International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 10, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i10.892

An AI-Based Framework for Predictive Vulnerability Assessment and Risk Prioritization in Critical Infrastructure Systems

Marcel Okoebor[1]

Publication Date: 2025/10/30

Abstract

Modern societies are based on Critical Infrastructure Systems (CIS) which are becoming more susceptible to attacks by cyber-criminals, brute force, natural calamities and system interdependencies. Classical risk management models like the RMF and PRAM have some formal guidelines but are faced with the fact that it is impossible to manage dynamic and volatile threats since they are by definition siloed and emergent. Recent developments in Artificial Intelligence (AI) provide a new opportunity to assess potential vulnerabilities and prioritize risks in a predictive manner, but the current applications are usually sector-specific, have low scalability, and lack interpretability and real-time adaptability. The current paper is a conceptual review that combines the theory of risk management, the literature on the assessment of vulnerability, and the application of AI in various fields. It also introduces some important gaps in the existing literature, such as the lack of coherent frameworks, as well as, the lack of discussion of domain-wide interdependencies. The study, in turn, proposes a new AI-based framework that includes data integration based on multiple sources, hybrid AI modelling, dynamic risk scoring, decision-support tools, and feedback loops. The framework helps to develop the theory of AI-based risk management and provides realistic directions to enhance predictive accuracy, prioritisation, and resilience in CIS. It also preconditions future empirical confirmation and application of policy.

Keywords: *Critical Infrastructure Systems; Risk Management; Vulnerability Assessment; Artificial Intelligence; Machine Learning; Predictive Analytics; Risk Prioritisation; Resilience*.

I. INTRODUCTION

Critical Infrastructure Systems (CIS) are the mainstay of present societies, including the energy sector, transport sector, water sector, telecommunication sector, and healthcare section (Bennett & Stephens, 2023). They are free flowing and their smooth running is the foundation of national security, economic stability, and public safety (Lewis, 2019). Yet, these systems are becoming more susceptible to various threats such as cyber-attacks, natural disasters, system failures, and disruption by human hands (World Economic Forum, 2024). CIS complexity and interdependence increases the impact of any disruption, and it tends to become a cascading failure in more than one sector (Rinaldi, Peerenboom, & Kelly, 2022). Considering this vulnerability, predictive vulnerability assessment and sound risk prioritisation have become essentials in addressing infrastructure resilience (Linkov et al., 2021). Despite the usefulness of traditional means of risk assessment, they tend to underrepresent the dynamic and changing nature of contemporary threats (Alderson, Brown, & Carlyle, 2022). Their ability to provide proactive and responsive solutions is frequently limited by rigid modelling, slow response mechanisms and poor integration of real time information (Kott & Linkov, 2019). In this respect, Artificial Intelligence (AI) is a promising paradigm shift (Javaid, Haleem, & Singh, 2023). Being able to handle large and diverse datasets, identify latent patterns, and predict areas of potential vulnerability, AI can contribute significantly to predictive assessment and prioritisation of risks (Yeboah-Ofori, Islam, & Lee, 2021). Combining machine learning, deep learning, and decision-support mechanisms, AI has the potential to make CIS risk management a proactive, adaptive system, rather than a reactive process.

This conceptual review aims to conduct a synthesis of the body of current theories, models, and methods that support vulnerability assessment and risk prioritisation and outline gaps that lead to the creation of an efficient AI-based framework. Likewise, by so doing, it offers a theoretical basis on which a new, proactive and smart framework of securing critical infrastructures can be built.

Okoebor, M. (2025). An AI-Based Framework for Predictive Vulnerability Assessment and Risk Prioritization in Critical Infrastructure Systems. *International Journal of Scientific Research and Modern Technology*, *4*(10), 81–85. https://doi.org/10.38124/ijsrmt.v4i10.892

