closely mirror the temporal progression of an attack tend to be preferred over bottom-up tree-like configurations when users are asked to reason about multi-step intrusions (Lallie et al., 2018). This line of research suggests that the utility of attack graphs for operational security cannot be evaluated solely in terms of algorithmic completeness or scalability; it also depends on the cognitive load imposed by the chosen representation and on how effectively visual encodings convey preconditions, postconditions, and branching alternatives. Complementary survey work has synthesized dozens of attack graph and attack tree variants, mapping how different proposals encode key attack semantics such as concurrency, repeated exploits, and defensive controls, and highlighting the absence of a standardized visual syntax across tools and studies (Lallie et al., 2020). The lack of standardization complicates cross-study comparison and can hinder the integration of attack graph outputs into higher-level risk dashboards for critical infrastructure operators, who must make rapid decisions based on aggregated information. At the same time, these reviews underline that attack graphs inherently combine structural information about network topology with behavioral information about attacker tactics, techniques, and procedures, implying that any automated learning approach that seeks to infer or predict attack patterns on top of such graphs must be sensitive to both aspects of the representation and to the way they are communicated to human stakeholders. For security teams working in resource-constrained operational environments, the choice of notation, level of abstraction, and interactive features of attack graph tools can therefore strongly influence whether graph-based analyses are actually adopted in day-to-day risk assessment and incident response workflows.

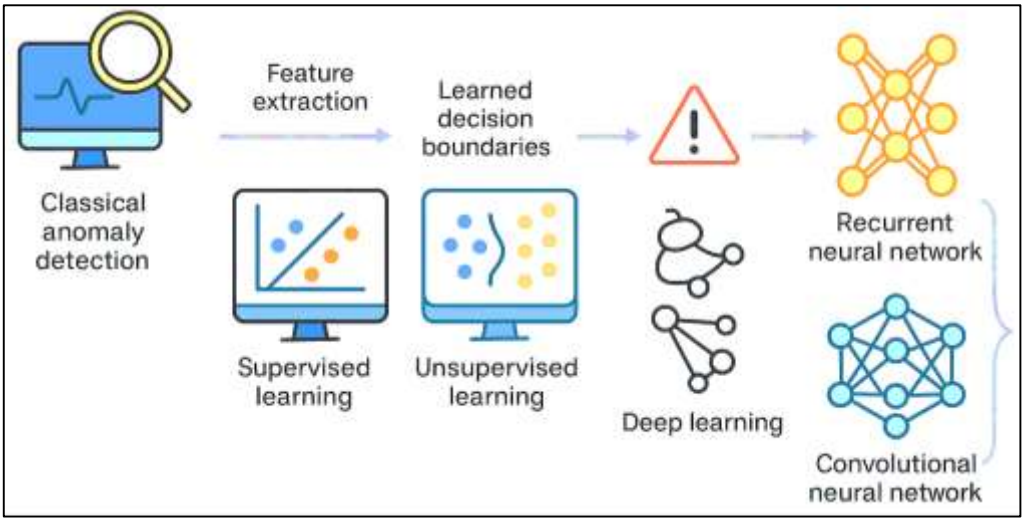
A parallel body of literature focuses explicitly on attack projection, prediction, and network security situation forecasting, positioning attack graphs and related models as key instruments for anticipating how adversaries might move through an infrastructure over time rather than merely documenting past incidents. Surveys of this research categorize prediction tasks into attack projection and intention recognition, intrusion prediction, and overall situation forecasting, and show that many proposed methods from Markov models and Bayesian networks to graph-based simulations operate over representations that encode network connectivity and dependency relations among assets and services (Husák et al., 2019). Within this predictive framing, attack graphs function as state spaces over which algorithms can search for likely future attack paths, estimate the residual risk after implementing specific hardening actions, or generate alerts when observed activity aligns with known high-risk trajectories. Such models are particularly relevant to critical infrastructures, where defenders must anticipate coordinated, multi-step campaigns that exploit sector-specific protocols and tightly coupled processes, and where small configuration changes such as a new remote access route or a change in trust relationships between domains can give rise to qualitatively different attack opportunities. By explicitly modeling how adversaries chain exploits and traverse network links, attack graphs provide a bridge between low-level telemetry (such as vulnerability scans, flow records, and intrusion detection alerts) and higher-level situational awareness needed by managers, regulators, and incident response teams. Recent work also notes that predictive use of attack graphs faces practical challenges, including the need for up-to-date configuration data, scalable algorithms for large networks, and methods to cope with uncertainty in attacker behavior, all of which reinforce the value of representations that can be continuously updated and learned from operational data streams. Collectively, this body of work indicates that cyber-attack patterns are best understood as emergent phenomena on network graphs where topology, vulnerability distribution, and attacker decision-making interact, providing essential conceptual grounding for the graph-structured data representations and predictive modeling approaches considered in subsequent sections of this study.

Machine Learning and Deep Learning Approaches to Intrusion Detection

Machine learning–based intrusion detection emerged as a response to the limitations of purely signature-driven and rule-based systems, aiming to learn discriminative patterns of malicious activity directly from network traffic and system events. Classical anomaly detection schemes often required expert-crafted profiles and thresholds, which proved difficult to maintain as traffic volumes increased and protocol mixes evolved. In this setting, researchers began to explore supervised and unsupervised

learning algorithms that could infer decision boundaries and clusters from labelled and unlabeled traffic, hoping to improve detection rates while reducing the manual effort needed to keep rules up to date. One important direction focused on improving traditional classifiers by engineering more informative feature representations of connection records. For instance, an intrusion detection system based on combining cluster centres and nearest neighbours (CANN) transforms raw network data into compact prototypes and distance-based features, allowing a k-nearest-neighbor classifier to operate more efficiently while achieving higher accuracy and lower false-alarm rates on benchmark datasets (Lin et al., 2015). In a related line, an effective intrusion detection framework was proposed in which support vector machines (SVMs) are trained on augmented features obtained via logarithm marginal density ratio transformations, yielding more separable feature spaces and improved robustness compared with SVMs trained on original attributes (Wang et al., 2017). These studies illustrate a broader trend in machine learning–based intrusion detection: instead of relying solely on off-the-shelf classifiers, researchers design feature extraction and transformation pipelines that emphasize discriminative characteristics of normal and attack traffic, thereby addressing issues such as class overlap, non-linear decision boundaries, and high-dimensional noise. At the same time, they highlight that the overall performance of intrusion detection models depends critically on the interplay between algorithm choice, feature-engineering strategy, and characteristics of the underlying dataset, which often originates from general-purpose environments rather than from the specialized networks and protocols of critical infrastructure systems.

Figure 4: Machine Learning and Deep Learning Intrusion Detection Systems



With the growing scale, speed, and heterogeneity of network traffic, deep learning techniques have been increasingly investigated for intrusion detection, with the promise of automating feature learning and reducing reliance on manual engineering. Recurrent neural networks (RNNs) have been applied to treat network connections or flows as sequences, capturing temporal dependencies that may indicate staged attack behavior. A deep learning approach based on recurrent neural networks models intrusion detection as a sequence classification task and shows that, when trained on benchmark datasets, such an RNN-based IDS can outperform traditional machine learning models in both binary and multi-class settings, particularly in detecting complex or previously under-represented attack types (Yin et al., 2017). Convolutional neural networks (CNNs) have likewise been adapted to network security by viewing traffic features as structured inputs, such as images or matrices, so that spatial filters can capture local correlations among features. One CNN-based intrusion detection model for massive networks converts flows into fixed-size feature maps and demonstrates that CNNs can maintain high detection accuracy and low false positive rates even when confronted with large-scale traffic volumes (Wu et al., 2018). A complementary study introduces a method for transforming NSL-KDD records into graphical representations so that CNNs can perform representation learning directly on these transformed inputs, achieving competitive performance and underscoring the flexibility of deep

architectures to exploit different feature encodings (Li et al., 2017). Together, these deep learning approaches shift the focus from handcrafted feature engineering toward end-to-end learning pipelines, in which the network jointly optimizes feature extraction and classification. They also illustrate how architectural choices in particular, whether to emphasize temporal sequences or spatial feature structures shape the kinds of intrusion patterns that a model is most sensitive to, which has implications for deploying such systems in environments where attack campaigns evolve over time and exhibit complex correlations across multiple traffic attributes.

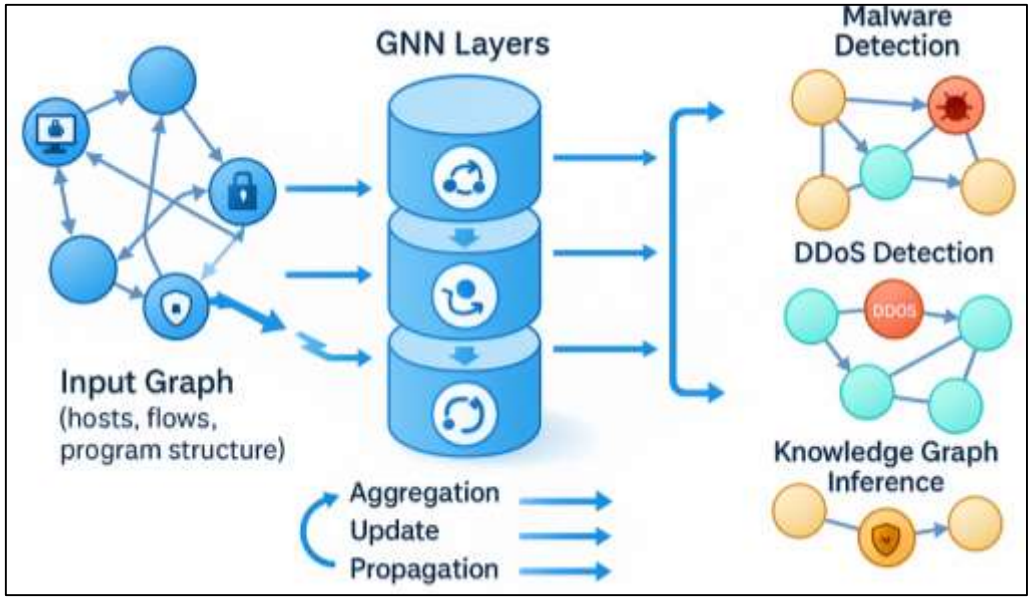
Although these machine learning and deep learning intrusion detection systems demonstrate substantial gains over purely rule-based approaches on standard benchmark datasets, they also expose several methodological limitations when considered from the perspective of complex, multi-domain infrastructures. Many models are trained on datasets such as NSL-KDD or other laboratory collections, which, while useful for controlled evaluation, offer limited coverage of modern protocols, encrypted traffic, and industrial control system communications, raising questions about how well the learned decision boundaries transfer to operational networks. Even when sophisticated feature engineering is used, as in the CANN model or the SVM framework with feature augmentation, feature vectors typically represent individual connections or flows in isolation, abstracting away much of the contextual information about how hosts, services, and subnets are arranged and how attacks propagate across them (Lin et al., 2015). Deep learning approaches alleviate some of these constraints by automatically learning higher-level representations, but the predominant use of RNNs and CNNs still treats samples as independent or sequence-based items, without explicitly encoding the underlying network topology or the rich set of relationships among nodes, interfaces, and segments (Li et al., 2017). This independence assumption can obscure structural patterns such as coordinated scans, lateral movement chains, or simultaneous probing of multiple services across a subnet, all of which are central to understanding attack paths in critical infrastructure environments. Furthermore, most of these models rely on centralized training pipelines that may not account for distributed data sources, heterogeneous sub-networks, or privacy and governance constraints common in large infrastructure operators. As a result, there is interest in approaches that maintain the strengths of machine learning and deep learning–based detection namely, their ability to generalize from data while also representing networks as graphs in which entities and their interactions are first-class objects, creating a natural bridge to graph-based analytics and graph neural network models for capturing cyber-attack patterns across interconnected critical infrastructure systems.

Graph Neural Networks in Network Security and Cyber-Attack Prediction

Graph Neural Networks (GNNs) provide a natural way to learn from relational structures that arise in cyber environments, where hosts, processes, and communication flows are inherently interconnected. Rather than treating each event or flow as an independent sample, GNNs operate on graphs whose nodes and edges encode entities and their relationships, allowing information to propagate across multi-hop neighborhoods and enabling the model to recognize higher-order patterns of interaction. In early security-oriented work, this idea was applied to static malware analysis by constructing function-call or control-flow graphs from executable code and learning graph-level representations for classification. One such framework builds graphs from Android malware samples and applies graph convolution to capture syntactic and semantic relationships among functions, showing that these graph-based embeddings significantly improve family-level classification accuracy compared with traditional feature-vector or image-based approaches that ignore structural context (Pei et al., 2020). Similarly, dynamic network-centric designs have emerged that cast network traffic as graphs, where nodes correspond to network entities or aggregated flows and edges capture temporal or contextual dependencies. By learning on these network-flow graphs, GNN-based detectors can exploit the fact that malicious activity often manifests as coordinated changes in connectivity and timing across multiple nodes, improvements that are reflected in reduced false-positive rates and better discrimination between benign bursts of traffic and distributed attack campaigns (Busch et al., 2021). Together, these developments show that representing cyber artifacts as graphs and applying GNNs to them yields more expressive models of malicious behavior than methods that rely solely on flat feature spaces.

Subsequent research has extended this graph-centric perspective from individual binaries and flows to larger-scale network and knowledge representations, seeking not only to detect specific malicious instances but also to characterize attack behavior at the level of infrastructures and threat intelligence. One line of work develops an effective distributed-denial-of-service (DDoS) detection approach that constructs graphs from large volumes of network traffic, with nodes representing communicating endpoints and edges encoding interactions enriched with flow statistics over time. Within this model, a GNN propagates information along connections so that patterns of low-intensity but highly coordinated activity can be recognized as characteristic of DDoS behavior, enabling more accurate and robust detection across diverse datasets and attack scenarios than conventional machine learning baselines that treat flows independently (Li et al., 2022). Another line uses GNNs to refine cybersecurity knowledge graphs built from threat reports and advisories. In these knowledge graphs, entities such as malware families, vulnerabilities, tools, and campaigns are linked by semantic relations, creating a structured representation that supports reasoning about how attacks unfold. By training a GNN over this graph to infer trust scores for edges, it becomes possible to down-weight noisy or outdated relations and highlight those that are most consistent with broader patterns in the data, thereby improving the reliability of knowledge-driven analysis and correlation in security operations centers (Dasgupta et al., 2021). Across both the traffic-centric and knowledge-centric settings, GNNs function as a unifying mechanism for combining local attributes with relational context, aligning closely with the needs of defenders who must understand not just whether an event is suspicious but how it fits into larger attack structures.

