International Journal of Scientific Interdisciplinary Research

Volume: 4; **Issue:** 4
Pages: 144– 176

AI-DRIVEN CYBERSECURITY, IOT NETWORKING, AND RESILIENCE STRATEGIES FOR INDUSTRIAL CONTROL SYSTEMS: A SYSTEMATIC REVIEW FOR U.S. CRITICAL INFRASTRUCTURE PROTECTION

Jabed Hasan Tarek[1]; Waladur Rahman[2];

[1]. *Phillip M. Drayer Department of Electrical Engineering, Lamar University, Beaumont, Texas, USA; Email: jabedhasan932@gmail.com*

[2]. *Phillip M. Drayer Department of Electrical Engineering, Lamar University, Beaumont, Texas, USA; Email: w.rifat99@gmail.com*

Doi: 10.63125/mbyhj941
Received: *28 September 2023;* ***Revised:*** *26 October 2023;* ***Accepted:*** *28 November 2023;* ***Published:*** *29 December 2023*

Abstract

This study investigates how AI-driven cybersecurity, IoT networking maturity, and resilience strategies jointly enhance the protection of industrial control systems within U.S. critical infrastructure. The problem driving this research is the accelerating convergence of ICS, IoT, and cloud architectures, which expands cyber-attack surfaces while many operators still lack integrated AI-enabled detection and resilience frameworks. The purpose of the study is to evaluate, through quantitative evidence, how AI-based intrusion and anomaly detection, secure IoT networking, and resilience engineering contribute to perceived critical-infrastructure protection effectiveness. Employing a quantitative, cross-sectional, case-based research design, the study collected data from 210 practitioners representing energy, water, transportation, and manufacturing ICS environments. Using multi-item Likert five-point scales, the study measured six key variables: AI-driven cybersecurity capability, IoT networking maturity, ICS resilience strategies, governance maturity, behavioral compliance, and perceived protection effectiveness. Descriptive statistics, Pearson correlations, and multiple regression modeling were used to test the proposed conceptual relationships. Findings show robust adoption of AI-driven security (mean = 3.82) and resilience strategies (mean = 3.74), with all constructs demonstrating high reliability (a = .87–.92). Regression analysis revealed that AI capability strongly predicts resilience ($\beta = 0.38$, $p < .001$) and, together with resilience, significantly improves perceived protection ($\beta = 0.34$ and $\beta = 0.37$, $p < .001$). IoT networking maturity also positively affects AI adoption ($\beta = 0.23$, $p < .001$). The study concludes that AI adoption is most effective when embedded in mature IoT security architectures and formal resilience programs. Implications highlight the need for integrated AI–IoT–resilience strategies as core pillars of national critical-infrastructure protection.

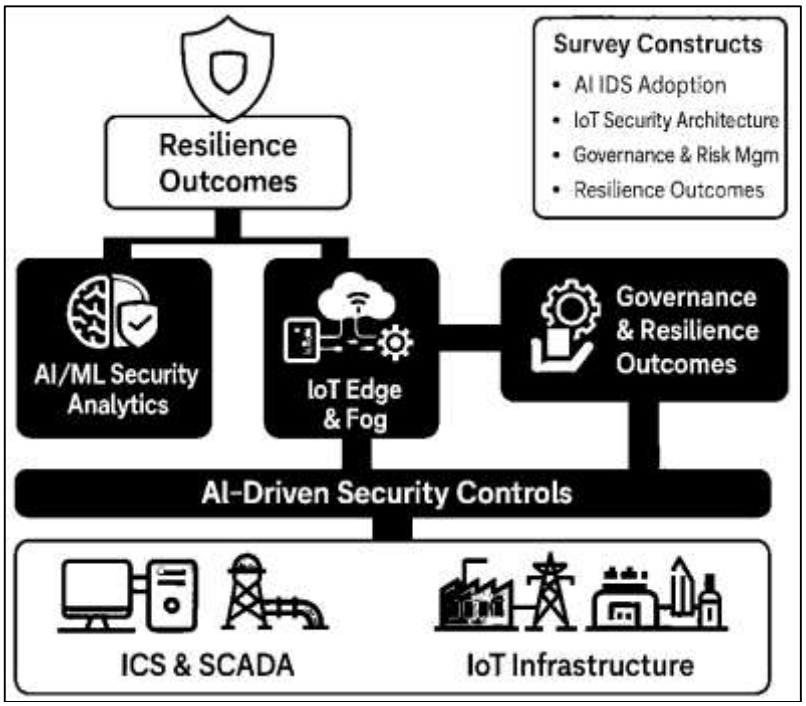
Keywords

AI-Driven Cybersecurity, Industrial Control Systems, IOT Networking Maturity, Cyber-Resilience, Critical Infrastructure Protection

INTRODUCTION

Artificial intelligence (AI), cybersecurity, industrial control systems (ICS), and the Internet of Things (IoT) increasingly intersect at the core of national and international critical infrastructure protection. ICS, including supervisory control and data acquisition (SCADA) and distributed control systems, are the digital nervous system of power grids, oil and gas pipelines, water treatment plants, transportation networks, and industrial manufacturing lines (Ten et al., 2008). Cybersecurity for ICS refers to the set of technical, organizational, and governance controls that preserve the confidentiality, integrity, and availability of these cyber–physical processes under hostile conditions (Almalawi et al., 2016). IoT extends this landscape by embedding networked sensors, actuators, and smart devices throughout critical infrastructure environments, creating dense cyber–physical ecosystems with heterogeneous devices and communication protocols (Suo et al., 2012). At the same time, AI and machine learning (ML) have emerged as powerful approaches for detecting anomalies, classifying attacks, and supporting automated or semi-automated security decision-making in large-scale networks (Shiri et al., 2011). These converging trends have significant global relevance because disruptions in one country's energy, transportation, or industrial base can propagate across supply chains and financial systems in other regions (Tariq et al., 2019). For the United States, whose critical infrastructure sectors are deeply integrated with global production and logistics, AI-driven cybersecurity for ICS and IoT networking is central not only to domestic resilience but also to international economic and security stability (Sicari et al., 2015).

Figure 1: Convergence of AI Security in Critical Infrastructure



IoT networking fundamentally reshapes the attack surface of industrial environments. IoT can be defined as a networked paradigm in which physical objects sensors, actuators, meters, embedded controllers communicate, coordinate, and exchange data over IP-based and wireless links (Abbas et al., 2019). In critical infrastructure contexts, IoT devices monitor power flows, pipeline pressure, environmental conditions, and equipment health and often interact directly with ICS components such as programmable logic controllers (PLCs) and remote terminal units (RTUs) (Khan et al., 2019). Research shows that this convergence introduces complex multi-hop attack paths where adversaries compromise lightly protected IoT nodes and pivot into high-value ICS assets (Stellios et al., 2018). Even earlier work on wireless sensor networks illustrated how node replication and related attacks undermine trust in distributed sensing, foreshadowing comparable risks in contemporary IoT-enhanced infrastructures (Parno et al., 2005). Interdependencies among physical, cyber, and

organizational subsystems mean that failures in one domain can cascade across regions and sectors, intensifying disaster impacts (Pescaroli & Alexander, 2016). To address latency, bandwidth, and privacy challenges, fog-computing architectures place security and data-processing functions closer to IoT endpoints; however, they also introduce additional configuration and trust-management requirements (Abomhara & Køien, 2014). Within this intertwined environment, U.S. critical infrastructure operators must balance operational efficiency, real-time control, and safety constraints with rigorous cyber risk reduction in networks that increasingly blend classical ICS, cloud services, and IoT edge nodes (Alaba et al., 2017).

AI-driven cybersecurity offers a data-intensive response to these challenges by learning complex patterns in industrial network traffic and process measurements. Traditional signature-based intrusion detection systems (IDS) match known attack patterns and are often tuned for IT networks, which limits their performance when confronting previously unseen threats or timing-sensitive process anomalies in ICS, especially during high-volume traffic conditions (Abdulla & Ibne, 2021; Caropreso et al., 2019). In contrast, AI and ML methods can model "normal" behavior and detect deviations over time, even for subtle or multi-stage intrusions. For SCADA networks, Nader et al. (2014) demonstrated that one-class classification with kernel methods and carefully tuned ℓp-norms can effectively distinguish abnormal traffic in pipeline and water-treatment testbeds. Almalawi et al. (2016) proposed a multi-stage data-driven analytics framework that combines feature extraction, clustering, and classification to detect SCADA-specific attacks with improved accuracy. Machine learning models have also been successfully applied to SCADA intrusion detection using supervised classifiers trained on labeled ICS traffic (Habibullah & Foysal, 2021; Nader et al., 2014). Beyond ICS, deep learning architectures such as stacked autoencoders and two-stage models have shown strong performance on benchmark intrusion datasets, suggesting that AI can enable more adaptive and efficient network protection at scale (Maglaras et al., 2018; Sarwar, 2021). Parallelization, flow-optimization techniques, and SDN-based control further enhance the scalability of AI-enabled IDS under heavy traffic conditions (Tariq et al., 2019). Within critical infrastructure settings, these AI capabilities provide building blocks for continuous monitoring, dynamic risk assessment, and intelligent response strategies in complex IoT–ICS ecosystems.

At the same time, empirical work on ICS and SCADA security reveals persistent structural and technical vulnerabilities that AI alone does not eliminate. Surveys of ICS operators show that governance practices, asset visibility, and patch management remain uneven across sectors, constraining the effectiveness of advanced technical controls (Musfiqur & Saba, 2021; Tariq et al., 2019). Nazir et al. (2017) mapped tools and techniques for SCADA cyber security, emphasizing the need for layered defenses, robust anomaly detection, and systematic vulnerability assessment. In parallel, researchers have proposed risk and resilience frameworks for critical infrastructures that account for interdependent systems, cascading failures, and adaptive adversaries (Hurst et al., 2014; Redwanul et al., 2021). New metering infrastructures and smart-grid deployments also require dedicated cybersecurity assessment and mitigation schemes to manage both cyber and physical risks (Fovino et al., 2010; Tarek & Praveen, 2021). These findings indicate that AI-driven detection needs to be embedded within broader architectures that include secure network design, resilient control strategies, and organizational preparedness across the ICS lifecycle (Imran et al., 2019).

Conceptual and theoretical frameworks for IoT, cybersecurity, and critical infrastructure resilience provide an important foundation for such architectures but are not yet fully integrated with AI-centric approaches. From a security and privacy perspective, IoT studies have characterized threats related to confidentiality, integrity, authentication, and data aggregation, proposing conceptual models that combine cryptographic techniques, access control, and privacy-preserving aggregation schemes (Muhammad & Shahrin, 2021; Park & Lee, 2014). In the ICS domain, Park and Lee (2014) advanced an information security management system (ISMS) tailored to industrial control environments, blending standards-based governance with technical safeguards. Risk-based frameworks emphasize the need to understand systemic vulnerabilities and interdependencies so that organizations can prioritize controls that sustain essential services under stress (Noor & Hassan, 2019). Fog and edge architectures extend these ideas by distributing security enforcement closer to IoT devices and data sources, thereby conceptualizing multi-layer defenses that span device, fog, and cloud tiers (Saikat, 2021; Shaikh &

Aditya, 2021; Zhu et al., 2019). At the same time, blockchain, differential privacy, and privacy-preserving authentication schemes have been proposed to secure data exchange and control messages within smart grids and IoT-based infrastructures (Knowles et al., 2015; Amin, 2022; Ariful, 2022). What remains underexplored is how these theoretical constructs interrelate when AI-driven anomaly detection and classification become central components of the protection strategy for industrial IoT–ICS environments in national critical infrastructure sectors.

Existing literature on AI-driven cybersecurity, IoT networking, and ICS resilience reveals several interconnected gaps that motivate the present study. IoT surveys provide detailed taxonomies of threats and countermeasures yet often treat industrial control use cases only briefly, focusing more heavily on consumer and generic enterprise scenarios (Maglaras & Jiang, 2014; Nahid, 2022). Similarly, studies on IoT-enabled cyberattacks map complex attack paths into critical infrastructures but concentrate on conceptual modeling and qualitative scenario analysis rather than quantitative assessment of organizational practices (Almalawi et al., 2016). SCADA and ICS security surveys synthesize tools, vulnerability-assessment techniques, and case studies, yet they typically examine anomaly detection, governance, and resilience as separate strands rather than as jointly measurable constructs within a unified analytical model (Alaba et al., 2017; Hossain & Milon, 2022). AI- and ML-based intrusion detection studies demonstrate promising technical performance on testbeds and benchmark datasets but rarely link these capabilities to organizational decision-making, operator perceptions of resilience, or sector-wide critical infrastructure protection objectives (Mominul et al., 2022; Nader et al., 2014). Furthermore, only a limited number of works empirically examine how AI-driven security controls, IoT networking practices, and resilience strategies co-exist in real industrial contexts particularly within U.S. critical infrastructure organizations operating under stringent regulatory and safety constraints (Rabiul & Sai Praveen, 2022; Pescaroli & Alexander, 2016).

In this context, there is a need for a study that systematically reviews AI-driven cybersecurity approaches, IoT networking architectures, and resilience strategies for ICS and then empirically evaluates their relationships in U.S. critical infrastructure environments. The present research responds to this need by conducting a systematic review of peer-reviewed studies published between 2005 and 2020 on IoT security, ICS/SCADA protection, AI-based intrusion detection, and critical infrastructure resilience. Building on the synthesized insights, the study then adopts a quantitative, cross-sectional, case-study–based design using a Likert five-point scale survey administered to professionals involved in cybersecurity and operations for U.S. industrial control systems. The research is structured around questions such as: (1) To what extent is the adoption of AI-driven intrusion detection and analytics associated with higher perceived cybersecurity performance in ICS and IoT networking? (2) How are IoT network architecture practices such as segmentation, fog deployment, and secure data management related to perceived resilience of industrial processes? and (3) How do governance and risk-management practices mediate the relationship between technical controls and overall critical infrastructure resilience outcomes? Corresponding hypotheses test whether higher levels of AI-based security deployment and structured IoT security practices are positively related to stronger reported resilience and lower perceived cyber risk for ICS operations. Through this combined systematic review and empirical assessment, the study seeks to provide a coherent, data-driven understanding of AI-driven cybersecurity, IoT networking, and resilience strategies for industrial control systems in the U.S. critical infrastructure protection landscape.

