Journal of Computer Science and Information Technology
ISSN: 3080-3586
DOI: https://doi.org/10.61424/jcsit.v3i2.1048
Date Published Online: September 18, 2026
Journal Homepage: https://bluemarkpublishers.com/index.php/JCSIT

JCSIT
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

Next-Generation Intelligent Systems in Modern Governance: Applications in Healthcare, Smart Mobility, Defense, and Economic Systems

Al Akhir
Business Analytics and Systems, University of Bridgeport, Bridgeport, USA
Corresponding Author: Al Akhir, **E-mail**: alakhir@my.bridgeport.edu

| ABSTRACT
Next-generation intelligent systems are changing the face of governance by combining artificial intelligence, distributed computing, real-time analytics, and adaptive decision-making in healthcare, smart mobility, defence, and economic systems. The study explores key competencies, governance mechanisms, areas of application, deployment practices, performance assessment methods, ethical issues, and future trends of these systems. Specific focus is on lifecycle-based governance, starting with data acquisition, model development, validation, deployment, continuous monitoring, risk assessment, modification, and decommissioning. The core technologies that are believed to enable low-latency, scalable, and context-aware governance are edge intelligence, decentralized computing, knowledge-based technologies, intelligent networking, and high-performance infrastructure. The analysis emphasizes the value of oversight by humans, transparency, accountability, protection of privacy, fair treatment, documentation, local validation, auditing, and compliance with regulations in the context of high-impact applications. Clinical safety, risk classification, post-deployment monitoring, and human override are highlighted by healthcare examples; smart mobility applications showcase the benefits of connected vehicles, IoT sensing, real-time analytics, and adaptive transportation management. Performance evaluation criteria include reliability, latency, fairness, robustness, drift, policy compliance, security, and user-reported incidents, and should be multidimensional. Some challenges that have not been resolved are the lack of transparency around algorithms, the varying quality of the data, the diversity of evaluation metrics, the varying regulations, complex AI ecosystems, and fragmented governance. Standardization of testing, ongoing assurance, stakeholder engagement, adaptive regulation, and international harmonization should continue to be a focus of future governance.

| KEYWORDS

Artificial Intelligence, Intelligent Governance, Healthcare AI, Smart Mobility, Risk Management.

| ARTICLE INFORMATION

ACCEPTED: July 12, 2026 **PUBLISHED:** September 18, 2026 **DOI:** https://doi.org/10.61424/jcsit.v3i2.1048

1. Introduction
Government has become more and more a field in which next-generation intelligent systems are leveraging decision-making, service delivery, public security, and institutional resilience in critical sectors like health care, smart mobility, defense, and economic systems. They are not just about traditional AI applications but about scalable, interconnected systems that can facilitate governance processes across the entire AI lifecycle, from development to validation, approval, deployment, ongoing monitoring, updates, and eventual deprecation [Shama, 2025]. These lifecycle governance methods can ensure intelligent systems are reliable, accountable, and adaptable to changing policy and regulatory needs. One of the key features of these systems is their platform-level and interoperable