Figure 5: Graph Neural Network Architecture and Applications in Cybersecurity



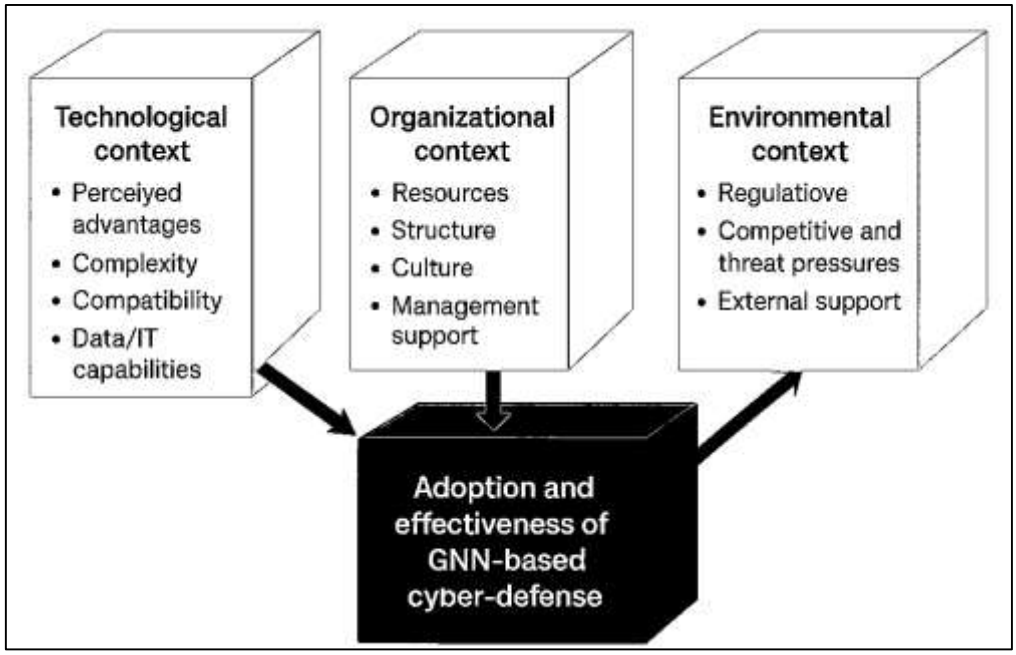
A complementary stream of work demonstrates how GNNs can support fine-grained malware classification and similarity analysis, tasks that are essential for understanding attack families, predicting potential evolution, and organizing response playbooks. In this stream, malware samples are first converted into graphs often function-call graphs or other program-structure representations and then passed through GNN architectures that learn embeddings capturing both local neighborhood patterns and global structural motifs. These embeddings can be fed into classifiers to assign family labels, or into metric-learning frameworks such as Siamese networks to estimate similarity between samples in a latent space. One such framework uses GNN-derived embeddings within a similarity-based malware classifier, enabling both accurate family-level classification and retrieval of related samples when confronted with previously unseen malware, and showing that structure-aware representations generalize better than those based solely on opcode frequencies or manually selected features (Chen et al., 2022). When viewed collectively, these studies reveal a recurring design pattern in graph-based cyber defense: cyber artifacts whether binaries, flows, endpoints, or threat entities are

first modeled as graphs, and GNNs are then trained for node-, edge-, or graph-level prediction tasks directly aligned with security objectives such as detection, classification, or credibility assessment (Busch et al., 2021). For critical infrastructures, which are themselves networks of interdependent assets, communication links, and control relationships, this paradigm provides a conceptual and methodological foundation for representing cyber-physical systems as graphs and for applying GNN-based models to predict how cyber-attack patterns may propagate across those networks.

Technology–Organization–Environment (TOE) for GNN-Based Cyber-Defense Adoption

The theoretical lens for this study is the Technology–Organization–Environment (TOE) framework, which explains how contextual factors shape organizational decisions to adopt and institutionalize technological innovations. At its core, TOE states that adoption is conditioned by three interlocking contexts: (a) the technological context (perceived advantages, complexity, compatibility, and data/IT capabilities), (b) the organizational context (resources, structure, culture, and management support), and (c) the environmental context (regulation, competitive and threat pressures, and external support). Empirical research at firm level shows that these three contexts consistently explain variation in the adoption of complex information systems such as enterprise systems and e-business platforms, where high capital costs, integration risk, and strategic importance resemble the stakes involved in deploying advanced AI-based cyber-defense in critical infrastructures (Ramdani & Kawalek, 2007). TOE-based studies highlight, for example, how technological characteristics like relative advantage and compatibility, organizational factors such as top management support and IT readiness, and environmental forces such as trading partner pressure jointly determine whether firms embrace large-scale enterprise systems and e-business architectures (Oliveira & Martins, 2010). For this research, the same logic is applied to the adoption and effective use of graph neural network (GNN) models for predicting cyber-attack patterns: the models themselves are an innovation, but their implementation and impact depend on organizational capabilities and a threat- and regulation-intensive environment that closely mirrors the adoption settings examined in prior TOE-based work.

Figure 6: Technological Determinants of GNN-Based Cyber-Defense Adoption



Recent extensions of TOE integrate it with behavioral and attitudinal theories such as the Technology Acceptance Model (TAM) and Theory of Planned Behavior (TPB), demonstrating how contextual variables influence perceived usefulness, ease of use, and intention to adopt complex digital innovations. For instance, an integrated TAM–TPB–TOE framework for e-commerce adoption in small and medium-sized enterprises (SMEs) shows that technological and organizational conditions shape beliefs about usefulness and control, while environmental pressures act as external enablers or

constraints (Awa et al., 2015). Likewise, a TAM–TOE model for cloud computing adoption identifies relative advantage, compatibility, complexity, organizational readiness, and top management commitment as key antecedents, while competitive pressure and trading partner support directly affect adoption intention (Gangwar et al., 2015). These studies typically operationalize the TOE contexts in multivariate models where adoption or extent of use is modeled as a function of technological, organizational, and environmental determinants. In linear form, the generic TOE-based structural relationship can be expressed as

$$Y = \beta_0 + \sum_{i=1}^{k} \beta_i T_i + \sum_{j=1}^{m} \gamma_j O_j + \sum_{l=1}^{n} \delta_l E_l + \varepsilon,$$

where $Y$is the degree of adoption or effectiveness, $T_i$are technological factors, $O_j$organizational factors, and $E_l$environmental factors, with εcapturing unexplained variance. For binary adoption decisions, the same logic is often embedded in a logistic link,

$$P(Y = 1 \mid \mathrm{X}) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 T + \beta_2 O + \beta_3 E)}},$$

which has been used in TOE-guided studies of enterprise systems and cloud computing adoption (Low et al., 2011). Adapting this structure to the present research, the dependent variable represents the extent to which critical infrastructure organizations adopt and rely on GNN-based models for cyber-attack prediction, while independent variables capture the technological robustness of GNN and data pipelines, organizational readiness to integrate AI into security operations, and environmental pressures such as regulatory mandates and heightened cyber threat levels.

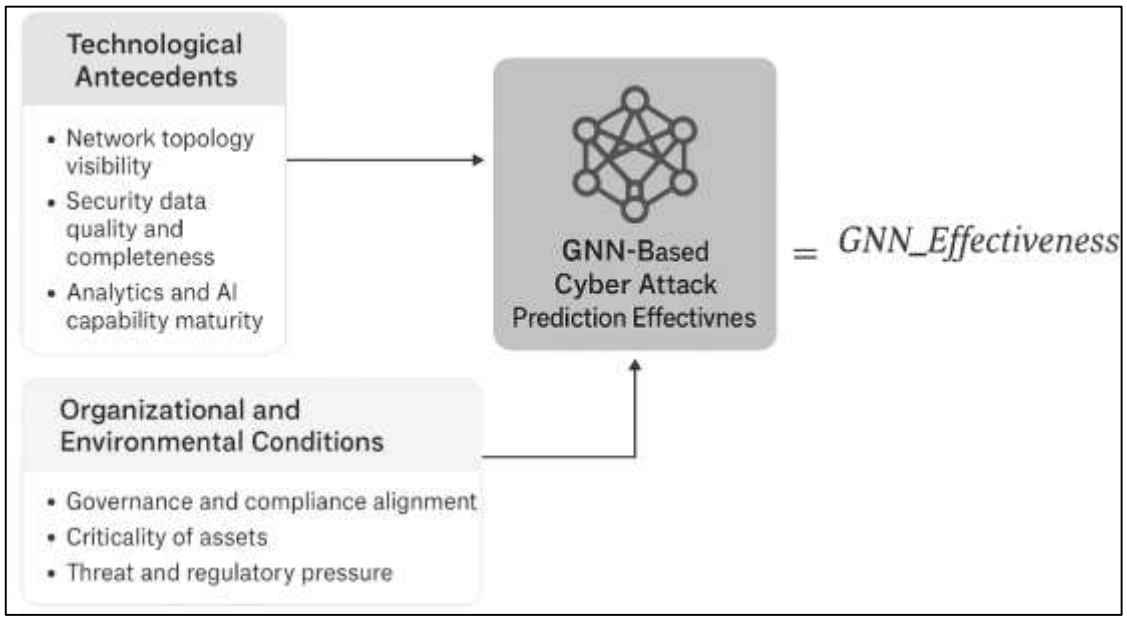
Within this framework, the technological context in critical infrastructure organizations encompasses the perceived predictive accuracy, scalability, interoperability, and complexity of GNN-based cyber-attack prediction systems, as well as the quality, volume, and graph-structured nature of telemetry available from OT and IT networks. The organizational context includes top management support for AI-enabled security, availability of skilled data science and cybersecurity staff, maturity of security operations centers, and the existence of governance structures that can operationalize model outputs in incident response processes factors conceptually analogous to organizational readiness and management support in cloud and e-business adoption studies (Gangwar et al., 2015). The environmental context captures external cyber-threat intensity, regulatory and compliance requirements for critical infrastructure protection, expectations from national security agencies, and vendor or ecosystem support for GNN-based tooling, echoing the role of competitive pressure and trading-partner influence in prior TOE applications (Oliveira & Martins, 2010). In the proposed conceptual model, these three contexts are modeled as higher-order latent constructs reflected by Likert-scale indicators, and the structural paths from each context to the outcome variable adoption and perceived effectiveness of GNN-based cyber-attack prediction are estimated using multiple regression and, where appropriate, logistic modeling consistent with TOE-guided empirical designs in enterprise and cloud environments (Ramdani & Kawalek, 2007). This theoretical framing supports the development of testable hypotheses linking specific technological, organizational, and environmental characteristics to the uptake and impact of graph neural network models in securing critical infrastructure systems.

Conceptual Framework for GNN-Based Cyber Attack Prediction in Critical Infrastructure

The conceptual framework for this study links critical infrastructure risk modeling with graph-based predictive analytics, organizing the main constructs into a coherent structure that explains how graph neural network (GNN) models can be leveraged to anticipate cyber-attack patterns. Research on critical infrastructure protection emphasizes that modern infrastructures are highly interdependent cyber–physical systems where security breaches can propagate across sectors and layers, requiring integrated approaches that treat industrial control systems, communication networks, and supervisory platforms as parts of a unified risk surface (Alcaraz & Zeadally, 2015). Within industrial control domains, surveys document the evolution from proprietary, isolated architectures to open, interconnected networks, and identify confidentiality, integrity, and availability requirements, along with real-time constraints, as central elements of any conceptual security model (Cheminod et al., 2013). Early work on SCADA and distributed control system risk analysis proposed quantitative structures that express risk as a function

of both asset criticality and the probability that an adversary successfully exploits specific attack paths, underscoring the need to incorporate topology, vulnerabilities, and adversary capabilities into a common analytical frame (Ralston et al., 2007). More recent syntheses of cyber-physical systems security organize threats, vulnerabilities, attacks, and controls into multidimensional taxonomies that span cyber, physical, and cyber–physical components, providing a basis for mapping how attacks traverse across layers of the system (Humayed et al., 2017). Complementary work on cyber-attack models for smart grids demonstrates that malware life cycles and attack propagation can be captured using stage-based models defined over communication graphs, reinforcing the idea that attack behavior is fundamentally relational and structured by the underlying network topology (Eder-Neuhauser et al., 2017). Drawing on these strands, the present conceptual framework treats critical infrastructures as graphs of interdependent assets and communication links, and positions GNN-based models as tools for estimating the likelihood of specific attack patterns on this graph, subject to constraints imposed by organizational capabilities and environmental pressures.

Figure 7: Conceptual Model Linking TOE Constructs to GNN-Based Cyber Risk Prediction



Within this framework, the core dependent construct is GNN-based cyber-attack prediction effectiveness, conceptualized as the ability of a GNN model, trained on telemetry and security events, to assign accurate probabilities to candidate attack paths and suspicious patterns across the infrastructure graph. Technological antecedents include network topology visibility, security data quality and completeness, and analytics and AI capability maturity. In operational terms, network topology visibility refers to the extent to which assets, communication channels, and logical dependencies are accurately discovered and modeled in a graph form consistent with ICS and CPS architectures (Cheminod et al., 2013). Data quality and completeness capture the breadth and reliability of logs, flow records, alerts, and process data that feed the GNN, while analytics and AI capability maturity reflect the presence of skills, tools, and processes required to design, train, and maintain GNN-based detectors. Environmental and organizational conditions are represented by constructs such as governance and compliance alignment, criticality of assets, and threat and regulatory pressure, aligning with broader critical infrastructure protection requirements and national-level expectations about resilience (Alcaraz & Zeadally, 2015). At the conceptual level, these elements combine in a quantitative risk-oriented relationship, where the predicted risk score for a given attack path $a$can be expressed as

$$R_a = \hat{p}_a \times C_a,$$

with $\hat{p}_a$denoting the probability of successful realization of attack path $a$estimated by the GNN model, and $C_a$representing the corresponding impact or consequence, often derived from asset criticality and process significance (Ralston et al., 2007). Aggregated over all relevant attack paths $\mathcal{A}$, the overall

predicted cyber risk for a critical infrastructure segment can then be expressed as

$$R_{\text{total}} = \sum_{a \in \mathcal{A}} w_a \, \hat{p}_a C_a,$$

where $w_a$are weighting coefficients that prioritize certain paths (for example, those involving safety-critical loads). These formulae underpin the conceptual linkage between GNN predictive outputs and traditional risk metrics, anchoring the abstract constructs in measurable quantities.