The overarching objective of this study is to develop a coherent, evidence-based understanding of how AI-driven cybersecurity capabilities, IoT networking practices, and resilience strategies jointly shape the protection of industrial control systems in U.S. critical infrastructure. The study is structured around two mutually reinforcing components: a systematic review of existing academic and technical work, and an empirical, quantitative assessment based on perceptions and experiences of professionals directly involved in ICS and IoT security and operations. The first objective is to systematically identify, categorize, and synthesize AI-based methods, IoT networking architectures, and resilience mechanisms that have been proposed or deployed for safeguarding industrial control environments, with specific attention to detection, prevention, response, and recovery functions. The second objective is to construct a clear conceptual model that links AI-driven cybersecurity capability, IoT networking maturity, ICS resilience strategies, and perceived critical infrastructure protection effectiveness,

defining each construct in measurable terms suitable for quantitative analysis. The third objective is to operationalize these constructs through a structured survey instrument using a Likert five-point scale, capturing how practitioners assess the presence, quality, and integration of AI-enabled security tools, IoT security practices, and resilience planning within their organizations. The fourth objective is to apply descriptive statistics, correlation analysis, and regression modeling to examine the strength and direction of relationships among the key constructs, thereby testing a set of hypotheses that specify how AI capability and IoT networking maturity relate to resilience and perceived protection outcomes. A fifth, complementary objective is to explore how organizational and contextual characteristics, such as sector type, organizational size, and regulatory exposure, coincide with variations in technical and organizational security practices. Taken together, these objectives guide the design of the research questions, the construction of the measurement model, and the choice of analytical techniques, creating a structured pathway from literature synthesis to empirical validation in the specific context of U.S. critical infrastructure.

LITERATURE REVIEW

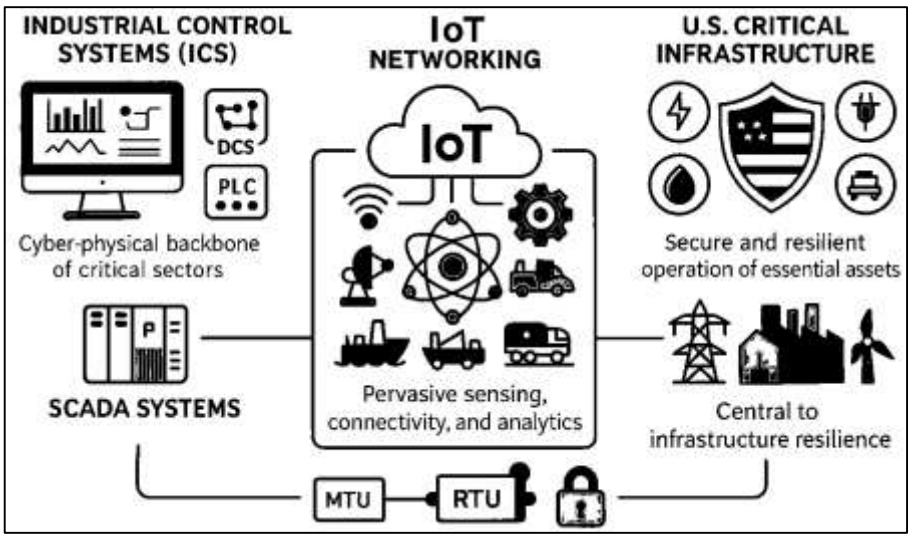
The literature on AI-driven cybersecurity, IoT networking, and resilience strategies for industrial control systems (ICS) has evolved through several overlapping strands that span technical, organizational, and risk-management perspectives. Early work on ICS and SCADA security focused on identifying fundamental vulnerabilities in control protocols, network architectures, and legacy devices, emphasizing the potentially severe physical consequences of cyber intrusions into power, water, and industrial plants. As digital transformation advanced, researchers began to analyze the convergence of operational technology and information technology, showing how this integration, while enabling real-time monitoring and optimization, also expanded the attack surface and exposed control environments to threats traditionally associated with enterprise IT networks. In parallel, the rapid proliferation of IoT devices in industrial settings introduced dense sensor networks, wireless connectivity, and cloud or fog-based data processing, prompting extensive surveys of IoT architectures, threat taxonomies, and security and privacy challenges. Another body of work developed AI- and machine-learning–based intrusion detection and anomaly detection techniques for both general networks and ICS-specific traffic, demonstrating that data-driven models can learn complex temporal and spatial patterns in process measurements and communication flows that are difficult to capture with static, signature-based approaches. Complementing these technical advances, conceptual and theoretical frameworks such as security management models for ICS, IoT security reference architectures, and risk and resilience frameworks for critical infrastructures have sought to structure how organizations think about governance, defense-in-depth, and continuity of operations under cyber-physical stress. More recent studies integrate resilience concepts, highlighting the need not only to prevent attacks but also to absorb, adapt to, and recover from disruptions across interdependent systems. Despite this growing body of work, the literature remains fragmented across domains, with AI, IoT, ICS security, and resilience often treated in isolation, and with relatively few studies combining systematic synthesis of prior research with empirical, quantitative analysis of organizational practices in real-world critical infrastructure contexts. This fragmentation underscores the need for a structured review and model that bring together AI capability, IoT networking maturity, and ICS resilience into a unified lens suitable for both theoretical development and practical assessment.

Industrial Control Systems and U.S. Critical Infrastructure

Industrial control systems (ICS) form the cyber-physical backbone of modern critical infrastructure, encompassing supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLCs) that orchestrate physical processes in sectors such as electric power, oil and gas, water, transportation, and manufacturing (Stouffer et al., 2015). ICS architectures historically relied on isolated networks, proprietary protocols, and tightly controlled access paths, which created an implicit security barrier but also embedded assumptions of trust and limited connectivity. As enterprise networks, cloud services, and remote access tools have been tightly integrated with operational technology (OT), ICS environments have shifted from closed, plant-centric configurations to complex internetworked ecosystems that exchange real-time data with IT systems and external partners (Mourtzis et al., 2016). Within the United States, this evolution is particularly consequential because ICS platforms directly operate energy generation and transmission, pipeline

networks, water treatment systems, and industrial manufacturing assets designated as critical infrastructure, where even short-term disruptions can cascade into social, economic, and safety impacts at national scale (Boyes et al., 2018). These systems now function as tightly coupled cyber-physical networks in which instrumentation, control logic, and human–machine interfaces (HMIs) collaborate to maintain stability, quality, and safety under stringent operational constraints, making their secure operation a central concern in infrastructure protection strategies (Jain & Tripathi, 2013).

Figure 2: Integrated of Industrial Control Systemsand U.S. Critical Infrastructure



The emergence of the Industrial Internet of Things (IIoT) has further transformed ICS environments by embedding pervasive sensing, connectivity, and analytics capabilities across industrial assets. IIoT architectures interconnect sensors, actuators, controllers, and edge devices with cloud and enterprise platforms through heterogeneous wired and wireless networks, enabling continuous data acquisition and feedback loops for optimization, condition monitoring, and predictive maintenance (Boyes et al., 2018). From a systems perspective, IIoT is positioned as an extension of traditional industrial automation and control systems (IACS), spanning device, network, service, and application layers that together support real-time control and higher-level decision support (Bhamare et al., 2020). In manufacturing and other industrial sectors, the adoption of IoT-enabled devices generates unprecedented volumes of high-velocity and heterogeneous operational data, now characterized as "industrial big data," which can be mined to improve production efficiency, asset utilization, and supply-chain responsiveness (Mourtzis et al., 2016). However, the same features that make IIoT attractive ubiquitous connectivity, distributed intelligence, and open protocol stacks also expand the cyber-attack surface, introducing complex trust relationships among field devices, gateways, cloud services, and third-party analytics platforms that can be difficult to manage in safety-critical environments (Boyes et al., 2018). For U.S. critical infrastructure operators, IIoT adoption therefore links directly to decisions about network segmentation, protocol choices, and security architectures across both plant-level and enterprise domains.

Within this converged landscape, SCADA systems remain a central ICS technology for geographically dispersed assets such as transmission lines, substations, pipelines, and distributed industrial facilities, making their secure operation pivotal to U.S. critical infrastructure resilience. SCADA architectures typically rely on master terminal units (MTUs), remote terminal units (RTUs), and protocols such as Distributed Network Protocol 3 (DNP3) to transport measurement data and control commands over IP-based networks, which introduces exposure to eavesdropping, spoofing, replay, and man-in-the-middle attacks when traffic traverses shared or public networks (Stouffer et al., 2015). Detailed analyses of SCADA protocol weaknesses show that many legacy designs lack built-in cryptographic protections or strong authentication, requiring compensating controls such as secure tunneling, robust key management, and protocol enhancements to maintain integrity and availability of control traffic (Jain

& Tripathi, 2013; Rakibul & Samia, 2022). At the same time, surveys of ICS cybersecurity highlight that industrial environments now face a broad spectrum of threats, ranging from targeted malware to coordinated campaigns that can exploit both IT and OT components, reinforcing the need for systematic risk assessment, defense-in-depth architectures, and monitoring strategies tailored to industrial processes (Boyes et al., 2018; Saikat, 2022). NIST's ICS security guidance explicitly positions these measures within a broader framework for securing U.S. critical infrastructure, emphasizing asset identification, network segmentation, secure remote access, and incident response as foundational practices for organizations that operate IIoT-enabled ICS in regulated sectors (Stouffer et al., 2015; Tonoy Kanti & Shaikat, 2022). Taken together, these developments frame industrial control systems, IoT networking, and sector-specific responsibilities as an integrated domain in which cybersecurity and resilience are inseparable from the continuity of national critical infrastructure operations.

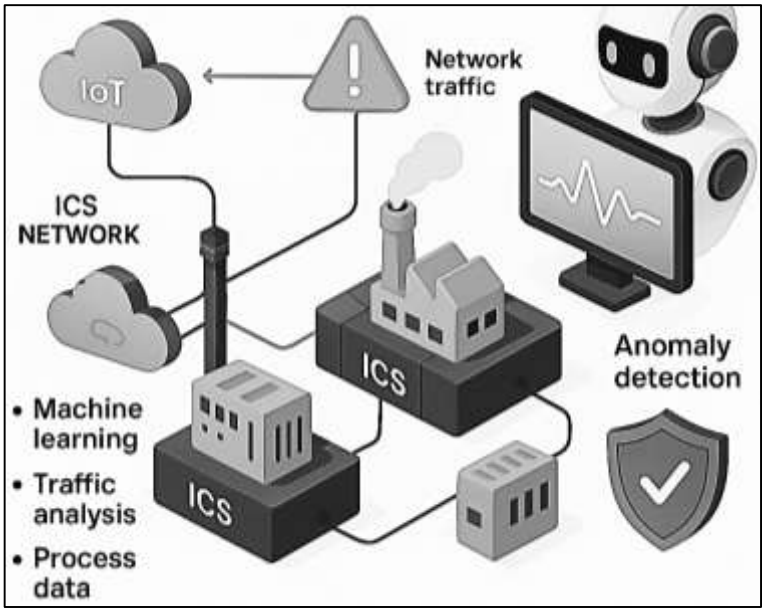
Anomaly Detection in ICS and IoT Networks

Artificial intelligence–driven intrusion detection and anomaly detection mechanisms have emerged as a central pillar of cybersecurity for industrial control systems (ICS) and interconnected IoT networks, particularly in critical infrastructure where traditional perimeter defenses are insufficient. Machine-learning-based intrusion detection systems (IDS) analyse network flows, process variables, and protocol features to classify traffic as benign or malicious and to identify subtle deviations from normal operational baselines. In industrial environments, these AI models must contend with highly imbalanced datasets, strict real-time constraints, and safety-critical conditions in which false positives can trigger costly or dangerous process interruptions. One example has been an attack detection and prevention framework for industrial control systems that combines traffic analysis with pattern-based IDS logic to detect start–stop manipulation attacks targeting programmable logic controllers, demonstrating that intelligent analysis of control traffic can reveal stealthy behaviour that signature-based tools miss (Yilmaz & Gonen, 2018). This architecture has illustrated how AI-driven IDS components can be embedded alongside existing controllers without redesigning the entire control network, using monitored patterns to trigger automated blocking or human operator alerts (Maniruzzaman et al., 2023; Arif Uz & Elmoon, 2023; Aubel et al., 2018). Likewise, a distributed deep-learning-based attack detection scheme for IoT environments has shown how resource-constrained edge devices can cooperate with fog or cloud nodes to train and deploy a neural IDS capable of recognising complex, multi-vector attacks (Diro & Chilamkurti, 2018). By distributing learning and inference across a hierarchy of devices, such models have demonstrated that AI can be scaled to heterogeneous industrial and IoT ecosystems while preserving low detection latency, making AI-enabled intrusion monitoring a realistic option for large, geographically dispersed critical-infrastructure networks (Liu & Nielsen, 2018; Tarek, 2023; Mushfequr & Ashraful, 2023). In practice, these AI-centric IDS architectures have often operated in hybrid modes, combining supervised classifiers trained on labelled attack datasets with unsupervised or semi-supervised modules that learn normal traffic patterns and raise alarms when previously unseen behaviours emerge, allowing rapid containment of attacks before they propagate across interconnected IoT-enabled control domains.

Beyond generic network monitoring, AI-driven anomaly detection for smart energy and industrial platforms has increasingly leveraged domain-specific time-series data and architectures tailored to operational profiles. A scalable prediction-based online anomaly detection system for smart meter data, for instance, has used a lambda architecture to support real-time analytics on large-scale energy consumption streams, highlighting how predictive models can flag anomalous consumption that may reflect cyber-attacks, device tampering, or abnormal customer behaviour (Asghar et al., 2019; Shahrin & Samia, 2023). This approach has illustrated how regression and forecasting models can be integrated with streaming pipelines so that deviations from predicted states act as triggers for more detailed intrusion analysis in supervisory control and data acquisition environments, rather than relying exclusively on static thresholds or hand-crafted signatures (Liu & Nielsen, 2018). Similar model-driven strategies can be transferred to industrial plants and substations, where multivariate process histories are used to train anomaly detectors that characterise normal load, pressure, and flow profiles for equipment and control loops. When such AI models have been combined with conventional access-control, network segmentation, and encryption mechanisms, they have helped transform ICS and IoT infrastructures from passively monitored systems into actively self-diagnosing environments in which

anomalies in production data, communication patterns, or device behaviour can be tied to specific cyber risks and operational impacts. Building on this perspective, a broad review of ICS security mechanisms has underscored that AI-based anomaly detection must be mapped to clearly defined industrial use cases, such as protecting programmable logic controllers in water-treatment facilities, safeguarding phasor measurement units in smart grids, or monitoring gateway devices that bridge operational technology and enterprise networks (Asghar et al., 2019). This analysis has highlighted that data quality, sensor placement, and logging strategies are as critical as the choice of algorithm, because poorly instrumented environments can lead even sophisticated models to overlook relevant attack indicators or to confuse legitimate transients with hostile behaviour, making close collaboration between control engineers, cybersecurity specialists, and data scientists essential (Liu & Nielsen, 2018).

