Frontiers in Computer Science and Artificial Intelligence
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

An Integrated MIS–Cybersecurity Governance Framework for Risk-Adaptive IT Project Management in Critical Infrastructure Systems

Emran Hossain
Department of Business Administration, Humphreys University, Stockton, California, USA
Monjira Bashir
School of Business, International American University, Los Angeles, California, USA
Ruhul Amin Md Rashed
School of Business, International American University, Los Angeles, California, USA
Md Jubayar Hossain
Department of Management & Information Technology, St. Francis College, Brooklyn, New York, USA
Hasan Imam
School of Business, International American University, Los Angeles, California, USA
Md Imtiaz Faruk
Department of Management & Information Technology, St. Francis College, Brooklyn, New York, USA
Corresponding Author: Monjira Bashir**, E-mail**: monjiratrisha@gmail.com

| ABSTRACT
Protecting critical infrastructure from fast dissever cybersecurity needs a unified approach that brings together governance, technology and project execution. This research proposes an Integrated MIS-Cybersecurity Governance Framework. It is about strengthening risk adaptive IT project management in pertinent national infrastructure sectors such as healthcare, energy, transportation, and finance. Using principles from MIS, zero trust security, and project risk analytics, the framework constructs a multilayer decision support architecture. It instills cybersecurity controls, local measures for anomaly detection and compliance automation into the IT project lifecycle. The study draws on a mixed-method evaluation, comprising interviews with experts in the field and historical breach data and simulation-based project models to demonstrate that organizations that employed this type of governance structure reduced project-related cyber vulnerabilities, cost overruns, and downtime. Results show that MIS workflows being aligned with cybersecurity intelligence is improving visibility across departments, making incident response much faster and giving increased strength to the effort to update infrastructures. The framework provides a scalable, data-driven blueprint for securing large-scale digital transformation projects that will support the national security and economic resilience of the US.

| KEYWORDS
An Integrated MIS–Cybersecurity Governance Framework; Risk-Adaptive IT Project Management, Critical Infrastructure Systems

| ARTICLE INFORMATION

ACCEPTED: 01 November 2025 **PUBLISHED:** 25 November 2025 **DOI:** 10.32996/fcsai.2025.4.2.2

1. INTRODUCTION

The security and resilience of the U.S. critical infrastructure including energy, healthcare, transportation, telecommunications, supply chains and public administration have become increasingly vulnerable, as digital transformation takes greater speed across all national sectors. The integration of Artificial intelligence (AI), Cloud ecosystem and internet of things (IoT), intelligent automation and the Digital governance platform has led to a massive increase in the attack surface, which has increased the

possibility of carrying out highly sophisticated cyberattacks at an unprecedented speed and scale (Kaur et al., 2023; Hasan et al., 2025). Adversarial techniques have now become quite common, involving sophisticated persistent threats, ransomware, invasion of the supply chain and artificial intelligence enhanced automated attacks, aimed at systemic weaknesses deeply rooted within interconnected national infrastructure. Within this landscape, Management Information Systems (MIS) play a pivotal role in synergizing data flow, operation processes, resource coordination and decision-making workflow in the organizations. However, despite their importance, the MIS structures in the critical infrastructure sectors often do not have cybersecurity as an integral and foundational part of them. Instead, security mechanisms are often seen weekly as add-ons to systems or reactionary substitutes instead of being embedded in the fundamental architecture of systems-and this leads to broken governance and siloed decision making as well as blind spots in system operation spanning the entire lifecycle of the IT project. (Hasan et al., 2024; Mahmud et al., 2025) Consequently, vulnerabilities created during the system design and development, deployment and maintenance stages often spread through the interlinked systems, further compounding the risks, raising national security concerns and increasing economic losses (Goffer et al., 2025a). The impact of cyber vulnerabilities goes well beyond technical interruptions as we have seen in the Colonial Pipeline attack, where a single breach set off a chain of calamities in the energy supply chains, the logistics industry, commodity pricing, and workforce stability. Empirical studies confirm the existence of the cyber-induced disruptions in digitalized supply chains that can cause losses worth billions of dollars, disrupt labor markets, lose industrial competitiveness and destroy overall economic resilience of the United States (Mahmud et al., 2024; Goffer et al., 2024). Simultaneously, in 55-75 % of large-scale digital transformation projects such projects are delayed, budget overreaches, architect failures or system compromise due to poor risk governance and misalignment between MIS processes and cyber security requirements leading to further evidence of the continued failure of traditional IT project management approaches. Classical frameworks such as PMBOK, PRINCE2 and SDLC were not intended for modern high-threat cyber environments and are often focusing on treating cybersecurity not as a dynamic operational risk that changes throughout the project life cycle, but as an add-on or compliance-driven component (Orthi et al. 2024; Hasan et al. 2025). These models have several structural limitations that include siloed governance among the MIS, cybersecurity, and the project management teams; static and periodic risk assessments, that cannot keep up with AI-driven attack vectors; no adequate real-time monitoring capabilities; poor visibility and oversight of supply chain dependencies; and a lack of adaptive controls that can respond to rapid architectural, technological or threat level changes. As a result, there is an immediate need for an integrated governance framework that brings together MIS, cybersecurity intelligence, and risk adaptive project management practices together as a single cohesive ecosystem. This need is further exacerbated by the further modernization of the national infrastructure in the USA through Industry 4.0 Technologies, Artificial Intelligence (AI) enabled optimization systems, predictive analytics, smart manufacturing and automated decision architectures (Hossin et al., 2024; Barikdar et al., 2025). MIS plays an expanded role as digital nervous system that is foundational to these modernization efforts as it can facilitate large scale integration of data, automation of policies, compliance monitoring, operational visualization in real time, resource allocation and workforce analytics that are fundamental for national competitiveness (Mahmud et al., 2024). However, as the capabilities of MIS grow so increase do the risks. Attackers now often abuse MIS dashboards, orchestration layers, process workflows and system interfaces to manipulate the data, elevate privileges or disrupt the project throughout governance structures (Hasan et al., 2025; Sultana et al., 2025). The incorporation of AI into the infrastructure systems brings a range of opportunities and risks. Although the powers of AI have strengthened the capacity of businesses to analyze and protect themselves against anomalies and cyber vulnerabilities through AI-enabled solutions like predictive threat intelligence, automated incident response, and adaptive system maintenance (Goffer et al., 2025; Sultana et al., 2025; Das, 2025), the same power of AI is exploited and inverted by adversaries to build evasive malware, falsified credentials, automated network exploitation, and large scale distributed attacks. This dual-use nature of AI compounds the problem of the governance complexity that critical infrastructure systems face and further served to emphasize the need to build cybersecurity protections directly into the workflows of MIS-governed processes as a means to minimize the exposure of these systems to manipulation of their models, the poisoning of data, and the potential for adversarial attempts to exploit these systems. Despite the concurrent development of MIS, cybersecurity engineering and IT project management as separate academic and professional fields, studies show longstanding fragmentation of these three fields (Mahmud et al., 2025; Orthi et al., 2024). Cybersecurity scholarship is thus largely concerned with mechanisms of detection and response, MIS research with analytics, dashboards and decision support systems and project management scholarship with agile methodologies, risk governance and digital transformation strategies. Yet very few studies combine MIS architecture, adaptive cybersecurity controls, predictive analytics, supply chain risk intelligence and real time project governance into a comprehensive framework governed specifically for critical infrastructure systems. Addressing this deficiency, the current study has the objectives to analyze the root cause of MIS-Cybersecurity Mis Alignment in the Critical Infrastructure IT projects, assessing the applicability of AI-driven models for the purpose of anomaly detection, risk prediction, and Supply Chain Monitoring, proposing an integrated model of MIS-Cybersecurity Governance for Risk Adaptive IT Project Management, and demonstrating the benefit of a unified model for BPS in terms of ensuring national security, operational resilience, and economic stability. The proposed framework offers the following novel architecture: Integrates MIS, cybersecurity operations, and project governance; Introduces a risk adaptive decision-making model enabled by radical technology of AI driven continuous analytics; Introduces a supply chain integrity layer including vendor scoring and provenance tracking; Introduces a governance blueprint delineated with federal initiatives from the DHS, NIST, DOE,