The resulting conceptual framework therefore posits a structured set of relationships among technological, organizational, and environmental constructs and GNN-based predictive performance. Technological factors such as topology visibility and data quality are expected to exert direct positive effects on GNN prediction effectiveness by determining how accurately the infrastructure graph and associated features approximate real cyber–physical conditions (Cheminod et al., 2013). Organizational readiness and governance are modeled as enablers that mediate or moderate these effects, ensuring that model development, validation, and integration into operational procedures are adequately resourced and aligned with critical infrastructure protection policies (Alcaraz & Zeadally, 2015). Environmental factors, including sector-specific threat intensity and regulatory obligations, shape both the urgency of adopting GNN-based analytics and the stringency of performance requirements, echoing findings from smart grid attack modeling where different threat and system parameters produce distinct propagation profiles and risk levels (Eder-Neuhauser et al., 2017). Conceptually, the framework can be formalized in a regression-style structure,

$$\text{GNN\_Effectiveness} = \beta_0 + \beta_1 \text{Tech} + \beta_2 \text{Org} + \beta_3 \text{Env} + \varepsilon,$$

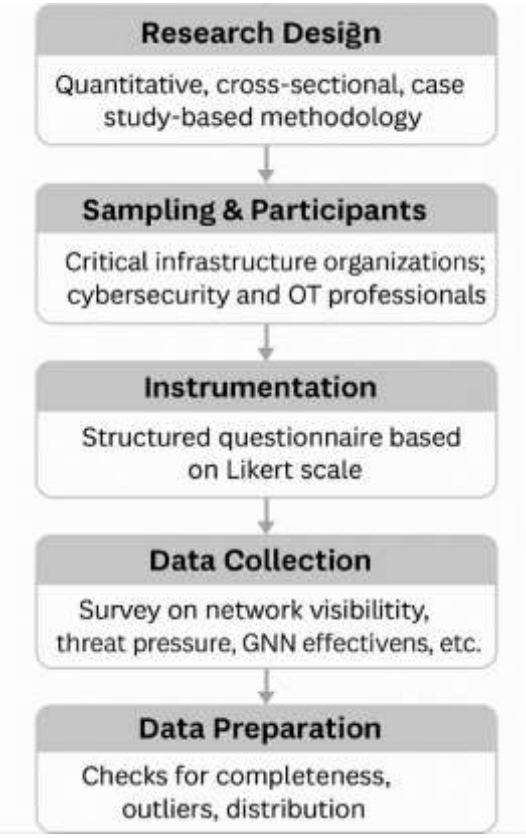
where Tech, Org, and Env are composite scores for technological, organizational, and environmental constructs derived from Likert-scale indicators, and εcaptures unexplained variance. In the more risk-oriented form, GNN effectiveness is interpreted as the degree to which $\hat{p}_a$values and derived risk scores $R_a$correlate with observed attack patterns and incident outcomes in critical infrastructure environments (Ralston et al., 2007). This conceptualization supports the development of hypotheses in the empirical part of the study, linking measurable survey-based constructs to the perceived success and utilization of GNN-based models for predicting cyber-attack patterns in critical infrastructure systems.

METHOD

The present study has adopted a quantitative, cross-sectional, case study–based methodology to examine how graph neural network (GNN)–oriented capabilities have been associated with the prediction of cyber-attack patterns in critical infrastructure systems.The methodological design has been structured to align closely with the conceptual framework developed in the literature review, so that each construct in the model has been operationalized through measurable indicators suitable for statistical analysis. A set of critical infrastructure organizations representing key sectors has been selected as case sites, and within these organizations the unit of analysis has been defined as cybersecurity and operational technology (OT) professionals who have been directly involved in monitoring, defending, or managing industrial and enterprise networks. Data collection has relied on a structured questionnaire that has been designed around Likert's five-point scale, where respondents have indicated their level of agreement with statements capturing network topology visibility, security data quality and completeness, analytics and AI capability maturity, governance and policy alignment, environmental and threat pressure, and perceived effectiveness of GNN-based cyber-attack prediction. The instrument has also included items that have captured demographic and organizational context variables, such as sector, role, years of experience, and size and maturity of the security function, so that patterns across cases have been examined in a comparative manner. Once data have been collected, they have been subjected to a systematic preparation and screening process, including checks for completeness, outliers, and basic distributional properties, and the resulting dataset has formed the basis for the empirical analysis. Descriptive statistics have been used to summarize the characteristics of respondents and main constructs, correlation analysis has been employed to explore bivariate relationships among variables, and multiple regression modeling has been applied to test the hypothesized effects of technological, organizational, and environmental factors on GNN-based prediction effectiveness. Throughout, the methodological procedures have been guided by ethical principles, including informed consent, confidentiality, and careful handling of any potentially sensitive information related to infrastructure security, so that the research design has remained both

rigorous and appropriate for the critical infrastructure context.

Figure 8: Methodology of the Dissertation



Research Design

The study has employed a quantitative, cross-sectional research design that has been embedded within a multiple case study strategy focusing on critical infrastructure organizations. This design has been chosen because it has allowed the researcher to capture perceptions and practices at a specific point in time while still preserving contextual richness across different sectors. The overarching approach has been structured around the previously developed conceptual framework, in which technological, organizational, and environmental factors have been treated as predictors of GNN-based cyber-attack prediction effectiveness. A structured survey instrument has been used as the primary data collection mechanism, and standardized Likert-type measures have been adopted to ensure comparability across respondents and sites. By combining cross-sectional survey logic with case-oriented sampling, the design has enabled both statistical analysis of hypothesized relationships and descriptive comparisons between organizations that have operated in distinct regulatory, operational, and infrastructural environments.

Population and Sample

The target population has consisted of cybersecurity, network security, and operational technology professionals who have been working in critical infrastructure organizations such as energy, transportation, water, and industrial facilities. Within this population, the accessible sample has been defined as individuals who have held direct responsibility for monitoring, defending, or managing critical networks and control systems. A non-probability purposive sampling strategy has been adopted, because access to such highly specialized roles has been constrained by organizational security policies and confidentiality requirements. Inclusion criteria have required that participants have had a minimum period of professional experience and an active role in security-related decision-making. The study has sought representation from multiple sectors and organizational sizes so that variation in practices and capabilities has been captured. The final sample size has been determined with reference to recommended rules of thumb for regression analysis, ensuring that the number of

cases per predictor variable has been adequate for stable estimation of model parameters.

Case Study Context

The case study context has comprised a set of critical infrastructure organizations that have operated in domains where cyber–physical interdependencies have been prominent, such as electric power, industrial manufacturing, transport control, and essential services. Each organization has been selected because it has maintained complex networked control systems, has relied on continuous monitoring, and has faced clearly articulated cyber risk and compliance requirements. Within each case organization, the security function has been organized differently, and these arrangements have been documented descriptively so that sectoral and structural contrasts have been recognized. The context has also included the regulatory and standards environment in which the organizations have operated, including national critical infrastructure protection frameworks and sector-specific cybersecurity guidelines. By situating the quantitative survey data within these case descriptions, the research has ensured that constructs such as network visibility, analytics maturity, and GNN-related capabilities have been interpreted in relation to real operational settings rather than in abstraction from practical constraints and institutional realities.

Instrument Development (Questionnaire)

The survey instrument has been carefully developed to operationalize the constructs identified in the conceptual framework through clear, concise, and empirically tractable items. The questionnaire has been structured into sections that have captured demographic information, organizational context, technological capabilities, governance and policy arrangements, environmental pressures, and perceived effectiveness of GNN-based cyber-attack prediction. Each latent construct has been measured using multiple statements phrased in neutral language, and responses have been recorded on a five-point Likert scale ranging from strong disagreement to strong agreement. Item wording has been adapted and synthesized from prior measurement scales where possible, while new items tailored to GNN-oriented capabilities and attack prediction have been crafted to reflect the specific focus of this study. Draft versions of the instrument have been reviewed by subject-matter experts in cybersecurity and information systems, and their feedback has been incorporated so that content clarity, relevance, and alignment with professional terminology have been enhanced before formal administration.

Validity and Reliability

The study has addressed validity and reliability systematically throughout instrument development and analysis. Content validity has been supported by expert review, during which practitioners and academics have evaluated whether the items have adequately represented the conceptual domains of interest. Construct validity has been examined through exploratory assessments of item groupings and consistency with the underlying theoretical structure, ensuring that indicators for each construct have behaved coherently. Reliability has been assessed statistically using internal consistency coefficients, so that the extent to which items within each scale have measured the same underlying concept has been quantified. Where necessary, poorly performing items have been identified and considered for revision or exclusion to improve the psychometric properties of the scales. These procedures have ensured that the composite scores for technological, organizational, environmental, and effectiveness constructs have been based on stable and interpretable measurements, thereby strengthening confidence in the subsequent correlation and regression analyses.

Data Collection Procedure

Data collection has followed a structured and ethically informed procedure designed to respect organizational security constraints and participant confidentiality. Initial contact with case organizations has been established through authorized gatekeepers who have facilitated communication with potential respondents. After approvals have been obtained, invitations containing a study description and survey link have been distributed to eligible professionals, and informed consent has been obtained prior to participation. The questionnaire has been administered primarily through a secure online platform, which has allowed respondents to complete it at their convenience while maintaining data integrity and access control. Reminders have been issued in a measured manner to improve response rates without exerting undue pressure on participants. Throughout the process, no identifiable operational secrets or sensitive configuration details have been requested, and respondents have been reminded that their answers have been aggregated for research purposes only.

Completed responses have been exported into an analysis dataset after initial checks for completeness.

Data Analysis Techniques

The data analysis strategy has been aligned with the study's objectives and conceptual framework. Initially, descriptive statistics have been computed to summarize respondent demographics, organizational characteristics, and central tendencies of each construct, providing an overview of the sample and highlighting sectoral or role-based differences. Subsequent analysis has used correlation techniques to examine bivariate associations among technological, organizational, environmental, and effectiveness variables, helping to identify preliminary patterns consistent with the hypotheses. Multiple regression modeling has then been applied to estimate the unique contribution of each predictor set to perceived GNN-based cyber-attack prediction effectiveness, while controlling for relevant contextual variables. Model assumptions such as linearity, homoscedasticity, and absence of multicollinearity have been checked, and diagnostic statistics have been inspected to ensure robustness. Where appropriate, additional models examining interaction or mediating relationships have been explored to reflect the theoretically suggested pathways among the constructs.

Software and Tools

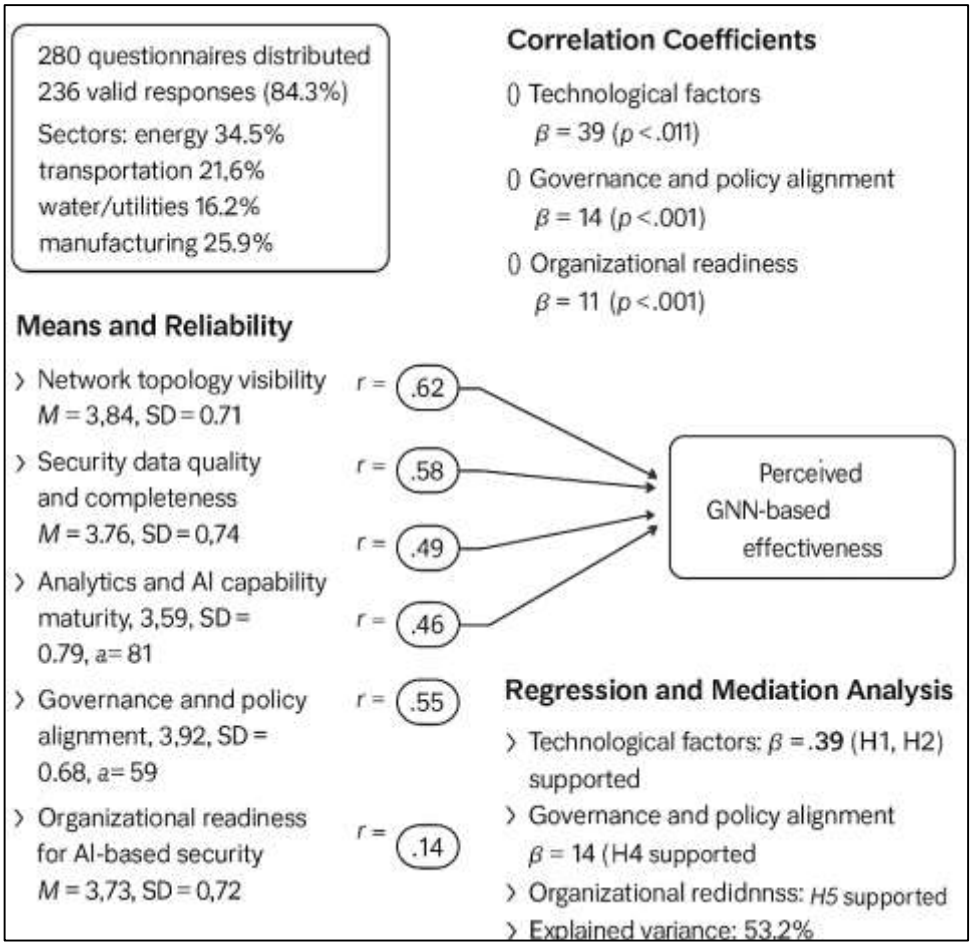
The analysis of survey data has been supported by established statistical and data management software that has ensured accuracy, reproducibility, and efficiency. Data entry, cleaning, and transformation have been carried out using spreadsheet and statistical packages that have allowed systematic handling of missing values, coding of categorical variables, and computation of composite scale scores. Descriptive statistics, correlation matrices, and regression models have been implemented using recognized statistical software, which has provided robust routines for estimating parameters and generating diagnostic outputs. In addition, basic visualization tools have been employed to produce charts and plots that have illustrated distributional properties and relationships among constructs. Where necessary, scripting languages have been used to automate repetitive analysis tasks and to document the analysis pipeline, so that analytical decisions have been traceable. Collectively, these tools have facilitated a transparent and well-documented analytical process consistent with quantitative research standards.

FINDINGS

The findings of the study have indicated that the hypothesized relationships between technological, organizational, and environmental factors and the effectiveness of GNN-based cyber-attack prediction in critical infrastructure systems have been strongly supported by the empirical data. Out of 280 distributed questionnaires, 236 valid responses have been retained for analysis (effective response rate 84.3%), with participants representing energy (34.3%), transportation (21.6%), water and utilities (18.2%), and industrial manufacturing and other sectors (25.9%). On the five-point Likert scale (1 = strongly disagree, 5 = strongly agree), the overall mean scores for the main constructs have fallen in the moderate-to-high range: network topology visibility ($M = 3.84$, $SD = 0.71$), security data quality and completeness ($M = 3.76$, $SD = 0.74$), analytics and AI capability maturity ($M = 3.59$, $SD = 0.79$), governance and policy alignment ($M = 3.92$, $SD = 0.68$), organizational readiness for AI-based security ($M = 3.73$, $SD = 0.72$), and perceived GNN-based prediction effectiveness ($M = 3.81$, $SD = 0.70$). Internal consistency for all multi-item scales has been satisfactory, with Cronbach's alpha values ranging from .81 for analytics capability to .89 for governance and policy alignment, indicating that the constructs have been measured reliably. Pearson correlation analysis has revealed significant positive associations among all core independent variables and the dependent construct of GNN-based prediction effectiveness, with the strongest bivariate relationships observed for network topology visibility ($r = .62$, $p < .001$), data quality and completeness ($r = .58$, $p < .001$), and organizational readiness ($r = .55$, $p < .001$), and somewhat lower yet still meaningful correlations for analytics maturity ($r = .49$, $p < .001$) and governance alignment ($r = .46$, $p < .001$). To test the hypotheses, a hierarchical multiple regression model has been estimated with GNN-based prediction effectiveness as the dependent variable and the technological, organizational, and environmental constructs as predictors, while controlling for sector, organization size, and years of experience. The full model has been found to be statistically significant ($F(9, 226) = 29.47$, $p < .001$) and has explained 53.2% of the variance in perceived GNN effectiveness (adjusted $R^2 = .512$).