II. THEORETICAL FOUNDATIONS

Structured theoretical models have long been used in risk management and vulnerability assessment to identify, analyse and mitigate threats within complex systems (Haimes, 2016). The most widespread among them is the Risk Management Framework (RMF), which offers systematic ways to categorise and assess the dangers and present the mechanisms of protection (Joint Task Force, 2018). Within the framework of critical infrastructure system (CIS), the RMF allows for structured decisions, as such risk management is carried out in a proactive manner, due to continuous monitoring, rather than in the reactive manner (Schoitsch, 2020). Still, regarding the same matter, the Project Risk Analysis and Management (PRAM) model can also be considered as a lifecycle approach in which the identification of risks is followed by risk mitigation strategies and analysis (Hopkin, 2018). The two frameworks are similar in that they both require systematic assessment, prioritisation, and responsiveness, which is essential with highly interdependent infrastructures (Aven, 2019). Another relevant conceptual framework that transcends risk avoidance to enable systems to absorb shocks, adapt and recover rapidly is the resilience theory (Hollnagel, Woods, & Leveson, 2006). This point of view is critical for CIS, in particular, where total risks cannot be removed (Linkov & Trump, 2019). Resilience theory promotes a balance between vulnerability decrease and adaptive capacity, so that decision-makers not only invest in robustness and recovery pathways, but also in preventive ones (Hosseini, Barker, & Ramirez-Marquez, 2016).

These models have structured foundations but in many cases, are limited by static methodologies and limited ability to predict (Zio, 2018). It is here that the transformational potential of Artificial Intelligence and Machine Learning (AI/ML) techniques can be found (Yuan, Li, & Wang, 2023). AI has the potential to upgrade old structures and add dynamic learning features, as it will enable systems to provide new risk evaluations according to the current state. Machine learning algorithms are able to identify changing patterns of threats, and deep learning models can identify covert vulnerabilities in complex interdependencies (Yeboah-Ofori et al., 2021). With the implementation of AI into the frameworks of RMF, PRAM, and resilience, CIS decision-making will become more forward-looking and proactive instead of retrospective (Kott & Linkov, 2019). In practice, AI develops the theoretical ideas of risk management and forms hybrid strategies, systematic framework, and adaptive intelligence (Javaid et al., 2023).

III. CRITICAL INFRASTRUCTURE VULNERABILITIES

Critical Infrastructure Systems (CIS) are vulnerable to a variety of threats posed by natural and manmade risks (World Economic Forum, 2024). Cybersecurity threats have become a dominant issue, and the growing digitisation exposes infrastructures to malware, ransomware and advanced persistent threats. Physical attacks, e.g. sabotage or terrorism, are still acute, especially in the transport and energy industry where interruption can put the whole economy on its knees (Lewis, 2019). Further, natural disasters, like floods, earthquakes, and storms, remain a risk to physical assets and they are more likely to multiply risks, by affecting power, communications, and emergency responses simultaneously (Linkov, Trump, Golan, & Keisler, 2021). The second area of increasing vulnerability is system interdependencies; a breakdown in one system component can cause a series of system failures in different industries, including healthcare, water supply, and finance (Rinaldi, Peerenboom, & Kelly, 2022). The difficulty in identifying, determining and prioritising these risks is enormous. Conventional surveillance systems tend to work in their own rooms, where there is little data exchange among the sectors, and situational awareness remains fractured (Kott & Linkov, 2019). Moreover, traditional risk evaluation is more likely to be based on the past and probabilistic scenarios that are unlikely to reflect emerging or fast changing threats (Zio, 2018). This establishes a gap between the identification of a risk and its treatment, which can be disastrous in situations with high stakes (Alderson, Brown, & Carlyle, 2022).

Ranking the risks is also a problem. The conventional techniques are considered to utilize subjective scoring or non-moving matrices which fails to reflect the dynamic relationship in CIS (Aven, 2019). An example of this is that a moderate risk in an energy system can, together with the weaknesses of communication networks, lead to a national emergency (Rinaldi et al., 2022). Such system dynamics are seldom reflected in traditional models. Artificial Intelligence can overcome the limitations and apply predictive analytics to use diverse, real-time data sets to expose unknown vulnerabilities (Yeboah-Ofori, Islam, & Lee, 2021). However, until these AI-enabled strategies are fully operationalised, CIS will still be vulnerable to dangers that can only be forecasted or prioritised ineffectively using traditional methods (Javaid, Haleem, & Singh, 2023).

