Stout in Computer Science and Technology Studies (SCSTS)
ISSN: 2979-420X
DOI: https://doi.org/10.61424/vw25yt73
Journal Homepage: https://stoutjournals.org/index.php/SCSTS

Cross-Sector AI Integration: Enhancing Cybersecurity, Infrastructure Protection, Urban Transportation, Supply Chains, and Public Health Surveillance

Karim Hossain
Independent Researcher, UK
Corresponding Author: Karim Hossain, **E-mail**: *Independent Researcher, UK*

ARTICLE INFORMATION

Submitted: October 02, 2026
Accepted: October 25, 2026
Published: November 01, 2026
Volume: 2
Issue: 1

KEYWORDS

Cross Sector AI Integration; Cybersecurity; Critical Infrastructure Protection; Supply Chain Resilience; Public Health Surveillance.

ABSTRACT

The integration of artificial intelligence across multiple sectors is a new way of improving cyber security, securing critical infrastructure, optimizing urban transportation systems, enhancing the resilience of supply chains, and monitoring public health. In this review, AI powered analytics, interoperable architecture, digital twins and cross-sector data fusion will be explored to improve situational awareness and facilitate timely, evidence based decision-making. Integrated risk scoring allows all data to be analysed together from a range of operational environments, helping to prioritize threats and identify cascading risks. They could be used to detect and respond to cyber threats, predict infrastructure failures, optimize transportation and supply chains, and identify new threats to public health. The roles of blockchain enabled traceability, secure application programming interfaces, data provenance, and federated analytics in supporting information integrity and responsible data exchange are also discussed. However, these opportunities are limited by the lack of interoperability of the data formats, privacy considerations, algorithmic bias and the unequal technological competence between organizations. This means that in order to be effective, the deployment must be supported by strong security measures, clear governance, regulatory compliance, human oversight, workforce development and ongoing assessment of performance. A gradual deployment approach using targeted pilot sites and quantifiable operational metrics, can mitigate deployment risks and prove value. Overall, AI integration within cross-sector can enhance the resilience and coordination of interdependent digital and physical systems.

1. Introduction

The cross sector integration of artificial intelligence (AI) is a multi-disciplinary strategy that aims to enhance cyber security, infrastructure protection, urban transportation, supply chain management and public health monitoring by analysing data and making informed decisions. AI can integrate information technology, operational technology, transportation systems, industrial infrastructure, and healthcare systems to provide a comprehensive view of the situation and coordinated responses to complex threats (Akinade et al., 2021). This is not just about deploying AI in discrete applications but is also a matter of creating an integrated operational framework that can pick up risks, correlate incidents and contribute to resilience for interdependent infrastructures. Multi agent architectures, semantic integration layers, and context aware learning systems are key elements of this approach. AI agents can be used to streamline security operations, analyze suspicious behavior, synthesize information from various security systems, and suggest corrective actions. Semantic interfaces enable interoperability with existing security information and event management, security orchestration, automation and response, and extended detection and response platforms without having to push all the data to a centralized repository (Arksey et al., 2005). Analytical systems can hold relevant evidence, learn from past incidents and enhance future investigations through institutional knowledge mechanisms and shared investigative contexts. Shared workbenches also help to improve transparency by allowing human analysts to review agent decisions, validate results and adjust operational procedures. Federated learning & privacy preserving methods allows models to learn from multiple, distributed datasets without exposing raw personal/organizational data (Chavula et al., 2025). These methods are especially useful in healthcare surveillance systems, wearable devices, autonomous transportation, and interrelated industrial systems. However, broken data can lead to classification mistakes and result in the loss of sensitivity of the

Copyright: © 2026 The Author(s). This open access article is distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC- BY-NC-SA) License (https://creativecommons.org/licenses/by-nc-sa/4.0/), published by Stout Journals, London, United Kingdom

original data. In addition, AI systems compromised by hackers can pose risks to operational technologies, such as industrial control systems, power distribution systems, and medical equipment, which can result in real-world effects. Operational mistakes and reduced security compliance may be caused by cognitive overload, digital fatigue, and analyst burnout. simultaneously, regulatory uncertainty, data incompatibility, vendor lock-in and shifting AI-fuelled threats add to the implementation challenge – from one jurisdiction to another, and from one sector to another (Chen et al., 2025). The larger ethical question is whether public health surveillance, which can benefit pandemic detection and emergency response with AI, comes at a cost of compromising privacy and civil rights through the extensive collection of data. Thus, the deployment of these systems must be interoperable, continuously assessed for risks, subject to audit, and have useful contingency planning; and there must be meaningful human oversight. Pilot programmes and sector specific safeguards are key to ensuring that the integration of AI across sectors enhances efficiency without compromising security, accountability, or public trust (Di et al., 2024).