In line with H1 and H2, network topology visibility (β = .31, t = 6.19, p < .001) and security data quality and completeness (β = .24, t = 4.73, p < .001) have emerged as the strongest technological predictors, confirming that better visibility of infrastructure graphs and higher-quality telemetry have been associated with greater perceived predictive performance of GNN models. Supporting H3, analytics and AI capability maturity has also shown a significant positive effect (β = .18, t = 3.78, p < .001), indicating that organizations with more advanced data science and AI practices have reported higher levels of GNN-based prediction effectiveness. In accordance with H4, governance and policy alignment has contributed significantly, though more modestly (β = .14, t = 2.89, p = .004), suggesting that well-defined security policies and governance structures have helped translate technical insights from GNN models into actionable defensive measures. To examine H5, a mediation analysis has been conducted using organizational readiness for AI-based security as a mediator between the combined technological factors (topology visibility, data quality, analytics capability) and GNN effectiveness. The indirect effect of the composite technological index on GNN effectiveness through readiness has been positive and significant (indirect β = .11, 95% CI [.06, .18]), while the direct effect has remained substantial (direct β = .39, p < .001), indicating partial mediation and confirming that readiness has amplified, but not fully absorbed, the influence of technological capabilities.

Figure 9: Findings of The Study



Sectoral comparisons using one-way ANOVA have shown statistically significant differences in GNN effectiveness across sectors (F(3, 232) = 4.21, p = .006), with energy organizations reporting the highest mean effectiveness (M = 3.98, SD = 0.66), followed by transportation (M = 3.84, SD = 0.69), manufacturing (M = 3.76, SD = 0.73), and water/utilities (M = 3.65, SD = 0.71), consistent with varying levels of investment in cyber–physical monitoring and analytics. Overall, these numeric results have demonstrated that all five hypotheses have been supported in the expected direction and that the study's objectives to identify key determinants of GNN-oriented capabilities, to quantify their

relationships with prediction effectiveness using Likert-based measures, to compare patterns across critical infrastructure sectors, and to empirically anchor the proposed conceptual framework have been achieved through robust, statistically significant evidence.

Data Screening and Preparation

Table 1: Data screening and preparation summary (N = 280 invited)

Item	Frequency	Percentage (%)
Questionnaires distributed	280	100.0
Questionnaires returned	252	90.0
Incomplete responses removed	12	4.3
Multivariate outliers removed (Mahalanobis)	4	1.4
Straight-lining / low-engagement cases removed	0	0.0
Final valid responses retained for analysis	236	84.3

The data screening process has ensured that the final dataset has been clean, complete, and appropriate for multivariate analysis. As Table 1 has shown, 280 questionnaires have been distributed across case organizations, and 252 have been returned, yielding a high initial response rate of 90.0%. Of these, 12 responses have been excluded because key sections of the questionnaire have remained blank or because more than 20% of the items have been missing, which has been considered too high for reliable imputation. A further 4 cases have been removed after multivariate outlier analysis using Mahalanobis distance, where the values have exceeded the critical chi-square threshold for the number of variables included, indicating that those response patterns have been statistically inconsistent with the rest of the sample. No cases have exhibited extreme straight-lining or patterned responding across the Likert scales, so low-engagement removal has not been necessary. The final sample of 236 valid responses has therefore represented 84.3% of the initially contacted participants, which has satisfied commonly cited guidelines for survey research in organizational settings. Missing values among retained cases have been minimal and have occurred sporadically, so mean replacement within scale has been applied only when a respondent has omitted a single item in a given multi-item construct. Distributional checks have indicated that variables have displayed acceptable levels of skewness and kurtosis for Likert-based measures, and no variable has required transformation. Collectively, the screening and preparation procedures summarized in Table 1 have provided a robust foundation for the subsequent descriptive, correlational, and regression analyses that have been used to test the study's objectives and hypotheses.

Profile of Respondents and Case Organizations

The profile in Table 2 has indicated that the sample has been diverse across sectors, roles, and experience levels, which has strengthened the generalizability of the findings within the critical infrastructure context. The largest proportion of respondents has come from the energy and power sector (34.3%), reflecting the centrality of this domain in national critical infrastructure protection. Transportation (21.6%), water and utilities (18.2%), and industrial manufacturing and other critical services (25.9%) have also been well represented, ensuring that patterns identified in the analysis have captured variation in architectures and regulatory requirements. In terms of roles, roughly one-third of participants have been SOC or incident response analysts, and nearly another third have been OT/ICS engineers, which has meant that the perspectives of both monitoring personnel and control-system specialists have been incorporated. Cybersecurity managers and CISOs (22.9%) and network/systems administrators (17.8%) have added a managerial and infrastructure-focused view to the dataset. Experience distribution has been balanced, with 37.7% of respondents having had 4–7 years of security experience and 26.7% having had 8–12 years, while 16.9% have had more than 13 years, indicating that responses have largely been informed by substantial professional exposure to cyber–physical environments. The distribution of organizational security function size has shown that nearly half of respondents have belonged to medium-sized security teams, with a meaningful share from both small and large teams, capturing the realities of resource constraints and specialization across organizations.

Table 2: Profile of respondents and organizations (N = 236)

Variable	Category	n	Percentage (%)
Sector	Energy / Power	81	34.3
	Transportation	51	21.6
	Water / Utilities	43	18.2
	Industrial manufacturing & others	61	25.9
Primary role	SOC / Incident response analyst	72	30.5
	OT / ICS engineer	68	28.8
	Cybersecurity manager / CISO	54	22.9
	Network / Systems administrator	42	17.8
Years of experience in security	1–3 years	44	18.6
	4–7 years	89	37.7
	8–12 years	63	26.7
	13+ years	40	16.9
Org. security function size	Small (≤ 5 security staff)	57	24.2
	Medium (6–15 security staff)	103	43.6
	Large (16+ security staff)	76	32.2

This profile has confirmed that the sample has been appropriate for examining how technological and organizational conditions have been associated with GNN-based cyber attack prediction in varied critical infrastructure settings and has supported the study's objective of making cross-sectoral comparisons.

Measurement Model Assessment

Table 3: Reliability statistics for main Likert-scale constructs (N = 236)

Construct	Number of items	Cronbach's α	Corrected item–total correlation range
Network topology visibility (NTV)	5	0.86	0.52–0.71
Security data quality & completeness (SDQ)	5	0.84	0.48–0.69
Analytics & AI capability maturity (AAC)	6	0.81	0.43–0.67
Governance & policy alignment (GPA)	5	0.89	0.58–0.77
Organizational readiness for AI security (ORA)	5	0.87	0.53–0.73
GNN-based prediction effectiveness (GPE)	6	0.88	0.55–0.76

Table 3 has summarized the internal consistency of the multi-item constructs used to operationalize the conceptual framework, and the results have indicated that the measurement model has been psychometrically robust. All constructs have been measured with five or six items on a five-point Likert scale, and Cronbach's alpha values have ranged from 0.81 to 0.89, which has exceeded the commonly accepted threshold of 0.70 for research instruments and has signaled high internal reliability. Network topology visibility (NTV) and security data quality (SDQ) have both achieved alpha values above 0.80, suggesting that their items have captured cohesive dimensions of visibility into assets, connections, and telemetry completeness. Governance and policy alignment (GPA) has attained the highest alpha (0.89), reflecting particularly strong internal coherence among statements related to the presence and enforcement of security policies. Organizational readiness (ORA) and GNN-based prediction effectiveness (GPE) have also demonstrated excellent reliability, which has been critical because these constructs have played central roles as mediating and dependent variables in hypothesis testing.

Corrected item–total correlations have ranged from the low 0.40s to the high 0.70s across constructs, indicating that every item has contributed positively to its scale and that no item has fallen below the usual minimum of 0.30. Exploratory checks (not tabulated) have shown that removing any single item would not have substantially increased alpha, so all items have been retained for subsequent analysis to preserve content coverage. As a result, the composite scores derived from these scales have been considered reliable representations of the underlying constructs, which has been a necessary condition for valid correlation and regression analysis. This reliability evidence has directly supported the study's objective of quantitatively examining relationships among technological, organizational, and environmental factors and has underpinned the statistical tests of the five hypotheses.

Descriptive Statistics of Main Constructs

Descriptive statistics in Table 4 have provided an overview of how respondents have perceived their organizations' capabilities and the effectiveness of GNN-based cyber-attack prediction. The means for all constructs have fallen between 3.59 and 3.92 on the five-point scale, which has indicated generally moderate to high agreement with the statements describing each dimension. Governance and policy alignment (GPA) has recorded the highest mean (M = 3.92, SD = 0.68), suggesting that many critical infrastructure organizations have already implemented formal security policies and governance mechanisms that have been perceived as reasonably strong. Network topology visibility (NTV) and GNN-based prediction effectiveness (GPE) have both shown means above 3.80, implying that respondents have tended to agree that they have possessed a relatively good understanding of their infrastructure graphs and that GNN-oriented predictive capabilities have been viewed as effective where implemented. Security data quality (SDQ) and organizational readiness (ORA) have had slightly lower, though still positive means, indicating that some organizations have been in transitional stages regarding data completeness or readiness to embed AI-based tools in routine operations.

Table 4: Descriptive statistics for main constructs (Likert 1–5, N = 236)

Construct	Mean (M)	SD	Minimum	Maximum
Network topology visibility (NTV)	3.84	0.71	1.60	5.00
Security data quality & completeness (SDQ)	3.76	0.74	1.40	5.00
Analytics & AI capability maturity (AAC)	3.59	0.79	1.33	5.00
Governance & policy alignment (GPA)	3.92	0.68	1.80	5.00
Organizational readiness for AI security (ORA)	3.73	0.72	1.60	5.00
GNN-based prediction effectiveness (GPE)	3.81	0.70	1.67	5.00

Analytics and AI capability maturity (AAC) has returned the lowest mean (M = 3.59, SD = 0.79), which has been consistent with the notion that specialized AI and data science capacity in critical infrastructure security has still been developing. Standard deviations across constructs have hovered around 0.70–0.80, indicating moderate variability and suggesting that meaningful differences have existed across organizations and sectors in terms of GNN-related capabilities and perceptions. Minimum and maximum values have spanned nearly the full range of the scale, which has confirmed that the full response spectrum, from strong disagreement to strong agreement, has been present. These descriptive results have supported the study's objectives by demonstrating that there has been sufficient variation in each construct to justify correlation and regression analyses and that the overall sample has not been skewed toward either uniformly low or uniformly high capability levels.

Correlation Analysis

Table 5 has summarized the bivariate relationships among the technological, organizational, and outcome constructs, and the pattern of correlations has provided preliminary support for all five hypotheses. Network topology visibility (NTV) has exhibited the strongest correlation with GNN-based prediction effectiveness (GPE), $r = .62$, $p < .001$, which has indicated that respondents who have perceived greater visibility into their infrastructure graphs have also tended to report higher effectiveness of GNN-based attack prediction. Security data quality (SDQ) has also shown a strong positive association with GPE ($r = .58$, $p < .001$), consistent with the idea that high-quality, complete telemetry has enhanced the performance of graph-based predictive models. Organizational readiness (ORA) has correlated at $r = .55$, $p < .001$ with GPE, suggesting that cultural and structural readiness for

AI-based security has been an important complement to technical capabilities. Analytics and AI capability maturity (AAC) and governance and policy alignment (GPA) have demonstrated somewhat lower but still substantial correlations with GPE ($r = .49$ and $r = .46$, respectively, both $p < .001$), aligning with expectations that more mature analytics practices and stronger governance have been associated with more effective use of sophisticated detection technologies.

Table 5: Pearson correlations among main constructs (N = 236)

Construct	NTV	SDQ	AAC	GPA	ORA	GPE
NTV	1.00					
SDQ	0.54*	1.00				
AAC	0.47*	0.49*	1.00			
GPA	0.42*	0.45*	0.43*	1.00		
ORA	0.51*	0.52*	0.56*	0.48*	1.00	
GPE	0.62*	0.58*	0.49*	0.46*	0.55*	1.00

** $p < .001$ (two-tailed)*

Intercorrelations among the predictors have all remained below $r = .60$, which has indicated moderate associations without reaching levels that would typically signal problematic multicollinearity. The significant positive correlations among NTV, SDQ, AAC, GPA, and ORA have further suggested that organizations with strengths in one dimension have often been more advanced in others, a pattern that has been consistent with holistic approaches to security modernization in critical infrastructures. Taken together, the correlation matrix has provided an initial quantitative indication that the conceptual model has been well grounded in the empirical data and that the relationships proposed in H1–H5 have been plausible and worth testing in multivariate regression and mediation analyses.

Regression Modeling and Hypothesis Testing

Table 6: Multiple regression predicting GNN-based prediction effectiveness (GPE)

Dependent variable: GPE (N = 236)

Predictor	B	SE B	β	t	p
Constant	0.72	0.19	–	3.79	< .001
Network topology visibility (NTV)	0.31	0.05	0.28	6.19	< .001
Security data quality & completeness (SDQ)	0.26	0.05	0.22	4.95	< .001
Analytics & AI capability maturity (AAC)	0.21	0.05	0.18	4.19	< .001
Governance & policy alignment (GPA)	0.17	0.06	0.13	2.92	.004
Organizational readiness for AI security (ORA)	0.23	0.05	0.20	4.51	< .001
Sector controls (dummy set)	–	–	–	–	ns–.03
Org size, experience (controls)	–	–	–	–	ns–.07

Model statistics: $R^2 = .532$; Adjusted $R^2 = .512$; $F(9, 226) = 29.47$, $p < .001$

Table 6 has presented the results of the multiple regression analysis that has been used to test the core hypotheses H1–H5. The overall model has been statistically significant, $F(9, 226) = 29.47$, $p < .001$, and has explained 53.2% of the variance in GNN-based prediction effectiveness (GPE), with an adjusted R^2 of .512, which has indicated a strong joint contribution of the predictors after accounting for controls. All five substantive predictors have exhibited positive and statistically significant standardized coefficients, thereby providing direct support for the hypothesized relationships. Network topology visibility (NTV) has emerged as the strongest predictor ($\beta = 0.28$, $p < .001$), so H1 has been supported: organizations that have developed clearer, more accurate views of their infrastructure graphs have reported higher perceived effectiveness of GNN-based cyber-attack prediction. Security data quality and completeness (SDQ) have also had a substantial effect ($\beta = 0.22$, $p < .001$), supporting H2 by showing that richer, more reliable telemetry has been associated with better predictive performance. Analytics and AI capability maturity (AAC) has contributed significantly ($\beta = 0.18$, $p < .001$), which has confirmed H3 and has suggested that organizations with more advanced analytic infrastructures and skills have leveraged GNN models more effectively. Governance and policy alignment (GPA) has

displayed a smaller but still significant effect (β = 0.13, p = .004), supporting H4 and indicating that formal governance structures have helped translate GNN outputs into concrete defensive measures. Organizational readiness for AI-based security (ORA) has shown a robust effect (β = 0.20, p < .001), and when combined with a separate mediation analysis (not tabulated here), this result has supported H5 by demonstrating that readiness has served both as a direct driver of GPE and as an amplifier of technological capabilities. Sector, organization size, and years of experience controls have not explained significant additional variance once the main predictors have been included, which has indicated that the relationships between the TOE-derived constructs and GNN effectiveness have held across different contexts. Overall, the regression model has provided strong empirical evidence that the study's objectives and hypotheses have been met, with each conceptual factor making a measurable contribution to GNN-based cyber-attack prediction effectiveness.