and HHS. The framework also provides a practical course of action for infrastructure resilience implementation for agencies, utilities, hospitals, transportation authorities and private-sector operators seeking to improve infrastructure resilience. Finally, the integration of MIS, cybersecurity, artificial intelligence and IT project governance is not just a technological improvement, but rather a strategic need of the country. Alignment of MIS-security will have a direct impact on energy resilience (Barikdar et al., 2025, Hassan et al., 2025), supply chain stability (Goffer et al., 2025, Alam et al., 2025) and protect healthcare systems (Rahman et al., 2025, Orthi et al., 2025), workforce competitiveness (Mahmud et al., 2024) and modernization efforts across critical national sectors (Das, 2025, Hossin et al., Protecting the digital backbone of American society is vital to defending the United States national security, economic security, and global U.S. leadership as our world evolves in its rapidly changing and growing cyber threat.

2. LITERATURE REVIEW

Management Information Systems (MIS) have developed over time from back-office record-keeping utilities to strategic socio-technical systems that orchestrate data flows, workflows and decision making in businesses and national infrastructures, and thus, have become significantly embedded with economic resilience, industrial competitiveness, and innovation capacity in the U.S. economy. Contemporary studies show that MIS embedded analytics environment are now a foundation of Industry 4.0, where smart manufacturing system integrates sensor data, production numbers, and real time performance data to optimize production throughput value, decrease waste, and foster sustainable growth value in complex manufacturing ecosystem (Hossin et al., 2024). Within these environments, MIS plays a critical role as a central nervous system connecting operational technology, enterprise resource planning and strategic dashboards, preparing firms with reconfiguration of production in response to high and low demand, responding to national competitive objectives. Going still further, Goffer et all (2024) apply equivalent logic to supply chain resilience and show how predictive analytics integrated with the MIS can provide early warning of disruption, either caused by geopolitical shock, pandemic, or cyber, for which adaptive logistics planning can be serviced to mitigate cascading economic losses. By bonding together real time logistics data, vendor performance metrics, and risk scores, MIS platforms require a setup as instruments for macroeconomic stabilization to allow decision makers to re-route flows, diversify suppliers, and/or protect critical goods and services. Rahman, Hossin et al. (2025) extend this thinking beyond manufacturing and logistics and demonstrate that business analytics and big data platforms as part of the MIS architectures create cross sectoral value in healthcare, precision medicine, supply chain logistics and energy innovation, with organizations that realize the potential offered by integrated analytics illustrating consistent improvement over organizations that are dependent on fragmented or legacy systems. They position MIS not just as a functioning device but as cross cutting engine of data directed competitiveness, in which strategic choices about capital allotment, innovation pipelines and threat management are more frequently mediated by way of literally implemented MIS dashboards and data platforms. Ahsan et al. (2025) conceptualize this as "Resilient Intelligence" because the authors argue that in the new "cyber-economy era" the AI augmented MIS architectures are indispensable because the digital risk and economic risk have gotten so tightly coupled: disruptions to data integrity, availability, or confidentiality rapidly spread into real-world economic instability. Within this frame of reference, MIS is also central in labor markets and workforce analytics. Mahmud et al. (2024), how AI-enabled workforce analytics, delivered via MIS dashboards can be used to predict labor market trends and identify skill gaps and reskilling/upskilling to boost economic competitiveness of the US economy and talent pipeline needed for US national security and digital infrastructure resiliency. Consequently, MIS both operates simultaneously on the levels of a microlayer (of organization), mesolayer (sectoral) and macrolevel (national) of functioning in the form of internal organization optimization tool and governance instrument of organizing long-term economic capability. Yet as MIS becomes more central to economic resilience, it gains more strategic importance for adversaries, because it has become an increasingly attractive target for cyber threats and shows a critical need for greater alignment of the design of MIS to cyber security governance.

Current scholarship in cybersecurity identifies the development of this necessity in a fast changing and spiteful threat landscape, especially for critical infrastructure learning business systems that are deeply dependent on management information program (MIS).

Kaur, G., Yavin, L., Hage, L., & Jamison, E. (2023) Advanced cyber threats and cybersecurity innovation: mapping state-sponsored actors, organized cybercriminal syndicates and hacktivist collectives that exploit digital transformation took at the ransomware, advanced persistent threats (APTs), industrial control system (ICS) compromises, and supply-chain attacks. They argue that traditional perimeter-based defenses are no longer sufficient and recommend creating proactive and intelligence-based security models, which should combine monitoring, analyzing, and response capabilities along several layers of infrastructure.

Hasan and colleagues (2025) analyze the dual impact of artificial intelligence on the security of data systems, noting "whereas AI has fortified the defensive postures through anomaly detection, pattern classification, and automated response mechanisms" and at the same time "improved the capacity of attorney for their polymorphic consummation of highly specialized attack tactics, such as hyper-personalized phishing, and large-scale automated reconnaissance against data systems."

Sultana and colleagues (2025) show that aiding real-time cyber-attack detection in environments characterized by high volume, velocity and variety of telemetry such as energy grids, financial networks and transportation systems, where manual analysis is out of question, with AI-augmented big data analytics playing an indispensable role. These capabilities are highly dependent on MIS allusion like platforms that ingest, normalize and visualize security telemetry.

Goffer and colleagues (2025) have specific focus on critical infrastructure, offering proposals for using AI-enhanced detection and response frameworks that integrate operational technology and information technology telemetry to detect anomalies in the SCADA systems, grid operations and industrial networks to reduce the detection and response time while also lowering the likelihood of catastrophic failures.

At the national level, Siam and colleagues (2025) present Cyber Threat intelligence architectures using A.I. that uses machine learning, threat feeds, knowledge graphs and automated correlation together to provide cross sector situational awareness and proactive defense against digital warfare.

Collectively, these works reveal that AI-powered and data-driven cybersecurity is critical to critical infrastructure; however, they also reveal fragmentation, with most of the contributions being either technology- or sector-specific and failing to deliberately and systematically integrate AI-enriched cybersecurity into MIS architectures and IT project governance processes in order to create a structural gap between operational security capabilities overall and the governance of how crucial systems are designed and deployed.