IV. AI IN RISK ASSESSMENT AND PREDICTIVE MODELLING

Artificial Intelligence (AI) has emerged as a powerful facilitator of predictive risk analysis of complex systems that extend beyond the limitations of traditional methods (Yuan, Li, & Wang, 2023). Decision trees and support vector machines are machine learning (ML) algorithms that are frequently used to categorize vulnerability and estimate system failure risks (Sarker, 2021). Deep learning (DL) builds upon this capability to process large and unstructured data streams, such as sensor feeds or network traffic, to find patterns that a human analyst would fail to spot (Goodfellow, Bengio, & Courville, 2016). Reinforcement learning (RL) can be useful specifically in dynamic environments, where it allows the adaptation to the learning process with feedback, with the goal of optimising response strategies in real time (Sutton & Barto, 2018). In a similar manner, fuzzy logic systems can be used to effectively address the

uncertainties that are part of the risk assessment approach, and expert systems are used to simulate human decision making in order to give systematic recommendations to neutralize the threat (Tzafestas, 2020). Such methods have already proven to be successful in other fields. ML algorithms are used in cybersecurity to predict the presence of an intrusion attempt with high accuracy (Khraisat, Gondal, Vamplew, & Kamruzzaman, 2019), whereas DL models identify anomalous network behaviour in real time (Yeboah-Ofori et al., 2021). In the energy industry, AI is used to predict failures of equipment and manage loads efficiently during threat situations (Bennett & Stephens, 2023). Predictive analytics are used in transport to improve the resilience of infrastructure by simulating zones with the highest accident rates and probability of a failure (Thakur, Malekian, & Bogatinoska, 2017). AI is used in healthcare to help identify the vulnerability of the system by identifying possible system bottlenecks in emergency preparedness (Aceto, Persico, & Pescapé, 2020).

However, all these successes are tainted with a few serious limitations. Scalability is another issue, since models trained on certain datasets generally fail to generalise on many different infrastructures (Arrieta et al., 2020). Another important issue is interpretability: high-stakes CIS decision-makers might be unwilling to adopt black-box AI models the predictions of which are not transparent (Adadi & Berrada, 2018). Real-time flexibility is also problematic and models have been shown to lag in threat environments that rapidly change (Yuan et al., 2023). Such loopholes highlight the necessity of more hybrid AI-based systems integrating predictive accuracy with transparency, flexibility, and cross-domain usability which is exactly what the current study seeks to achieve.

V. RISK PRIORITISATION APPROACHES

Risk management of critical infrastructure requires not just vulnerabilities to be identified, but prioritisation of the vulnerabilities based on urgency and potential impact (Aven, 2019). The conventional methods of risk prioritisation generally use quantitative risk scoring, where risk is prioritised according to measures of likelihood and severity (Haimes, 2016). Probabilistic models also generalize this by providing estimates of probabilities of adverse events, and in many cases using statistical distributions to provide predictions (Zio, 2018). Another approach that has gained popularity is multi-criteria decision analysis (MCDA) in which risk is weighted against other factors, such as cost, impact on society and system resilience (Linkov & Moberg, 2011). These methods offer organised forms of prioritisation, although they lose their value in very complex interdependent settings (Rinaldi, Peerenboom, & Kelly, 2022). The weaknesses of conventional approaches are in their inability to move over time and in their use of simplistic assumptions (Alderson, Brown, & Carlyle, 2022). Quantitative scoring can tend to overly simplify risk assessment by simply grading risks according to inflexible numerical scales without reflecting interdependencies or cascading effects among infrastructure sectors (Kott & Linkov, 2019). More advanced, probabilistic models still are constrained by past data which might not capture emerging or new threats (Zio, 2018). In a similar way, MCDA can be very much subjective in nature, in that the weight attributed to individual criteria may be based on a human judgement instead of objective analysis (Ishizaka & Nemery, 2013). These disadvantages make traditional prioritisation methods ineffective to transform networked CIS environments (Yuan, Li, & Wang, 2023).

AI-based predictive analytics will offer an avenue to address these shortcomings (Javaid, Haleem, & Singh, 2023). Through the analysis of various types of data, including sensor data and cyber logs, AI models can dynamically change their prioritisation based on changing risk profiles (Yeboah-Ofori, Islam, & Lee, 2021). Because AI has the capability to model both direct and indirect effects, it can help identify systemic weaknesses, which would not otherwise be visible in a static model (Thakur, Malekian, & Bogatinoska, 2017). Beyond that, hybrid cycles that integrate ML and decision-support systems enhance transparency and augment scalability across domains (Arrieta et al., 2020). By doing so, AI can help turn risk prioritisation into a dynamic, data-driven approach that is based on the real complexity of critical infrastructures and is no longer a subjective and static process.