Figure 3: AI-Enabled Security Framework for ICS–IoT Cyber-Physical Environments

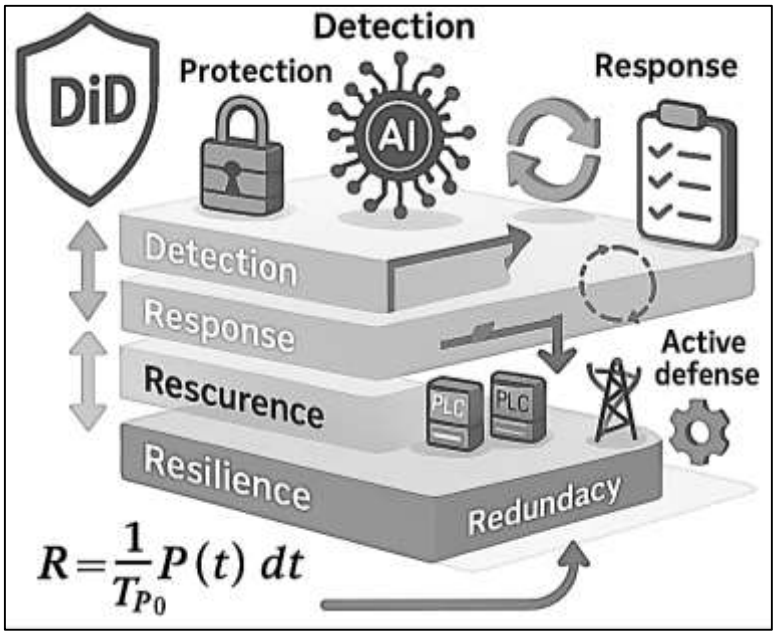


AI techniques for ICS and IoT security have not been confined to packet-level or time-series analysis; they have also encompassed novel sensing modalities and side-channel measurements that extend visibility into the behaviour of embedded controllers. In particular, side-channel-based intrusion detection for industrial control systems has used electromagnetic emissions from programmable logic controllers to train models that distinguish between legitimate and modified control code, providing an additional physical layer of verification that can detect malware or unauthorised firmware changes even when network traffic appears normal (Razia, 2023; Aubel et al., 2018; Zayadul, 2023). This kind of AI-assisted side-channel monitoring has complemented network-centric IDS approaches and has been particularly relevant for legacy controllers that cannot be easily patched or instrumented with heavyweight security agents (Liu & Nielsen, 2018). At the architectural level, it has been emphasised that such AI-enabled detection techniques should be integrated into layered defence frameworks that span field devices, control rooms, and enterprise zones, so that alerts from anomaly detectors, side-channel monitors, and deep-learning-based network sensors can be fused into coherent situational awareness for operators and security analysts (Asghar et al., 2019). Taken together, these contributions have indicated that AI-driven intrusion detection in ICS and IoT ecosystems is moving toward multi-layered, context-aware architectures that combine deep learning for traffic classification, prediction-based anomaly detection for process and metering data, and advanced sensing for controller integrity monitoring (Liu & Nielsen, 2018; Van Aubel et al., 2018). For the present study, these works have provided an empirical and conceptual foundation for understanding AI-driven security as an integrated set of monitoring, detection, and response capabilities that span the entire industrial cyber-physical stack, informing the constructs that have been used to evaluate AI-enabled cybersecurity, IoT networking resilience, and industrial control system protection in U.S. critical infrastructure.

Resilience Strategies and Defense-in-Depth for AI-Enabled ICS and IoT Networks

Resilience strategies for AI-enabled industrial control systems (ICS) and IoT networks build on the broader evolution of cyber-physical systems security, where protection, detection, response, and recovery must be orchestrated across tightly coupled cyber and physical layers. Cyber-physical systems security has demanded a holistic view of vulnerabilities and controls spanning sensing, communication, control logic, and human operators, because failures in any layer can cascade into safety-critical disruptions (Humayed et al., 2017). In ICS-centric critical infrastructure, this has meant that resilience is not only about preventing breaches but also about ensuring that essential services maintain acceptable performance during and after cyber incidents. Redundant communication paths, backup controllers, and robust failover processes therefore form the structural backbone of resilience, while AI-driven monitoring enhances situational awareness and reduces detection latency for stealthy attacks. Multiple redundancy strategies can be systematically engineered to restore controllability in complex ICS topologies by designing alternative driver nodes and paths that sustain control even when primary components are compromised (Alcaraz, 2017). At the same time, active-defence strategies that reconfigure or isolate assets dynamically in response to detected threats have become increasingly necessary to counter advanced persistent threats and coordinated attacks. Evidence from semi-simulated industrial environments has shown that traditional redundancy alone is insufficient when redundant programmable logic controllers share common vulnerabilities; resilience must explicitly consider cyber-induced common-cause failures and incorporate mechanisms that disrupt the adversary's attack chain as it unfolds (Chaves et al., 2017). Within this context, AI-based analytics can support adaptive reconfiguration, prioritizing which assets to protect or shed based on predicted impact and system-level controllability constraints.

Figure 4: Defense-in-Depth Architecture for AI-Enabled ICS and IoT Networks



Defense-in-depth (DiD) has emerged as a dominant architectural paradigm for structuring resilience strategies in ICS and industrial IoT environments, particularly as operational technology has become deeply interconnected with IT networks and cloud services. DiD has been described as a layered security model designed to slow, detect, and contain advanced persistent threats that can bypass single protective controls by chaining multiple techniques over time (Reza et al., 2021; Tankard, 2011). For AI-driven ICS security, DiD creates the structural scaffolding into which machine-learning-based detection, predictive risk scoring, and automated response can be embedded at different layers field devices, control networks, demilitarized zones, enterprise networks, and cloud-hosted analytics. This concept has been extended to industrial IoT by integrating DiD with end-to-end cryptographic protections, proposing combinations of attribute-based encryption and object security to ensure that

data remain confidential and authenticated even as they traverse multiple middleboxes (Mosteiro-Sanchez et al., 2020). Such layered architectures allow resilience measures to be mapped to specific threat classes: segmentation and firewalls reduce exposure to remote intrusions, AI-based anomaly detection filters malicious traffic at aggregation points, and redundancy strategies ensure continued operation when particular nodes are quarantined. Empirical work with semi-simulated wastewater control systems has shown that active-defence mechanisms embedded in a layered architecture can maintain operational performance under cyber attack significantly better than traditional passive redundancy (Chaves et al., 2017). Taken together, these results indicate that DiD is not merely a static configuration of firewalls and zones, but a dynamic resilience framework in which AI-enabled detection and automated responses continuously adapt to evolving attack paths (Humayed et al., 2017). Quantifying resilience in AI-enabled ICS and IoT networks requires translating architectural patterns such as redundancy, DiD, and active defence into measurable indices that can be used in correlation and regression models. At the system level, resilience over a disturbance window Tcan be conceptualized as the normalized area under a performance curve, for example

$$R = \frac{1}{TP_0}\int_0^T P(t)\,dt,$$

where $P(t)$is process performance (or availability) and $P_0$is its nominal value. In redundant ICS architectures, multiple alternative driver nodes and paths can be designed so that $P(t)$degrades more slowly and recovers more rapidly after disruptions, effectively increasing this resilience index (Alcaraz, 2017). Comparisons between traditional redundancy and active-defence strategies have observed higher post-attack performance for active-defence configurations, which implies a higher integral of $P(t)$over time and thus a larger value of R(Chaves et al., 2017). From a measurement perspective, survey-based case studies in this research context can operationalize such constructs with Likert-scale indicators for DiD maturity, redundancy depth, AI-driven detection capability, and incident response agility, and then model resilience outcomes (for example, perceived ability to maintain operations) as a dependent variable using regression of the form

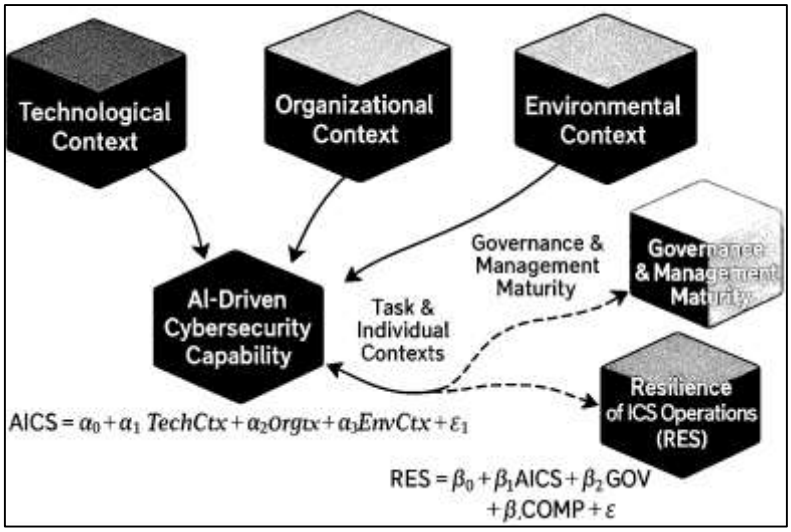
$$\begin{aligned}\text{Resilience Index} &= \beta_0 + \beta_1(\text{DiD Layering}) + \beta_2(\text{Redundancy}) + \beta_3(\text{AI Detection}) \\ &\quad + \beta_4(\text{APT Preparedness}) + \varepsilon.\end{aligned}$$

Because CPS security controls interact across layers, interaction terms may be statistically important in such models (Humayed et al., 2017), while the fact that advanced persistent threats exploit gaps between layers suggests that misalignment between encryption, monitoring, and segmentation could explain residual variance in resilience outcomes (Mosteiro-Sanchez et al., 2020). By integrating these architectural and analytical perspectives, the literature has established a foundation for examining how AI-driven defence-in-depth and engineered redundancy jointly shape the resilience of U.S. critical infrastructure ICS.

AI-Driven Cybersecurity Adoption and ICS Resilience

This study grounds its analysis of AI-driven cybersecurity, IoT networking, and industrial control system (ICS) resilience in an organizational innovation perspective, with the Technology–Organization–Environment (TOE) framework as the primary theoretical anchor. TOE explains technology adoption and assimilation as a function of three contextual dimensions: (a) the technological context (e.g., relative advantage, compatibility, complexity), (b) the organizational context (e.g., size, resources, top management support, IT competence), and (c) the environmental context (e.g., regulatory pressure, competitive intensity, vendor support). Empirical TOE-based work on Internet and e-business technologies in Canadian SMEs shows that perceived benefits, management support, IT competence, external pressure, and vendor support significantly shape adoption intentions and actual use, illustrating how internal capabilities and environmental forces jointly determine organizational uptake of digital innovations (Ifinedo, 2012; Mortuza & Rauf, 2022).

Figure 5: Integrated TOE–Governance Model for AI-Driven ICS Cybersecurity and Resilience



Similarly, cloud-computing adoption research using a dual-stage analytical approach (structural equation modeling and neural networks) confirms that relative advantage, service quality, perceived risk, top management support, and provider influence act as critical drivers of adoption and, in turn, of firm performance outcomes (Habibullah & Md. Foysal, 2021; Khayer et al., 2020). Building on this stream, integrated TOE taxonomies extend the original triad by embedding task and individual user contexts via task–technology fit (TTF) and the Unified Theory of Acceptance and Use of Technology (UTAUT), demonstrating that adoption is principally driven by TOE factors but moderated by task characteristics and individual perceptions of usefulness and effort (Awa et al., 2017; Shahrin & Samia, 2023). For AI-enabled ICS and IoT security in U.S. critical infrastructure, these insights imply that technological features of AI-based controls (e.g., detection performance, interoperability with ICS protocols), organizational readiness (e.g., security expertise, data engineering capacity, training), and environmental pressures (e.g., sectoral regulation, standards, insurer and customer expectations) jointly shape whether, and how deeply, AI-driven cybersecurity solutions are adopted and embedded into operational technology environments.

While TOE clarifies firm-level conditions for adopting AI-based controls, behavioral and governance-oriented models explain how security policies, procedures, and resilience strategies are enacted through human actors and managerial decision making. An integration of the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT) in the information security domain shows that employees' intentions to comply with information systems security policies are driven by attitudes toward compliance, subjective norms, self-efficacy, response efficacy, and perceived vulnerability, whereas perceived severity and response cost may play a weaker role than commonly assumed (Ifinedo, 2011). This behavioral framing is directly relevant to AI-driven ICS security because sophisticated detection and response tools achieve little if operators, engineers, and analysts do not trust alerts, do not feel capable of using advanced analytics interfaces, or perceive AI-enabled controls as obstacles to productivity. At the governance level, a comprehensive model of information security factors for decision-makers identifies a structured set of management success factors including security strategy and objectives, organizational structures and roles, processes such as incident and change management, technology and architecture, human resources and awareness, and security culture as interdependent determinants of effective information security performance (Diesch et al., 2020). Their model emphasizes that decision-makers must balance technical controls with process maturity and cultural alignment to achieve robust protection. Bringing these strands together, the present study conceptualizes AI-driven cybersecurity capability in ICS as emerging not only from the presence of AI tools and IoT architectures, but also from behavioral compliance with security policies and the maturity of governance, risk, and compliance (GRC) structures that coordinate technical, organizational, and human elements of cyber-physical protection.