designs, which connect diverse computing resources, edge computing, distributed networks, and cutting-edge communication technologies [Abdullah, 2023]. These features allow for low-latency and context-aware processing in dynamic environments where decisions need to be made quickly. In the field of smart mobility, intelligent systems can assist autonomous transportation, traffic control, and real-time monitoring of the infrastructure. They can support clinical decision-making, patient monitoring, resource management, and public health management within the healthcare sector. Threat detection, situational awareness, predictive analysis, and decision support are all areas where defense applications can be helped, and in the economic sector, intelligent forecasting, risk assessment, financial monitoring, and strategic resource management are all areas where economic systems can be supported [Kandeel, 2024]. The convergence of these technologies allows public institutions to respond to the changing and complex conditions more effectively. However, with rising autonomy and complexity of intelligent systems, effective governance is still necessary, as it can present a wide range of technical, ethical, legal, and societal risks. Governance frameworks thus highlight the need to continuously evaluate risks, provide transparency, make clear the interpretability, fairness, and privacy protection, as well as security and accountability, throughout the AI lifecycle [Xiao, 2023]. Data governance is especially relevant due to the fact that the quality, representativeness, and security of data directly affect system performance and can also be a factor in discriminatory or inaccurate results. Mechanisms for monitoring for bias and validating the model, for auditability, for documentation, and for human oversight are thus needed to ensure proper institutional control over automated decision-making. Human-in-the-loop approaches are particularly critical in contexts of high risk where mistakes could impact patient wellbeing, public safety, personal rights, or financial health [He, 2024]. These needs can be fulfilled by intelligent governance platforms that enable them to integrate risk scoring, compliance assessment, real-time alerts, monitoring dashboards, metadata management, and automated audit records. These mechanisms enable organizations to detect performance deterioration, new threats, variance from the model, and bias in the model before they have meaningful impacts. Adaptive and continually learning systems require continuous monitoring, as their behavior may change due to the introduction of new data, operational conditions, or external factors [Zhang, 2025]. Governance, therefore, should not be seen as an approval process, but rather as an ongoing process. Another challenge is regulatory coordination and jurisdictional differences linked to the use of intelligent systems in various governance fields. It's important that healthcare systems are able to find a middle ground between innovation and patient safety, privacy, equity, and accountability to professionals. In smart mobility, decision-making processes must be reliable and transparent, and they have to be safe, infrastructurally sound, and take responsibility for autonomous actions [Li, 2021]. For defense applications, there is a need for a balance of security and operational reliability with proper human control. Economic systems must take care of risks related to financial stability, market integrity, privacy, and unequal access to automated services. Regulations and institutional arrangements may create governance gaps and lead to variations across these areas. Harmonized risk assessment procedures, measurable auditing practices, standardized documentation, and ongoing regulatory monitoring are thus becoming more important [Taha, 2025]. Overall, next-generation intelligent systems mark a shift from stand-alone AI applications to more comprehensive governance systems that can assist in complex public and economic activities. The successful application of their implementation depends on a combination of technological capability, operational efficiency, human oversight, ethical responsibility, and regulatory compliance.

2. Core Capabilities, Governance Principles, and Operational Governance Mechanisms

Next-generation intelligent systems for governance applications combine high-end computing, intelligent networking, all-the-time monitoring, and adaptive decision-making with the aim of enabling critical sectors like health care, smart mobility, defense, and economic systems [Abdullah, 2025]. They have the primary functions of distributed intelligence, real-time processing, adaptive resource management, continuous risk assessment, and human-centered oversight. These systems can operate in an ultra-low-latency and context-aware manner by leveraging edge intelligence and decentralized computing, thereby minimizing reliance on centralized cloud infrastructure. This prioritisation of essential tasks can also be supported by advanced communication technologies, such as network slicing and emerging 6G technologies, in situations where connectivity may be limited or when there is high demand. For autonomous navigation, clinical decision support, traffic management, defense analytics, and other applications that demand quick responses, such architectures are beneficial [Cai, 2019]. The process is basically a cycle of data gathering, local processing, task allocation, centralized or distributed processing, decision making, monitoring, and feedback-based adaptation. Edge nodes handle tasks that require immediate analysis, and cloud infrastructure is always available for tasks that are more complex or centralized. Intelligent orchestration can dynamically decide where and how to process the task, based on network conditions, the urgency of the task, computational needs, and available resources [Shama, 2023]. Changing operational conditions are addressed by adaptive routing and resource allocation, which ensure service quality. Alternative communication methods could also be implemented to maintain essential functions in the event that network connectivity is unreliable. This continuous operating loop enables intelligent systems to adapt their behavior based on modifications in data, environmental conditions, system performance, and governance requirements. Another basic functionality is real-time monitoring (Table 1) [Nguyen, 2022]. Data quality, model performance, system behavior, and potential biases are continually monitored, giving an early warning mechanism for emerging risks. If degradation, anomalies, or inequitable results are identified, then corrective measures can be taken, which might include retraining, recalibration, audit, or temporary intervention. The use of this approach is especially relevant to systems deployed across a variety of populations and environments, as initial system performance can vary across time [Salman, 2022]. The responsibility of human supervisors is not just to keep the automated tools running, but also to review and assess system performance, analyze important findings, take corrective action as needed, and make sure that the automated decision is consistent with safety and ethical standards. Intelligent computing, continuous monitoring, adaptive orchestration, human oversight, lifecycle management, and accountable governance are all important to the effective operation of next-generation intelligent systems [Rahman, 2024]. The operating loop should link the technical processes with organizational and regulatory controls to continually assess the performance of the system, its safety, fairness, and compliance. This allows for the use of sophisticated AI functions in healthcare, smart mobility, defence, and economic systems without compromising public welfare, individual rights, institutional accountability, and societal trust.