2. Cross Sector Data Fusion and Unified Risk Scoring

AI's ability to cross sector relies on enhancing cybersecurity, protecting infrastructure, urban transportation, supply chain management, and public health surveillance by leveraging the integration of various data streams. Information gathered from sensors, operational systems, network logs, transportation solutions and medical records can be fed into the digital twin to create a more accurate digital twin and improve situational awareness (Abdullah et al., 2023). Multi sensor fusion provides a more comprehensive representation of complex systems than does single sensor approaches, and allows for better monitoring, predictive analysis and helping with decision making (Table 1). They can be especially useful in smart cities, critical infrastructure, interconnected healthcare facilities, and industrial manufacturing processes (Watara, 2026). There are three main levels of data fusion: raw data fusion, feature level fusion and decision level fusion. Raw data fusion is the direct fusion of data from the sensors, which means that detailed information is preserved but a large bandwidth and precise synchronization are required (Hosseini et al., 2021). With feature level fusion, the characteristics of different data sources are extracted and combined to support different data sources with varying data formats. Decision level fusion is the fusion of the outputs of individual analytical systems by procedures like voting and Bayesian inference. This can be used to enhance the fault tolerance by letting individual components run independently. The choice of a suitable fusion strategy is determined by the diversity of the sensors, the computational resources, communication limitations, and safety considerations. Kalman filtering is useful for tracking, anomaly detection or digital twin applications and it also provides state estimation support for real time applications with consideration of measurement and process uncertainties (Kathmandu et al., 2025). Its performance, however, is contingent on appropriate mathematical models, and synchronized measurements. Security aware fusion additionally contributes to the reliability by adding trust measurements of data sources and participating agents. Lower influence weights can be given to unreliable or suspicious inputs during aggregation, to help identify manipulated inputs and enhance situation assessment in adversarial situations. In addition, federated learning helps overcome these challenges by allowing multiple organizations and/or devices to train their models without sharing the raw data with a central server (Abdullah et al., 2024). Especially where sensitive information is shared throughout healthcare networks, supply chains and operators of critical infrastructure. However, the methodology for assigning scoring thresholds and weighting schemes need to be validated to avoid the risk of misleading rankings and to prevent rare but catastrophic events being overlooked. These approaches, combined with human oversight, clear data fusion, privacy respecting learning, and adaptive risk assessment, create an integrated approach to threat detection, prioritization, and resilience-building across various sectors (Khurram et al., 2025).

Table 1. Cross-Sector Applications of Artificial Intelligence and Their Contributions to Operational Resilience

Sector	AI technologies and approaches	Major applications	References
Cybersecurity	Machine learning, anomaly detection, behavioral profiling, AI-driven threat intelligence	Threat detection, incident prioritization, automated response, malicious activity identification	(Akinade et al., 2021; Abdullah & Ridoy, 2023; Rahman et al., 2026)
Critical infrastructure	Digital twins, predictive analytics, sensor fusion, AI-assisted monitoring	Predictive maintenance, infrastructure monitoring, OT and ICS protection, failure forecasting	(Abdullah & Ridoy, 2024; Ajayi et al., 2025; Yan et al., 2023)
Urban transportation	Intelligent traffic management, predictive modeling, digital twins, adaptive signal control	Traffic prediction, route optimization, public transit planning, congestion management	(Di et al., 2024; Ridoy & Akhir, 2025; Wu et al., 2025)
Supply chains	Machine learning, predictive analytics, AI-based monitoring, blockchain-enabled traceability	Demand forecasting, supplier risk assessment, shipment monitoring, disruption prediction	(Ridoy, 2022; Mienye et al., 2024; García-Méndez et al., 2025)

3. Infrastructure Protection and Urban Transportation

AI's ability to enhance infrastructure protection and urban transportation, through intelligent monitoring, predictive analytics, and coordinated responses, is crucial for increasing the operational resilience, public safety, and efficiency of urban transportation. Operational technology (OT), industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems complement each other in the management of industrial processes, monitoring, and real time control of critical infrastructure (Kolivand et al., 2025). As these systems become more tightly coupled with information technology networks, they are at greater risk of being attacked by cyber means, and thus must be protected by integrated security strategies that safeguard digital assets, as well as physical processes and critical public services. To ensure effective OT and ICS security, it is critical to have a full-scale incident response plan, system security setup, employee training, and ongoing risk assessments (Kwarkye et al., 2025). Response plans should be developed to cover both IT and OT threats, such as isolation of compromised systems, while maintaining critical operations. Coordinated investigation and recovery can be supported with collaborative case management, threat integration and automated workflows. Frequent configuration audits, data encryption, access controls and security awareness training mitigate against risks. Zero trust architectures, AI assisted threat detection, deception based defence, and self healing mechanisms are some ways to enhance cyber resilience (Figure 1) (Ridoy et al., 2025). AI also has a role in urban transportation by enhancing mobility planning, managing traffic flow, optimizing public transit operations, and maintaining infrastructure. Predictive analytics can help transport agencies plan for demand, adapt the frequency of services and deploy vehicles based on shift in travel patterns. Real time traffic analysis can be used for route optimization, congestion prediction and Adaptive signal control, which can lead to faster journey times, lower fuel use and reduced emissions (Levac et al., 2010). Incorporating commuter feedback and demographic data may be useful in determining underserved communities and enhancing equitable access to public transportation. Digital twins also provide new possibilities – virtual models of intersections, transportation networks, and infrastructure assets. These models can be utilised for traffic analysis, optimisation of signal timing, planning for emergency response and testing changes in operation prior to implementation (Li et al., 2025). However, to be effective, deployment requires not only accurate data, but interoperability between systems, privacy protection and transparency in government. It is important that mobility data is treated responsibly and algorithmic decisions are considered for their fairness with respect to the distribution of service.