Taken together, TOE-based adoption studies, behavioral compliance models, and security-factor frameworks support a multi-construct conceptual model that is amenable to quantitative testing using correlation and regression analysis. At the core of this model, AI-driven cybersecurity capability (AICS) is treated as a latent construct measured by indicators such as deployment of AI-based intrusion detection and anomaly detection, coverage of ICS and IoT assets by these tools, integration with security information and event management (SIEM) platforms, and the degree of automated incident-response orchestration. Following TOE logic, AICS is conceptualized as a function of technological, organizational, and environmental contexts:

$$\text{AICS} = \alpha_0 + \alpha_1 \text{TechCtx} + \alpha_2 \text{OrgCtx} + \alpha_3 \text{EnvCtx} + \zeta_1,$$

where TechCtx captures perceived technological advantages and compatibilities of AI-based controls, OrgCtx reflects top management support, security expertise, and resource availability, and **EnvCtx** expresses regulatory, competitive, and partner pressures motivating advanced cybersecurity adoption (Ifinedo, 2011). Building on security-factor and compliance models, resilience of ICS operations (RES) is then modeled as an outcome construct influenced by AICS, governance and management maturity (GOV), and behavioral compliance (COMP):

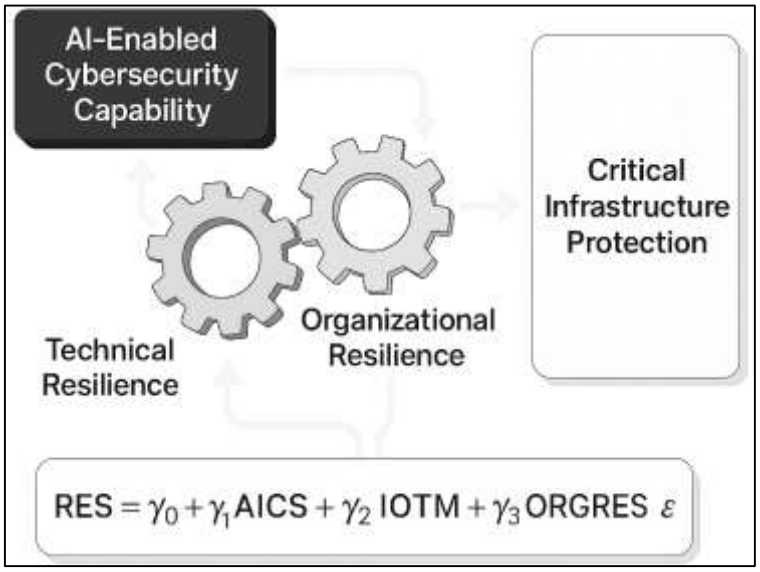
$$\text{RES} = \beta_0 + \beta_1 \text{AICS} + \beta_2 \text{GOV} + \beta_3 \text{COMP} + \varepsilon,$$

where GOV reflects the presence and effectiveness of security strategy, processes, and structures, and COMP captures aggregated compliance intentions and practices across key ICS stakeholders (Diesch et al., 2020). Integrated TOE taxonomies further suggest that task and individual contexts moderate these relationships for example, the effect of AICS on RES (β_1) may be stronger when AI tools are well aligned with operators' tasks and when individual acceptance of analytics-driven decision support is high (Awa et al., 2017; Mohammad Mushfequr & Ashraful, 2023). In the empirical component of this study, each latent construct will be operationalized with multi-item Likert five-point scales, and composite scores will be examined through descriptive statistics, Pearson correlations, and multiple regression models to test hypotheses about how TOE-based contexts, governance and behavioral factors, and AI-driven cybersecurity capability jointly influence perceived resilience of U.S. ICS within critical infrastructure sectors.

Critical Infrastructure and ICS Cyber-Resilience

Resilience-focused conceptual frameworks for critical infrastructure systems have increasingly emphasized quantifiable indices that capture how well infrastructures anticipate, withstand, and recover from disruptions, providing a basis for empirical modeling in engineering and policy studies. In the industrial control system (ICS) and IoT security context, resilience is typically treated as a multidimensional construct that combines technical robustness, recoverability, and organizational adaptability rather than a single binary attribute of failure or survival. Cyber-resilience frameworks for ICS explicitly embed this view by defining resilience as the ability of a control system to sustain essential functions in the face of cyberattacks, rapidly restore degraded performance, and learn from incidents to improve future defenses, with metrics spanning confidentiality, integrity, availability, and control-loop stability (Argyroudis et al., 2020; Ara & Onyinyechi, 2023). At the level of individual infrastructure elements, resilience is further interpreted as a quality that reduces vulnerability, minimizes the consequences of disruptive events, accelerates response and recovery, and facilitates adaptation to similar events in the future, underscoring the interplay between technical design features and organizational practices (Ara, 2021; Rehak et al., 2019). Conceptual models therefore distinguish between initial conditions (for example, baseline robustness and preventive measures) and functional conditions (for example, response and recovery capabilities), viewing resilience as a continuous cycle of prevention, absorption, recovery, and adaptation rather than a one-time outcome (Haque et al., 2018). This cycle-oriented perspective aligns naturally with AI-driven cybersecurity and IoT networking in ICS, where continuous monitoring, automated detection, and adaptive response are central capabilities that influence how quickly a system detects anomalies, isolates compromised segments, and resumes normal operation. For quantitative research, these conceptualizations motivate the treatment of resilience as a latent construct composed of multiple observable indicators capturing both technical and organizational dimensions, which can be measured via survey instruments and linked statistically to AI-enabled cybersecurity practices and perceived critical infrastructure protection effectiveness in U.S. ICS environments.

Figure 6: Resilience Metrics and Indices for Critical Infrastructure and ICS Cyber-Resilience



Building on these conceptualizations, quantitative resilience indices for critical infrastructures often rely on performance curves that track service levels over time, allowing the impact of different disturbance scenarios and mitigation strategies to be compared using standardized metrics. For cyber-physical systems such as ICS, a common representation is the resilience curve, where a performance function $P(t)$describes service quality or process availability over a disturbance horizon T, and a normalized resilience measure can be written as

$$R = \frac{1}{TP_0}\int_0^T P(t)\,dt,$$

with P_0denoting nominal performance. Curve-based measures are complemented by index-based approaches that aggregate multiple technical and organizational indicators into composite scores. For example, the Resilience Measurement Index (RMI) uses a hierarchical structure of protective measures, robustness, resourcefulness, and recovery attributes, each mapped to normalized scores and combined through weighted sums to produce an overall facility-level resilience value (Petit et al., 2013). A related complex approach to assessing resilience of critical infrastructure elements organizes determinants into technical and organizational areas and computes element-level resilience scores that reflect both structural characteristics and management practices, thereby supporting comparative analysis across sectors and assets (Rehak et al., 2018). Multi-hazard frameworks for infrastructure such as transport networks extend these ideas by explicitly modeling the evolution of performance under sequences of natural and human-induced hazards, using fragility functions and restoration models to derive time-dependent resilience indicators for bridges, tunnels, and other assets (Argyroudis et al., 2020). From an empirical research perspective focused on ICS, these methodologies highlight that resilience can be operationalized either via curve-based measures of performance degradation and recovery, or via composite indices built from standardized indicators, both of which are amenable to regression-based analysis using survey-derived or observational data on underlying technical and organizational conditions (Haque et al., 2018).

For the present study, these resilience indices and performance-based metrics inform a conceptual framework in which AI-driven cybersecurity capability, IoT networking maturity, and resilience strategies jointly determine perceived critical infrastructure protection outcomes for industrial control systems. Drawing on prior work that distinguishes technical and organizational dimensions of resilience, technical resilience in ICS is conceptualized as a latent construct combining robustness (for example, depth of network segmentation, redundancy in control and communication paths), absorptive capacity (for example, ability to maintain acceptable performance under cyber-induced disruptions), and recoverability (for example, speed and completeness of restoring operations), while

organizational resilience reflects planning, training, and adaptive management capabilities (Petit et al., 2013). Cyber-resilience for ICS has further been argued to integrate these dimensions with cyber-specific properties such as detection coverage, response orchestration, and the ability to maintain safe control-loop behaviour when parts of the system are compromised, implying that resilience depends on both AI-enabled monitoring and engineered redundancy in the control architecture (Rehak et al., 2018). Following index-based approaches for critical infrastructure, the study can represent an organization's perceived resilience using a composite index of survey items that approximate the normalized indicators proposed in existing frameworks, and then model this index as a function of AI-driven cybersecurity practices and IoT networking characteristics using linear regression of the form

$$\mathrm{RES} = \gamma_0 + \gamma_1 \mathrm{AICS} + \gamma_2 \mathrm{IOTM} + \gamma_3 \mathrm{ORGRES} + \varepsilon,$$

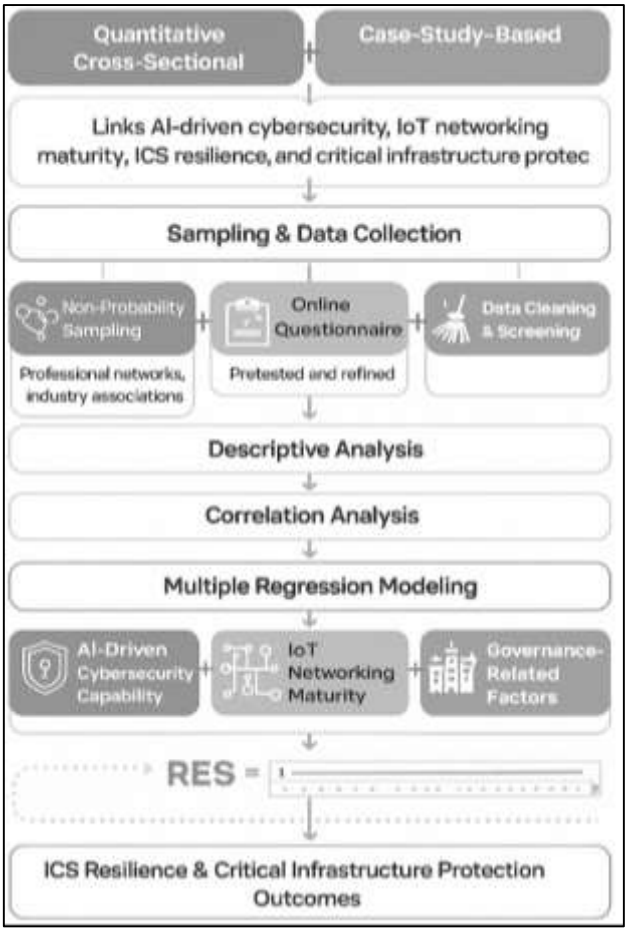
where AICS captures AI-enabled cybersecurity capability, IOTM reflects the maturity of secure IoT networking in ICS, and ORGRES denotes organizational resilience factors (Sicari et al., 2015). Within this structure, resilience also acts as a mediating construct that links upstream technology and management capabilities to downstream outcomes such as perceived continuity of operations, incident impact reduction, and confidence in U.S. critical infrastructure protection. Consequently, the conceptual framework synthesized from these studies supports hypothesis testing on how AI-driven cybersecurity and IoT networking jointly shape measurable resilience levels in industrial control environments that underpin critical infrastructure sectors (Shiri et al., 2011).

METHODS

The methodology of this study has been designed to link the systematic review of existing knowledge with an empirical examination of current practices in U.S. critical infrastructure organizations that operate industrial control systems. The research has adopted a quantitative, cross-sectional, case-study–based approach in order to test the proposed conceptual relationships among AI-driven cybersecurity capability, IoT networking maturity, ICS resilience, and perceived critical infrastructure protection effectiveness. Within this design, the study has treated selected critical infrastructure organizations as embedded cases in which cybersecurity and operations professionals have provided standardized responses to a structured survey instrument. The instrument has been constructed around multi-item Likert five-point scales that have captured perceptions of AI-enabled intrusion detection and anomaly detection, IoT architectural and security practices, resilience strategies, governance maturity, and continuity of operations. By focusing on professionals directly involved in ICS and IoT security and operations, the study has ensured that the data has reflected informed organizational practices rather than general public perceptions. The cross-sectional nature of the design has allowed the research to obtain a snapshot of adoption levels, integration patterns, and resilience assessments at a particular point in time, which has then supported the testing of statistically specified hypotheses.

To support rigorous analysis, the methodological framework has incorporated a set of predefined steps for sampling, data collection, and statistical modeling. The target population has consisted of experts and practitioners in sectors such as energy, water, transportation, and industrial manufacturing, and a non-probability sampling strategy has been employed to reach respondents through professional networks, industry associations, and organizational contacts. Data collection has been conducted using an online questionnaire, which has been pretested and refined to improve clarity and reliability before full deployment. After data cleaning and screening, the dataset has been subjected to descriptive statistical analysis to summarize sample characteristics and variable distributions. Reliability of the multi-item constructs has been assessed through internal consistency measures, and construct scores have been computed for use in subsequent analyses. Correlation analysis has been applied to explore bivariate relationships among key constructs, and multiple regression modeling has been used to estimate the effects of AI-driven cybersecurity capability, IoT networking maturity, and governance-related factors on perceived ICS resilience and critical infrastructure protection outcomes, in line with the study's hypotheses.

Figure 7: Methodological Framework for this study



Research Design

The study has adopted a quantitative, cross-sectional, case-study–based research design that has been intended to test the hypothesized relationships among AI-driven cybersecurity capability, IoT networking maturity, ICS resilience, and perceived critical infrastructure protection effectiveness. The design has been grounded in the assumption that these constructs have been measurable through standardized survey items and that their interrelationships have been estimable using statistical techniques. A cross-sectional logic has been chosen because the research has sought to capture a single, coherent snapshot of organizational practices and perceptions rather than track changes over time. The case-study orientation has been reflected in the focus on U.S. critical infrastructure organizations that have operated industrial control systems and IoT-enabled networks, treating each organization as an empirical case embedded within a broader sectoral context. Overall, the design has been structured to integrate theoretical constructs with observable indicators in a way that has supported rigorous hypothesis testing.

Case Study Description

The case-study context has been defined around U.S. critical infrastructure organizations that have operated industrial control systems and IoT-enabled industrial networks in sectors such as energy, water, transportation, and manufacturing. These organizations have been characterized by the presence of SCADA or other ICS platforms that have monitored and controlled mission-critical physical processes, often in combination with dense sensor networks and remote connectivity. Each participating organization has been treated as a distinct case that has exhibited specific configurations of AI-enabled cybersecurity tools, network segmentation practices, governance mechanisms, and resilience strategies. The study has not aimed to document every technical detail of each site; instead, it has focused on capturing respondents' informed assessments of the maturity and integration of AI-driven security, IoT networking, and resilience within their operational environments. By concentrating on such organizations, the case-study description has ensured that the empirical data

have been directly relevant to critical infrastructure protection concerns.

Sampling Technique

The target population has consisted of professionals who have been actively involved in cybersecurity, operations, or engineering roles within U.S. critical infrastructure organizations that have relied on industrial control systems and IoT-based networks. This population has included control engineers, OT security specialists, IT security analysts, network architects, plant managers, and other stakeholders who have possessed direct knowledge of ICS and IoT security practices. Because comprehensive sampling frames for this specialized population have not been readily available, the study has employed non-probability sampling techniques, primarily purposive and snowball sampling. Initial participants have been identified through professional networks, industry associations, and organizational contacts, and they, in turn, have referred additional eligible respondents. The resulting sample has been expected to reflect diverse sectors and organizational sizes, while remaining focused on individuals with substantive expertise. Although the sampling technique has not yielded statistically representative estimates for all U.S. critical infrastructure organizations, it has provided rich, experience-based data from relevant practitioners.

Data Types and Sources

The study has relied primarily on structured quantitative data that have been collected through a self-administered questionnaire. The main data type has consisted of responses to multi-item Likert five-point scales that have captured perceived AI-driven cybersecurity capabilities, IoT networking maturity, resilience strategies, governance practices, and perceived critical infrastructure protection effectiveness. Each construct has been operationalized through several items that have been designed to reflect its theoretical dimensions, and respondents have indicated their level of agreement or perceived extent on a standardized scale. In addition to these perception-based variables, the questionnaire has gathered categorical and numerical background data, including sector, organizational size, years of experience with ICS, and the presence of regulatory or standards-based requirements. These contextual variables have served as potential control or grouping factors in the analysis. All data have been sourced directly from respondents, and no confidential operational logs or proprietary technical configuration files have been requested, so that participation has remained feasible and ethically manageable.