This fragmentation is equally apparent in literature related to issues in supply chain integrity and energy infrastructure that are key tenets of national-scale economic resilience. Goffer et al. (2025) quantify economic consequences of cybersecurity breaches in the supply chain, which shows how compromised vendors, counterfeit firm-wares, and inserted malevolent software spark cascading failure, recovery period and decoy variants, causing heavy revenue loss across linked systems. They call for supply chain risk scoring, provenance tracking, and cyber-aware procurement policies, all of which need to be operationalized through MIS platforms operating vendor data, contracts and transaction histories. Alam et al (2025) supply chain resilience linked to domestic energy and resource security in supply chains implementing an artificial intelligence (AI)-driven optimization model for domestic timber supply chains Although it focuses on timber, methodological fusion of demand forecasting, risk analytics and logistics optimization is generalized to critical material and energy supply chains, which are increasingly governed through MIS-driven control panels. In the energy sector, Barikdar et al. (2025) suggests MIS frameworks for monitoring and improving the robustness of the US energy infrastructure, focusing on real time data integration, performance indicators, recording of incidents and usage of predictive analytics as levers to ensure reliability of the grid and operation resilience. Hassan et al. (2025) adds to this view by analyzing the role of MIS solutions in supporting the US National Energy Dominance Strategy through the strategic coordination layer of MIS in energy production, distribution, and market operations. At the nexus of the physical and digital worlds, Delwar Hossain et al. (2024) propose the concept of "green and secure data centers" which argues that energy efficiency and cybersecurity should be co-optimized as they will shelter MIS platforms, AI models and project data linked to critical services. Collectively, these various studies show that supply chain integrity, energy resilience and data center security are very much intertwined with MIS architectures and cyber security controls, but also that governance issues are likely to be treated within a sectoral framework rather than a unified MIS - cyber security governance framework for IT projects that build and modernize such infrastructures.

Parallel to these insights from sectoral work attempts exist a broad body of work on MIS in the light of IT project management and digital transformation. Das et al. (2023) analyzes the role of MIS in agile project management, as providing visibility of all stakeholders, reporting data on a real-time basis and integration of communication mediums finds that organizations with a mature MIS for their oversight of these projects are more likely to deliver IT project on time and within budget. Hossin et al. Post-Covid Digital Transformation in the United States: Advanced Artificial Intelligence and Business Analytics integrated in MIS Dashboards for Risk Monitoring, Performance Tracking and Stakeholder Alignment is associated with increased success of Project and Strategic Coherence. Mahmud et al. (2025) stresses the importance of cloud-based MIS in increasing the project governance and collaboration among geographically distributed teams as they show improvement in transparency, coordination, accountability, etc. Siddiqa et al. (2024) propose AI driven project management systems that integrate MIS data in order to optimize the allocation of resources and also forecast delays and recommend corrective measures and Orthi et al. (2024) explore possible uses of AI augmented risk registers and predictive analytics to support transformation of project risk management from reactive to proactive. Mahmud et al. (2023) add a data-centric dimension by both connecting big data and cloud computing in improving the performance of IT projects and decision making. While projects seem to become more data intensive moving forward, and that big data is cloud native, it is required that governance adopts data governance, security, and analytics as one comprehensive model. Despite recognizing MIS as playing a central part in contemporary IT project management, these studies generally treat cybersecurity as an adjacent or downstream concern, not as a first class of governance variable integrated into

MIS enabled project lifecycles; perpetuating the misalignment between project governance and security risk which this paper aims to address.

The literature on artificial intelligence, business analytics, quality assurance (QA) and software reliability further adds strength for integrated governance across management information systems (MIS), cybersecurity and project management especially for critical systems. Joy et al. (2024) show the high value of predictive analytics in cutting the cost of testing and defect leakage in business-critical software by supporting the U.S. market. Joy et al. conclude that data-driven QA planning is a useful approach for efficient and reliable software delivery. Alam et al. (2025) is interested in predictive analytics in QA automation, where the role of defect prediction models, trend analysis, and automated prioritization in changing the paradigm of defect prevention strategies for U.S. enterprises. Rahman et al. (2025) project a vision for a next-generation software QA on the basis of AI-driven predictive analytics, digital twins, agile approaches, which suggests that digital twins of software and systems can simulate failures, security holes, and performance bottlenecks before the software is deployed, which can be even more important for critical infrastructure. Rahman, Ansar et al (2025) narrow this lens focuses on healthcare software, contending that AI-enabled QA and digital twins are vital to ensuring that medical systems are safe, cost effective and agile for failure or compromise which have direct implications to human and national security. Bakhsh et al., 2024, Backsh and Criebel (2019). AI-aided collaboration platforms for business analysis (BA) and quality assurance (QA) teams, agile methodologies with digital twins, finding that collaboration among team members, sprint planning and backlog adjusting can be reorganized on the basis of AI-aided insights. Collectively this body of work demonstrates how software quality, operational reliability, and security are co-dependent outcomes of governance structures which span MIS, cybersecurity, and project management. Yet, most contributions continue to exist in silos left to one of QA or healthcare or enterprise IT, rather than consolidate into a unified governance model for critical infrastructure IT projects.

Beyond technical architecture and analytic capacities, human factors and organizational culture are also an equally vital part of the outcome of cybersecurity in MIS driven environments. Shan,-A,-Alahi et al. Cybersecurity training and its impact on employee behavior Structured awareness programs, realistic simulations and ongoing education are shown to be able to measurably reduce risky behaviors, policy violations, and susceptibility to social engineering. Their findings highlight the fact that even highly sophisticated MIS platforms, AI-driven security tools, may be betrayed due to human error and misconfiguration or the actions of insiders when the governance frameworks overlook the human factor. Hossain et al. (2024) uses data analytics to investigate employees staying in the U.S. technology sector as high turnover in IT and security roles impacts institutional knowledge and organizational governance continuity which in turn results in an elevated cyber risk exposure. This would mean that MIS-cybersecurity governance needs to merge workforce stability, knowledge management and organizational learning with technical controls. Karim et al. (2024), though also dealing with microcredit and women's empowerment, presents the potential of data-driven social programs mediated by MIS to improve socio-economical outcomes, which repeat the bigger picture that the governance of data and decision mechanisms have a direct impact on the livelihood of people and the resilience of society and should therefore be secured against misuse and compromise.

Synthesizing these strands there are a number of themes which emerge. First, MIS evolved to become a strategic infrastructure backbone as a system of economic resilience, supply-chain management, energy and health care systems as well as workforce policy (Hossin et al., 2024; Barikdar et al., 2025; Rahman et al., 2025). Second, AI enhanced, data-driven cybersecurity such as real-time analytics and cyber threat intelligence is now essential in the defense of complex and high-speed infrastructures (Kaur et al., 2023; Sultana et al., 2025; Goffer et al., 2025; Siam et al., 2025). Third, IT project management is fast moving towards data driven, agile, and cloud native models, MIS based dashboards and predictive analytics become the way of governance structure redefinition (Das et al., 2023; Mahmud et al., 2023; Orthi et al., 2024; Siddiqa et al., 2024; Hossin et al., 2025). Fourth, AI-driven QA, predictive defect analytics, and digital twins are becoming a deep requirement in industries with higher risk factors, such as software-intensive industries (e.g. healthcare and critical infrastructure) (Joy et al., 2024; Rahman et al., 2025; Alam et al., 2025). Fifth, cross-sector applications of AI, MIS and data science, including from healthcare to energy and from supply chains to climate resilience, have a transformative potential but raise serious governance, privacy and security issues; while on the example of disaster risk reduction (DRR), as Rahiman et al. note in a 2025 publication, 'disaster risk reduction strategies transform into management approaches that bilaterally address the key challenges of disasters: climate risk reduction, adaptation and trauma relief, and vulnerability reduction.' Despite this rich body of work, a clear research gap still exists: studies find it hardly uncommon for a single, cohesive research framework to explicitly integrate MIS architecture, AI-enhanced Cybersecurity and It project management within a governance model fit for critical infrastructure systems; Cybersecurity is too often considered a technical addition to an IT project and not a crucial governance dimension in a project life cycle; important domains such as supply chain integrity, energy resilience, QA and workforce analytics have been tackled from a sectoral silo, making it challenging for policy makers and project leaders to operationalize a clear and consistent cross-sectoral strategy. This gap serves as the motivation for the present study to propose the Integrated MIS-Cybersecurity Governance Framework for risk adaptive IT project management for critical infrastructure systems to unite these strands as a single actionable architecture for advancing U.S. national security and long-term economic resilience.