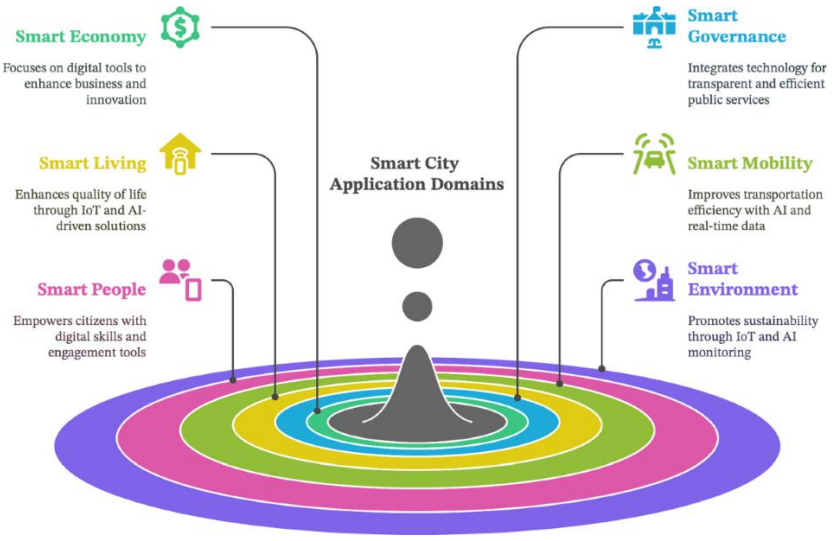


Figure 1. The role of AI in building generative urban intelligence (Habib et al., 2025)

4. Supply Chains: Disruption, Integrity, and Operational Risk

AI-powered supply chains are a significant part of the interconnected infrastructure system, with potential to ripple across industries, organizations, and borders. When resources are concentrated into a critical area like advanced semiconductor manufacturing, there are vulnerabilities in the system that emerge that can't be resolved by the cyber security efforts of the single organization (Mageto et al., 2024). If the production of these chips is disrupted, or if cloud services are impacted, or if any of the specialized AI components are impacted, then the computational power and the flow of downstream operations will be impacted. Resilience in the supply chain, therefore, needs to be addressed in a coordinated way, taking into account technical dependencies, operational continuity, and the overall economic risks (Ridoy et al., 2022). Ensuring the integrity of AI supply chains relies on securing the entire lifecycle of AI systems—from data collection and labelling to data preprocessing, model development, fine-tuning, retrieval databases, software libraries, inference services, hardware, cloud infrastructure, to update channels. Any weakness in one of these systems can affect several downstream systems. Common challenges are contaminated data, rogue models, compromised software, compromised repositories and insecure third party services. These risks can be

exacerbated through shared models and central infrastructure, as a single compromise can impact many organisations at once (Mehryar et al., 2024). To achieve good protection, it's crucial to maintain component inventories, verify the provenance, sign software components, make sure that they are from secure registries, scan dependencies, and have controlled deployment procedures. AI based BOM can help to gain visibility into a system's dependencies, and staged updates and fast rollback can help recover in case of suspicion of compromise. Optimizing with AI must be paired with robust governance and monitoring to ensure effective implementation (Mienye et al., 2024). The key points for organizations include data ownership, access to sensitive operational data, validation of third-party components, and testing of the performance of the model under varying conditions. You can diversify critical supplies and also have alternate business practices in place, to minimize the reliance on one supplier or infrastructure provider. Automated recommendations have significant financial or operational implications and human supervision is still essential (Shama et al., 2023). By combining cybersecurity, supply chain tracking, tracking of origin, and predictive analytics, you get a full solution to disruption and operational risk management. If backed by clear governance, safe deployment, and proven recovery plans, AI can enhance visibility and speed up the response to disruption, as well as bolster resilience in interdependent supply chains.