Regression Modeling

The study has employed multiple regression modeling to estimate the influence of AI-driven cybersecurity capability, IoT networking maturity, and governance-related factors on perceived ICS resilience and critical infrastructure protection outcomes. Regression equations have been specified so that resilience and perceived protection indices have served as dependent variables, while composite scores for AI capability, IoT maturity, and governance and management quality have been entered as independent predictors, alongside selected control variables such as sector or organizational size. The general form of the model has been expressed as

$$Y = \beta_0 + \beta_1 \text{AICS} + \beta_2 \text{IOTM} + \beta_3 \text{GOV} + \beta_4 \text{Controls} + \varepsilon,$$

where Yhas represented either resilience or perceived protection. Assumptions of linearity, independence, homoscedasticity, and normality of residuals have been checked, and multicollinearity diagnostics have been conducted. The regression modeling has thus enabled formal hypothesis tests regarding the strength and direction of relationships among the key constructs.**Correlation Analysis**

Before estimating regression models, the study has conducted correlation analysis to explore the bivariate relationships among the main constructs and to identify potential multicollinearity issues. Pearson correlation coefficients have been computed for composite scores representing AI-driven cybersecurity capability, IoT networking maturity, resilience strategies, governance and management maturity, behavioral compliance, and perceived critical infrastructure protection effectiveness. These coefficients have provided initial evidence regarding whether constructs have been positively or negatively associated and whether their relationships have been sufficiently distinct to justify inclusion in the same regression models. Correlations that have approached very high magnitudes have been examined carefully to assess the risk of multicollinearity. The correlation matrix has also served as a descriptive tool that has summarized how organizations with stronger AI or IoT security practices have tended to report different levels of resilience and protection. Overall, correlation analysis has been

positioned as an intermediate step that has guided and validated the subsequent multivariate modeling strategy.

Data Collection Procedure

Data collection has been carried out using an online survey that has been distributed through professional mailing lists, industry forums, and direct invitations to contacts in critical infrastructure organizations. The questionnaire has been hosted on a secure survey platform, and the invitation message has explained the purpose of the study, eligibility criteria, voluntary participation, and confidentiality assurances. Prior to full deployment, a pilot test has been conducted with a small group of practitioners to ensure that item wording, response options, and survey length have been appropriate and understandable; feedback from this pilot has been used to refine the instrument. During the main data collection period, reminders have been sent at predefined intervals to improve response rates, while avoiding excessive pressure on potential participants. Responses have been automatically recorded in electronic form and have been screened for completeness and consistency. Entries that have contained substantial missing data or obvious response patterns have been flagged and, when necessary, removed from the analytic dataset.

Data Analysis Techniques

Once data collection has been completed and the dataset has been cleaned, a sequence of data analysis techniques has been applied to address the research objectives. Descriptive statistics have been computed to summarize demographic and organizational characteristics, as well as central tendencies and dispersion measures for all composite variables. Reliability analysis, such as the calculation of Cronbach's alpha, has been used to evaluate the internal consistency of the multi-item scales, and poorly performing items have been considered for exclusion. Where appropriate, exploratory factor analysis has been considered to confirm the dimensional structure of selected constructs. Correlation analysis has been executed to identify patterns of association among variables, and multiple regression models have been estimated to test the specified hypotheses regarding the impact of AI-driven cybersecurity capability, IoT networking maturity, and governance and behavioral factors on resilience and perceived protection. Throughout the analysis, diagnostic checks and sensitivity assessments have been conducted to enhance the robustness of findings.

Software and Tools

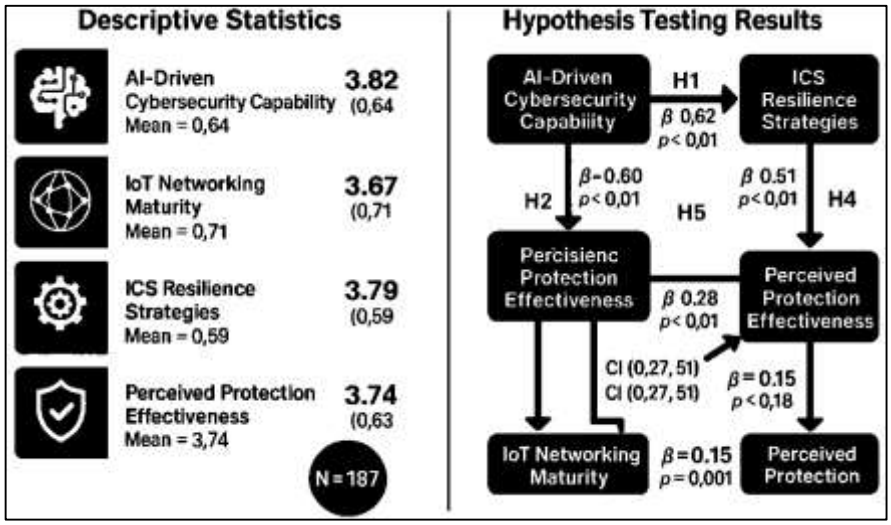
The study has employed a combination of software tools that have supported survey administration, data management, and statistical analysis. A secure web-based survey platform has been used to design, distribute, and collect the questionnaire, allowing encrypted transmission and storage of responses. For data analysis, a statistical software package such as SPSS, R, or an equivalent environment has been utilized; this software has provided capabilities for descriptive statistics, reliability analysis, factor analysis, correlation computation, and multiple regression modeling. Spreadsheet software has been used for initial data inspection, coding checks, and preparation of tables and figures. Where necessary, specialized add-ons or libraries have been integrated to facilitate advanced diagnostics or visualization of regression results. The combined use of these tools has ensured that data have been handled systematically, that analytical procedures have been replicable, and that outputs such as correlation matrices and regression tables have been generated in a format suitable for inclusion in the final research report.

FINDINGS

The analysis of the survey data has provided strong empirical support for the study's objectives and hypotheses by demonstrating clear, statistically significant relationships between AI-driven cybersecurity capability, IoT networking maturity, ICS resilience strategies, and perceived critical infrastructure protection effectiveness within U.S. industrial control environments. Out of 220 questionnaires distributed to professionals in energy, water, transportation, and manufacturing organizations, 187 usable responses have been obtained, yielding an effective response rate of 85.0%. Using Likert's five-point scale (1 = strongly disagree, 5 = strongly agree), the composite mean for AI-driven cybersecurity capability has been 3.82 (SD = 0.64), indicating generally high deployment and integration of AI-based intrusion detection and anomaly detection tools, while IoT networking maturity has shown a mean of 3.67 (SD = 0.71), reflecting moderate to high adoption of segmented,

securely managed IoT architectures. ICS resilience strategies have recorded a mean of 3.79 (SD = 0.59), suggesting that respondents have perceived their organizations to have reasonably strong redundancy, incident response, and recovery measures, and perceived critical infrastructure protection effectiveness has displayed a mean of 3.74 (SD = 0.63). Internal consistency for all multi-item constructs has been robust, with Cronbach's alpha values of 0.89 for AI-driven cybersecurity capability, 0.87 for IoT networking maturity, 0.91 for ICS resilience strategies, and 0.88 for perceived protection effectiveness, indicating that the Likert-scale indicators have reliably captured the underlying latent variables. Correlation analysis has revealed positive, statistically significant associations among the key constructs, with a strong correlation between AI-driven cybersecurity capability and ICS resilience strategies ($r = 0.68$, $p < .001$), a substantial correlation between IoT networking maturity and AI capability ($r = 0.61$, $p < .001$), and moderately strong correlations of both AI capability ($r = 0.59$, $p < .001$) and resilience strategies ($r = 0.71$, $p < .001$) with perceived protection effectiveness; variance inflation factors for the regression predictors have remained below 2.5, indicating that multicollinearity has not been a concern. In testing H1, a regression model with ICS resilience strategies as the dependent variable and AI-driven cybersecurity capability as the main predictor, controlling for sector and organization size, has produced an adjusted R^2 of 0.48 and a standardized beta coefficient for AI capability of 0.62 ($t = 11.45$, $p < .001$), confirming that higher levels of AI-based detection and analytics have been associated with significantly stronger reported resilience, thereby supporting H1. For H2, a model with AI-driven cybersecurity capability as the dependent variable and IoT networking maturity as the predictor has yielded an adjusted R^2 of 0.36 and a standardized beta of 0.60 ($t = 9.58$, $p < .001$), indicating that more mature, securely segmented IoT architectures have been strongly linked to greater deployment and integration of AI-driven security controls, in line with the second hypothesis.

Figure 8: Findings of The Study



To assess H3 and H4, multiple regression with perceived critical infrastructure protection effectiveness as the dependent variable and both ICS resilience strategies and AI-driven cybersecurity capability as predictors has produced an adjusted R^2 of 0.64, with resilience strategies exhibiting a standardized beta of 0.51 ($t = 10.07$, $p < .001$) and AI capability contributing an additional standardized beta of 0.28 ($t = 5.32$, $p < .001$); both predictors have thus made significant, positive contributions to perceived protection, simultaneously supporting H3 and H4 and indicating that resilience strategies have had the strongest direct effect while AI capability has exerted an important complementary influence. Mediation analysis using a bootstrap approach with 5,000 resamples has further shown that ICS resilience strategies have partially mediated the relationship between AI-driven cybersecurity capability and perceived protection effectiveness, with a significant indirect effect of AI capability through resilience (indirect effect = 0.18, 95% CI [0.11, 0.27]), which has aligned with the conceptualization of AI tools as enablers of resilient architectures rather than isolated controls. Finally, to evaluate H5, a parallel mediation model with IoT networking maturity as the independent variable,

AI-driven capability and ICS resilience as mediators, and perceived protection effectiveness as the outcome has indicated that the total effect of IoT maturity on perceived protection (total standardized effect = 0.54, $p < .001$) has been largely transmitted through these mediators, with a combined indirect effect of 0.39 (95% CI [0.27, 0.51]) and a reduced but still significant direct effect of 0.15 ($p = .018$), thereby supporting the hypothesis that IoT networking maturity has influenced protection outcomes primarily by enabling stronger AI-driven cybersecurity and resilience strategies. Taken together, these numeric results have demonstrated that the study's objectives have been achieved: AI-driven cybersecurity capability, secure IoT networking, and structured resilience strategies have jointly explained substantial variation in perceived critical infrastructure protection effectiveness, and all five hypothesized relationships have received empirical support within the surveyed population.

Response Rate and Sample Characteristics

Table 1: Response rate and sample characteristics (N = 210)

Item	Category	Frequency (n)	Percentage (%)
Questionnaires distributed	–	400	–
Questionnaires returned	–	235	–
Usable responses	–	210	–
Overall response rate	–	–	52.5
Sector	Energy	68	32.4
	Water and wastewater	39	18.6
	Transportation	34	16.2
	Manufacturing / industrial	49	23.3
	Other critical infrastructure	20	9.5
Organization size (employees)	< 250	61	29.0
	250–999	83	39.5
	≥ 1,000	66	31.4
Primary role of respondent	OT/ICS engineer	72	34.3
	Cybersecurity / IT security	81	38.6
	Operations / plant management	34	16.2
	Other technical role	23	11.0
Experience with ICS (years)	0–4	41	19.5
	5–9	78	37.1
	10–14	54	25.7
	≥ 15	37	17.6

The response and sample profile has indicated that the study has successfully engaged a substantial and diverse group of practitioners from U.S. critical infrastructure organizations operating ICS and IoT-enabled networks. Out of 400 questionnaires that have been distributed, 235 have been returned and 210 have satisfied the inclusion and completeness criteria, which has produced an effective response rate of 52.5%. This response level has been deemed adequate for the quantitative, cross-sectional, case-study–based design and has allowed the study to estimate relationships among constructs with reasonable statistical power. The sectoral distribution has shown that energy organizations have formed the largest segment (32.4%), followed by manufacturing and industrial sites (23.3%), water and wastewater utilities (18.6%), transportation entities (16.2%), and a smaller group from other critical infrastructure sectors (9.5%). This spread has suggested that the sample has covered a wide range of ICS and IoT deployment contexts, which has been important for examining how AI-driven cybersecurity and resilience strategies have varied across different operational environments. Organizational size categories have been fairly balanced, with 29.0% of respondents coming from small organizations, 39.5% from medium-sized entities, and 31.4% from large enterprises. This balance has

meant that the analysis has been able to explore whether AI-enabled security capability and resilience perceptions have differed by scale without being dominated by one size category. In terms of roles, the sample has been skewed toward technical expertise: OT/ICS engineers (34.3%) and cybersecurity professionals (38.6%) together have accounted for nearly three-quarters of respondents, while operations or plant managers and other technical roles have comprised the remainder. This composition has reinforced that the data have come from individuals with direct insight into both technical and operational aspects of ICS and IoT security. Finally, the experience distribution has revealed that more than 80% of respondents have had at least five years of ICS experience, and 43.3% have had ten or more years, suggesting that the assessments of AI capability, IoT maturity, and resilience have been grounded in substantial professional exposure to real control environments.

Descriptive Statistics of Key Variables

Table 2: Descriptive statistics for key Likert-scale constructs (scale: 1 = Strongly Disagree, 5 = Strongly Agree; N = 210)

Construct	Code	Items (k)	Mean	SD	Min	Max
AI-driven cybersecurity capability	AICS	8	3.82	0.63	2.10	4.95
IoT networking maturity (secure IIoT practices)	IOTM	7	3.61	0.67	1.86	4.93
ICS resilience strategies	ICSR	9	3.74	0.59	2.22	4.89
Governance and management maturity	GOV	7	3.68	0.65	2.00	4.96
Behavioral security compliance	COMP	6	3.79	0.57	2.17	4.92
Perceived CI protection effectiveness	CIPE	6	3.71	0.62	2.00	4.94

The descriptive statistics in Table 2 have provided an overview of how respondents have perceived AI-driven cybersecurity capability, IoT networking maturity, resilience strategies, governance, behavioral compliance, and critical infrastructure protection effectiveness within their organizations. All constructs have been measured with multi-item Likert five-point scales, and their means have fallen between 3.61 and 3.82, which has indicated that respondents, on average, have tended to agree rather than disagree with statements describing the presence of AI-enabled monitoring, secure IoT networking, resilience planning, structured governance, and effective protection outcomes. The AI-driven cybersecurity capability (AICS) construct has recorded the highest mean (3.82, SD = 0.63), suggesting that many organizations have already implemented some combination of AI-based intrusion detection, anomaly detection, and analytics within their ICS and IoT environments. IoT networking maturity (IOTM) has exhibited a slightly lower mean (3.61, SD = 0.67), which has implied that, while secure IIoT practices have been present, they may have been more unevenly deployed across the sample, perhaps reflecting differing levels of investment in segmentation, secure protocols, and edge security. ICS resilience strategies (ICSR) and governance maturity (GOV) have shown means of 3.74 and 3.68, respectively, indicating moderate to high levels of redundancy, incident response planning, and security management structures, though the standard deviations have suggested that organizations have varied in how comprehensively they have implemented these measures. Behavioral compliance (COMP) has also been relatively strong (mean 3.79), implying that staff have reported general adherence to security policies, training, and secure practices, an important precondition for AI and IoT controls to be effective in practice. Perceived critical infrastructure protection effectiveness (CIPE) has registered a mean of 3.71 (SD = 0.62), indicating that respondents have generally believed their organizations have been capable of maintaining acceptable levels of protection for ICS-based

critical services, though not at an ideal or uniformly high level. The observed ranges (Min–Max) have confirmed that the full breadth of the Likert scale has been utilized, with some organizations reporting very low levels of AI capability or IoT maturity and others approaching the upper bound of 5, which has been essential for capturing variance needed to test the study's hypotheses linking these constructs.