VI. SYNTHESIS AND IDENTIFIED GAPS

The above overview of theoretical backgrounds, vulnerabilities of critical infrastructure systems (CIS), uses of artificial intelligence (AI), and the current risk prioritisation strategies identifies the advances achieved and the gaps that still remain in the current body of literature. Rational approaches such as Risk Management Framework (RMF), PRAM and resilience theory provide a methodical baseline around which decisions are made but still restricted by inflexible methodological approaches to the dynamic nature of modern threats (Kott & Linkov, 2019; Zio, 2018). Likewise, although risk prioritisation techniques such as probabilistic models and multi-criteria decision analysis can provide effective ranking mechanisms, they cannot compete with complex interrelationships and cascading failure that are the hallmarks of CIS (Rinaldi et al., 2022; Alderson et al., 2022). AI-based techniques offer significant innovations, as they allow predictive vulnerability analysis and anomaly detection and adaptive learning in areas like cybersecurity, energy, transport, and healthcare (Sarker, 2021; Yeboah-Ofori et al., 2021). Nevertheless, such applications have not been developed as interfaces across infrastructures, but as sector-specific applications (Bennett & Stephens, 2023). Moreover, most AI versions are affected by scalability, interpretability, and real-time threat adaptation issues (Arrieta et al., 2020; Yuan et al., 2023). Deep learning is not a transparent black box and is therefore harder to have trust in in a high stakes context (Adadi & Berrada, 2018), and reinforcement learning algorithms often require controlled conditions that are not easily available in critical infrastructure (Sutton & Barto, 2018). The missing thing, then, is a converged, cross-

domain framework integrating the systematic organization of traditional risk management with the dynamical learning ability of AI (Javaid et al., 2023). Such a framework should be built to incorporate several sources of data, offer clear and understandable outputs, prioritize risks in real time, and address systemic interdependencies across infrastructure sectors (Linkov, Trump, Golan, & Keisler, 2021). The need to fill these gaps makes it reasonable to develop an AI-based conceptual framework that is predictive, flexible, and decision-oriented. This framework aims to go beyond siloed applications by providing an integrated and intelligent vulnerability assessment and risk prioritisation system in critical infrastructures.

- *Conceptual Framework Development*

Table 1 Conceptual Framework Development

Component	Description	How It Addresses Gaps
Data Sources	Multi-layered inputs including sensor data, network logs, environmental data, and historical incident records.	Enhances cross-domain applicability by integrating heterogeneous datasets for holistic risk assessment.
AI Models	Hybrid use of machine learning, deep learning, reinforcement learning, and fuzzy logic.	Enables predictive accuracy, real-time adaptability, and management of uncertainties.
Risk Scoring Mechanism	Dynamic, AI-enhanced scoring system that accounts for likelihood, severity, and cascading interdependencies.	Moves beyond static quantitative models, providing context-aware prioritisation of risks.
Decision-Support System	Visual dashboards and explainable AI tools that communicate risk levels and recommendations to stakeholders.	Improves interpretability, trust, and actionable insights for decision-makers.
Feedback and Learning Loop	Continuous monitoring and updating of models based on new threats and outcomes.	Ensures adaptability and resilience against evolving, real-time vulnerabilities.

This model combines systematic risk management values and dynamic AI functions. Its decision-support system assists in bridging the gap between advanced AI outputs and the real decision-making process by integrating predictive analytics into an iterative feedback loop and transforming vulnerability assessments into a dynamically changing process. In this manner, it provides a unified and open-ended solution to the dynamics of the contemporary CIS.

VII. IMPLICATIONS FOR RESEARCH AND PRACTICE

The contribution of this framework is theoretical because the paper presents AI integrated into the resilience model and risk management models to assess risks and provide a dynamic and multi-domain approach to risk assessment. In practice, it allows greater anticipatory accuracy, prioritisation of risks, and proactive robustness in basic infrastructures based on real-time, data-driven decisions. In the context of future studies, robustness has to be tested empirically using sector-specific data. It must also have cross-sector applications and fit to national policy frameworks to enable scalability, accountability and institutional adoption to render the framework scholarly and transformationally useful.