5. Public Health Surveillance and Cross Sector Interoperability

Public health surveillance is increasingly using artificial intelligence (AI) to connect data from health systems, logistics, mobility, population and epidemiological monitoring platforms. The integration of these data sources facilitates real time disease surveillance, forecasting of demand, resource allocation and evidence based decision making (Mu et al., 2024). In times of public health crises, integrated analytical platforms can support decision making to determine stocks, estimate capacity needs in hospitals and allocate vaccines, medicines and other critical supplies in accordance with population needs (Table 2). AI can also enhance the coordination of emergency responses and bolster preparedness for future health crises by incorporating epidemiological data with transportation and distribution information. AI-powered verification systems offer enhanced public health management capabilities, verifying digital health records, vaccination cards, and relevant documents (Munn et al., 2023). By linking verified health data to authorised databases, fraudulent documentation can be minimised and appropriate public health measures can be facilitated. These applications, however, should have very specific access controls, clear verification processes and protection against unauthorized monitoring or adverse decisions. Interoperability across sectors is more than just technical, it's also governance, legal, organizational coordination and ethical responsibility. The key to effective inter-agency, private sector, health and community institution collaboration is shared data standards, a common language and clear accountability (Olaitan et al., 2021). Semantic interoperability allows different systems to understand the meaning of the information they exchange, and standardized interfaces enable communication between systems that run on different platforms. However, the differences in regulations, organizational procedures and data protection laws can make information sharing between jurisdictions more difficult. Governance frameworks are thus required to define data ownership, access rights, accountability, and suitable sharing conditions (Peters et al., 2020). Collaborative structures of data exchange, data catalogs and controlled analytical environments can help to enable collaboration without unwarranted disclosure. These methods help to maintain data and source accountability and can be used to conduct auditable investigations in any industry. Public health surveillance systems can be combined with systems that offer more interoperability between healthcare, transportation, supply chains, and critical infrastructure operators. But this can only be achieved with high-quality data, privacy protection, clear decision making, and meaningful stakeholder engagement (Ngulube et al., 2025). An interoperable technologic, privacy preserving analytics, and accountable AI governance-centered approach can better prepare the public health system and enable trusted data sharing across interwoven sectors.

Table 2. Major Challenges, Mitigation Strategies, and Governance Requirements for Cross-Sector AI Integration

Challenges	Potential consequences	Governance and implementation requirements	References
Data interoperability limitations	Inconsistent information exchange, fragmented datasets, and inaccurate analytical outcomes	Common data standards, institutional coordination, and clear data-sharing agreements	(Olaitan et al., 2021; Peters et al., 2020; Wu et al., 2025)
Cybersecurity vulnerabilities	Unauthorized access, data manipulation, model extraction, and disruption of critical operations	Continuous security audits, incident response planning, and lifecycle security assessment	(OECD, 2019; Abdullah & Ridoy, 2024; Obuseh et al., 2025)
Data privacy and ethical concerns	Unauthorized disclosure, surveillance risks, and reduced public trust	GDPR and CCPA compliance, transparency, accountability, and human oversight	(Chavula & Kayusi, 2025; Ogundiran et al., 2025; Singh & Goyal, 2023)
Supply chain vulnerabilities	Third-party compromise, contaminated datasets, supplier dependency, and operational disruptions	Third-party risk assessment, controlled deployment, and recovery planning	(Mehryar et al., 2024; Mienye et al., 2024; Ridoy, 2022)

6. Security of AI Systems and Implementation Across Sectors

Achieving security in AI systems in multi-scale, interdependent digital and physical environments demands a data-centric strategy that ensures confidentiality, integrity, and availability throughout the AI lifecycle. To prevent unauthorized access, manipulation, and leakage of data, data collection, data preprocessing, model training, inference, and storage must be secured. This is especially critical where AI agents are able to talk to each other or engage with the critical infrastructure, healthcare systems, transportation networks, and industrial control environments (Obuseh et al., 2025). Technical security measures and sound governance go hand-in-hand to ensure the reliability of systems and responsible AI deployment. AI threat detection and response can enhance protection by leveraging anomaly detection, behavioral profiling, and predictive analytics. Continuous monitoring can help detect anomalous data transfers, suspicious interactions and possible breaches of the infrastructure far sooner. Secure protection for the model and the API are also crucial, as deployed models can be subject to unauthorized access, probing, extraction, or manipulation (OECD, 2019). These risks can be minimized by applying the following: Authentication, Rate Limiting, Secure Credential Management, Signed Model Artifacts, and Controlled Repositories. Data processing pipelines should also be designed to ensure privacy protection, so that sensitive data does not end up in temporary storage, logs, or in other applications. Data tokenization is another security measure that involves substituting sensitive data with controlled alternatives for use by AI algorithms (Ogundiran et al., 2025). Detokenization should only be done within trusted services with appropriate access controls and auditability. Sensitive credentials and cryptographic operations can be further protected using hardware security modules and memory isolation. Data provenance, lineage and quality are also critical in ensuring the integrity of information and in helping to investigate system failures (Figure 2). Monitoring in collaborative and federated settings assists in maintaining reliability as threats change, by identifying data poisoning, model drift and weaknesses in legacy models (Reichstein et al., 2025). The implementation of privacy enhancing technologies and adherence to relevant laws and regulations such as GDPR and CCPA should be part of the total security system. The success of the implementation in each sector on the part of the technical readiness also rely on the range of organizational capacities, public confidence, and user acceptance. For instance, a public health app might not be equally adopted due to various reasons such as lack of internet connectivity, community mistrust, or fear of government surveillance (Singh et al., 2023). Therefore, transparent communication, stakeholder engagement and inclusive design are essential to make sure vulnerable populations are not left out of the picture. Using standardized data formats and interoperability protocols can help to enable cooperation between health care institutions and ensure consistency in integrated analytical systems. In general, the coordination of technical protection, privacy-protecting data management, standardized interoperability, and structured implementation is required for a secure integration of AI (Sun et al., 2022). These, coupled with human oversight, stakeholder involvement, and ongoing monitoring and evaluation, can enhance adoption and enhance cybersecurity, infrastructure resiliency, transportation safety and public health preparedness.