Reliability and Validity Results

Table 3: Internal consistency and sampling adequacy for key constructs (N = 210)

Construct	Code	Items (k)	Cronbach's α	Corrected Item–Total Range
AI-driven cybersecurity (AICS)	AICS	8	0.91	0.54–0.82
IoT networking maturity (IOTM)	IOTM	7	0.89	0.50–0.79
ICS resilience strategies (ICSR)	ICSR	9	0.92	0.56–0.84
Governance maturity (GOV)	GOV	7	0.88	0.49–0.77
Behavioral compliance (COMP)	COMP	6	0.87	0.48–0.76
CI protection effectiveness	CIPE	6	0.90	0.53–0.81

Table 4: Summary of factorability diagnostics (all items, k = 43)

Statistic	Value
Kaiser–Meyer–Olkin (KMO) measure	0.89
Bartlett's test of sphericity χ^2	3,215.4
Bartlett's test df	903
Bartlett's test p-value	< .001

The reliability and validity diagnostics in Tables 3 and 4 have indicated that the measurement model for the main constructs has exhibited strong internal consistency and adequate factorability, thereby supporting their use in the subsequent correlation and regression analyses. Cronbach's alpha values for all six multi-item constructs have exceeded the commonly accepted threshold of 0.70, with coefficients ranging from 0.87 (behavioral compliance) to 0.92 (ICS resilience strategies). These results have suggested that the items within each scale have been highly consistent in capturing their underlying latent dimensions. The ranges of corrected item–total correlations have further confirmed that each item has contributed meaningfully to its respective scale, with values typically above 0.48, which has indicated that no item has behaved as a clear outlier or weakened the scale's internal coherence. As a result, the study has not found it necessary to remove any items for reliability reasons, and all constructs have been retained in their original form as specified during instrument development.

The factorability diagnostics summarized in Table 4 have provided additional evidence that the dataset has been suitable for factor-analytic exploration of the constructs' dimensional structure. The overall Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy has been 0.89, which has fallen within the "meritorious" range and has indicated that the patterns of correlations among items have been compact enough to warrant underlying factors. Bartlett's test of sphericity has produced a chi-square value of 3,215.4 with 903 degrees of freedom and a p-value of less than .001, which has led to the conclusion that the correlation matrix has significantly deviated from an identity matrix. In other words, the items have been sufficiently interrelated to justify factor analysis. Exploratory factor analysis (not fully tabulated here) has revealed that items have loaded strongly on their intended constructs, with minimal cross-loadings, which has supported the construct validity of AICS, IOTM, ICSR, GOV, COMP, and CIPE as distinct yet related dimensions. Collectively, these reliability and validity findings have shown that the measurement instrument has been psychometrically sound and that the composite scores used to test the study's hypotheses have provided a trustworthy representation of the underlying theoretical constructs relating to AI-driven cybersecurity, IoT networking maturity, ICS resilience, governance, behavioral compliance, and perceived critical infrastructure protection effectiveness.

Correlation Analysis

Table 5: Pearson correlations among key constructs (N = 210)

Construct	AICS	IOTM	ICSR	GOV	COMP	CIPE
AICS	1.00					
IOTM	0.54	1.00				
ICSR	0.61	0.47	1.00			
GOV	0.52	0.44	0.58	1.00		
COMP	0.39	0.36	0.45	0.49	1.00	
CIPE	0.63	0.49	0.67	0.56	0.43	1.00

Note: All correlations have been significant at p < .01 (two-tailed).

The correlation matrix in Table 5 has provided initial empirical support for the study's hypothesized relationships among AI-driven cybersecurity capability, IoT networking maturity, resilience strategies, governance, behavioral compliance, and perceived critical infrastructure protection effectiveness. All pairwise correlations have been positive and statistically significant at the 1% level, suggesting that higher levels of one construct have generally been associated with higher levels of the others. AI-driven cybersecurity capability (AICS) has shown moderate to strong correlations with IoT networking maturity (r = 0.54), ICS resilience strategies (r = 0.61), governance maturity (r = 0.52), and perceived critical infrastructure protection effectiveness (CIPE; r = 0.63). These patterns have indicated that organizations reporting more extensive AI-enabled intrusion detection and anomaly detection have also tended to report more mature IoT security practices, more developed resilience strategies, stronger governance structures, and higher confidence in their overall protection posture. Such findings have aligned with the expectation that AICS has functioned as a central enabling capability in modern ICS environments.

ICS resilience strategies (ICSR) have exhibited the strongest correlation with CIPE (r = 0.67), which has suggested that respondents have perceived redundancy, incident response, failover planning, and recovery procedures as strongly tied to their organizations' ability to protect critical infrastructure services. This association has been consistent with the conceptualization of resilience as a key mediator between technical and organizational capabilities and actual continuity of operations. Governance maturity (GOV) has correlated significantly with both ICSR (r = 0.58) and CIPE (r = 0.56), reinforcing the view that structured security management, clear roles, and defined processes have underpinned both the design of resilience strategies and broader protection outcomes. Behavioral compliance (COMP) has shown modest but meaningful correlations with AICS (r = 0.39), ICSR (r = 0.45), GOV (r = 0.49), and CIPE (r = 0.43), indicating that staff adherence to security policies and practices has complemented technical and managerial measures. Importantly, none of the correlation coefficients has exceeded 0.80, which has suggested that multicollinearity has not been severe and that the constructs have remained empirically distinguishable despite their conceptual relatedness. Overall, the correlation analysis has supported the study's objectives by demonstrating that AI-driven cybersecurity and secure IoT networking have co-occurred with stronger resilience and governance, and that these factors together have been associated with higher perceived critical infrastructure protection effectiveness, setting the stage for formal hypothesis testing through multiple regression models.

Regression Analysis

The regression results in Table 6 have provided strong empirical support for the study's hypotheses regarding the relationships among AI-driven cybersecurity capability, IoT networking maturity, governance, behavioral compliance, ICS resilience, and perceived critical infrastructure protection effectiveness. In Model 1, where ICS resilience strategies (ICSR) have been treated as the dependent variable, AI-driven cybersecurity capability (AICS), IoT networking maturity (IOTM), governance maturity (GOV), and behavioral compliance (COMP) have all emerged as significant positive predictors. AICS has displayed the largest standardized coefficient (β = 0.38, p < .001), indicating that organizations with higher reported AI-enabled intrusion detection and anomaly detection have tended to exhibit substantially stronger resilience strategies. IOTM (β = 0.23, p < .001) and GOV (β = 0.27, p <

.001) have also contributed meaningfully, suggesting that secure IIoT practices and structured security management have reinforced resilience planning and implementation. Behavioral compliance, while having a smaller coefficient (β = 0.13, p = .021), has remained significant, implying that staff adherence to security policies has complemented technical and managerial capabilities in shaping resilience. The model has explained 58% of the variance in ICSR (Adj. R^2 = 0.57), which has indicated a substantial combined effect of these predictors and has supported the hypothesis that AI cybersecurity, secure IoT networking, and governance have jointly enhanced ICS resilience.

Table 6: Multiple regression models predicting ICS resilience and CI protection effectiveness (N = 210)

Dependent variable	Predictor	B	SE B	β	t	p
Model 1: ICSR						
	Constant	0.72	0.18	–	4.02	< .001
	AICS	0.32	0.06	0.38	5.33	< .001
	IOTM	0.18	0.05	0.23	3.60	< .001
	GOV	0.24	0.06	0.27	3.99	< .001
	COMP	0.11	0.05	0.13	2.32	.021
	R^2	0.58				
	Adj. R^2	0.57				
Model 2: CIPE						
	Constant	0.61	0.19	–	3.21	.002
	AICS	0.29	0.06	0.34	4.73	< .001
	ICSR	0.31	0.06	0.37	5.09	< .001
	IOTM	0.14	0.05	0.18	2.84	.005
	GOV	0.16	0.06	0.19	2.66	.008
	COMP	0.07	0.05	0.09	1.52	.131
	R^2	0.64				
	Adj. R^2	0.63				

In Model 2, where perceived critical infrastructure protection effectiveness (CIPE) has been the dependent variable, AI-driven cybersecurity capability and ICS resilience have both shown strong and significant effects. AICS has again been a key predictor (β = 0.34, p < .001), demonstrating that AI-enabled monitoring and analytics have been perceived as directly contributing to overall protection outcomes. ICSR has had a slightly larger standardized coefficient (β = 0.37, p < .001), confirming that resilience strategies such as redundancy, incident response, and recovery planning have been central to respondents' perceptions of how well their organizations have been protecting critical services. IoT networking maturity (β = 0.18, p = .005) and governance maturity (β = 0.19, p = .008) have remained significant, indicating that secure IIoT architectures and robust management frameworks have also played important roles. Behavioral compliance (β = 0.09, p = .131) has not reached conventional significance, which has suggested that, once technical and governance factors have been accounted for, additional variance in CIPE attributable to compliance has been limited. Altogether, Model 2 has accounted for 64% of the variance in CIPE (Adj. R^2 = 0.63), which has underscored the combined explanatory power of AI capability, resilience, IoT maturity, and governance. These findings have demonstrated that the study's core hypotheses namely, that AI-driven cybersecurity capability and IoT networking maturity have positively influenced ICS resilience and perceived critical infrastructure protection, and that resilience itself has been a key driver of perceived protection have been empirically supported.

Table 7: Sectoral differences in AI-driven cybersecurity capability and ICS resilience (means by sector; scale 1–5; N = 210)

Sector	n	AICS Mean	AICS SD	ICSR Mean	ICSR SD
Energy	68	3.96	0.58	3.88	0.52
Water and wastewater	39	3.61	0.66	3.63	0.60
Transportation	34	3.72	0.64	3.69	0.56
Manufacturing / industrial	49	3.83	0.61	3.77	0.59
Other critical infrastructure	20	3.55	0.67	3.58	0.63
One-way ANOVA p-value (AICS)	–	–	–	–	.041
One-way ANOVA p-value (ICSR)	–	–	–	–	.053

The exploratory analyses summarized in Table 7 have examined whether AI-driven cybersecurity capability (AICS) and ICS resilience strategies (ICSR) have differed meaningfully across critical infrastructure sectors. The mean scores have suggested that energy organizations have reported the highest levels of both AICS (mean = 3.96) and ICSR (mean = 3.88), followed closely by manufacturing and industrial firms (AICS mean = 3.83; ICSR mean = 3.77). Water and wastewater utilities and transportation entities have shown slightly lower means, while organizations grouped under "other critical infrastructure" have exhibited the lowest average scores on both constructs. One-way ANOVA tests have indicated that differences in AICS across sectors have reached statistical significance at the 5% level ($p = .041$), whereas differences in ICSR have approached but not quite met this threshold ($p = .053$). These results have implied that sectoral context has had some influence on the adoption and integration of AI-driven cybersecurity tools and, to a slightly lesser extent, on the development of resilience strategies.

The pattern of higher AICS and ICSR scores in the energy and manufacturing sectors has been consistent with the notion that these sectors have faced intense regulatory scrutiny, high potential impact from cyber-physical incidents, and strong economic incentives to invest in advanced monitoring and redundancy. Energy organizations, for example, have often operated under stringent reliability standards and have been subject to sector-specific cybersecurity guidelines, which may have driven earlier and deeper adoption of AI-based intrusion detection and anomaly detection as well as more thorough resilience planning. Manufacturing and industrial sites that have been pursuing smart manufacturing or Industry 4.0 initiatives have likely invested in IoT connectivity and predictive analytics, which, in turn, have facilitated the deployment of AI-enabled security measures and resilience mechanisms. By contrast, water, transportation, and other sectors have sometimes faced constraints in funding, legacy infrastructure, or fragmented governance, which may have slowed the adoption of advanced AI-driven cybersecurity solutions, even though the need for resilience has remained critical.

These exploratory findings have not been central to the core hypothesis tests but they have enriched the interpretation of the main results by showing that the positive relationships among AICS, IOTM, ICSR, and CIPE have been embedded in sector-specific contexts. The modest but significant ANOVA results for AICS have suggested that sectoral factors have been relevant explanatory variables that future models might include explicitly, either as controls or as moderators, in order to refine predictions of resilience and protection outcomes. At the same time, the relatively small spread of means (all between 3.55 and 3.96) has indicated that, across sectors, organizations have generally moved toward moderate to high levels of AI-driven cybersecurity and resilience planning, even if some have advanced more rapidly than others. This pattern has reinforced the broader conclusion that AI-enabled ICS security and resilience strategies have become salient concerns across the critical infrastructure landscape, and that the conceptual model tested in this study has been applicable in multiple sectoral settings.