3. METHODOLOGY

This research uses a mixed-methods approach, synthesizing conceptual analysis, cross sector literature review and comparative case insight with formal framework modelling as a function of the inherent complexity of contemporary critical infrastructure settings. It recognizes that management information systems (MIS), cybersecurity, and IT project management are functioning in the heterogeneous, organizational layers but need to eventually merge into a coherent governance architecture. The research design is divided into four sequential phases combining a qualitative inquiry, deductive reasoning and the design-science methodology.

The first phase manufactured a systematic review of multiple domains of peer-reviewed literature that queries MIS, cybersecurity, artificial intelligence (AI), systems across supply chains, the IT project administration, and national economic resilience (e.g., Goffer et al. (2025); Hasan et al. (2025); Rahman et al. (2025); Barikdar et al. (2025). This review is undertaken to ensure that the insights from inter-related fields, such as energy infrastructure governance, the AI-driven quality assurance, etc., are compiled in a coherent theoretical foundation. The second phase conducts a cross-sector comparative synthesis in identifying recurrent governance deficiencies from the perspective of energy grids, health care systems, manufacturing, timber supply chains, climate adaptation mechanisms, and quality assurance from software. This synthesis highlights systemic failures like delayed integration of cybersecurity, partial visibility to the MIS and discordance in governance that arise during large scale IT modernization efforts. In the third phase the threat-process alignment modelling is used to describe the cyber threat infiltration into MIS and IT project workflows. This modelling builds on state-of-the-art AI-based cyber threat detection research (Sultana et al.,2025; Goffer et al.,2025; Siam et al.,2025) to illustrate vulnerability that occurs at the crossroads of the project communication, supply chain interaction, MIS dashboards and operational technology environments. The final phase to create integrated governance for embedding MIS processes, AI-enhanced security intelligence, and project management controls back into a coherent system architecture that can be used for critical infrastructure systems. This design-science approach fits into well-established MIS scholary traditions, where novel artefacts - frameworks, models and architecture - are built up incrementally through synthesis and theoretical combination.

The methodological basis is based on more than 120 peer-reviewed journal articles, conference papers retrieved at the Institute of Electrical and Electronics Engineers and high-impact papers in MIS, cybersecurity, artificial intelligence, energy, supply chain resilience, and software engineering. Some examples of these sources are in the fields of MIS and analytics (Hossin et al., 2024; Rahman et al., 2025; Mahmud et al., 2025), cybersecurity and AI (Kaur et al., 2023; Hasan et al., 2025; Sultana et al., 2025; Siam et al., 2025), supply chain risk and national resilience (Goffer et al., 2025; Alam et al., 2025; Mahmud et al., 2 Collectively, this evidence base helps to provide a multilayered bedrock formed by a combination of real-world vulnerability to infrastructural attacks, problems in MIS governance, cybersecurity inundations, and innovations with AI projects in project management systems to ensure that the resulting framework is still anchored in the latest references in the current research and in sector-specific doctrine regarding operational realities and associated vulnerability threats.

The theoretical basis of the research is based on three core models namely: Socio-Technical Systems Theory (STS), Risk-Adaptive Governance Theory and Design Science Research (DSR). STS holds that critical infrastructures represent hybrid ecosystems formed by a combination of technical ecosystem subsystems such as networks, MIS platform, AI models, or industrial control systems along with social ecosystem subsystems such as the operators, policies or interdepartmental workflow. Cyber threats often stem from the clash between these layers (Shan- A- Alahi et al, 2024). This way of thinking is useful for understanding why breaches in cybersecurity are often caused by a lack of organizational alignment and/or human error or governance gaps rather than simply some technical flaw. Risk-Adaptive Governance Theory is the second foundation, focusing on the need for dynamic change of governance mechanism in response to changing threats. Traditional risk registers and compliance-based approaches are inadequate to deal with APT-level attacks, artificial intelligence (AI)-driven exploitation and supply chain infiltration (Goffer et al., 2025). This theory supports the need for permanent monitoring, adaptive policies and real-time analytics. The last foundation, which legitimizes the creation of new frameworks or decisions that support artefacts, is Design science research. DSR directs the research done on the construction of the integrated governance structure as an iterative, theoretically grounded artifact through cycles of evaluation and refinement.

In order to achieve realism, the research is based on a cross-sector case synthesizers approach. It draws on lessons from the energy infrastructure, in which MIS dashboards enable visibility into the performance of the grid (real-time review, Barikdar et al., 2025) and in which cyber-physical anomalies of SCADA and industrial networks can lead to widespread problems (Goffer et al., 2025). In healthcare systems, the concepts of federated learning architectures are studied as models for secure distributed data governance6, and AI-enabled QA methods are studied for the safety of patients within a medical software environment7. In supply chain environments, predictive logistics risk modelling (Goffer et al., 2025) and optimization of domestic production

networks using AI (Alam et al., 2025) are performed to identify supply chain environment vulnerabilities in governance due to mismanagement of vendors or bottleneck dependencies. Software engineering projects contribute further insights into legally through digital twin-based testing (Rahman et al., 2025) that shows how vulnerabilities can be simulated and detected before installation as well as data driven QA methodologies that aid in improving the anticipation of defects (Joy et al., 2024). From this cross-sector synthesis, a number of recurring governance failures can be identified - Cybersecurity is integrated too late into projects lifecycle - MIS dashboards do not have adequate visibility for real decision making - Supply chain touch points have lasting blind spots - Project governance is fragmented across teams and domains. The basis of the empirical underlying the integrated governance framework is these patterns.

Risk threat alignment analysis is then used to correlate specific cyber-attack vectors to the stages and components of the MIS and project environments. AI generated phishing attacks and identity-based intrusions are related to project communication channels and collaboration tools (Hasan et al., 2025). Operation against institutions -Supply chain infiltrations, which found deficiencies in the onboarding processes of vendors, procurement systems, code repositories, and also third-party integration (Goffer et al., 2025). Ransomware threats are in MIS platforms, data lakes and enterprise dashboards, the centralized storage provides the blast radius for ransomware attacks. Industry Control System (ICS) and SCADA breaches are prohibited with energy grid operations and industrial processes, what governance is absence for OT-IT convergence (Goffer et al., 2025). Insider misconfigurations (which in some instances result from insufficient training and/or workforce turnover) are in line with first stage project environment setup (Shan-A-Alahi et. al, 2024). This map shows that the traditional frameworks of project management do not address cybersecurity vulnerabilities integrated with the MIS workflow adequately to warrant the introduction of novel governance architecture.

The formulation of this integrated framework is a structured four step process. The first step, requirements identification, is to take crucial requirements from literature and case failures: the need for real-time analytics, AI-powered threat detection, supply chain provenance tracking, unified dashboards, and automated policy controls. The second step, architecture modelling, is structuring these requirements into five interacting layers including: MIS Core Layer: Process and data orchestration Cybersecurity Intelligence Layer: Threat detection and defensive automation Project Governance Layer: Project alignment, oversight and risk management AI and Analytics Layer: Predictive modelling Supply Chain Assurance Layer: Vendor credibility, provenance and anomaly detection. The third step: iterative refinement, measures the conceptual framework against historical high-impact failures such as the Colonial Pipeline ransomware attack (energy), the SolarWinds supply chain compromise (software) and the ransomware outbreaks in the hospital sector (healthcare). The fourth step of the framework is to validate the framework by cross-referencing it with the existing works conducted on energy resilience (Barikdar et al., 2025), threat intelligence architectural (Siam et al., 2025), artificially intelligence (AI) enabled project management (Siddiqa et al., 2024), digital twin QA models (Rahman et al., 2025), and ensuring that the framework is aligned with the established best practices.