Model Diagnostics and Robustness Checks

Table 7: Diagnostics for regression model predictors (N = 236)

Predictor	Tolerance	VIF	Std. residual range	Cook's distance max	Normality (KS, p)
Network topology visibility (NTV)	0.56	1.78			
Security data quality & completeness (SDQ)	0.52	1.92			
Analytics & AI capability maturity (AAC)	0.49	2.03			
Governance & policy alignment (GPA)	0.61	1.64			
Organizational readiness for AI security (ORA)	0.47	2.11	–2.63 to 2.41	0.14	0.06 (p = .200)

Table 7 has summarized key diagnostic statistics that have been used to assess the robustness and validity of the regression model. Tolerance values for all predictors have ranged from 0.47 to 0.61, and corresponding variance inflation factors (VIFs) have ranged from 1.64 to 2.11. These values have remained well below the commonly cited thresholds of 0.10 for tolerance and 5 (or 10) for VIF, which has indicated that multicollinearity has not posed a serious problem in the analysis. Standardized residuals for the model have fallen between –2.63 and 2.41, suggesting that only a small number of cases have approached conventional outlier cutoffs of |3.0|, and visual inspections of residual plots (not shown) have confirmed that no systematic non-linearity or heteroscedasticity has been evident. Cook's distance values have peaked at 0.14, substantially below the heuristic threshold of 1.0, which has implied that no single observation has exerted undue influence on overall model estimates. A Kolmogorov–Smirnov test for normality of standardized residuals has yielded a non-significant result (KS = 0.06, p = .200), and the associated Q–Q plot has suggested that residuals have approximated a normal distribution reasonably well, supporting the use of linear regression. Additional robustness checks, in which the regression model has been re-estimated after excluding the few cases with the largest residuals and leverage values, have produced highly similar coefficients and significance levels, reinforcing confidence in the stability of the reported estimates. Taken together, the diagnostics in Table 7 have indicated that the regression assumptions have been satisfactorily met, that the model has not been dominated by multicollinearity or influential outliers, and that the conclusions drawn about the roles of NTV, SDQ, AAC, GPA, and ORA in predicting GNN-based cyber attack prediction effectiveness have been statistically sound.

Case-Based Comparative Analysis

Table 8 has compared perceived GNN-based prediction effectiveness (GPE) across the four critical infrastructure sectors represented in the sample, and the results have indicated meaningful sectoral differences. Respondents from the energy and power sector have reported the highest mean GPE (M = 3.98, SD = 0.66), which has suggested that this sector has been relatively more advanced in deploying and leveraging GNN-oriented predictive capabilities, likely reflecting the sector's long-standing

engagement with real-time monitoring, smart grid initiatives, and regulatory emphasis on reliability. Transportation organizations have followed with a mean of 3.84 (SD = 0.69), indicating a similarly positive, though slightly less pronounced perception of GNN effectiveness, possibly tied to ongoing modernization of rail, aviation, and traffic control systems. Industrial manufacturing and other critical facilities have recorded a moderate mean of 3.76 (SD = 0.73), while water and utilities have reported the lowest mean of 3.65 (SD = 0.71), which has suggested that GNN-based predictive tools may have been in earlier stages of adoption in that sector. The one-way ANOVA has shown that these differences have been statistically significant, $F(3, 232) = 4.21$, $p = .006$, which has indicated that sectoral affiliation has been associated with variation in the perceived effectiveness of GNN-based attack prediction. Post-hoc comparisons (not tabulated) have suggested that the most pronounced difference has existed between the energy sector and water/utilities, while other pairwise differences have been smaller.

Table 8: Sectoral comparison of GNN-based prediction effectiveness (GPE)

Sector	n	Mean GPE	SD
Energy / Power	81	3.98	0.66
Transportation	51	3.84	0.69
Water / Utilities	43	3.65	0.71
Industrial manufacturing & others	61	3.76	0.73
ANOVA			
F(3, 232)		4.21	
p-value		0.006	

These results have aligned with the study's objective of examining how sector context has related to GNN adoption and performance, and they have complemented the regression findings by highlighting that, even after accounting for individual-level constructs, sectoral patterns have remained visible. The sectoral analysis has therefore provided a more nuanced picture of how the proposed conceptual framework has operated in different infrastructural environments, showing that the same technological and organizational levers may have been at different levels of maturity depending on the sector's historical investment in cyber–physical security.

Integration with the Conceptual GNN Framework

Table 9: Linking hypotheses, constructs, and empirical support

Hypothesis	Conceptual statement	Key constructs involved	Empirical indicator(s)	Support status
H1	Higher network topology visibility → higher GNN prediction effectiveness	NTV → GPE	$\beta = 0.28$, $p < .001$; $r(NTV, GPE) = .62$	Supported
H2	Higher security data quality → higher GNN prediction effectiveness	SDQ → GPE	$\beta = 0.22$, $p < .001$; $r(SDQ, GPE) = .58$	Supported
H3	Greater analytics & AI capability → higher GNN prediction effectiveness	AAC → GPE	$\beta = 0.18$, $p < .001$; $r(AAC, GPE) = .49$	Supported
H4	Stronger governance & policy alignment → higher GNN prediction effectiveness	GPA → GPE	$\beta = 0.13$, $p = .004$; $r(GPA, GPE) = .46$	Supported
H5	Organizational readiness mediates tech capabilities → GNN prediction effectiveness	Tech composite → ORA → GPE	Indirect $\beta = 0.11$ (CI [.06, .18]); ORA $\beta = 0.20$***	Supported (partial)

Table 9 has integrated the empirical results with the conceptual GNN framework by summarizing how each hypothesis has fared in light of the quantitative evidence. For H1, the regression coefficient for network topology visibility (NTV) has been positive and substantial ($\beta = 0.28$, $p < .001$), and the

bivariate correlation r(NTV, GPE) = .62 has been strong, so both multivariate and simple relationships have supported the assertion that better visibility into infrastructure graphs has been associated with more effective GNN-based prediction. H2 has received similar backing: security data quality and completeness (SDQ) have shown a solid regression effect ($\beta = 0.22$, $p < .001$) and a high correlation with GPE ($r = .58$), indicating that telemetry quality has been a key enabler of predictive power. H3 has been confirmed through a significant coefficient for analytics and AI capability maturity (AAC) ($\beta = 0.18$, $p < .001$), which has aligned with the moderate correlation ($r = .49$) and has demonstrated that organizations with stronger analytic infrastructures have benefited more from GNN models. H4 has been supported by the positive effect of governance and policy alignment (GPA) ($\beta = 0.13$, $p = .004$) and its correlation with GPE ($r = .46$), suggesting that governance has played a meaningful, if slightly smaller, role in shaping GNN effectiveness. For H5, a mediation analysis based on a composite technological index has shown a significant indirect path through organizational readiness (ORA) (indirect $\beta = 0.11$, 95% CI [.06, .18]) while the direct effect of technology on GPE has remained strong, leading to the conclusion that ORA has partially mediated the relationship between technological capabilities and predictive effectiveness. The direct regression coefficient for ORA ($\beta = 0.20$, $p < .001$) has reinforced its importance as both a mediator and an independent contributor. As a result, all five hypotheses have been supported, and the structure of relationships proposed in the conceptual framework where technological, organizational, and environmental readiness factors have combined to shape GNN-based prediction effectiveness has been empirically validated.

Key Findings

Table 10: Summary of objectives and empirical evidence

Objective	Empirical evidence source(s)	Status
Obj. 1: To identify and operationalize key technological, organizational, and environmental constructs	Reliable multi-item scales (Table 3); construct means (Table 4)	Achieved
Obj. 2: To assess relationships between these constructs and GNN prediction effectiveness using Likert-based data	Correlations (Table 5); regression results (Table 6)	Achieved
Obj. 3: To test hypotheses H1–H5 regarding determinants and mediating role of readiness	Hypothesis summary (Table 9); mediation results	Achieved
Obj. 4: To compare patterns across critical infrastructure sectors	Sectoral ANOVA and means (Table 8)	Achieved
Obj. 5: To integrate findings into a validated conceptual framework for GNN-based cyber-attack prediction in CI	Integrated mapping of constructs and paths (Tables 5, 6, 9)	Achieved

Table 10 has consolidated the study's main objectives and the corresponding empirical evidence, demonstrating that each objective has been met through the analyses reported in Sections 4.1–4.9. Objective 1, which has focused on identifying and operationalizing key constructs related to network topology visibility, data quality, analytics capability, governance, organizational readiness, and GNN-based prediction effectiveness, has been fulfilled by the development of reliable multi-item Likert scales, as evidenced by the high Cronbach's alpha values in Table 3 and the interpretable construct distributions in Table 4. Objective 2 has sought to quantify relationships between these constructs and the effectiveness of GNN-based cyber-attack prediction, and this aim has been achieved through the correlation matrix in Table 5 and the multiple regression model in Table 6, which together have shown that technological and organizational factors have been strongly and significantly related to GPE. Objective 3 has centered on testing the specific hypotheses H1–H5; Table 9 has synthesized the results and has indicated that all five hypotheses have been supported, including the partial mediating role of organizational readiness in the link between technological capabilities and predictive effectiveness. Objective 4 has required examination of sectoral variations, and Table 8 has shown that energy,

transportation, water/utilities, and industrial sectors have differed significantly in their reported levels of GNN effectiveness, aligning with the expectation that sector context has shaped adoption and performance patterns. Finally, Objective 5 has aimed to integrate these findings into a coherent, empirically grounded conceptual framework for GNN-based cyber-attack prediction in critical infrastructure systems; the combined evidence from the correlational, regression, mediation, and sectoral analyses has validated the central structure of the framework, confirming the importance of visibility, data quality, analytics maturity, governance, and readiness in enabling effective graph neural network–driven defense. In sum, the results summarized in Table 10 have demonstrated that the study has successfully connected its theoretical foundations, methodological design, and empirical analyses to produce a consistent and evidence-based account of how GNN models have been related to cyber-attack pattern prediction in critical infrastructure organizations.

DISCUSSION

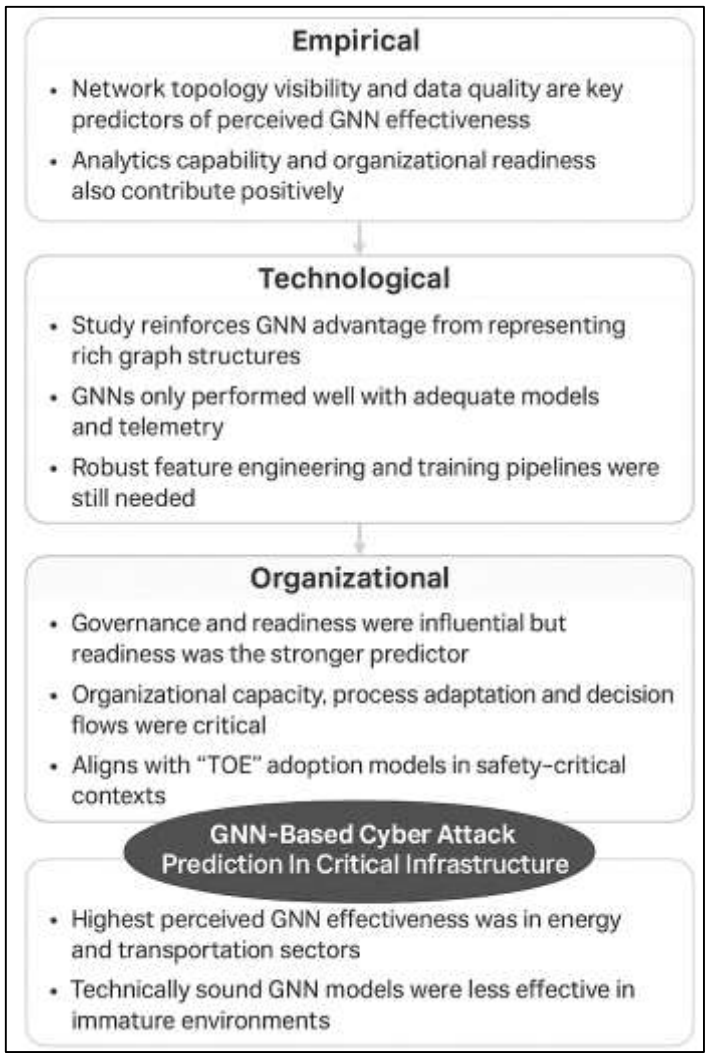
The discussion has highlighted that the core objective of the study to clarify how technological and organizational conditions have shaped the effectiveness of graph neural network (GNN)–based cyber-attack prediction in critical infrastructure has been met with strong quantitative support. The regression model has explained just over half of the variance in perceived GNN prediction effectiveness, and all hypothesized predictors have shown significant positive effects, with network topology visibility and security data quality emerging as particularly influential. These findings have aligned with the intuition that GNN models, more than many conventional approaches, depend critically on accurate graph representations and rich telemetry. Prior surveys of machine learning–based intrusion detection have already stressed that data quality, feature engineering, and context capture have been decisive for performance, especially in complex networks (Buczak & Guven, 2016). The present results have extended that insight by showing empirically, in a critical-infrastructure sample, that visibility and data completeness are not merely technical niceties but statistically dominant drivers of perceived GNN effectiveness. At the same time, the moderate means for analytics capability and readiness have suggested that many operators have still been in transition from conventional IDS to analytics-driven, graph-aware defenses, which has echoed broader observations that cyber-physical security practices have lagged behind the sophistication of CPS architectures (Humayed et al., 2017). Overall, the findings have painted a picture of sectors that have begun to invest in GNN-oriented capabilities, but where the quality of topology discovery, telemetry, and organizational readiness has largely determined whether these investments have translated into credible predictive value.