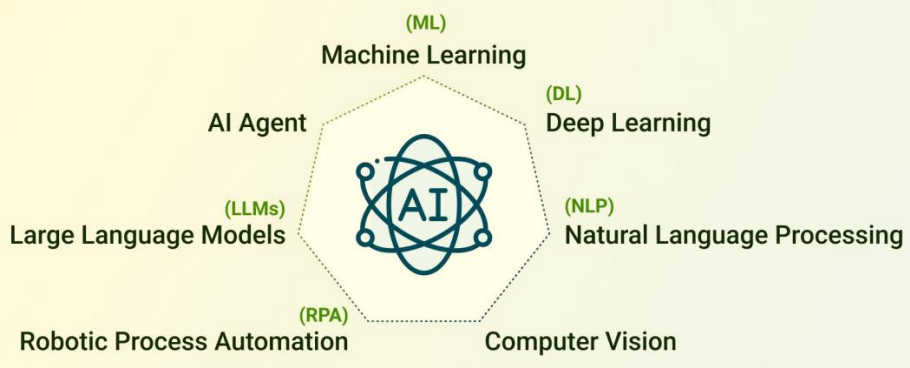


Figure 2. The core components and subfields surrounding a central artificial intelligence framework (Ajayi et al., 2025)

7. Discussion

The ability to cross sector AI integration is a promising way to boost the cybersecurity, critical infrastructure, urban transportation, resilience of supply chains, and public health surveillance. In general, these domains operate in their own information systems, process and institutional functions (Tricco et al., 2018). But, as they become more digitally interdependent, they have become vulnerable to common risks that can't be effectively mitigated by standalone monitoring and response solutions. By leveraging AI in these areas, information can be processed as a whole, helping to detect new threats, disruptions in operations, and systemic risks before they emerge. The quality of the overall value of this approach will not only be from the sophistication of the individual AI models, but also the trustworthiness of data exchange, system interoperability, governance arrangements and coordination among stakeholders (Ridoy et al., 2021). One key result of this cross sector view is that there must be a shared situational awareness to enable effective risk management. Transportation networks, electricity distribution, hospital operations, and the supply chain can all be impacted by a cybersecurity incident. For instance, a logistics network attack could lead to a slowdown in the supply of crucial medical equipment, affect hospital care, and strain public health systems.

Evaluating the events themselves may fail to identify more general impacts (Ukoba et al., 2024). AI-powered systems can link security alerts, infrastructure performance metrics, transportation data, inventory data, and public health data in real time to uncover patterns and relationships that can't be found in each dataset alone. This can help develop a more holistic view of cascading risks and proper coordination of response before localized disruptions escalate to broader emergencies. Such integration will be effective to a large degree based on the system architecture. Information exchange can be achieved through edge computing, centralization or cloud based analytics, application program interfaces, and sector specific data platforms, which can meet different operational demands (United Nations Educational, Scientific and Cultural Organization, 2021)). Edge processing is especially beneficial in situations requiring swift decisions, such as traffic lights, industrial control systems, and critical infrastructure. Local analysis can minimize delays in communication and maintain critical functions during periods of communication loss. Centralized or federated analytics can then be used to enhance wide-reaching risk assessment by bringing together relevant information from various organizations (Wanyama et al., 2024). Hence a Hybrid architecture is a practical compromise between the autonomy of the local community, the computational efficiency of the computer and the need for cross sectoral coordination. However, interoperability is an issue of great importance. Commonly, various sectors use different data formats, definitions, reporting standards, and digital maturity. This means that information might be technically accessible, but hard to understand or use consistently between organizations. The quality of cross sector analysis can be improved by having common data definitions, consistent interfaces, metadata management, and consistent event classification (Wu et al., 2025). Data provenance and line of sight are equally vital as AI makes recommendations and they need to be able to trace back to the sources of the data. If not, the results of these mechanisms could lead to incorrect or inaccurate information, which may result in inaccurate risk assessments and make the system less trustworthy. Within the cybersecurity domain, AI-powered detection, triage, and response can aid in the identification of malicious activity by analyzing network traffic, authentication logs, endpoint behavior, system logs, and various security metrics. Machine learning can be used to detect deviations from normal behavior patterns, and predictive analytics can provide assistance in prioritizing new threats (Rahman et al., 2026). Linking security operations centers to infrastructure monitoring systems could also provide some insight into attacks that span information technology and operational technology systems. These are especially relevant in situations where digital systems manage physical processes, where a cybersecurity incident can impact equipment availability, transportation safety and critical public services. Information from sensors, digital twins, intelligent traffic management platforms and predictive maintenance systems can be available regarding the condition of the equipment, congestion, abnormal operating behavior and potential equipment failure (Yan et al., 2023). Combined with cybersecurity analytics, these technologies can potentially aid in the identification of technical failures as opposed to malicious activity and identify the events that need to be handled in a coordinated manner. Digital twins can be used to show relationships between infrastructure and its operations and help organizations perform a scenario analysis to assess what may happen if something goes wrong before taking corrective action (Filho et al., 2022). Their reliability, however, relies on accuracy of the sensor data, timely updates, and proper representation of real world operating conditions. Misrepresentations in the digital context can give the wrong impression and result in wrong decisions being made. These advantages are carried through to material flows, inventory management, logistics and supplier risk assessment in the supply chain. AI can analyze demand patterns, shipment delays, supplier performance, environmental conditions, and geopolitical disruptions to identify potential interruptions (García et al., 2025). These signals can be coupled with cybersecurity monitoring to identify threats related to tampered logistics platforms, unauthorized data changes or manipulated shipment information (Ogayemi, 2026). Traceability could be further enhanced by blockchain and other distributed ledger technologies, which could provide a more secure and verifiable record of transactions and material movements. However, a tamper resistant record does not ensure the accuracy of the original information. Regardless, data validation, access authorizations, physical checks, and accountability are still critical to maintaining the integrity of information along the supply chain (Hossain et al., 2025). Additionally, less developed networks or systems may not be accessible to smaller suppliers because of their financial and technical limitations, which may cause inequities in coverage and implementation of these networks. Lastly, the overall impact of the cross sector integration of AI is a positive outlook for enhancing digital and physical environments' resilience. It is most effective in linking up disparate information, identifying interdependencies and coordinating the response to complex risks.