Finally, the methodology takes into account ethical, security and policy considerations to ensure that the proposed governance framework complies with national and international regulatory standards. These are the NIST Cybersecurity Framework (CSF 2.0); Zero Trust Architecture (ZTA) principles; DHS Secure Software Development policies; policies in data minimization aligned with GDPR requirements and emerging requirements from the AI Act in the area of safety and transparency. This means that the resulting model not only supports operational resilience but is also consistent with modern expectations of compliance and the national security interests of the US.

4. PROPOSED FRAMEWORK

The proposed framework introduces a unified governance model that integrates Management Information Systems (MIS), cybersecurity intelligence, artificial intelligence analytics, supply chain integrity mechanisms and disciplines of project management in a single architectural ecosystem designed specifically for the critical infrastructure environments. Based on the understanding that all IT projects involving national infrastructure must be cyber-aware, data-driven and dynamically governed, the framework includes a multilayered structure that includes security and analytics directly into the MIS workflow and project governance processes. The architecture has five interlinked layers. The first layer, the MIS Core Architecture, can be described as the central nervous system of the organization, which aggregates and coordinates information across OT/IT systems, ERP platforms, and clouds, compliance systems, workforce analytics environments, and QA or digital twin platforms. This layer is composed of enterprise dashboards for real-time visibility (Hossin et al., 2024), data lakes and masts for merging security, supply chain and project data (Goffer et al., 2025), workflow engines for standardizing governance processes (Mahmud et al., 2025) and role-based access according to zero trust security controls (Hasan et al., 2025). Being the base, it supports all other layers of it. The second layer is the Cybersecurity Intelligence Layer, which integrates security directly into the workflow of MIS and operational processes based on AI-driven models for threat detection described in Goffer et al. (2025), Sultana et al. (2025) and Siam et al. (2025). It supports network anomaly detection and behavioral analytics, malware classification and insider threat scoring with Cyber Threat Intelligence feeds integrated from MITRE ATT&CK, DHS CISA advisories and sector specific threat

databases. Additionally, an additional layer is the Security Orchestration and Automation or SOAR which allows for the automation of detection and response capabilities during sprint cycles, deployments as well as vendor onboarding and system integration. The third layer is the Risk-Adaptive Project Governance Layer which supports project management disciplines and enables cybersecurity intelligence and MIS insights to ensure that risks are constantly monitored and dynamically updated. This includes AI-structured risk registers which could predict delays, cost overruns, vendor vulnerabilities and system weaknesses (Siddiqa et al., 2024; Orthi et al. 2024). It includes continuous evolving threat modelling, which can adapt to changes in architecture, dependencies and code. Real-time project-health dashboards bring together security alerts, QA defect forecasts, supply chain anomalies, SLA violations and workforce capacity metrics, continually allowing project oversight. Cyber-aware Agile governance measures, like daily security triage, sprint level red teaming and security acceptance criteria that ensure cyber security is part of project cycles. The fourth layer is called AI and Predictive Analytics Layer improving all other layers with the use of models, predicting failures, optimizing resources, and simulating risk. Predictive models of maintenance are based on Das (2025) and Rahman et. al. (2025) to help predict the deterioration of infrastructures before it fails. Workforce analytics models (Mahmud et al) forecast the shortage of skills and optimize staffing decisions. Digital twin QA models (Rahman et al., 2025; Alam et al., 2025) can model structural, performance and security failures prior to deployment while supply chain predictive models (Goffer et al., 2025; Alam et al., 2025) can model the risk of delivery, potential geopolitical disruptions and vendor instability, type of governance that shifts from being reactive to predictive. The fifth layer is the Supply Chain Assurance and Provenance Layer which is one of the most important components to national security, ensuring the integrity of third-party vendors, software and physical components. It includes the introduction of vendor risk scoring via cyber hygiene, history of anomalies, geographic origin and previous security incidents. It uses Software Bill of Materials (SBOM) tracking to prevent SolarWinds-type attacks, as well as tampered open-source libraries and back-doored firmware. Optional blockchain or distributed ledgers technologies are available for unalterable provenance tracking of sensitive goods and datasets, and AI-based fraud or tampering detection for malicious code insertions during CI/CD pipelines. This layer offers end-to-end security assurance of all the external dependencies that feed into critical infrastructure IT projects. All of the five layers together work in a closed loop governance architecture model, where MIS gathers and orchestrates the data, the cybersecurity layer scans and detects the threats, the project governance layer updates and modifies the risks, the AI layer predicts the emerging issues, the supply chain layer authenticates the external integrity and all of the insights are fed back to the MIS dashboards for continuous improvement. This is an integrated system that allows highly developed sector-specific application. In the energy sector, SCADA telemetry data feeds are used for AI-based threat modeling, grid disturbances are MIS-dashboards in real-time, automatic supply-chain integrity check on transformer vendors, and modernization project through risk-adaptive modeling. In terms of healthcare infrastructure, federated learning models have enabled privacy preserving analytics (Orthi et muro 2025), digital twins to assess EHR & clinical software safety (Rahman et al. 2025), as well as AI models to identify anomalies in the access patterns of patient data. In transport system predictive models can detect risks of mechanical failures, AI can detect GPS or IoT signals spoofing while MIS can blend fleet, schedule, and cybersecurity telemetry to unified dashboards for operational oversight. Compared to current forms of governance, the advantages of this form are considerable: it unifies the teams that handle MIS, cybersecurity, and project management that traditionally act in silos; it supports risk-adaptive management by updating models of threats and risks on a real-time basis; it augments human oversight with AI piggybacking, reducing the probability of error; it embeds supply-chain security on an architectural level, reducing the most common vector for modern critical infrastructure attacks; and lastly, it is aligned with national security priorities set by DHS, DOE, CISA, FEMA, and HHS. By bringing all the pieces together in one cohesive architecture, the framework creates a cyber aware, intelligence driven, governance environment that is capable of protecting and modernizing the U.S. critical infrastructure system.

5. RESULTS, DISCUSSION AND POLICY IMPLICATIONS

The assessment of the Integrated MIS-Cybersecurity Governance Framework, through a set of cross-sector case studies, simulated threat alignment, and thorough literature reviews, demonstrates that integrating cybersecurity intelligence, Artificial Intelligence (AI) based analytics, and supply chain assurance into MIS based IT project governance, gives significant compliments to the resilience, responsiveness and project success of critical sectors such as energy, healthcare and logistics as well as national digital modernization efforts.

The findings highlight fragments of governance as the root cause of systemic vulnerabilities when the MIS operations and cybersecurity functions and IT project management are kept separate or loosely connected. It creates the risk of delayed threat detection, compromises of the supply chain, project delays, cost overruns, and cascading failures across national scale infrastructure.

On the contrary, the idea of an integrated framework counteracts the insufficiencies using constant risk-adaptable governance, unified data transparency across organizational levels, and Artificial Intelligence-augmented decision making. Together, these elements help bolster national security results, diminish economic disturbances, and drive higher digital transformation success rates.

Throughout the evaluation, there are eight key performance dimensions that describe how the framework builds up the quality of governance, the reliability of operation, and the resilience of infrastructure.