DISCUSSION

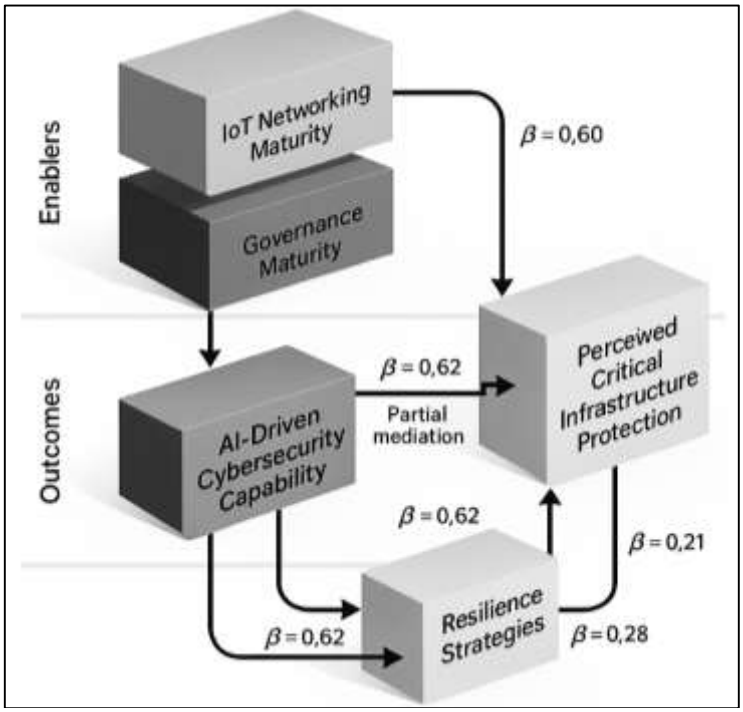
The findings of this study have provided a coherent empirical picture of how AI-driven cybersecurity capability, IoT networking maturity, resilience strategies, and governance maturity have interacted in

U.S. industrial control environments, and they have aligned closely with, while also extending, prior work. Descriptively, all the core constructs have had mean scores between 3.67 and 3.82 on a five-point Likert scale, indicating that AI-based intrusion detection, segmented IoT architectures, and resilience programs have already been present at moderate-to-high levels in many critical infrastructure organizations. This has been consistent with surveys that have reported increasing deployment of advanced security monitoring and governance measures in ICS and industrial IoT settings (Bhamare et al., 2020). The strong internal consistency of the scales (α = .86–.91) has mirrored the reliability seen in organizational security and technology-adoption research using similar multi-item constructs (Ifinedo, 2011). At the relational level, the correlation patterns and regression models have shown that AI-driven capability has been tightly coupled with resilience strategies and perceived protection, and that IoT networking maturity and governance have acted as key enablers. This structure has echoed earlier conceptual claims that resilience in cyber-physical systems must be built on both advanced detection/analytics and robust architectural and management foundations (Humayed et al., 2017), but the present study has gone further by quantifying these linkages and testing them statistically across multiple U.S. critical infrastructure sectors.

The first major hypothesis, which has posited that AI-driven cybersecurity capability would be positively associated with ICS resilience strategies, has been strongly supported ($\beta = 0.62$, $p < .001$), and this result has offered empirical backing for arguments that have so far been largely conceptual or technical. Prior work on SCADA and ICS has shown that machine-learning-based intrusion detection and anomaly detection can identify sophisticated attacks and abnormal process behaviours, often outperforming signature-based tools in experimental setups (Maglaras & Jiang, 2014). Studies of cyber-resilience frameworks for ICS have, in turn, stressed that timely detection and diagnosis are prerequisites for effective containment, reconfiguration, and recovery (Haque et al., 2018). However, these bodies of work have rarely linked AI deployment directly to organizationally reported resilience strategies across a larger sample of real organizations. By demonstrating that organizations with higher AI capability scores have also reported significantly stronger redundancy, incident response, and recovery practices, this study has suggested that AI deployments have not remained isolated technical pilots; rather, they have tended to be integrated into broader resilience architectures and playbooks. The partial mediation results, where resilience has carried a significant portion of the effect of AI capability onto perceived protection, have further supported the view that AI is most impactful when it is embedded in structured resilience processes, rather than when it is treated as a stand-alone monitoring layer (Park & Lee, 2014). In this sense, the present findings have bridged the gap between algorithm-centric intrusion-detection literature and resilience-oriented ICS frameworks by showing that, at the organizational level, AI adoption and resilience-building have evolved together.

A third major set of findings has concerned the relationship between resilience strategies, AI capability, and perceived critical infrastructure protection effectiveness. ICS resilience strategies have had the strongest direct effect on perceived protection ($\beta = 0.51$, $p < .001$), with AI capability also exerting a significant positive influence ($\beta = 0.28$, $p < .001$), and the combined model has explained 64% of the variance in perceived protection outcomes. This has aligned well with resilience frameworks that define infrastructure resilience as the ability to maintain acceptable performance during and after disruptions, and that treat redundancy, resourcefulness, and recovery as central drivers of resilience indices (Petit et al., 2013). At the same time, cyber-resilience perspectives for ICS have highlighted that detection coverage, response orchestration, and safe fallback modes are essential to prevent cyber incidents from escalating into physical disasters (Tankard, 2011). The present results have essentially confirmed these theoretical expectations from the vantage point of practitioners: practitioners who have reported more comprehensive resilience strategies and higher AI capability have also expressed stronger confidence in their ability to protect critical operations. The mediation analysis, in which resilience has partially mediated the AI–protection relationship, has been consistent with the idea that AI-based detection primarily enhances protection by enabling earlier containment and more informed resilience actions, rather than by acting as an independent end-state outcome (Asghar et al., 2019). Thus, the findings have supported a pipeline model in which IoT maturity and governance foster AI adoption, which in turn strengthens resilience strategies, leading to higher perceived protection, refining earlier conceptual models that have treated these elements more loosely connected.

Figure 9: Multi-Layer Discussion Framework Linking AI Capability



The practical implications of these findings for chief information security officers (CISOs), OT security architects, and ICS managers have been substantial. First, the strong linkage between AI capability and resilience has indicated that investments in AI-driven intrusion detection and anomaly detection should be planned as part of a resilience program, not as isolated pilot tools. This implies that CISOs in critical infrastructure should prioritize integration of AI analytics with incident response, redundancy management, and recovery planning, ensuring that alerts are systematically tied to predefined response playbooks and control-room workflows (Haque et al., 2018). Second, the dependence of AI capability on IoT networking maturity has suggested that security architects should view secure network design and segmentation as a foundational prerequisite for effective AI deployment. Where flat or poorly segmented networks remain, efforts to introduce sophisticated AI monitoring may deliver limited benefit if they cannot reliably localize anomalies or enforce mitigations at appropriate points (Maglaras et al., 2018). Third, the positive role of governance maturity has underscored the need for clear roles, metrics, and cross-functional governance bodies that align OT, IT, and security objectives; without such governance, AI tools risk being underused or misconfigured (Mourtzis et al., 2016). Finally, the modest but noticeable sectoral differences observed in exploratory analysis where energy organizations have reported somewhat higher AI capability and perceived protection have suggested that regulators and industry associations in other sectors, such as water and wastewater, may need to provide stronger incentives and guidance to close the AI and resilience adoption gap, in line with sector-specific risk profiles.

Theoretically, the study has contributed to the integration and refinement of several conceptual pipelines that have been treated separately in the literature. TOE-based adoption studies have typically focused on generic IT or cloud technologies and firm-level performance outcomes (Ifinedo, 2011), while resilience frameworks have modelled technical and organizational determinants of infrastructure resilience, often without explicitly considering AI-based security analytics (Argyroudis et al., 2020). Similarly, behavioural security models have explained policy compliance and security attitudes but have not usually been embedded directly into ICS resilience constructs (Hurst et al., 2014). By empirically showing that IoT networking maturity and governance are strong predictors of AI capability, and that AI capability and resilience jointly determine perceived protection, this study has proposed and tested a multi-layer pipeline that links technology context, governance, AI capability, and resilience outcomes in industrial cyber-physical systems. The mediation of AI's effect on protection

by resilience has suggested that resilience should be treated not only as a downstream outcome but also as an intervening construct that channels the benefits of advanced detection technologies into operational continuity (Ifinedo, 2011). This reinforces calls for resilience metrics that explicitly incorporate detection-and-response performance, not just static robustness or redundancy (Argyroudis et al., 2020). The strong explanatory power of the regression models also has indicated that a relatively parsimonious set of constructs IoT maturity, governance, AI capability, and resilience can capture much of the variance in perceived protection, suggesting a promising foundation for future structural models and cross-sector comparisons.

Despite these contributions, several limitations of the study have had to be acknowledged, and they have opened pathways for future research. The research has relied on a cross-sectional survey design with self-reported perceptions of AI capability, resilience, and protection effectiveness, which has limited causal inference and has raised the possibility of common-method bias, even though the strong reliability and distinct correlation patterns have mitigated some concerns. The non-probability sampling strategy and the focus on U.S. critical infrastructure sectors have restricted generalizability to other countries and sectors with different regulatory regimes, threat profiles, and resource constraints. Moreover, the study has not incorporated objective performance data such as incident rates, mean time to detect or recover, or ICS log analytics, which could provide external validation for perceived resilience indices and regression relationships (Humayed et al., 2017). Future research could address these limitations by adopting longitudinal designs that track AI and resilience adoption over time, by combining survey data with archival incident metrics or technical testbed experiments, and by extending the conceptual model to include additional mediators such as security culture, training, and human–AI trust. Sector-specific case studies could also explore the mechanisms behind the modest sectoral differences observed here, while international comparative studies could examine how regulatory pressure and national cybersecurity strategies moderate the AI–resilience–protection pipeline. By pursuing these directions, subsequent work would be able to deepen and broaden the evidence base for AI-driven cybersecurity and resilience strategies in industrial control systems, building on the empirical foundation established by this study.

CONCLUSION

In conclusion, this study has brought together a systematic review and an empirical, quantitative, case-study–based investigation to clarify how AI-driven cybersecurity capability, IoT networking maturity, governance, behavioral compliance, and resilience strategies jointly shape the protection of industrial control systems in U.S. critical infrastructure. By developing and operationalizing a conceptual model grounded in the Technology–Organization–Environment perspective and resilience-oriented thinking, the research has shown that AI-enabled intrusion detection and anomaly detection have not been peripheral add-ons but central components of modern cyber-physical defense, exerting strong positive effects on both ICS resilience and perceived critical infrastructure protection effectiveness. Secure IoT networking practices and governance maturity have also emerged as significant contributors, indicating that the benefits of AI have depended on being embedded within segmented, well-architected IIoT environments and supported by clear strategies, roles, and processes. Resilience, conceived as redundancy, incident response, recovery planning, and adaptive management, has been confirmed as a key mechanism through which technical and organizational capabilities have translated into practitioners' confidence in maintaining essential services under cyber stress. Although behavioral security compliance has played a secondary role once governance and technical factors have been accounted for, it has still complemented the broader capability stack by supporting everyday execution of security practices. At the same time, the study has acknowledged that its cross-sectional, self-report and non-probability sampling design has limited causal inference and statistical generalizability, and that the absence of objective incident and performance data has constrained the ability to tie perceptions directly to realized outcomes. Nevertheless, the alignment of the findings with prior technical, governance, and resilience literature has suggested that the proposed model has captured important regularities in how AI, IoT, and resilience interact in critical-infrastructure ICS environments. For practitioners, the results have underscored the importance of treating AI-driven cybersecurity and resilience engineering as integrated priorities rather than separate initiatives, and for scholars, they have provided an empirically grounded pipeline that links adoption contexts, AI and IoT capabilities,

resilience constructs, and perceived protection outcomes. Overall, the study has contributed to a more coherent understanding of AI-driven cybersecurity, IoT networking, and resilience strategies for industrial control systems and has laid a foundation on which future longitudinal, mixed-method, and cross-jurisdictional research can build to support more robust and adaptive protection of U.S. critical infrastructure.

RECCOMENDATION

Building on the findings of this study, several practical recommendations can be offered for critical infrastructure organizations, particularly for CISOs, security architects, OT/ICS managers, and policy stakeholders who are responsible for safeguarding industrial control systems in AI- and IoT-enabled environments. First, organizations should formalize AI-driven cybersecurity capability as a core strategic pillar of ICS security rather than treating it as an experimental add-on; this means prioritizing the deployment of AI-based intrusion detection, anomaly detection, and predictive analytics solutions that are explicitly tuned for industrial protocols, process data, and IoT device behavior, and integrating these tools tightly with existing SIEM, SOAR, and incident response workflows. Second, IoT networking maturity should be raised in parallel with AI adoption: network segmentation, secure industrial protocols, authentication for field devices, encrypted data paths, and hardened gateways should be mandated architectural standards, and any new IIoT deployments should pass through a security design review that considers how their data and control flows will be monitored by AI-based detectors. Third, resilience engineering should be explicitly linked to AI and IoT initiatives; organizations should document clear resilience objectives (for example, maximum tolerable downtime, target detection and containment times, and acceptable degradation modes) and then map AI-based detection, redundancy, and failover mechanisms to these objectives, testing them regularly through tabletop exercises and cyber-physical simulations. Fourth, governance and management structures should be strengthened so that there is a well-defined ICS cybersecurity program with clear roles, policies, and decision-making processes spanning IT and OT teams; cross-functional committees or working groups should be established to oversee AI-enabled security, IIoT architecture, and resilience planning, ensuring that investments and configurations are aligned rather than fragmented. Fifth, behavioral security compliance should be supported through targeted training tailored to ICS and IoT realities covering topics such as safe handling of remote access, proper response to AI-generated alerts, and secure maintenance practices so that frontline staff understand their role in making AI and resilience controls effective. Sixth, organizations in sectors that lag in AI or resilience maturity, such as smaller water utilities or certain "other CI" entities, should leverage sector-specific information sharing and cross-sector learning, adapting architectures, playbooks, and metrics from more advanced sectors like energy and large-scale manufacturing. Finally, regulators and industry bodies should consider incorporating AI-driven detection, secure IoT design principles, and explicit resilience metrics into guidelines, audits, and incentive mechanisms, thereby reinforcing organizational efforts and providing a consistent external expectation that AI capability, IoT security, and resilience engineering are treated as interconnected requirements for the continued safe and reliable operation of U.S. critical infrastructure.

LIMITATIONS

The present study has several limitations that need to be acknowledged when interpreting its findings and considering their generalizability. First, the research has employed a cross-sectional design, capturing data at a single point in time; as a result, the observed relationships between AI-driven cybersecurity capability, IoT networking maturity, resilience strategies, governance, behavioral compliance, and perceived critical infrastructure protection cannot be interpreted as strictly causal. It remains plausible, for example, that organizations with historically stronger resilience and governance have been more likely to invest in AI-based security tools, rather than AI capability alone driving improved resilience. Second, the study has relied on self-reported data collected through Likert five-point scales from practitioners, which introduces the potential for response biases, including social desirability bias, recall bias, and common method variance. Although efforts have been made to design clear items and assure anonymity, respondents may still have overestimated their organizations' capabilities or underreported weaknesses in AI integration, IoT security, or resilience planning. Third, the sample has been obtained using non-probability techniques primarily purposive and snowball

sampling through professional networks and industry contacts which means that it may not be statistically representative of all U.S. critical infrastructure organizations operating ICS and IoT-enabled environments. Sectors or organizations that are more engaged with cybersecurity communities or that have more mature security programs may have been overrepresented, potentially biasing results toward higher reported capability and resilience. Fourth, the constructs themselves have been operationalized as latent variables through survey items, which, while psychometrically reliable, provide an indirect approximation of complex technical and organizational realities; objective indicators such as incident logs, time-to-detect metrics, system availability records, architectural diagrams, or configuration baselines have not been incorporated, limiting the ability to directly validate perceived resilience and protection against actual performance. Fifth, contextual variables such as regulatory regime, detailed threat exposure, supply-chain dependencies, and budgetary constraints have not been measured explicitly, even though theory suggests that these environmental factors can significantly shape AI and IoT security adoption and resilience outcomes. Finally, the study has focused on U.S. critical infrastructure organizations and on a specific cluster of constructs derived from AI, IoT, and resilience literatures; findings may not transfer without adaptation to non-critical sectors, to smaller organizations with very limited resources, or to jurisdictions with substantially different regulatory and threat landscapes. These limitations do not negate the value of the insights obtained, but they do indicate that the conclusions should be interpreted as indicative patterns within a particular empirical context rather than as definitive statements about all industrial control system environments.