Table 1. Core Governance and Operational Mechanisms for Next Generation Intelligent Systems

Governance component	Key mechanisms	Application across sectors	Reference
AI lifecycle governance	Model development, validation, deployment, continuous monitoring, modification, and decommissioning	Healthcare, smart mobility, defense, and economic systems	[1,2]
Risk management	Risk scoring, data quality assessment, fairness assessment, red teaming, adversarial testing, and risk based controls	High risk and regulated AI applications	[8,22]
Human oversight	Human in the loop decision making, override mechanisms, escalation procedures, and supervisory controls.	Clinical decision support, autonomous mobility, defense analytics	[5,9]
Transparency and accountability	Documentation, audit trails, validation summaries, monitoring records, incident reports, and change control	Public sector and high impact AI systems	[11,24]
Data governance and privacy	Data minimization, federated learning, differential privacy, access control, and secure data stewardship	Healthcare, finance, public services, and economic systems	[1,11]
Continuous monitoring	Drift detection, bias monitoring, performance alerts, anomaly detection, and real time dashboards	Operational AI systems requiring continuous assurance	[2,6]
Regulatory alignment	Regulatory surveillance, compliance assessment, cross jurisdictional coordination, and adaptive controls	Multinational and highly regulated AI environments	[10,11]

3. Application Domains, Enabling Technologies, and Policy and Regulatory Landscape

In various critical governance areas such as healthcare, smart mobility, defense, public services, and economic systems, next-generation intelligent systems are being deployed. To ensure governance, their entire AI lifecycle should incorporate risk management, resilience, accountability, and regulatory oversight [Shama, 2024]. Healthcare governance focuses on a focus on clinically supervised AI systems that link research, deployment, and patient care with a systematic inventory, validation, monitoring, documentation, and incident management. This approach is conducive to patient safety and clinical accountability while acknowledging that risks associated with AI involve more than just the technologies themselves, but are also caused by interactions between technologies, people, organizational processes, and operational contexts [Ridoy, 2025]. Governance is gradually moving from a traditional, one-off service delivery approach to a service-oriented approach with continuous improvement, risk management in advance, and shared responsibility, which is more prevalent in all application domains. These methods aim to leverage automation and service distribution while ensuring accountability through ongoing governance and multi-functional accountability for decisions and results related to the use of AI [Istepanian, 2018]. For instance, transparency, explainability, consumer protection, and periodic auditing are highlighted in financial systems to ensure that automated decisions have meaningful explanations and are accountable. Other tools include algorithmic auditing, controlled testing, and evaluation of intelligent systems under realistic conditions in the context of regulatory sandboxes and policy-based governance [Selna, 2022]. The scope of intelligent governance is not limited to healthcare and finance, but includes all aspects of public service transformation, smart mobility, defense, and economic systems. AI can be integrated at every phase of research, development, deployment, and operation on integrated platforms, along with validation, runtime control, monitoring, and documentation. This enables organisations to ensure transparency, regulatory compliance, deployment readiness, safety, and reliability in various environments (Table 2) [Hu, 2025]. Overall, the goal is to make sure technological innovation is useful for the public good and effective institutions and to not undermine accountability or public trust. Cross-medium analytical reasoning is the further reinforcement of such capabilities, which is realized through the combination of unified indicators, relational understanding, knowledge mining, construction of a knowledge map, knowledge evolution, inference, intelligent description, and generation. These technologies, in conjunction with verification systems and special analytical engines, enable intelligent systems to find relationships and insights in various information types [Gardašević, 2020]. This is especially important in the governance context where decisions might be based on heterogeneous data from several institutions, platforms, and operational contexts. The development of intelligent information infrastructure is also a prerequisite for the development of smart economies, intelligent societies, and national security. The infrastructure includes the transmission of information, storage of data, computing and processing power, enhanced network capacities, Internet of Things infrastructure, low-latency communication, throughput, data security and privacy [Baker, 2017]. These capabilities deliver the backbone for computing and communications for large-scale AI applications in healthcare, mobility, defense, and economic systems. Other infrastructure for intelligent governance are high performance computing, distributed energy networks, intelligent energy storage, and responsive energy supply systems. These technologies can help match the demand for computing with the available resources in real time, providing scalable AI services and resilient operations [Balasundaram, 2023]. In the healthcare sector and smart mobility, disruptions to services can have a serious impact on service continuity and public safety, making reliable computing and energy infrastructures even more critical to applications (Figure 1). With advanced knowledge, computing technology, risk-based governance, measurable oversight, and flexible regulatory processes, intelligent systems can be used to enhance public service capabilities, economic resilience, safety, and national capabilities, and retain public trust.