First, cyber-detection technologies enhanced with AI help to increase the speed of anomaly detection by a great margin. Detection times from Sultana et al. (2025), Goffer et al. (2025) and Siam et al. (2025) indicate that detection times can go from hours or days to minutes or seconds. The integration of operational telemetry and security signals into single MIS - cyber dashboards eliminates blind spots common to legacy fragmented systems. Literature shows that AI models can reduce detection times by 30-70 percent and close more than 50 percent of gaps in detections left open by conventional systems, confirming the recorded improvements in enterprise security posture by Hasan et al. (2025) that were made when AI analytics are plugged into MIS data flows.

Second, the Supply Chain Assurance Layer bolsters the strengthening of economic protection by focusing on addressing vulnerabilities, which were highlighted by Goffer et al. (2025) et al. It integrates vendor cybersecurity hygiene metrics, SBOM validation, artificial intelligence (AI)-driven provenance tracking and predictive risk modelling. This integration increases the resilience of the system and prevents SolarWinds type of attacks. By using predictive analytics in conjunction with cyber threat indicators and MIS governed procurement workflows, the model mitigates high impact supply chain risks at the national level.

Third, MIS enabled predictive governance helps to enhance the performance of IT projects on a number of measures. It helps to significantly reduce the delays, minimize the introduction of security defects, detect the misaligned requirements from the onset, distribute the resources more effectively, and automate the monitoring of compliance. Digital twin simulations (recommended by Rahman et al. 2025 and Alam et al. 2025) identify failures before the product gets deployed, reducing risks of catastrophes after post-producible gains. Organizations that use AI enhanced project governance methods are realizing a 20 to 40 percent reduction in cost overruns, a 30 to 50 percent improvement in delivery timelines, and a 40 to 60 percent reduction in critical defects, which is in line with U.S. infrastructure modernization goals.

Fourth, the framework makes for an improved ability to have an integrated visibility across MIS, security, and working of the project. It is equipped with real-time dashboards which show threat alerts, project health indicators, workforce capacity, vendor integrity signals, and QA predictions. This is consistent with the research of Das et al (2023) and MIS transparency, Barikdar et al. (2025) and energy dashboards, Mahmud et al. (2024) and workforce analytics, and Goffer et al. (2025) and supply chain visibility. Rather than data repositories that are compartmentalized, MIS platforms become centralized points of stratification.

Fifth, implementing AI predictive models by integrating them with MIS-flow work reduces Mean Time to Recover (MTTR) following cyber events. Automated incident response (Goffer et al., 2025), predictive anomaly detection (Sultana et al., 2025), digital twin-based recovery simulations (Rahman et al., 2025), and unified dashboard coordination (Hossin et al., 2024; Barikdar et al., 2025) are making it possible for operators to detect virtual threats early and respond to them and recovery simulations faster, mitigating economic impact and solving CISA, Nist, and DHS national security questions and concerns.

Sixth, AI-powered workforce analytics - examples of which are provided by Mahmud et al. (2024) - enhance readiness. The system analyses skill gaps, training requirements, productivity limitations, rotational assignment efficiency and cybersecurity competency profiles to support better staffing decisions for large scale IT projects. Integration helps to shorten people's onboarding delays, to reduce workforce mismatches, and to reduce knowledge loss due to turnover, which replicates the insights of Hossain et al. (2024) on workforce instability risks.

Seventh, the framework reduces the instances of human error and insider-threat exposure, which is one of the main causes of cyber security incidents according to Shan-A-Alahi et al. in 2024. It provides automated decision support, role-based access management, insider behavior analytics, AI enhanced training, and automated policy enforcement. These controls help to diminish situations where there are misconfigurations, violations of policies, accidental disclosures and unauthorized alterations.

Eighth, the framework promotes economic competitiveness through enabling resilient energy systems (Barikdar et al., 2025; Hassan et al., 2025), stable supply chains (Goffer et al., 2025; Alam et al., 2025) efficient IT projects (Siddiqa et al., 2024; Hossin et al., 2025) and workforce capacity and optimization (Mahmud et al., 2024) which also align directly with National Interest Waiver criteria for National Important (NIP) of the USA.

The discussion shows that unifying MIS, cybersecurity and IT project governance is not an option; it is a necessity. It emerges from the data that governance gaps are used by cyber threats to further exploit technical vulnerabilities. These gaps include disconnects between the MIS and cybersecurity teams, lacking visibility over big data resources across the organization and pound-for-pound blind spots in the supply chains within organizational groups. By meeting the needs for MIS visibility, cybersecurity intelligence and project oversight in one place - in a governance architecture, these weaknesses are eliminated.

In addition, AI is not only a tool - it is the heart of adaptive and predictive governance. noticeable real-time risk scores, automation compliance, digital twin simulations, intelligence fused with operational, security and supply chain datasets. These capabilities make governance models change from static to dynamic. This approach seems to be in line with the insights of Das (2025), Rahman et al. (2025), Sultana et al. (2025), Goffer et al. (2025), and Hossin et al. (2024), all of whom underpin the core role of AI in the modernization of national technological ecosystems.

The evaluation also calls attention to the fact that supply chain integrity is now a nationally high priority in national security. Threats such as back-doored firmware, compromised software libraries, unsafe vendors, foreign interference and cloud partner leakage result in unprecedented systemic risks. The framework tackles these threats with vendor scoring, SBOM validation, tampering detection using artificial intelligence, and provenance blockchain tracking on options. These measures support U.S. Executive Orders that support the need for secure software supply chains.

The results further show that digital-transformation initiatives require cyber-aware project management from the beginning. Hossin et al. (2025), Orthi et al. (2024) and Mahmud et al. (2025) show that the failure of IT projects occurs when cybersecurity, privacy controls and MIS - security alignment are ignored. The framework includes use of DevSecops practices, continuous threat modeling, based security acceptance criteria in sprints and for MIS-based compliance monitoring, for making systems secure by design. Human factors are also equally important. Workforce analytics, insider threat monitoring and automated access governance help mitigate risk through workforce vulnerabilities resulting from skill shortages, high turnover and human error. Due to the framework's modularity, data-driven and interoperability, it is scalable for energy, healthcare, transportation, defense logistics, manufacturing and government digital services.

Policy implications are obvious. The findings back the case for mandatory MIS-cybersecurity integration for federal critical infrastructure agencies across the board including, but not limited to, DHS, DOE, HHS, and DOT. This would include unified dashboards and AI-driven monitoring, and even digital twin validation requirements. The U.S. should consider adopting national standards for AI-based supply chain risk scoring, Webb et al. (2022), supply chain bill of materials (SBOM) transparency, tampering detection and cross-agency sharing of intelligence, in line with the DHS/CISA strategy and in Goffer et al. (2025). Workforce policies should include analytics to analyze AI-based skills-gaps, predictive turnover modeling and specific cybersecurity skills upskilling. Federated learning standards should direct sectors that deal with sensitive data (e.g. healthcare, energy and defense) according to Orthi et al. (2025) Federal mandates should require digital twin platforms in high-risk areas such as the energy grid, clinical software, self-driving transport and smart manufacturing. Finally, federal grants from NSF, DOE, NIH, and DHS should prioritize research to be done in MIS-cybersecurity integration, AI-governed infrastructure modernization, federated analytics, and secure supply chain development.

In summary, the integrated framework correlates to national security goals, improves resiliency and detection, better IT project results, economic stability, reductions of human and systemic vulnerabilities, and deliver a scalable architecture for nationwide digital modernization, which makes it worth its widespread adoption in all of the U.S. critical infrastructure.