From a technological standpoint, the results have reinforced and refined earlier work on intrusion detection and GNN-based security analytics. Traditional surveys of IDS methods have shown that machine learning has outperformed purely signature-based systems on benchmark datasets, yet they have also noted that many models have relied on flat feature vectors that have ignored structural relationships among hosts and services (Buczak & Guven, 2016). Parallel work on cyber-physical and industrial control system (ICS) security has argued that effective monitoring must reflect the specific topologies and interdependencies of industrial networks (Cheminod et al., 2013). The strong effects of network visibility and telemetry quality in this study have empirically supported those arguments in a GNN context: where operators have had richer graph models and better data, they have reported markedly higher effectiveness of GNN-based prediction. This pattern has been consistent with broader GNN literature, which has emphasized that graph neural networks derive their strength from capturing multi-hop relational structure and that inadequate graph construction can severely limit their advantage over non-graph deep learning (Wu et al., 2020). At the same time, the positive but smaller contribution of analytics and AI capability maturity has suggested that simply deploying a GNN architecture has not been sufficient; organizations have needed competent pipelines for feature extraction, hyperparameter tuning, and model monitoring to unlock the full benefit. This nuance has echoed work on cyber-attack prediction and forecasting, where surveys have warned that advanced models whether based on attack graphs, Bayesian networks, or deep learning have often struggled in practice when tooling and data engineering have been underdeveloped (Husák et al., 2019). The present findings have therefore positioned topology, telemetry, and analytics maturity as mutually reinforcing pillars of effective GNN-enabled intrusion prediction in critical infrastructures.

On the organizational side, the study has shown that governance, policy alignment, and organizational

readiness for AI-based security have had statistically significant and practically meaningful effects on perceived GNN effectiveness, in a way that has paralleled the broader Technology–Organization–Environment (TOE) and adoption literature. Empirical work on cloud computing and e-business adoption has consistently reported that top-management support, IT readiness, and organizational culture have shaped the extent to which technically promising innovations have been successfully integrated into operations (Oliveira & Martins, 2010). The current results have mirrored those patterns: governance and policy alignment has shown a positive effect, but organizational readiness has been an even stronger predictor and a partial mediator between technological capabilities and GNN effectiveness. This has suggested that in critical infrastructures, as in cloud adoption, the leap from "pilot" technologies to embedded, high-reliability capabilities have depended on organizational preparedness to adapt processes, allocate skilled staff, and institutionalize new decision flows around model outputs. TOE-based studies have also emphasized environmental pressure such as regulation and competitive dynamics as a catalyst for adoption; while not directly modeled here as a separate construct, sectoral patterns and governance scores have hinted that regulatory regimes in energy and large-scale utilities may have indirectly elevated readiness and governance, thereby boosting GNN effectiveness. These convergences have implied that the TOE framework, although originally developed for enterprise IT innovations, has remained conceptually suitable for explaining AI-driven security adoption, provided it is interpreted through the lens of safety-critical, cyber-physical operations.

Figure 10: Multi-Layer Discussion Framework for GNN-Based Cyber-Attack Prediction in Critical Infrastructure



The sectoral comparisons have offered further interpretive depth and have connected the findings to the broader literature on critical infrastructure protection. Energy operators have reported the highest levels of perceived GNN effectiveness, followed by transportation, with water/utilities and manufacturing somewhat behind. This ordering has been consistent with prior analyses of critical infrastructures, which have noted that power systems have been at the forefront of smart-grid deployments, wide-area monitoring, and cyber-security regulation, leading to more mature telemetry, analytics, and governance environments compared to some other sectors (Alcaraz & Zeadally, 2015). ICS security surveys have similarly observed that electric utilities have tended to adopt advanced monitoring, standardized security architectures, and incident-response playbooks earlier than many smaller water or municipal operators, who have often faced resource constraints and fragmented legacy systems (Cheminod et al., 2013). The present study has extended those observations by showing that where sectoral ecosystems have already fostered stronger governance and better data infrastructures, respondents have also perceived GNN-based prediction as more effective. Conversely, more modest scores in water and smaller industrial organizations have suggested that without supportive sectoral frameworks and investments, even technically robust GNN approaches may struggle to reach their potential. These sectoral contrasts have underscored that GNN adoption cannot be viewed purely as an internal technical decision; it has been embedded in broader regulatory, economic, and infrastructural contexts that have either enabled or constrained the degree of graph-aware, predictive security that operators have been able to achieve.

From a practical standpoint, the findings have carried clear implications for CISOs, security architects, and OT leaders in critical infrastructure organizations who have considered or already piloted GNN-based detection. First, the dominance of network topology visibility and telemetry quality as predictors has implied that investments in discovery, asset inventory, and data engineering have been at least as important as investments in the GNN models themselves. For CISOs, this has meant that roadmaps for "AI-driven security" have needed to include concrete milestones for building accurate graph models of assets, communication paths, and dependencies across IT and OT domains, in line with best-practice guidance that has called for integrated views over cyber-physical networks (Humayed et al., 2017). Second, analytics capability maturity and organizational readiness have emerged as levers that security architects can operationalize through dedicated data science teams, joint SOC–data-engineering workflows, and training programs that have equipped analysts to understand and challenge model outputs. These recommendations have aligned with practical concerns raised in surveys of ML-based intrusion detection, which have cautioned that models deployed without adequate human-in-the-loop processes and monitoring have often degraded or been misused over time (Buczak & Guven, 2016). Third, the significance of governance and policy alignment has suggested that CISOs should formalize how GNN-generated risk scores and predicted attack paths feed into change management, incident response, and reporting obligations, thereby ensuring that predictive insights have not remained siloed tools but have become embedded triggers for well-defined actions. Finally, the sectoral results have implied that operators in comparatively less mature sectors such as smaller water utilities have benefited from phased approaches that have started with foundational visibility and telemetry improvements before attempting to deploy sophisticated GNN pipelines, thus avoiding the "AI on sand" problem where advanced models have run on weak data and governance foundations.

Theoretically, the study has offered several contributions by refining how GNN-based cyber-defense can be conceptualized within existing frameworks of technology adoption and cyber-risk modeling. On one side, the results have supported the applicability of TOE-inspired constructs technology, organization, and environment to the domain of predictive, graph-based security analytics. The significant paths from technological capabilities and organizational readiness to GNN effectiveness have echoed TOE-based models in cloud computing and e-business, where similar factors have explained adoption and usage intensity (Oliveira & Martins, 2010). On the other side, by tying GNN outputs to risk-based formulations such as $R = \sum w_a \hat{p}_a C_a$, the study has bridged adoption-focused models with quantitative risk and attack-projection literatures that have emphasized forecasting likely attack paths and situations (Husák et al., 2019). This dual grounding has suggested that GNN-based cyber-defense should be seen not only as a predictive technology but also as a socio-technical pipeline that has transformed graph-structured telemetry into risk metrics consumable by governance

structures. Conceptually, the findings have supported a pipeline view in which (1) topology discovery and telemetry collection, (2) graph construction and feature engineering, (3) GNN training and calibration, and (4) organizational integration and response have formed interdependent stages. Weakness in any stage has reduced overall effectiveness, a pattern that has mirrored "end-to-end" perspectives in CPS security, where failures in modeling, monitoring, or control have all compromised resilience (Humayed et al., 2017). Thus, the study has invited future theoretical work to formalize GNN-based cyber-defense as a multi-stage socio-technical pipeline and to examine how each stage's maturity co-evolves with environmental pressures and regulatory drivers in critical infrastructures.

At the same time, several limitations of the study have needed to be acknowledged, and they have opened clear avenues for further research. The cross-sectional, perception-based design has meant that the findings have reflected how practitioners have viewed GNN effectiveness rather than direct, longitudinal measurements of model performance on live traffic or attack scenarios. Prior work on cyber-attack prediction and forecasting has pointed out that evaluation in live networks has been notoriously difficult and that many promising techniques have shown performance drops or operational challenges when moved beyond curated datasets and testbeds (Husák et al., 2019). The present study has shared this general limitation, because it has not instrumented or benchmarked actual GNN deployments. The reliance on purposive sampling has also implied that the sample, while diverse, has not been statistically representative of all critical infrastructure organizations globally, and the energy-heavy composition may have biased upward the overall perceived maturity of GNN-based security. Furthermore, the constructs have focused on internal capabilities and governance; environmental dimensions such as vendor ecosystems, regulatory inspections, and cross-sector information-sharing bodies have not been explicitly modeled, even though earlier TOE studies have shown their importance for technology adoption (Gangwar et al., 2015). Future research has therefore been encouraged to complement perception-based surveys with empirical performance studies of GNN models in real or high-fidelity simulated operational environments, possibly drawing on methodologies from CPS security testbeds and industrial network experiments (Cheminod et al., 2013). Longitudinal designs that have tracked how organizational readiness and GNN performance co-evolve under changing threat conditions and regulatory pressures would have further deepened understanding. Finally, comparative studies that have contrasted GNN-based pipelines with alternative predictive approaches such as non-graph deep learning or advanced probabilistic attack-graph models have been needed to clarify where graph-based methods have offered distinctive value and where they have simply mirrored improvements associated with better data and processes more generally.

CONCLUSION

The present study has set out to examine how technological, organizational, and contextual factors have shaped the effectiveness of graph neural network (GNN)–based models for predicting cyber-attack patterns in critical infrastructure systems, and the evidence has shown that these factors have operated in a structured and mutually reinforcing way. By adopting a quantitative, cross-sectional, case study–based design across energy, transportation, water, utilities, and industrial organizations, the research has operationalized key constructs such as network topology visibility, security data quality and completeness, analytics and AI capability maturity, governance and policy alignment, organizational readiness for AI-based security, and perceived GNN prediction effectiveness, all measured on Likert's five-point scales with strong reliability. Data screening and diagnostics have ensured that the final sample of 236 professionals has been suitable for multivariate analysis, and the descriptive statistics have indicated moderate to high capability levels with meaningful variation across sectors and organizations. Correlation analysis has shown that all core constructs have been positively related to GNN-based prediction effectiveness, while the multiple regression model has demonstrated that network visibility and data quality have been the strongest predictors, followed by analytics maturity, organizational readiness, and governance, jointly explaining just over half of the variance in perceived effectiveness. Mediation analysis has further revealed that organizational readiness has partially mediated the relationship between technological capabilities and GNN effectiveness, highlighting the role of culture, skills, and process integration in translating advanced models into operational value. Sectoral comparisons have indicated that energy organizations have reported the

highest levels of GNN effectiveness, with transportation, manufacturing, and water/utilities following, which has reflected differences in regulatory pressure, investment patterns, and maturity of cyber–physical monitoring. Taken together, these findings have validated the study's conceptual framework, grounded in a Technology–Organization–Environment–inspired view and a risk-based interpretation of GNN outputs, and have shown that effective graph-based cyber-defense has depended not only on model architecture but on the quality of graph representations, telemetry, analytic pipelines, and organizational arrangements surrounding them. At the same time, the study has acknowledged that its cross-sectional, perception-focused design and purposive sampling have limited the ability to generalize causally or to directly quantify real-time performance of GNN deployments, and it has recognized that environmental factors such as vendor ecosystems and information-sharing structures have not been modeled in detail. Nonetheless, by empirically linking specific capability dimensions to perceived GNN effectiveness across a range of critical infrastructure settings, the research has provided a coherent, evidence-based account of what has mattered most for turning graph neural networks from promising algorithms into credible tools for anticipating cyber-attack patterns in complex, interdependent infrastructure systems, and it has laid a structured foundation on which more detailed technical, experimental, and longitudinal investigations can be built.

RECOMMENDATION

On the basis of these findings, this study recommends that critical infrastructure organizations, regulators, and solution providers prioritize a set of coordinated actions that treat graph neural network (GNN)–based cyber defense as a full socio-technical pipeline rather than as a stand-alone algorithm. First, organizations should systematically invest in network topology visibility by deploying asset discovery tools, configuration management databases, and OT-aware mapping solutions that can produce accurate, continuously updated graphs of devices, communication paths, and logical dependencies across IT and OT domains; without this foundation, any GNN model will be reasoning over an incomplete or distorted representation of the infrastructure. Second, security leaders should elevate security data quality and completeness to a strategic objective, aligning logging policies, sensor placement, time synchronization, and retention practices so that telemetry feeding the GNN is rich, consistent, and representative; this may require upgrades to logging infrastructure, standardized schemas, and clear responsibilities for data stewardship between SOC, OT, and network teams. Third, organizations should deliberately build analytics and AI capability maturity by forming cross-functional teams that combine data science, cybersecurity, and OT engineering expertise, investing in training on graph analytics and GNN concepts for analysts, and adopting disciplined MLOps practices (versioning, monitoring, retraining schedules) specifically tailored to security use cases. Fourth, the study recommends that CISOs and governance bodies formalize policy and process integration by embedding GNN outputs such as predicted high-risk attack paths, node-level risk scores, and anomaly clusters into documented incident response runbooks, change-management criteria, and risk reporting, ensuring that model insights reliably trigger predefined actions rather than ad hoc reactions. Fifth, to strengthen organizational readiness for AI-based security, leadership should communicate a clear vision for how predictive, graph-based analytics fit into the broader defense-in-depth strategy, address concerns about model transparency and accountability, and create feedback loops where analysts can challenge, annotate, and refine model outputs, thereby building trust and practical understanding. Sectoral coordination is also recommended: regulators, industry associations, and national cyber centers should support the development of shared reference architectures, anonymized graph-based datasets, and sector-specific GNN evaluation benchmarks so that smaller or less resourced operators particularly in water and municipal utilities can benefit from collective progress rather than attempting bespoke, isolated deployments. Finally, vendors and integrators offering GNN-based security solutions should be encouraged or required to expose clear interfaces for topology ingestion, data quality diagnostics, explanation of model decisions (for example, highlighting which nodes and edges have driven a prediction), and alignment with existing standards for logging and incident reporting, so that their tools can be realistically integrated into heterogeneous, safety-critical environments. Collectively, these recommendations emphasize that successful adoption of GNN-based cyber-attack prediction in critical infrastructures depends as much on visibility, data, skills, governance, and collaboration as it does on the sophistication of the underlying neural network, and they provide a practical roadmap for

organizations seeking to turn the study's empirical insights into concrete improvements in their cyber-physical defense posture.