Figure 1. Key technologies toward smart healthcare systems based on IoT [Lakshmi, 2025]

Table 2. Application Areas, Performance Measures, and Governance Priorities

Application domain	Major AI applications	Key performance and governance measures	Principal governance priorities	Reference
Healthcare	Clinical decision support, patient risk prediction, medical analytics, patient monitoring	Accuracy, fairness, model drift, clinical safety, human override, incident rate	Patient safety, clinical validation, privacy, explainability, regulatory compliance	[9,17,31,32]
Smart mobility	Autonomous vehicles, intelligent traffic management, fleet optimization, connected transportation	Latency, task failure rate, traffic efficiency, safety events, network reliability	Human supervision, infrastructure coordination, real time monitoring, public safety	[4,37,38]
Economic systems	Financial decision support, fraud detection, risk assessment, automated services	Fairness, explainability, policy violation rate, anomaly rate, accuracy	Consumer protection, transparency, nondiscrimination, auditability	[11,15]
Public governance	Automated decision making, public service optimization, eligibility assessment	Bias, transparency, auditability, incident frequency, compliance	Accountability, fairness, redress, stakeholder participation	[11,14]
Cross domain AI infrastructure	Edge computing, distributed intelligence, knowledge computing, real time analytics	Processing time, network latency, scalability, resource efficiency	Security, interoperability, resilience, data governance	[4,18,19]

4. Case Studies and Performance Evaluation

Multiple cross-domain studies and case studies of actual deployments illustrate the application of next-generation intelligent systems into governance structures in healthcare, smart mobility, defense, and economic systems [Ijaz, 2015]. The applications demonstrate that the engagement of more than technical know-how is required to be successful. Structured governance, risk assessment, human oversight, continuous monitoring, regulatory compliance, and measurable performance evaluation must also be part of the systems. Healthcare organizations place a particular importance on the necessity of comprehensive and coherent AI governance frameworks that can be customized to meet the needs of organizations of varying resources, knowledge, and institutional capacity [Ridoy, 2021]. There are already frameworks and methodologies available for assessing the level of readiness for implementing AI governance in healthcare organizations, which have been created to recognize readiness and resolve the drawbacks of resource-heavy governance structures. There must be a clear governance process in place prior to and following healthcare deployment. Prior to deployment, an assessment should be conducted to determine if a system is clinically, technically, ethically, and organizationally ready for deployment [Sikdar, 2020]. Risk Acceptance processes should specify who can approve deployment and when. When deployed, ongoing monitoring should evaluate the performance, fairness, data quality, and model drift. Escalation mechanisms should be clearly defined to enable human intervention if there is a significant deviation, correction, temporary suspension, or additional validation. Healthcare risk management should also integrate AI tools with current regulatory frameworks and clinical processes and have a robust documentation system and post-deployment monitoring system [Khan, 2025]. For systems that offer patient-specific recommendations or clinical decision support, regulatory classification should be of special interest for healthcare systems. These systems can have evolving requirements, depending on their function and level of risk, for clinical decision support software or software used as a medical device. Governance must then be documented, risk classified, validated, and have a human override that is clearly defined. Machine learning governance for operations should also include ensuring validated models are kept on track to support organisational and regulatory goals and outputs are linked to actionable clinical and operational outcomes [Qi, 2025]. Collecting and retaining centralized evidence, model lineage, and approval logs, along with runtime monitoring, can help ensure that the system stays safe and responsible all the way through its life cycle. The deployment and long-term reliability of intelligent systems for modern governance requires a solid framework of continuous measurement, documented assurance, and clearly defined mechanisms for intervention.