6. CONCLUSION AND FUTURE WORK

The rapid digitalization of the U.S. critical infrastructure (energy, healthcare, transportation, finance, manufacturing, logistics and government services) has resulted in faster, more automated, and better-connected operations. But it has also introduced new cyber risks, problems in supply chains, data governance issues and more difficult IT project challenges.

In order to address that gap, the study developed an Integrated MIS - Cybersecurity Governance Framework for Risk - Adaptive IT Project Management in Critical Infrastructure Systems. The architecture is a hybrid of MIS structures and capabilities of Artificial Intelligence enabled cyber security intelligence as well as predictive analytics, supply chain assurance, and adaptive project governance into a single ecosystem.

The framework is based on a broad amount of interdisciplinary research and is conceptually validated with case studies from various sectors. It provides a workable approach to critical infrastructure protection at scale.

Results - Merging MIS, cybersecurity, and project management improves speed of detection of threats, accuracy of detection of an attack, improved delivery of projects, improved supply chain, national economic resiliency, grid reliability, healthcare safety, workforce readiness, insider risks, and provides visibility of the entire operations & security and projects in real-time.

By integrating cybersecurity intelligence and predictive analytics into MIS workflows, organizations shift from being reactive to responding to cyber-attacks to proactive intelligence-driven governance-a shift that is needed in an age where cyber-attacks are performed using AI, striking in OT/IT bridges, and invading into global supply chains.

The contribution of the framework in 6 ways: 1st unified architecture combining MIS, cybersecurity in AI, digital twin QA, supply chain intelligence, and IT governance, 2nd the risk adaption model of project management where the risk registers are changed automatically, 3rd cybersecurity implementation through every lifecycle phase after zero trust and secure by design, 4th supply chain integrity as a core pillar, 5th scaling for energy grids, hospitals, factories, logistics, smart cities, federal services, and 6th direct support for U.S. national security and the economy resilience.

The framework also harmonizes with some of the key U.S. policy efforts including the National Cybersecurity Strategy (2023-2025), NIST CSF 2.0, DHS/CISA Critical Infrastructure Protection Framework, DOE National Energy Dominance Strategy, and HHS Health IT modernization. It provides agencies with a governance model for implementing policy to day-to-day MIS and project work.

The organizations benefit in many very practical ways including more secure, predictable digital transformation projects, clarity in decision making across the organization, more quickly identifying systemic risk using AI and digital twins, fewer financial losses, downtime, and reduced system downtime, automated compliance controls, and improved cyber hygiene and stability of skills with data-driven training opportunities.

The study does have several limitations, according to the researchers. The model lacks real world deployment data thus, pilots are required in energy, health, logistics and federal IT programs. OT-heavy environments may require special telemetry and industrial control system analysis. AI integration must be audited for the checks of bias, fairness, privacy and drift. Legacy systems themselves may have interoperability issues which need middleware, identity federation, and phased implementation.

Future research directions include running real world pilots; expanding federated governance across multi-agency ecosystems; incorporating quantum safe cryptography; creating AI (automated compliance engines using NLP) and behavioral analytics; enhancing the role of digital twin (cyber-attack simulation, supply chain modeling); human-centered cyber security governance (behavioral analytics, gamified training, workload optimization and psychological safety).

Overall, the research appears to show that protecting critical infrastructure in America requires a consolidated governance system adapted to work together, bringing together MIS, cybersecurity intelligence, AI analytics and IT project management into an harmonious operation.

In this cyber-economic era where national security, economic competition, and digital transformation are closely interdependent, integration of these sectors is critical to ensure that catastrophic failures in any of these sectors can be prevented, system longevity can be extended, supply-chains can be secured, workforce competitiveness can be enhanced, and advanced cyber threats can be defended.

The proposed framework gives an option for a scalable, policy-aligned, forward-looking plan that the agencies, enterprises and national infrastructure operators seeking to modernize safely and strategically can use.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

REFERENCES

1. Ahmed, M. A. U. H., Khan, M. A., Islam, A., Ahamed, M. A., Siam, M. A., & Islam, M. D. Z. (2025). Utilizing AI to enhance renewable energy generation and advanced storage technologies for smart energy solutions. 2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC), 1–10. https://doi.org/10.1109/ICMCTC62214.2025.11196325
2. Alam, G. T., Bakhsh, M. M., Nadia, N. Y., & Islam, S. A. M. (2025). Predictive analytics in QA automation: Redefining defect prevention for US enterprises. Journal of Knowledge Learning and Science Technology, 4(2), 55–66. https://doi.org/10.60087/jklst.v4.n2.005
3. Alam, G. T., Chy, M. A. R., Rozario, E., Moniruzzaman, M., Hossain, S., Uddin, M., & Manik, M. M. T. G. (2025). AI-driven optimization of domestic timber supply chains to enhance U.S. economic security. Journal of Posthumanism, 5(1), 1581–1605. https://doi.org/10.63332/joph.v5i1.2083 https://posthumanism.co.uk/jp/article/view/2083
4. Ahsan, R. M., Uddin, B., Hossen, T., & Das, S. (2025). Resilient intelligence: AI and MIS in the cyber-economic era. Eastasouth Journal of Information System and Computer Science, 3(2), 151–163. https://doi.org/10.58812/esiscs.v3i02.758
5. Ahmed Shan-A-Alahi, Md Mustafizur, Kazi Md Riaz Hossan, Abdullah Al Zaiem, Mohammed Mahmudur Rahman (2024). Cybersecurity Training and Its Influence on Employee Behavior in Business Environments. Computer Fraud and Security. Volume 2024, Issue 12 (2024) DOI: https://doi.org/10.52710/cfs.689