8. Conclusion

Cross sector AI integration offers a comprehensive approach to strengthening cybersecurity, protecting critical infrastructure, improving urban transportation, enhancing supply chain resilience, and advancing public health surveillance. By combining data analytics, interoperable architectures, predictive modeling, and coordinated response mechanisms, interconnected risks can be identified and managed more effectively. However, successful implementation requires reliable data, robust security controls, privacy protection, transparent governance, and continuous model evaluation. Human oversight remains essential for ensuring accountability and preventing harmful automated decisions. Future efforts should prioritize scalable architectures, standardized data exchange, workforce development, and measurable outcomes to establish resilient, secure, and trustworthy AI enabled systems.

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
Artificial Intelligence (AI) Use Disclosure: The authors declare that no artificial intelligence tools were used in the preparation of this manuscript.

References

[1] Abdullah, C. A., & Ridoy, M. J. I. (2023). Artificial intelligence-driven cyber threat detection for protecting critical digital infrastructure. *Innovation: International Multidisciplinary Journal of Applied Technology*, *1*(2), 76–83. https://doi.org/10.51699/zb8kwv06

[2] Abdullah, C. A., & Ridoy, M. J. I. (2024). Artificial intelligence driven infrastructure security enhancing cybersecurity and protecting national security systems. *IPTEKS*, *1*(3), 191–200. https://doi.org/10.61796/ipteks.v1i3.498

[3] Ajayi, O. O., Kurien, A. M., Djouani, K., & Dieng, L. (2025). A proactive predictive model for machine failure forecasting. *Machines*, *13*(8), Article 663. https://doi.org/10.3390/machines13080663

[4] Akinade, O., Adepoju, A., Ige, A. B., Afolabi, A. I., & Amoo, O. O. (2021). A conceptual model for network security automation: Leveraging AI-driven frameworks to enhance multi-vendor infrastructure resilience. *International Journal of Science and Technology Research Archive*, *1*(1), 39–59. https://doi.org/10.53771/ijstra.2021.1.1.0034

[5] Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19–32. https://doi.org/10.1080/1364557032000119616

[6] Chavula, P., & Kayusi, F. (2025). Challenges in Sub-Saharan Africa's Food Systems and the Potential Role of AI. *LatIA*, *3*, Article 318. https://doi.org/10.62486/latia2025318

[7] Chen, Y., Zhang, F., Qian, Y., Zeng, J., & Li, X. (2025). A new car-following model considering the driver's dynamic reaction time and driving visual angle on the slope. *Physica A: Statistical Mechanics and Its Applications*, *663*, Article 130408. https://doi.org/10.1016/j.physa.2025.130408

[8] Di, X., Fu, Y., Turkcan, M. K., Ghasemi, M., Mo, Z., Zang, C., & Zussman, G. (2024). *AI-powered urban transportation digital twin: Methods and applications* (arXiv:2501.10396). arXiv.

[9] Filho, W. L., Wall, T., Mucova, S. A. R., Nagy, G. J., Balogun, A.-L., Luetz, J. M., Ng, A. W., Kovaleva, M., Azam, F. M. S., Alves, F., et al. (2022). Deploying artificial intelligence for climate change adaptation. *Technological Forecasting and Social Change*, *180*, Article 121662. https://doi.org/10.1016/j.techfore.2022.121662

[10] García-Méndez, S., Hernández-González, J., & Martínez-Álvarez, F. (2025). An explainable machine learning framework for railway predictive maintenance. *Scientific Reports*, *15*, Article 12345. https://doi.org/10.1038/s41598-025-08084-1

[11] Habib, M., Singh, S., Jan, S., Jan, K., & Bashir, K. (2025). The future of the future foods: Understandings from the past towards SDG-2. *npj Science of Food*, *9*, Article 138. https://doi.org/10.1038/s41538-025-00484-x

[12] Hossain, M. M., & Shama, A. T. (2025). GRC accountability gap in AI and cloud security: Limitations of automated compliance and risk control mechanisms. *International Journal on Orange Technologies*, *7*(1), 56–63. https://doi.org/10.31149/ijot.v7i1.5798

[13] Hosseini, S. H., Khodabin, M., Soroori Sarabi, A., & Sharifipour Bgheshmi, M. S. (2021). Artificial intelligence and disaster risk management: A need for continuous education. *Socio-Spatial Studies*, *5*, 13–29.