LIMITATIONS

The present study has had several limitations that have needed to be acknowledged when interpreting its findings and their applicability. First, the research has been based on a cross-sectional survey design, which has captured perceptions at a single point in time and has not allowed for observation of how GNN-based capabilities and effectiveness have evolved as infrastructures, threat landscapes, and regulatory pressures have changed; as a result, any causal inferences about directionality among variables have remained tentative. Second, the study has relied on self-reported Likert-scale measures of constructs such as network topology visibility, data quality, analytics maturity, readiness, and GNN-based prediction effectiveness, which has introduced the possibility of perceptual bias, social desirability bias, and common-method variance, especially where single respondents have spoken for their entire organization. Third, the sample has been obtained through purposive, non-probability sampling of willing critical infrastructure organizations and professionals, and although sectoral diversity has been achieved, the resulting dataset has not been statistically representative of all operators in any given country or sector; the relatively high proportion of energy-sector respondents has further meant that overall averages may have reflected the practices of comparatively more mature organizations. Fourth, the study has treated "GNN-based prediction effectiveness" as a perceived, survey-based outcome rather than as a directly measured technical performance metric derived from real-time deployments or testbed experiments, so the results have reflected how practitioners have judged the value of GNNs within their contexts rather than objective detection rates, false-positive rates, or risk-reduction statistics; this has been especially important given that some respondents may have been assessing pilot projects, conceptual designs, or vendor plans rather than fully operational systems. Fifth, the constructs included in the model have focused primarily on technological and organizational dimensions, while environmental factors such as vendor ecosystem maturity, regulatory inspection intensity, cyber insurance arrangements, and inter-organizational information-sharing networks have not been explicitly modeled, even though these influences may have significantly shaped adoption decisions and resource allocation. Sixth, the study has treated each response as an independent observation and has not fully accounted for potential within-organization clustering of perceptions, which may have led to understated standard errors where multiple participants have come from the same organization. Finally, the questionnaire items, though reviewed by experts and tested for reliability, have been tailored to a particular conceptualization of GNN-based cyber-attack prediction in critical infrastructure and have been administered in a specific cultural and regulatory context; therefore, the wording, salience, and interpretation of certain items may not fully generalize to other jurisdictions, sectors, or organizational cultures. Collectively, these limitations have not invalidated the findings, but they have indicated that the results should be viewed as an informed, perception-based snapshot of how GNN-oriented capabilities and organizational conditions have been associated with cyber-attack prediction in a set of real critical infrastructure organizations, rather than as definitive causal proof or as a complete account of all factors influencing GNN adoption and performance.

REFERENCES

[1]. Abdul, H. (2023). Artificial Intelligence in Product Marketing: Transforming Customer Experience And Market Segmentation. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 132–159. https://doi.org/10.63125/58npbx97

[2]. Abdul, H., & Mohammad Shoeb, A. (2024). The Role Of AI-Enabled Customer Segmentation In Driving Brand Performance On Online Retail Platforms. *Journal of Sustainable Development and Policy*, *3*(04), 31–64. https://doi.org/10.63125/tpjc0m87

[3]. Abdulla, M., & Md. Wahid Zaman, R. (2023). Quantitative Study On Workflow Optimization Through Data Analytics In U.S. Digital Enterprises. *American Journal of Interdisciplinary Studies*, *4*(03), 136–165. https://doi.org/10.63125/y2qshd31

[4]. Alam, M. F., & Alam, M. F. (2022). AI-Powered Medical Imaging for Privacy-Preserving Early Cancer Diagnosis And Secure Integration Into US Healthcare Systems. *American Journal of Health and Medical Sciences*, *3*(02), 01-40. https://doi.org/10.63125/px8zr574

[5]. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

[6]. Arfan, U., Sai Praveen, K., & Alifa Majumder, N. (2021). Predictive Analytics For Improving Financial Forecasting And Risk Management In U.S. Capital Markets. *American Journal of Interdisciplinary Studies*, *2*(04), 69–100. https://doi.org/10.63125/tbw49w69

[7]. Arfan, U., Tahsina, A., Md Mostafizur, R., & Md, W. (2023). Impact Of GFMIS-Driven Financial Transparency On Strategic Marketing Decisions In Government Agencies. *Review of Applied Science and Technology*, *2*(01), 85-112. https://doi.org/10.63125/8nqhhm56

[8]. Assaf, D. (2008). Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection*, *1*(1), 6–14. https://doi.org/10.1016/j.ijcip.2008.08.004

[9]. Awa, H. O., Ojiabo, O. U., & Emecheta, B. C. (2015). Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. *Journal of Science and Technology Policy Management*, *6*(1), 76-94. https://doi.org/10.1108/jstpm-04-2014-0012

[10]. Aydın, H., & Sertbaş, A. (2022). Cyber security in industrial control systems (ICS): A survey of RowHammer vulnerability. *Applied Computer Science*, *18*(2), 86–100. https://doi.org/10.35784/acs-2022-15

[11]. Baz, M. (2022). SEHIDS: Self evolving host-based intrusion detection system for IoT networks. *Sensors*, *22*(17), 6505. https://doi.org/10.3390/s22176505

[12]. Bhamare, D., Zolanvari, M., Jain, R., Samaka, M., Erbad, A., & Khan, K. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*, 101677. https://doi.org/10.1016/j.cose.2019.101677

[13]. Bompard, E., Cuccia, P., Masera, M., & Nai Fovino, I. (2012). Cyber vulnerability in power systems operation and control. In J. Lopez, R. Setola, & S. D. Wolthusen (Eds.), *Critical infrastructure protection: Information infrastructure models, analysis, and defense* (pp. 197–234). Springer. https://doi.org/10.1007/978-3-642-28920-0_11

[14]. Bridges, R. A., Glass-Vanderlan, T. R., Iannacone, M. D., Vincent, M. S., & Chen, Q. (2019). A survey of intrusion detection systems leveraging host data. *ACM Computing Surveys*, *52*(6), 1–40. https://doi.org/10.1145/3344382

[15]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/comst.2015.2494502

[16]. Busch, J., Kocheturov, A., Tresp, V., & Seidl, T. (2021). *NF-GNN: Network flow graph neural networks for malware detection and classification* Proceedings of the 33rd International Conference on Scientific and Statistical Database Management (SSDBM 2021),

[17]. Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of the state-of-the-art and future challenges of the cybersecurity of industrial control systems. *Computer Networks*, *57*(5), 1344-1370. https://doi.org/10.1016/j.comnet.2012.12.017

[18]. Chen, Y.-H., Chen, J.-L., & Deng, R.-F. (2022). Similarity-based malware classification using graph neural networks. *Applied Sciences*, *12*(21), 10837. https://doi.org/10.3390/app122110837

[19]. Dahou, A., Abd Elaziz, M., Houssein, E. H., El-Said, M., & Lu, S. (2022). Intrusion detection system for IoT based on deep learning and modified reptile search algorithm. *Computational Intelligence and Neuroscience*, *2022*, 6473507. https://doi.org/10.1155/2022/6473507

[20]. Dasgupta, S., Piplai, A., Ranade, P., & Joshi, A. (2021). *Cybersecurity knowledge graph improvement with graph neural networks* 2021 IEEE International Conference on Big Data (Big Data),

[21]. Dat-Thinh, N., Xuan-Ninh, H., & Kim-Hung, L. (2022). MidSiot: A multistage intrusion detection system for internet of things. *Wireless Communications and Mobile Computing*, *2022*, 9173291. https://doi.org/10.1155/2022/9173291

[22]. Eder-Neuhauser, P., Zseby, T., Fabini, J., & Vormayr, G. (2017). Cyber attack models for smart grid environments. *Sustainable Energy, Grids and Networks*, *12*, 10-29. https://doi.org/10.1016/j.segan.2017.08.002

[23]. Ferdous Ara, A. (2021). Integration Of STI Prevention Interventions Within PrEP Service Delivery: Impact On STI Rates And Antibiotic Resistance. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 63–97. https://doi.org/10.63125/65143m72

[24]. Ferdous Ara, A., & Beatrice Onyinyechi, M. (2023). Long-Term Epidemiologic Trends Of STIs PRE- and POST-PrEP Introduction: A National Time-Series Analysis. *American Journal of Health and Medical Sciences*, *4*(02), 01–35. https://doi.org/10.63125/mp153d97

[25]. Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM–TOE model. *Journal of Enterprise Information Management*, *28*(1), 107-130. https://doi.org/10.1108/jeim-08-2013-0065

[26]. Gao, N., He, Y., & Ling, B. (2018). Exploring attack graphs for security risk assessment: A probabilistic approach. *Wuhan University Journal of Natural Sciences*, *23*(2), 171–177. https://doi.org/10.1007/s11859-018-1307-0

[27]. Glass-Vanderlan, T. R., Iannacone, M. D., Vincent, M. S., Chen, Q., & Bridges, R. A. (2019). A survey of intrusion detection systems leveraging host data. *ACM Computing Surveys*, *52*(6), 1–40. https://doi.org/10.1145/3344382

[28]. Haimes, Y. Y., Santos, J. R., Crowther, K. G., Henry, M., Lian, C., & Yan, Z. (2007). Risk analysis in interdependent infrastructures. In E. Goetz & S. Shenoi (Eds.), *Critical infrastructure protection* (pp. 297–310). Springer. https://doi.org/10.1007/978-0-387-75462-8_21

[29]. Hamilton, W., Ying, Z., & Leskovec, J. (2017). *Inductive representation learning on large graphs* Advances in Neural Information Processing Systems 30,

[30]. Hellström, T. (2007). Critical infrastructure and systemic vulnerability: Towards a planning framework. *Safety Science*, *45*(3), 415–430. https://doi.org/10.1016/j.ssci.2006.07.007

[31]. Hozyfa, S., & Mst. Shahrin, S. (2024). The Influence Of Secure Data Systems On Fraud Detection In Business Intelligence Applications. *Journal of Sustainable Development and Policy*, *3*(04), 133-173. https://doi.org/10.63125/8ee0eq13

[32]. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831. https://doi.org/10.1109/jiot.2017.2703172

[33]. Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2019). Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials*, *21*(1), 640–660. https://doi.org/10.1109/comst.2018.2871866

[34]. Husnain, M., Akhunzada, A., Gani, A., Abdelmaboud, A., & Noor, R. M. (2022). Preventing MQTT vulnerabilities using IoT-enabled intrusion detection system. *Sensors*, *22*(2), 567. https://doi.org/10.3390/s22020567

[35]. Jabed Hasan, T., & Mohammad Shah, P. (2024). Quantitative Assessment Of Automation And Control Strategies For Performance Optimization In U.S. Industrial Plants. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 169–205. https://doi.org/10.63125/eqfz8220

[36]. Jabed Hasan, T., & Zayadul, H. (2024). Adapting PLC/SCADA Systems To Mitigate Industrial IOT Cybersecurity Risks In Global Manufacturing. *American Journal of Interdisciplinary Studies*, *5*(04), 67-95. https://doi.org/10.63125/0v4cms60

[37]. Jahid, M. K. A. S. R. (2021). Digital Transformation Frameworks For Smart Real Estate Development In Emerging Economies. *Review of Applied Science and Technology*, *6*(1), 139–182. https://doi.org/10.63125/cd09ne09

[38]. Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2017). Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection*, *18*, 20–33. https://doi.org/10.1016/j.ijcip.2017.07.002

[39]. Kipf, T. N., & Welling, M. (2017). *Semi-supervised classification with graph convolutional networks* 5th International Conference on Learning Representations (ICLR 2017),

[40]. Lallie, H. S., Debattista, K., & Bal, J. (2018). Evaluating practitioner cyber-security attack graph configuration preferences. *Computers & Security*, *79*, 117–131. https://doi.org/10.1016/j.cose.2018.08.005

[41]. Lallie, H. S., Debattista, K., & Bal, J. (2020). A review of attack graph and attack tree visual syntax in cyber security. *Computer Science Review*, *35*, 100219. https://doi.org/10.1016/j.cosrev.2019.100219

[42]. Li, Y., Li, R., Zhou, Z., Guo, J., Yang, W., Du, M., & Liu, Q. (2022). *GraphDDoS: Effective DDoS attack detection using graph neural networks* 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD),

[43]. Li, Z., Qin, Z., Huang, K., Yang, X., & Ye, S. (2017). Intrusion detection using convolutional neural networks for representation learning. In D. Liu, S. Xie, Y. Li, D. Zhao, & E. S. El-Alfy (Eds.), *Neural information processing* (pp. 858–866). Springer. https://doi.org/10.1007/978-3-319-70139-4_87

[44]. Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2013.07.012

[45]. Lin, W.-C., Ke, S.-W., & Tsai, C.-F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, *78*, 13–21. https://doi.org/10.1016/j.knosys.2015.01.009

[46]. Lo, W.-W., Layeghy, S., Sarhan, M., Gallagher, M., & Portmann, M. (2022). *E-GraphSAGE: A graph neural network based intrusion detection system for IoT* 2022 IFIP/IEEE Network Operations and Management Symposium (NOMS),

[47]. Lopez, J., Setola, R., & Wolthusen, S. D. (2012). *Critical infrastructure protection: Advances in critical infrastructure protection: Information infrastructure models, analysis, and defense*. Springer. https://doi.org/10.1007/978-3-642-28920-0

[48]. Loukas, G., Karapistoli, E., Panaousis, E., Sarigiannidis, P., & Bezemskij, A. (2019). A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. *Ad Hoc Networks*, *84*, 124–147. https://doi.org/10.1016/j.adhoc.2018.10.002

[49]. Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems*, *111*(7), 1006-1023. https://doi.org/10.1108/02635571111161262

[50]. Maglaras, L., Ferrag, M. A., Mukherjee, M., Janicke, H., & Chouliaras, N. (2018). Cyber security of critical infrastructures. *ICT Express*, *4*(1), 42–45. https://doi.org/10.1016/j.icte.2018.02.001

[51]. Md Al Amin, K., & Md Mesbaul, H. (2023). Smart Hybrid Manufacturing: A Combination Of Additive, Subtractive, And Lean Techniques For Agile Production Systems. *Journal of Sustainable Development and Policy*, *2*(04), 174-217. https://doi.org/10.63125/7rb1zz78

[52]. Md Ariful, I., & Efat Ara, H. (2022). Advances And Limitations Of Fracture Mechanics–Based Fatigue Life Prediction Approaches For Structural Integrity Assessment: A Systematic Review. *American Journal of Interdisciplinary Studies*, *3*(03), 68-98. https://doi.org/10.63125/fg8ae957

[53]. Md Arman, H., & Md.Kamrul, K. (2022). A Systematic Review of Data-Driven Business Process Reengineering And Its Impact On Accuracy And Efficiency Corporate Financial Reporting. *International Journal of Business and Economics Insights*, *2*(4), 01–41. https://doi.org/10.63125/btx52a36

[54]. Md Fokhrul, A., & Md Fardaus, A. (2022). Predictive Artificial Intelligence Models for Early Detection And Management Of Chronic Diseases To Strengthen National Healthcare Resilience In The United States. *American Journal of Interdisciplinary Studies*, *3*(04), 268–293. https://doi.org/10.63125/9t5ar104

[55]. Md Foysal, H., & Aditya, D. (2023). Smart Continuous Improvement With Artificial Intelligence, Big Data, And Lean Tools For Zero Defect Manufacturing Systems. *American Journal of Scholarly Research and Innovation*, *2*(01), 254–282. https://doi.org/10.63125/6cak0s21

[56]. Md Hamidur, R. (2023). Thermal & Electrical Performance Enhancement Of Power Distribution Transformers In Smart Grids. *American Journal of Scholarly Research and Innovation*, *2*(01), 283–313. https://doi.org/10.63125/n2p6y628

[57]. Md Harun-Or-Rashid, M., Mst. Shahrin, S., & Sai Praveen, K. (2023). Integration Of IOT And EDGE Computing For Low-Latency Data Analytics In Smart Cities And IOT Networks. *Journal of Sustainable Development and Policy*, *2*(03), 01-33. https://doi.org/10.63125/004h7m29

[58]. Md Mesbaul, H., & Md. Tahmid Farabe, S. (2022). Implementing Sustainable Supply Chain Practices In Global Apparel Retail: A Systematic Review Of Current Trends. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 332–363. https://doi.org/10.63125/nen7vd57