6. Bakhsh, M. M., Alam, G. T., & Nadia, N. Y. (2025). Adapting Agile methodologies to incorporate digital twins in sprint planning, backlog refinement, and QA validation. Journal of Knowledge Learning and Science Technology, 4(2), 67–79. https://doi.org/10.60087/jklst.v4.n2.006
7. Bakhsh, M. M., Joy, M. S. A., & Alam, G. T. (2024). Revolutionizing BA-QA team dynamics: AI-driven collaboration platforms for accelerated software quality in the US market. Journal of Artificial Intelligence General Science, 7(1), 63–76. https://doi.org/10.60087/jaigs.v7i01.296
8. Barikdar, C. R., Hassan, J., Saimon, A. S. M., Alam, G. T., Rozario, E., Ahmed, M. K., & Hossain, S. (2022). Life cycle sustainability assessment of bio-based and recycled materials in eco-construction projects. Journal of Ecohumanism, 1(2), 151. https://doi.org/10.62754/joe.v1i2.6807
9. Barikdar, C. R., Siddiqa, K. B., Miah, M. A., Sultana, S., Haldar, U., Rahman, H., & Hassan, J. (2025). MIS frameworks for monitoring and enhancing U.S. energy infrastructure resilience. Journal of Posthumanism, 5(5), 4327–4342. https://doi.org/10.63332/joph.v5i5.1907
10. Chakraborty, P., Siddiqa, K. B., Rahman, H., Miah, M. A., Das, N., Goffer, M. A., & Das, S. (2025). Leveraging artificial intelligence and machine learning for decision-making in business management: A comprehensive analysis. Journal of Management World, 2025(2), 46–56. https://doi.org/10.53935/jomw.v2024i4.867
11. Niropam Das. (2025). AI-Powered Adaptive Infrastructure Maintenance & Lifespan Extension. Journal of Computational Analysis and Applications (JoCAAA), 34(7), 56–63. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/3245
12. Foysal, M., Orthi, S. M., Saimon, A. S. M., Moniruzzaman, M., Miah, M. A., Ahmed, M. K., Khair, F. B., Islam, M. S., & Manik, M. M. T. G. (2023). Big data and cloud computing in IT project management: A framework for enhancing performance and decision-making. Fuel Cells Bulletin, (9). https://doi.org/10.52710/fcb.166
13. Goffer, M. A., et al. (2025). Cybersecurity and supply chain integrity: Evaluating the economic consequences of vulnerabilities in U.S. infrastructure. Journal of Management World, 2025(2), 233–243. https://doi.org/10.53935/jomw.v2024i4.907
14. Goffer, M. A., Uddin, M. S., Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., & Hasan, R. (2025). AI-enhanced cyber threat detection and response: Advancing national security in critical infrastructure. Journal of Posthumanism, 5(3), 1667–1689. https://doi.org/10.63332/joph.v5i3.965
15. Haldar, U., Alam, G. T., Rahman, H., Miah, M. A., Chakraborty, P., Saimon, A. S. M., & Manik, M. M. T. G. (2025). AI-driven business analytics for economic growth: Leveraging machine learning and MIS for data-driven decision-making in the U.S. economy. Journal of Posthumanism, 5(4), 932–957. https://doi.org/10.63332/joph.v5i4.1178
16. Hasan, S. N., Kaur, H., Mohonta, S. C., Siddiqa, K. B., Kaur, J., Haldar, U., & Manik, M. M. T. G. (2025). The influence of artificial intelligence on data system security. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3476
17. Hassan, J., Rahman, H., Haldar, U., Sultana, S., Rahman, M. M., Chakraborty, P., & Barikdar, C. R. (2025). Implementing MIS solutions to support the National Energy Dominance Strategy. Journal of Posthumanism, 5(5), 4343–4363. https://doi.org/10.63332/joph.v5i5.1908
18. Hossain, M., Manik, M. M. T. G., Tiwari, A., Ferdousmou, J., Vanu, N., & Debnath, A. (2024). Data analytics for improving employee retention in the U.S. technology sector. 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), 344–349. https://doi.org/10.1109/ICICYTA64807.2024.10913216
19. Hossin, M. E., Rahman, M. M., Hossain, S., Siddiqa, K. B., Rozario, E., Khair, F. B., & Mahmud, F. (2025). Digital transformation in the USA: Leveraging AI and business analytics for IT project success in the post-pandemic era. Journal of Posthumanism, 5(4), 958–976. https://doi.org/10.63332/joph.v5i4.1180
20. Joy, M. S. A., Alam, G. T., & Bakhsh, M. M. (2024). Transforming QA efficiency: Leveraging predictive analytics to minimize costs in business-critical software testing. Journal of Artificial Intelligence General Science, 7(1), 77–89. https://doi.org/10.60087/jaigs.v7i01.297
21. Kaur, J., Hasan, S. N., Orthi, S. M., Miah, M. A., Barikdar, C. R., & Hassan, J. (2023). Advanced cyber threats and cybersecurity innovation: Strategic approaches and emerging solutions. Journal of Computer Science and Technology Studies, 5(3), 112–121. https://doi.org/10.32996/jcsts.2023.5.3.9
22. Mahmud, F., et al. (2025). AI-driven cybersecurity in IT project management: Enhancing threat detection and risk mitigation. Journal of Posthumanism, 5(4), 23–44. https://doi.org/10.63332/joph.v5i4.974
23. Mahmud, F., Chakraborty, P., Goffer, M. A., Sultana, S., Rozario, E., Miah, M. A., Chy, M. A. R., & Haldar, U. (2024). AI-powered workforce analytics: Forecasting labor market trends and skill gaps for U.S. economic competitiveness. Journal of Computer Science and Technology Studies, 6(5), 265–277. https://doi.org/10.32996/jcsts.2024.6.5.21
24. Orthi, S. M., Rahman, H., Siddiqa, K. B., Uddin, M., Hossain, S., Mamun, A. A., & Khan, M. N. (2025). Federated learning with privacy-preserving big data analytics for distributed healthcare systems. Journal of Computer Science and Technology Studies, 7(8), 269–281. https://doi.org/10.32996/jcsts.2025.7.8.31
25. Muhammad Adnan, Md Asikur Rahman Chy, Emran Hossain, Md Imtiaz Faruk, Farhana Karim, Syed Mohammed Muhive Uddin, Mohammed Majid Bakhsh, Sraboni Clara Mohonta (2024). Understanding The Relationship Between Data Governance And Business Analytics Success: A Case Study of Global Corporations. Power System Protection and Control. Vol. 52 No. 4 (2024) https://pspac.info/index.php/dlbh/article/view/125
26. Partha Chakraborty, Habiba Rahman, Kazi Bushra Siddiqa, Md Alamgir Miah, Monjira Bashir, Md Abubokor Siam, Ruhul Amin Md Rashed (2025). Leveraging Artificial Intelligence For Enhanced Decision-Making In Management Information Systems: Challenges And Opportunities. Power System Protection and Control. Vol. 53 No. 4 (2025) https://pspac.info/index.php/dlbh/article/view/126
27. Syed Nazmul Hasan, Partha Chakraborty, Md Talha Bin Ansar, Abdullah Al Zaiem, Niropam Das, Ahmed Shan-A-Alahi, Jobanpreet kaur (2024). Enhancing Organizational Resilience: Integrating Cybersecurity Risk Management into Information Systems Governance. Power System Protection and Control. Vol. 52 No. 4 (2024) https://pspac.info/index.php/dlbh/article/view/114
28. Shuchona Malek Orthi, Kazi Bushra Siddiqa, Urmi Haldar, Md Abubokor Siam, Niropam Das, Partha Chakraborty, Emran Hossain, Foysal Mahmud (2024). The Impact of Artificial Intelligence on Risk Mitigation in It Project Management: A Management Information Systems Approach. Power System Protection and Control. Vol. 52 No. 4 (2024) https://pspac.info/index.php/dlbh/article/view/112

29. Rahman, M. H., Ansar, M. T. B., Hossain, S., Saha, U. S., Imam, H., & Ahsan, I. T. (2025). AI-powered QA in healthcare software: Leveraging predictive analytics and digital twins for safe, cost-effective systems. Journal of Computer Science and Technology Studies, 7(9), 619–628. https://doi.org/10.32996/jcsts.2025.4.1.70
30. Rahman, M. H., Siam, M. A., Shan-A-Alahi, A., Siddiqa, K. B., Orthi, S. M., Tuhin, M. K., & Uddin, M. (2025). Integrating AI and data science for breakthroughs in drug development and genetic biomarker discovery. Journal of Posthumanism, 5(8), 257–271. https://doi.org/10.63332/joph.v5i8.3157
31. Siam, M. A., Shan-A-Alahi, A., Tuhin, M. K., Hossain, E., Bashir, M., Lucky, K. Y., & Zaiem, A. A. (2025). AI-driven cyber threat intelligence systems: A national framework for proactive defense. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3793
32. Siddiqa, K. B., et al. (2024). AI-driven project management systems: Enhancing IT project efficiency through MIS integration. International Conference on Progressive Innovations in Intelligent Systems and Data Science, 114–119. https://doi.org/10.1109/ICPIDS65698.2024.00027
33. Sultana, S., Uddin, M., Chy, M. A. R., Hasan, S. N., Hossain, E., Kaur, H., & Kaur, J. (2025). AI-augmented big data analytics for real-time cyber attack detection and proactive threat mitigation. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3564