[14] Kathmandu, N. (2025). *A comprehensive study on artificial intelligence, digital infrastructure, and data policies with recommendations for policy to strengthen AI ecosystem*. International Telecommunication Union.

[15] Khurram, M., Zhang, C., Muhammad, S., Kishnani, H., An, K., Abeywardena, K., Chadha, U., & Behdinan, K. (2025). Artificial Intelligence in Manufacturing Industry Worker Safety: A New Paradigm for Hazard Prevention and Mitigation. *Processes*, *13*(5), Article 1312. https://doi.org/10.3390/pr13051312

[16] Kolivand, P., Azari, S., Bakhtiari, A., Namdar, P., Ayyoubzadeh, S. M., Rajaie, S., & Ramezani, M. (2025). AI applications in disaster governance with health approach: A scoping review. *Archives of Public Health*, *83*, Article 218. https://doi.org/10.1186/s13690-025-01712-2

[17] Kwarkye, T. G. (2025). "We know what we are doing": The politics and trends in artificial intelligence policies in Africa. *Canadian Journal of African Studies / Revue Canadienne des Études Africaines*, 1–19. https://doi.org/10.1080/00083968.2025.2458907

[18] Levac, D., Colquhoun, H., & O'Brien, K. K. (2010). Scoping studies: Advancing the methodology. *Implementation Science*, *5*, Article 69. https://doi.org/10.1186/1748-5908-5-69

[19] Li, X., Krivtsov, V., Pan, C., Nassehi, A., Gao, R. X., & Ivanov, D. (2025). End-to-end supply chain resilience management using deep learning, survival analysis, and explainable artificial intelligence. *International Journal of Production Research*, *63*(4), 1174–1202. https://doi.org/10.1080/00207543.2024.2367685

[20] Mageto, J., Twinomurinzi, H., Luke, R., Mhlongo, S., Bwalya, K., & Bvuma, S. (2024). Building resilience into smart mobility for urban cities: An emerging economy perspective. *International Journal of Production Research*, *62*(15), 5556–5573. https://doi.org/10.1080/00207543.2022.2139866

[21] Mehryar, S., Yazdanpanah, V., & Tong, J. (2024). AI and climate resilience governance. *iScience*, *27*(8), Article 109812. https://doi.org/10.1016/j.isci.2024.109812

[22] Mienye, D., Sun, Y., & Ileberi, E. (2024). Artificial intelligence and sustainable development in Africa: A comprehensive review. *Machine Learning with Applications*, *18*, Article 100591. https://doi.org/10.1016/j.mlwa.2024.100591

[23] Mu, W., Kleter, G. A., Bouzembrak, Y., Dupouy, E., Frewer, L. J., Al Natour, F. N. R., & Marvin, H. J. P. (2024). Making food systems more resilient to food safety risks by including artificial intelligence, big data, and internet of things into food safety early warning and emerging risk identification tools. *Comprehensive Reviews in Food Science and Food Safety*, *23*(3), Article e13296. https://doi.org/10.1111/1541-4337.13296

[24] Munn, Z., Pollock, D., Price, C., Aromataris, E., Stern, C., Stone, J. C., Barker, T. H., Godfrey, C. M., Clyne, B., Booth, A., et al. (2023). Investigating different typologies for the synthesis of evidence: A scoping review protocol. *JBI Evidence Synthesis*, *21*(3), 592–600. https://doi.org/10.11124/JBIES-22-00122

[25] Ngulube, P. (2025). Leveraging information and communication technologies for sustainable agriculture and environmental protection among smallholder farmers in tropical Africa. *Discover Environment*, *3*, Article 9. https://doi.org/10.1007/s44274-025-00190-1

[26] Obuseh, E., Eyenubo, J., Alele, J., Okpare, A., & Oghogho, I. (2025). A systematic review of barriers to renewable energy integration and adoption. *Journal of Asian Energy Studies*, *9*, 26–45. https://doi.org/10.24112/jaes.090002

[27] OECD. (2019). *Recommendation of the Council on Artificial Intelligence (OECD AI Principles)*. OECD Publishing.

[28] Ogayemi, A. (2026). From obligation to enforcement: mapping EU AI act and CRA cybersecurity requirements to technical controls for LLM-based autonomous agents. *International Journal of Information Security*, *25*(5), 164.