VIII. CONCLUSION

The study has identified the weaknesses of conventional risk assessment frameworks, industry-specific AI implementations, and fixed prioritisation approaches to the full range of critical infrastructure risks. The suggested AI-based architecture helps fill these gaps and consider adaptive learning, transparency, and cross-domain applicability. Predictive and decision-support capabilities make it possible to build resilience dynamically in high-stakes settings. The framework does not only enrich the academic knowledge, but offers the platform through which academic knowledge can be empirically affirmed and operationalized, and ultimately render critical infrastructures immune to evolving vulnerabilities and systemic perturbations.

RECOMMENDATIONS

It also represents a supposed sign that scholars are expected to dedicate their attraction in the delivery of the empirical validation of the framework in multiple infrastructure sectors to award accountability and scalability. The national risk management strategies should include AI-based tools to allow policymakers to focus on resilience planning. Practitioners will implement explainable AI mechanisms as a way to improve transparency and foster trust among interested parties. Academia, industry and government now need to come together and hone the framework and make it internationalisation friendly and sensitive to emerging threats in an increasingly globalised and digitalised world.

REFERENCES

[1]. Aceto, G., Persico, V., & Pescapé, A. (2020). The role of Information and Communication Technologies in healthcare: Taxonomies, perspectives, and challenges. *Journal of Network and Computer Applications, 107*, 102–137.

[2]. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access, 6*, 52138-52160.

[3]. Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2022). Assessing and improving the operational

resilience of critical infrastructures. *Operations Research, 70*(2), 749-769.
[4]. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82-115.
[5]. Aven, T. (2019). The call for a shift from risk to resilience: What does it mean? *Risk Analysis, 39*(6), 1196-1203.
[6]. Bennett, M., & Stephens, P. (2023). *Governing critical infrastructure: Protecting society in an interconnected world*. Routledge.
[7]. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
[8]. Haimes, Y. Y. (2016). *Risk modeling, assessment, and management* (4th ed.). John Wiley & Sons.
[9]. Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. CRC Press.
[10]. Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (5th ed.). Kogan Page Publishers.
[11]. Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety, 145*, 47-61.
[12]. Ishizaka, A., & Nemery, P. (2013). *Multi-criteria decision analysis: Methods and software*. John Wiley & Sons.
[13]. Javaid, M., Haleem, A., & Singh, R. P. (2023). A review on artificial intelligence (AI) and its potential for enhancing resilience in critical infrastructure. *Sustainable Operations and Computers, 4*, 1-9.
[14]. Joint Task Force. (2018). *Risk management framework for information systems and organizations* (NIST Special Publication 800-37, Rev. 2). National Institute of Standards and Technology.
[15]. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*(1), 1-22.
[16]. Kott, A., & Linkov, I. (Eds.). (2019). *Cyber resilience of systems and networks*. Springer International Publishing.
[17]. Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: Defending a networked nation* (3rd ed.). John Wiley & Sons.
[18]. Linkov, I., & Moberg, E. (2011). *Multi-criteria decision analysis: Environmental applications and case studies*. CRC Press.
[19]. Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience*. Springer.
[20]. Linkov, I., Trump, B. D., Golan, M., & Keisler, J. M. (2021). Enhancing resilience in post-COVID societies: The role of AI and digital governance. *Nature Sustainability, 4*(9), 752-754.
[21]. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2022). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 42*(1), 11-25.
[22]. Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science, 2*(3), 1-21.
[23]. Schoitsch, E. (2020). Integrated risk management and security for critical infrastructures. In *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops* (pp. 3-15). Springer International Publishing.
[24]. Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction* (2nd ed.). MIT Press.
[25]. Thakur, A., Malekian, R., & Bogatinoska, D. C. (2017). Internet of Things based solutions for road safety and traffic management in intelligent transportation systems. In *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 504-509). IEEE.
[26]. Tzafestas, S. G. (2020). *Expert systems in engineering applications*. Springer International Publishing.
[27]. World Economic Forum. (2024). *The Global Risks Report 2024*. World Economic Forum.
[28]. Yeboah-Ofori, A., Islam, S., & Lee, S. W. (2021). A survey on AI-enabled cybersecurity for critical infrastructure protection. *IEEE Access, 9*, 165395-165414.
[29]. Yuan, F., Li, M., & Wang, L. (2023). Artificial intelligence for risk analysis in complex systems: A state-of-the-art review. *Reliability Engineering & System Safety, 230*, 108919.
[30]. Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety, 177*, 176-190.