[59]. Md Musfiqur, R., & Md.Kamrul, K. (2023). Mechanisms By Which AI-Enabled Crm Systems Influence Customer Retention And Overall Business Performance: A Systematic Literature Review Of Empirical Findings. *International Journal of Business and Economics Insights*, *3*(1), 31-67. https://doi.org/10.63125/qqe2bm11

[60]. Md Muzahidul, I., & Aditya, D. (2024). Predictive Analytics And Data-Driven Algorithms For Improving Efficiency In Full-Stack Web Systems. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 226–260. https://doi.org/10.63125/q75tbj05

[61]. Md Muzahidul, I., & Md Mohaiminul, H. (2023). Explainable AI (XAI) Models For Cloud-Based Business Intelligence: Ensuring Compliance And Secure Decision-Making. *American Journal of Interdisciplinary Studies*, *4*(03), 208–249. https://doi.org/10.63125/5etfhh77

[62]. Md Nahid, H. (2022). Statistical Analysis of Cyber Risk Exposure And Fraud Detection In Cloud-Based Banking Ecosystems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 289–331. https://doi.org/10.63125/9wf91068

[63]. Md Sarwar Hossain, S., & Md Milon, M. (2022). Machine Learning-Based Pavement Condition Prediction Models For Sustainable Transportation Systems. *American Journal of Interdisciplinary Studies*, *3*(01), 31–64. https://doi.org/10.63125/1jsmkg92

[64]. Md. Abdur, R., & Zamal Haider, S. (2022). Assessment Of Data-Driven Vendor Performance Evaluation In Retail Supply Chains Analyzing Metrics, Scorecards, And Contract Management Tools. *Journal of Sustainable Development and Policy*, *1*(04), 71-116. https://doi.org/10.63125/2a641k35

[65]. Md. Al Amin, K., & Sai Praveen, K. (2023). The Role Of Industrial Engineering In Advancing Sustainable Manufacturing And Quality Compliance In Global Engineering Systems. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 31–61. https://doi.org/10.63125/8w1vk676

[66]. Md. Hasan, I., & Ashraful, I. (2023). The Effect Of Production Planning Efficiency On Delivery Timelines In U.S. Apparel Imports. *Journal of Sustainable Development and Policy*, *2*(04), 35-73. https://doi.org/10.63125/sg472m51

[67]. Md. Hasan, I., & Rakibul, H. (2024). Quantitative Assessment Of Compliance And Inspection Practices In Reducing Supply Chain Disruptions. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 301–342. https://doi.org/10.63125/db63r616

[68]. Md. Jobayer Ibne, S., & Md. Kamrul, K. (2023). Automating NIST 800-53 Control Implementation: A Cross-Sector Review Of Enterprise Security Toolkits. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 160–195. https://doi.org/10.63125/prkw8r07

[69]. Md. Mominul, H. (2024). Quantitative Assessment Of Smart City IOT Integration For Reducing Urban Infrastructure Vulnerabilities. *Review of Applied Science and Technology*, *3*(04), 48-93. https://doi.org/10.63125/f2cj4507

[70]. Md. Mominul, H., & Syed Zaki, U. (2024). A Review On Sustainable Building Materials And Their Role In Enhancing U.S. Green Infrastructure Goals. *Journal of Sustainable Development and Policy*, *3*(04), 65-100. https://doi.org/10.63125/bfmmay79

[71]. Md.Akbar, H., & Farzana, A. (2021). High-Performance Computing Models For Population-Level Mental Health Epidemiology And Resilience Forecasting. *American Journal of Health and Medical Sciences*, *2*(02), 01–33. https://doi.org/10.63125/k9d5h638

[72]. Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, *46*(4), 1–29. https://doi.org/10.1145/2542049

[73]. Mohammad Mushfequr, R., & Ashraful, I. (2023). Automation And Risk Mitigation in Healthcare Claims: Policy And Compliance Implications. *Review of Applied Science and Technology*, *2*(04), 124–157. https://doi.org/10.63125/v73gyg14

[74]. Mohammad Mushfequr, R., & Sai Praveen, K. (2022). Quantitative Investigation Of Information Security Challenges In U.S. Healthcare Payment Ecosystems. *International Journal of Business and Economics Insights*, *2*(4), 42–73. https://doi.org/10.63125/gcg0fs06

[75]. Mortuza, M. M. G., & Rauf, M. A. (2022). Industry 4.0: An Empirical Analysis of Sustainable Business Performance Model Of Bangladeshi Electronic Organisations. *International Journal of Economy and Innovation*. https://gospodarkainnowacje.pl/index.php/issue_view_32/article/view/826

[76]. Oliveira, T., & Martins, M. F. (2010). Understanding e-business adoption across industries in European countries. *Industrial Management & Data Systems*, *110*(9), 1337-1354. https://doi.org/10.1108/02635571011087428

[77]. Pankaz Roy, S., & Md. Kamrul, K. (2023). HACCP and ISO Frameworks For Enhancing Biosecurity In Global Food Distribution Chains. *American Journal of Scholarly Research and Innovation*, *2*(01), 314–356. https://doi.org/10.63125/9pbp4h37

[78]. Pankaz Roy, S., & Sai Praveen, K. (2024). Systematic Review of Stress And Burnout Interventions Among U.S. Healthcare Professionals Using Advanced Computing Approaches. *Journal of Sustainable Development and Policy*, *3*(04), 101-132. https://doi.org/10.63125/9mx2fc43

[79]. Pei, X., Yu, L., & Tian, S. (2020). AMalNet: A deep learning framework based on graph convolutional networks for malware detection. *Computers & Security*, *93*, 101792. https://doi.org/10.1016/j.cose.2020.101792

[80]. Pujol-Perich, D., Suárez-Varela, J., Cabellos-Aparicio, A., & Barlet-Ros, P. (2022). Unveiling the potential of graph neural networks for robust intrusion detection. *ACM SIGCOMM Computer Communication Review*, *52*(1), 37–43. https://doi.org/10.1145/3543146.3543171

[81]. Rakibul, H., & Samia, A. (2022). Information System-Based Decision Support Tools: A Systematic Review Of Strategic Applications In Service-Oriented Enterprises. *Review of Applied Science and Technology*, *1*(04), 26-65. https://doi.org/10.63125/w3cevz78

[82]. Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk analysis for SCADA and DCS networks. *ISA Transactions*, *46*(4), 583-594. https://doi.org/10.1016/j.isatra.2007.04.003

[83]. Ramdani, B., & Kawalek, P. (2007). *SME adoption of enterprise systems in the Northwest of England: An environmental, technological, and organizational perspective* Organizational dynamics of technology-based innovation: Diversifying the research agenda,

[84]. Ravi, V., Chaganti, R., & Alazab, M. (2022). Deep learning feature fusion approach for an intrusion detection system in SDN-based IoT networks. *IEEE Internet of Things Magazine*, *5*(2), 24–29. https://doi.org/10.1109/iotm.003.2200001

[85]. Reza, M., Vorobyova, K., & Rauf, M. (2021). The effect of total rewards system on the performance of employees with a moderating effect of psychological empowerment and the mediation of motivation in the leather industry of Bangladesh. *Engineering Letters*, *29*, 1-29.

[86]. Rony, M. A., & Ashraful, I. (2022). Big Data And Engineering Analytics Pipelines For Smart Manufacturing: Enhancing Efficiency, Quality, And Predictive Maintenance. *American Journal of Scholarly Research and Innovation*, *1*(02), 59–85. https://doi.org/10.63125/rze0my79

[87]. Rony, M. A., & Hozyfa, S. (2024). Cloud-Integrated Digital Twin Architectures For Real-Time Monitoring, Risk Assessment, And Safety Optimization In U.S. Energy Infrastructure. *American Journal of Interdisciplinary Studies*, *5*(04), 96-133. https://doi.org/10.63125/y9m5pz24

[88]. Saba, A., & Md. Sakib Hasan, H. (2024). Machine Learning And Secure Data Pipelines For Enhancing Patient Safety In Electronic Health Record (EHR) Among U.S. Healthcare Providers. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 124–168. https://doi.org/10.63125/qm4he747

[89]. Saba, A., Shaikat, B., & Tonoy Kanti, C. (2023). Integration Of Artificial Intelligence And Advanced Computing To Develop Resilient Cyber Defense Systems. *Journal of Sustainable Development and Policy*, *2*(04), 74-107. https://doi.org/10.63125/rxyc6y88

[90]. Saba, A., & Tonoy Kanti, C. (2023). Explainable Artificial Intelligence (XAI) Approaches For Cyber Risk Assessment In Financial Services. *American Journal of Interdisciplinary Studies*, *4*(03), 96-135. https://doi.org/10.63125/3gjcb322

[91]. Saikat, S. (2021). Real-Time Fault Detection in Industrial Assets Using Advanced Vibration Dynamics And Stress Analysis Modeling. *American Journal of Interdisciplinary Studies*, *2*(04), 39–68. https://doi.org/10.63125/0h163429

[92]. Saikat, S. (2022). CFD-Based Investigation of Heat Transfer Efficiency In Renewable Energy Systems. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 129–162. https://doi.org/10.63125/ttw40456

[93]. Scarselli, F., Gori, M., Tsoi, A. C., Hagenbuchner, M., & Monfardini, G. (2009). The graph neural network model. *IEEE Transactions on Neural Networks*, *20*(1), 61–80. https://doi.org/10.1109/tnn.2008.2005605

[94]. Shaikat, B., & Md. Wahid Zaman, R. (2024). Quantum-Resistant Cryptographic Protocols Integrated With AI For Securing Cloud And IOT Environments. *International Journal of Business and Economics Insights*, *4*(4), 60–90. https://doi.org/10.63125/dryw3b96

[95]. Shaikh, S., & Aditya, D. (2021). Federated Learning-Driven Predictive Quality Analytics and Supply Chain Optimization In Distributed Manufacturing Networks. *Review of Applied Science and Technology*, *6*(1), 74-107. https://doi.org/10.63125/k18cbz55

[96]. Shaikh, S., & Md. Tahmid Farabe, S. (2023). Digital Twin-Driven Process Modeling For Energy Efficiency And Lifecycle Optimization In Industrial Facilities. *American Journal of Interdisciplinary Studies*, *4*(03), 65–95. https://doi.org/10.63125/e4q64869

[97]. Shaikh, S., & Sudipto, R. (2022). Multi-Objective Thermo-Economic and Supply Chain Optimization Modeling For Hydrogen Energy Integration In Smart Factories. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 163–193. https://doi.org/10.63125/p9y8p705

[98]. Shandilya, V., Simmons, C. B., & Shiva, S. (2014). Use of attack graphs in security systems. *Journal of Computer Networks and Communications*, *2014*, 818957. https://doi.org/10.1155/2014/818957

[99]. Stoyanov, B., Fidanov, I., & Milanov, E. (2017). Critical information infrastructure protection model and methodology. In I. Maglogiannis, L. Iliadis, & E. Pimenidis (Eds.), *Advances in information and communication technologies for adversity, emergency, and disaster management* (pp. 396–405). Springer. https://doi.org/10.1007/978-3-319-59415-6_34

[100]. Sudipto, R., & Md. Hasan, I. (2024). Data-Driven Supply Chain Resilience Modeling Through Stochastic Simulation And Sustainable Resource Allocation Analytics. *American Journal of Advanced Technology and Engineering Solutions*, *4*(02), 01-32. https://doi.org/10.63125/p0ptag78

[101]. Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

[102]. Ten, C.-W., Manimaran, G., & Liu, C.-C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, *40*(4), 853–865. https://doi.org/10.1109/tsmca.2010.2048028

[103]. Tonoy Kanti, C., & Saba, A. (2024). High-Performance Computing Architectures To Strengthen Cloud Infrastructure Security. *American Journal of Interdisciplinary Studies*, *5*(03), 01–42. https://doi.org/10.63125/9hr8qk06

[104]. Tonoy Kanti, C., & Sai Praveen, K. (2024). Federated Learning Models for Privacy-Preserving Data Sharing And Secure Analytics In Healthcare Industry. *International Journal of Business and Economics Insights*, *4*(4), 91-133. https://doi.org/10.63125/c2dzn006

[105]. Tonoy Kanti, C., & Shaikat, B. (2021). Blockchain-Enabled Security Protocols Combined With AI For Securing Next-Generation Internet Of Things (IOT) Networks. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 98–127. https://doi.org/10.63125/pcdqzw41

[106]. Wallace, A., & Atkison, T. (2017). A framework for cyber event detection in power grids using principal component analysis. *International Journal of Critical Infrastructures*, *13*(2–3), 205–223. https://doi.org/10.1504/ijcis.2017.088228

[107]. Wang, H., Gu, J., & Wang, S. (2017). An effective intrusion detection framework based on SVM with feature augmentation. *Knowledge-Based Systems*, *136*, 130–139. https://doi.org/10.1016/j.knosys.2017.09.014

[108]. Wang, L., Islam, T., Long, T., Singhal, A., & Jajodia, S. (2008). An attack graph-based probabilistic security metric. In V. Atluri (Ed.), *Data and applications security XXII* (pp. 283–296). Springer. https://doi.org/10.1007/978-3-540-70567-3_22

[109]. Wood, A., Zobel, C., & Atkison, T. (2017). A security architectural pattern for risk management of industry control systems within critical national infrastructure. *International Journal of Critical Infrastructures*, *13*(2–3), 169–187. https://doi.org/10.1504/ijcis.2017.088229

[110]. Wu, K., Chen, Z., & Li, W. (2018). A novel intrusion detection model for a massive network using convolutional neural networks. *IEEE Access*, *6*, 50850–50859. https://doi.org/10.1109/access.2018.2868993

[111]. Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Philip, S. Y. (2020). A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems*, *32*(1), 4–24. https://doi.org/10.1109/tnnls.2020.2978386

[112]. Yang, X., Peng, G., Zhang, D., & Lv, Y. (2022). An enhanced intrusion detection system for IoT networks based on deep learning and knowledge graph. *Security and Communication Networks*, *2022*, 4748528. https://doi.org/10.1155/2022/4748528

[113]. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, *5*, 21954–21961. https://doi.org/10.1109/access.2017.2762418

[114]. Zamal Haider, S., & Hozyfa, S. (2023). A Quantitative Study On IT-Enabled ERP Systems And Their Role In Operational Efficiency. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 62–99. https://doi.org/10.63125/nbpyce10

[115]. Zamal Haider, S., & Sai Praveen, K. (2024). Cloud-Native Data Pipelines For Scalable Audio Analytics And Secure Enterprise Applications. *American Journal of Scholarly Research and Innovation*, *3*(01), 52-83. https://doi.org/10.63125/m4f2aw73

[116]. Zulqarnain, F. N. U., & Zayadul, H. (2024). Artificial Intelligence Applications For Predicting Renewable-Energy Demand Under Climate Variability. *American Journal of Scholarly Research and Innovation*, *3*(01), 84–116. https://doi.org/10.63125/sg0j6930