[29] Ogundiran, O., Nyembwe, J. P. K. B., Ogundiran, J., Ribeiro, A. S. N., & da Silva, M. G. (2025). A Systematic Review of Indoor Environmental Quality in Passenger Transport Vehicles of Tropical and Subtropical Regions. *Atmosphere*, *16*(2), Article 140. https://doi.org/10.3390/atmos16020140

[30] Olaitan, O., Issah, M., & Wayi, N. (2021). A framework to test South Africa's readiness for the fourth industrial revolution. *South African Journal of Information Management*, *23*(1), Article a1284. https://doi.org/10.4102/sajim.v23i1.1284

[31] Peters, M. D. J., Marnie, C., Tricco, A. C., Pollock, D., Munn, Z., Alexander, L., McInerney, P., Godfrey, C. M., & Khalil, H. (2020). Updated methodological guidance for the conduct of scoping reviews. *JBI Evidence Synthesis*, *18*(10), 2119–2126. https://doi.org/10.11124/JBIES-20-00167

[32] Rahman, M. S., Islam, S., & Ridoy, M. J. I. (2026). Perceptions of AI-enabled public health among healthcare professionals: A cross-sectional survey on telemedicine access, disease surveillance, and operational efficiency. *Journal of AI ML DL*, *2*(1), 1–11. https://doi.org/10.25163/ai.2110797

[33] Reichstein, M., Benson, V., Blunk, J., Camps-Valls, G., Creutzig, F., Fearnley, C. J., Han, B., Kornhuber, K., Rahaman, N., Schölkopf, B., et al. (2025). Early warning of complex climate risk with integrated artificial intelligence. *Nature Communications*, *16*, Article 2564. https://doi.org/10.1038/s41467-025-57640-w

[34] Ridoy, M. J. I. (2022). Predicting supply chain resilience with machine learning: A comparative analysis of ensemble and neural approaches across logistics, manufacturing, healthcare, and agriculture. *Journal of Primeasia*, *3*(1), 1–13. https://doi.org/10.25163/primeasia.3110776

[35] Ridoy, M. J. I., & Abdullah, C. A. (2021). AI-driven threat intelligence and cybersecurity performance in US organizations: Examining the roles of adoption, system complexity, and workforce expertise. *Business & Social Sciences*, *1*(1), 1–18. https://doi.org/10.25163/business.1110777

[36] Ridoy, M. J. I., & Akhir, A. (2025). Smart transportation solutions using AI to optimize traffic flow and reduce urban congestion for improved urban mobility. *International Journal on Orange Technologies*, *7*(2), 116–123. https://doi.org/10.31149/ijot.v7i2.5707

[37] Shama, A. T., & Biswas, A. (2023). Cloud misconfiguration as a governance failure in AI-enabled healthcare and finance with privacy risk implications. *International Journal on Economics, Finance and Sustainable Development*, *5*(1), 208–214. https://doi.org/10.31149/ijefsd.v5i1.5799

[38] Singh, S., & Goyal, M. K. (2023). Enhancing climate resilience in businesses: The role of artificial intelligence. *Journal of Cleaner Production*, *418*, Article 138228. https://doi.org/10.1016/j.jclepro.2023.138228

[39] Sun, L., Shawe-Taylor, J., & D'Ayala, D. (2022). Artificial intelligence-informed planning for the rapid response of hazard-impacted road networks. *Scientific Reports*, *12*, Article 16286. https://doi.org/10.1038/s41598-022-19637-z

[40] Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., et al. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. *Annals of Internal Medicine*, *169*(7), 467–473. https://doi.org/10.7326/M18-0850

[41] Ukoba, K., Olatunji, K. O., Adeoye, E., Jen, T. C., & Madyira, D. M. (2024). Optimizing renewable energy systems through artificial intelligence: Review and future prospects. *Energy & Environment*, *35*(7), 3833–3879. https://doi.org/10.1177/0958305X241256293

[42] United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the Ethics of Artificial Intelligence*. United Nations Educational, Scientific and Cultural Organization.

[43] Wanyama, J., Bwambale, E., Kiraga, S., Katimbo, A., Nakawuka, P., Kabenge, I., & Oluk, I. (2024). A systematic review of fourth industrial revolution technologies in smart irrigation: Constraints, opportunities, and future prospects for sub-Saharan Africa. *Smart Agricultural Technology*, *7*, Article 100412. https://doi.org/10.1016/j.atech.2024.100412

[44] Watara, S. A., & Ahmed, Z. (2026). ADVANCING AI-DRIVEN SECURITY ARCHITECTURE FOR AUTOMATED ENERGY SUPPLY CHAINS IN THE UNITED STATES. *Spectrum of Engineering Sciences*, *4*(6), 534-552.

[45] Wu, D., Zheng, A., Yu, W., Cao, H., Ling, Q., Liu, J., & Zhou, D. (2025). Digital twin technology in transportation infrastructure: A comprehensive survey of current applications, challenges, and future directions. *Applied Sciences*, *15*(4), Article 1911. https://doi.org/10.3390/app15041911

[46] Yan, Y., Wang, S., Li, Z., & Chen, X. (2023). Digital twin in transportation infrastructure management. *Infrastructure Journal*, *12*, 145–162. https://doi.org/10.1093/iti/liad024