5. Governance, Risk Management, Ethics, and Future Directions

Integrated governance, risk management, and assurance activities throughout the AI lifecycle are critical for responsible deployment of next-generation intelligent systems. Organizations should have a clearly defined risk management flow, including who is responsible for data quality, what criteria should trigger monitoring, what the criteria should be for remediation, and what the data quality requirements are. Data quality assessment, input validation, red teaming, adversarial testing, fairness assessment, and data leakage and unintended exposure are aspects of pre-deployment and operational assurance [Shama, 2025]. These activities help to detect technical, security, and ethical vulnerabilities before they can have meaningful consequences. Governance mechanisms should also cover incident response, vendor escalation, and rollback for systems that fail the validation or create unacceptable risks once deployed. Learning from incidents should be fed into the next risk assessment, governance controls, system changes and organisational practice – making assurance a process of continual learning. While there is increasing awareness of the importance of "trusted" AI, there are still considerable problems in measurement of and assurance for intelligent systems [Khalid, 2025]. One of the key challenges posed by this is the absence of a common set of metrics for evaluating applications in different organizations and application areas (Figure 2). The definitions, thresholds, and assessment procedures may vary across systems, making them difficult to compare and making it difficult to have a consistent expectation for safety, fairness, and reliability. Manual evaluation can also be labor-intensive and limit the scope of governance activities. Difficulties in fragmented development processes arise when responsibilities and evidence are spread out among several teams, and establish single points of accountability for the entire lifecycle of the development process [Xie, 2025]. Some additional issues are poor data quality, synthetic data risks, disjointed governance, and the lack of practical tools and resources for good bias mitigation. Therefore, the need for continuous, automated, and transparent evaluation becomes more and more relevant for building scalable and trustworthy AI governance systems. In governance-intensive applications like economic systems, defense, smart mobility, and healthcare, ethical issues are especially important. The key issues of accountability, fairness, transparency, privacy, and potential disparate impacts on individuals and population groups are central [Ridoy, 2025]. Algorithmic audits and algorithmic impact assessments may be used to understand and prevent harms before deployment and to track harms during operation. These kinds of evaluations can be conducted on systems that are utilized for eligibility, fraud and risk detection, public services, security applications, and other consequential decision-making systems.