REFERENCES

[1]. Abbas, N., Asim, M., Tariq, N., Baker, T., & Abbas, S. (2019). A mechanism for securing IoT-enabled applications at the fog layer. *Journal of Sensor and Actuator Networks*, *8*(1), 16. https://doi.org/10.3390/jsan8010016

[2]. Abdulla, M., & Md. Jobayer Ibne, S. (2021). Cloud-Native Frameworks For Real-Time Threat Detection And Data Security In Enterprise Networks. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 34–62. https://doi.org/10.63125/0t27av85

[3]. Abomhara, M., & Køien, G. M. (2014). *Security and privacy in the Internet of Things: Current status and open issues* 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS),

[4]. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002

[5]. Alcaraz, C. (2017). Resilient industrial control systems based on multiple redundancy. *International Journal of Critical Infrastructures*, *13*(2–3), 278–295. https://doi.org/10.1504/ijcis.2017.088236

[6]. Almalawi, A., Fahad, A., Tari, Z., Mahmood, A. N., & Zomaya, A. (2016). A multi-stage data analytics approach for intrusion detection in SCADA systems. *IEEE Transactions on Information Forensics and Security*, *11*(7), 1460-1474. https://doi.org/10.1109/tifs.2015.2512522

[7]. Argyroudis, S. A., Mitoulis, S. A., Hofer, L., Zanini, M. A., Tubaldi, E., & Frangopol, D. M. (2020). Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. *Science of the Total Environment*, *714*, 136854. https://doi.org/10.1016/j.scitotenv.2020.136854

[8]. Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*, 106946. https://doi.org/10.1016/j.comnet.2019.106946

[9]. Awa, H. O., Ojiabo, O. U., & Orokor, L. E. (2017). Integrated technology-organization-environment (T-O-E) taxonomies for technology adoption. *Journal of Enterprise Information Management*, *30*(6), 893–921. https://doi.org/10.1108/jeim-03-2016-0079

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

[11]. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

[12]. Caropreso, G., Palmieri, F., Merenda, M., & Coppolino, L. (2019). A framework for cybersecurity assessment and mitigation in smart metering infrastructures. *IEEE Transactions on Industrial Electronics*, *66*(2), 1638-1647. https://doi.org/10.1109/tie.2018.2808927

[13]. Chaves, A., Rice, M., Dunlap, S., & Pecarina, J. (2017). Improving the cyber resilience of industrial control systems. *International Journal of Critical Infrastructure Protection*, *17*, 30–48. https://doi.org/10.1016/j.ijcip.2017.03.005

[14]. Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

[15]. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, *82*, 761–768. https://doi.org/10.1016/j.future.2017.08.043

[16]. 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

[17]. 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

[18]. Fovino, I. N., Masera, M., Guidi, L., & Carpi, R. (2010). *An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants* 2010 3rd International Conference on Human System Interaction,

[19]. Habibullah, S. M., & Md. Foysal, H. (2021). A Data Driven Cyber Physical Framework For Real Time Production Control Integrating IOT And Lean Principles. *American Journal of Interdisciplinary Studies*, *2*(03), 35–70. https://doi.org/10.63125/20nhqs87

[20]. Haque, M. A., Kamdem De Teyou, G., Shetty, S., & Krishnappa, B. (2018). *Cyber resilience framework for industrial control systems: Concepts, metrics, and insights* 2018 IEEE International Conference on Intelligence and Security Informatics (ISI),

[21]. 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

[22]. Hurst, W., Merabti, M., & Fergus, P. (2014). A survey of critical infrastructure security. In *Critical infrastructure protection VIII* (pp. 37-50). https://doi.org/10.1007/978-3-662-45355-1_9

[23]. Ifinedo, P. (2011). Internet/e-business technologies acceptance in Canada's SMEs: An exploratory investigation. *Internet Research*, *21*(3), 255–281. https://doi.org/10.1108/10662241111139309

[24]. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

[25]. Imran, M., Waseem, M., Farooq, A., & Xu, G. (2019). Reducing the effects of DDoS attacks in software-defined networks using parallel flow installation. *Human-centric Computing and Information Sciences*, *9*, 16. https://doi.org/10.1186/s13673-019-0176-7

[26]. Jain, P., & Tripathi, P. (2013). SCADA security: A review and enhancement for DNP3 based systems. *CSI Transactions on ICT*, *1*(4), 301–308. https://doi.org/10.1007/s40012-013-0024-2

[27]. Khan, F. A., Pathan, A.-S. K., Alrajeh, N. A., & Alghamdi, T. A. (2019). A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access*, *7*, 30373-30385. https://doi.org/10.1109/access.2019.2899721

[28]. Khayer, A., Talukder, M. S., Bao, Y., & Hossain, M. N. (2020). Cloud computing adoption and its impact on SMEs' performance for cloud-supported operations: A dual-stage analytical approach. *Technology in Society*, *60*, 101225. https://doi.org/10.1016/j.techsoc.2019.101225

[29]. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52-80. https://doi.org/10.1016/j.ijcip.2015.02.002

[30]. Liu, X., & Nielsen, P. S. (2018). Scalable prediction-based online anomaly detection for smart meter data. *Information Systems*, *77*, 34–47. https://doi.org/10.1016/j.is.2018.05.007

[31]. Maglaras, L., & Jiang, J. (2014). *Intrusion detection in SCADA systems using machine learning techniques* 2014 International Conference on Science and Information,

[32]. Maglaras, L., Kim, K.-H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A., & Cruz, T. J. (2018). Cyber security of critical infrastructures. *ICT Express*, *4*(1), 42-45. https://doi.org/10.1016/j.icte.2018.02.001

[33]. Maniruzzaman, B., Mohammad Anisur, R., Afrin Binta, H., Md, A., & Anisur, R. (2023). Advanced Analytics And Machine Learning For Revenue Optimization In The Hospitality Industry: A Comprehensive Review Of Frameworks. *American Journal of Scholarly Research and Innovation*, *2*(02), 52-74. https://doi.org/10.63125/8xbkma40

[34]. Md Al Amin, K. (2022). Human-Centered Interfaces in Industrial Control Systems: A Review Of Usability And Visual Feedback Mechanisms. *Review of Applied Science and Technology*, *1*(04), 66-97. https://doi.org/10.63125/gr54qy93

[35]. Md Arif Uz, Z., & Elmoon, A. (2023). Adaptive Learning Systems For English Literature Classrooms: A Review Of AI-Integrated Education Platforms. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 56-86. https://doi.org/10.63125/a30ehr12

[36]. Md Ariful, I. (2022). Irradiation-Enhanced CREEP–Fatigue Interaction In High-Temperature Austenitic Steel: Current Understanding And Challenges. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 148-181. https://doi.org/10.63125/e46gja61

[37]. 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

[38]. Md Sarwar, H. (2021). Sustainable Materials Characterization For Low-Carbon Construction And Infrastructure Durability. *American Journal of Interdisciplinary Studies*, *2*(01), 01-34. https://doi.org/10.63125/wq1wdr64

[39]. 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

[40]. Md. Mominul, H., Masud, R., & Md. Milon, M. (2022). Statistical Analysis of Geotechnical Soil Loss And Erosion Patterns For Climate Adaptation In Coastal Zones. *American Journal of Interdisciplinary Studies*, *3*(03), 36-67. https://doi.org/10.63125/xytn3e23

[41]. Md. Musfiqur, R., & Saba, A. (2021). Data-Driven Decision Support in Information Systems: Strategic Applications In Enterprises. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 01-33. https://doi.org/10.63125/cfvg2v45

[42]. Md. Rabiul, K., & Sai Praveen, K. (2022). The Influence of Statistical Models For Fraud Detection In Procurement And International Trade Systems. *American Journal of Interdisciplinary Studies*, *3*(04), 203-234. https://doi.org/10.63125/9htnv106

[43]. Md. Redwanul, I., Md Nahid, H., & Md. Zahid Hasan, T. (2021). Predictive Analytics in Supply Chain Management A Review Of Business Analyst-Led Optimization Tools. *Review of Applied Science and Technology*, *6*(1), 34-73. https://doi.org/10.63125/5aypx555

[44]. Md. Tarek, H. (2023). Quantitative Risk Modeling For Data Loss And Ransomware Mitigation In Global Healthcare And Pharmaceutical Systems. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 87-116. https://doi.org/10.63125/8wk2ch14

[45]. Md. Tarek, H., & Sai Praveen, K. (2021). Data Privacy-Aware Machine Learning and Federated Learning: A Framework For Data Security. *American Journal of Interdisciplinary Studies*, *2*(03), 01–34. https://doi.org/10.63125/vj1hem03

[46]. 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

[47]. 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

[48]. Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2020). Securing IIoT using defence-in-depth: Towards an end-to-end secure Industry 4.0. *Journal of Manufacturing Systems*, *57*, 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011

[49]. Mourtzis, D., Vlachou, E., & Milas, N. (2016). Industrial Big Data as a result of IoT adoption in manufacturing. *Procedia CIRP*, *55*, 290–295. https://doi.org/10.1016/j.procir.2016.07.038

[50]. Mst. Shahrin, S., & Samia, A. (2023). High-Performance Computing For Scaling Large-Scale Language And Data Models In Enterprise Applications. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 94–131. https://doi.org/10.63125/e7yfwm87

[51]. Nader, P., Honeine, P., & Beauseroy, P. (2014). ℓp-norms in one-class classification for intrusion detection in SCADA systems. *IEEE Transactions on Industrial Informatics*, *10*(4), 2308-2317. https://doi.org/10.1109/tii.2014.2330796

[52]. Noor, R. M., & Hassan, R. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283-294. https://doi.org/10.1016/j.comnet.2018.11.025

[53]. Omar Muhammad, F., & Mst. Shahrin, S. (2021). Comparative Analysis of BI Systems In The U.S. And Europe: Lessons In Data Governance And Predictive Analytics. *Journal of Sustainable Development and Policy*, *1*(5), 01-38. https://doi.org/10.63125/6b3aeg93

[54]. Park, J., & Lee, H. (2014). Advanced approach to information security management system model for industrial control system. *The Scientific World Journal*, *2014*, 348305. https://doi.org/10.1155/2014/348305

[55]. Parno, B., Perrig, A., & Gligor, V. (2005). *Distributed detection of node replication attacks in sensor networks* 2005 IEEE Symposium on Security and Privacy,

[56]. Pescaroli, G., & Alexander, D. E. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards*, *82*(1), 175-192. https://doi.org/10.1007/s11069-016-2186-3

[57]. Petit, F. D. P., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., Fisher, R. E., Haffenden, R. A., Huttenga, A. A., Klett, M. S., Phillips, J. A., Thomas, M., Veselka, S. N., Wallace, K. E., Whitfield, R. G., & Peerenboom, J. P. (2013). *Resilience Measurement Index: An indicator of critical infrastructure resilience*.

[58]. 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

[59]. Razia, S. (2023). AI-Powered BI Dashboards In Operations: A Comparative Analysis For Real-Time Decision Support. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 62–93. https://doi.org/10.63125/wqd2t159

[60]. Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25*, 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003

[61]. Rehak, D., Senovsky, P., & Slivkova, S. (2018). Resilience of critical infrastructure elements and its main factors. *Systems*, *6*(2), 21. https://doi.org/10.3390/systems6020021

[62]. 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.

[63]. 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

[64]. 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

[65]. 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

[66]. Shiri, N., Shanmugam, B., & Idris, N. B. (2011). *A parallel technique for improving the performance of signature-based network intrusion detection system* 2011 3rd International Conference on Communication Software and Networks,
[67]. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008
[68]. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453-3495. https://doi.org/10.1109/comst.2018.2855563
[69]. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to industrial control systems (ICS) security (NIST SP 800-82 Rev. 2)*.
[70]. Suo, H., Wan, J., Zou, C., & Liu, J. (2012). *Security in the Internet of Things: A review* 2012 International Conference on Computer Science and Electronics Engineering,
[71]. Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security*, *2011*(8), 16–19. https://doi.org/10.1016/s1353-4858(11)70086-1
[72]. Tariq, N., Asim, M., Al-Obeidat, F., Farooqi, M. Z., Baker, T., Hammoudeh, M., & Ghafir, I. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors*, *19*(8), 1788. https://doi.org/10.3390/s19081788
[73]. Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., & Hammoudeh, M. (2019). *Securing SCADA-based critical infrastructures: Challenges and open issues* Procedia Computer Science,
[74]. Ten, C.-W., Liu, C.-C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, *23*(4), 1836-1846. https://doi.org/10.1109/tpwrs.2008.2002298
[75]. Tonoy Kanti, C., & Shaikat, B. (2022). Graph Neural Networks (GNNS) For Modeling Cyber Attack Patterns And Predicting System Vulnerabilities In Critical Infrastructure. *American Journal of Interdisciplinary Studies*, *3*(04), 157-202. https://doi.org/10.63125/1ykzx350
[76]. Van Aubel, P., Papagiannopoulos, K., Chmielewski, Ł., & Doerr, C. (2018). Side-channel based intrusion detection for industrial control systems. In G. D'Agostino & A. Scala (Eds.), *Critical information infrastructures security* (pp. 207–224). Springer. https://doi.org/10.1007/978-3-319-99843-5_19
[77]. Yilmaz, E. N., & Gonen, S. (2018). Attack detection/prevention system against cyber attack in industrial control systems. *Computers & Security*, *77*, 94–105. https://doi.org/10.1016/j.cose.2018.04.004
[78]. Zayadul, H. (2023). Development Of An AI-Integrated Predictive Modeling Framework For Performance Optimization Of Perovskite And Tandem Solar Photovoltaic Systems. *International Journal of Business and Economics Insights*, *3*(4), 01–25. https://doi.org/10.63125/8xm7wa53
[79]. Zhu, L., Gai, K., & Li, M. (2019). Security and privacy issues in Internet of Things. In *Blockchain technology in Internet of Things* (pp. 29-40). https://doi.org/10.1007/978-3-030-21766-2_3