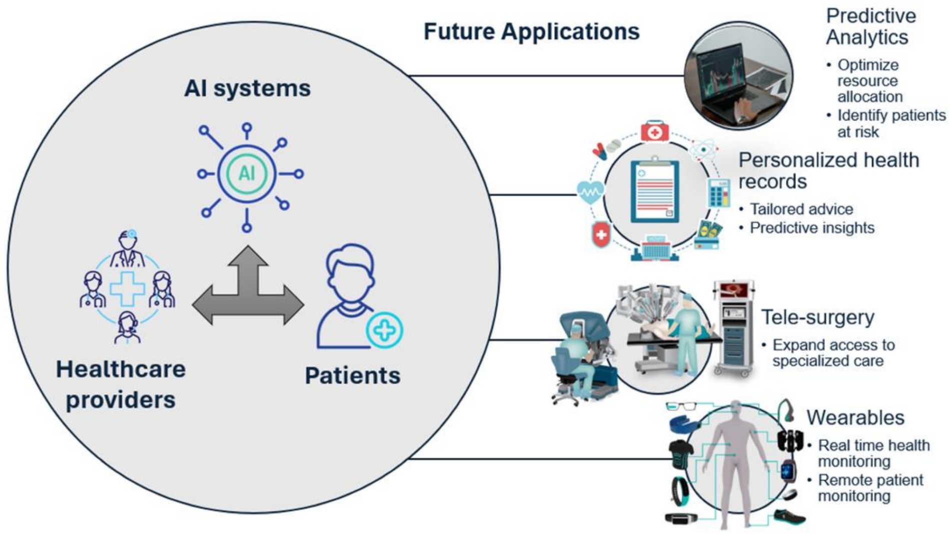

Figure 2. Integration of AI systems, healthcare providers, and patients to enable future applications [Selem, 2025]

6. Discussion

Modern governance is experiencing a transformation, as next-generation intelligent systems are incorporating artificial intelligence, distributed computing, real-time analytics, and ongoing risk management into critical public and economic activities [Zhou, 2025]. In all sectors such as health, smart mobility, defence, and the economy, the added value of these technologies is not just in automation but in their facilitation of complex decision-making, enhanced service provisioning, increased resilience, and adaptation to rapidly changing operational conditions. The analysis shown in this study suggests that successful deployment is achieved through the integration of technical capabilities with governance, human oversight, regulatory compliance, and ongoing assurance. Intelligent systems, then, must be regarded as sociotechnical infrastructures and not just computational tools [Pham, 2025]. This includes a fundamental shift from single AI applications to platform-level governance architectures, running through the entire lifecycle of the system. While traditional methods largely focused on model development and deployment, next-generation governance put forth the idea that the process involves ongoing monitoring, validation, and model modification or retirement. This lifecycle approach is especially crucial as data distributions, operational environments, and user interactions evolve, which may result in changes to AI behaviors [Magara, 2024]. Reliability is therefore needed following deployment and requires continuous monitoring of model drift, data quality, fairness, security, and performance. The governance process is not just an approval process, but it is an assessment and adaptation process. These systems are also supported by a technical architecture that significantly influences their governance capabilities. Edge Intelligence and Decentralized Computing enable processing of time-sensitive information near its source, minimizing latency and reliance on centralized cloud systems [Hossain, 2024]. This matters especially for autonomous mobility, clinical decision support, defense analytics, and any applications with potentially severe repercussions for delayed responses. Distributed architectures can also enhance resilience in situations where connectivity is scarce or network demand is great. The dynamic allocation of tasks among edge nodes, vehicles, and cloud services can be accomplished based on the processing needs, network conditions, and task urgency through intelligent orchestration [Zhao, 2010]. These functions make up an operating cycle that involves the collection, processing, analysis, action, and continual adaptation of data. But it is not enough to have high-tech solutions to be a good governor. The more autonomous and adaptive an intelligent system is, the more it requires of human authority to be clearly defined. In no way should human oversight be seen as a person standing close to an automated system. Effective supervision involves having the right skills, knowledge, access, and powers to intervene and having clear escalation protocols [Al-Sanjary, 2019]. For instance, in healthcare, doctors need to grasp the constraints of the AI's recommendations and take action when the AI suggests a course of action that contradicts clinical evidence or a patient's situation. The same applies to autonomous mobility, defense, and economic systems, where automated decisions could influence public safety, security, or economic returns. Therefore, human in the loop (HITL) governance is most effective when it is accompanied by institutional processes and not just seen as a technical control. Another core issue of intelligent governance is the ability to manage risk [Cui, 2024]. The reviewed material highlights the need to move from a reactive to a proactive approach for risk identification and mitigation. Vulnerabilities can be found before they cause loss of life via data quality checks, input thresholds, fairness assessments, leakage detection, red teaming, adversarial testing, and continuous performance monitoring. Risk scoring can also offer an organization a framework to prioritize governance efforts by system impact and operating conditions [Ridoy, 2022]. The level of effort spent on validation, monitoring, audit, and review should be greater for high-risk applications than for systems where consequences are limited. This proportional approach enables governance resources to be focused on those areas that may cause the most damage if they fail. The healthcare sector is a good example of how this can be implemented. In the healthcare sector, AI could be used to assist in diagnosis, clinical decisions, patient monitoring, resource management, and more [Taware, 2025]. Their governance needs to therefore link technical validation to clinical workflows, patient safety, documentation, and regulatory requirements. Organizations can use readiness assessment to see if they have the institutional capacity to deploy AI responsibly. Other protections include pre-deployment gates, risk acceptance procedures, fairness evaluation, drift detection, and post-market monitoring. Importantly, the granting of regulatory clearance is not a substitute for suitability. Local validation is still required, as a system which works well in one population, institution, or operational setting may not work the same in another. Smart mobility is a counterpoint but complementary example. ITS harnesses the power of AI, IoT networking, connected vehicles, and real-time data analysis to enhance traffic flow, route optimization, fleet management, and regional connectivity [Kumar, 2025]. The implementation of autonomous and semi-autonomous fleet systems can be one way to enhance efficiency in high-volume logistics operations, and intelligent traffic management can help to alleviate congestion and enhance transportation coordination. The Greater Bay Area provides examples of deployment, including connected and automated vehicles, real-time sensing, and cross-border coordination for regional mobility. However, they need to be phased in, with public and private coordination, remote supervision, and local adaptation to the infrastructure and regulatory environment [Du, 2025]. In the context of mobility governance, this shows that intelligent automation has to be co-located with physical infrastructure and human responsibility. Fragmentation of regulation is another big hurdle. The rules for AI governance depend on the jurisdiction, and an intelligent system can be active in multiple jurisdictions at once. Governance gaps can exist based on differing needs for privacy, safety, transparency, nondiscrimination, cybersecurity, and automated decision-making [Ibrahim, 2025]. To solve this issue, risk-based approaches to regulation have been developed, whereby higher obligations are imposed on systems with higher potential to cause harm. But continuously learning AI systems bring challenges to traditional approval processes, as their behavior could change over time after approval or deployment. Compliance has to be ensured throughout the operational life of the system; regulatory monitoring and adaptive governance are therefore needed [Wang, 2025]. Patient safety and clinical validation are key aspects of healthcare; AI and physical infrastructure must be coordinated for smart mobility; robust security and human control are crucial in defense; and transparency, fairness, and consumer protection in economic systems.

7. Conclusion

Next-generation intelligent systems can substantially strengthen modern governance by improving decision-making, service delivery, resilience, and operational efficiency across healthcare, smart mobility, defense, and economic systems. Their responsible deployment requires more than technical performance, demanding continuous risk assessment, human oversight, transparency, privacy protection, and regulatory alignment throughout the AI lifecycle. Effective governance should integrate local validation, documentation, auditing, performance monitoring, and adaptive controls to address emerging risks. Future progress will depend on standardized evaluation, stakeholder participation, interoperable governance frameworks, and internationally aligned policies. A balanced approach can support technological innovation while protecting safety, fairness, accountability, and public trust.

Author Contributions

A.A. conceived the study, conducted the literature review, analyzed and synthesized the relevant literature, and drafted, revised, and approved the final manuscript.

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. and Ridoy M. J. I., (2023) Artificial intelligence-driven cyber threat detection for protecting critical digital infrastructure, *Innov.: Int. Multidiscipl. J. Appl. Technol.*, vol. 1, no. 2, pp. 76–83, 2023, doi: 10.51699/zb8kwv06.
[2] Abdullah C. A. and Ridoy M. J. I., (2025) Artificial intelligence driven infrastructure security enhancing cybersecurity and protecting national security systems, *J. Technol. Sci.*, vol. 1, no. 3, pp. 191–200, 2025, doi: 10.61796/ipteks.v1i3.498.
[3] Al-Sanjary O. I., Vasuthevan S., Omer H. K., Mohammed M. N., and Abdullah M. I., (2019) An Intelligent Recycling Bin Using Wireless Sensor Network Technology, in *Proc. 2019 IEEE Int. Conf. Autom. Control Intell. Syst. (I2CACIS)*, Selangor, Malaysia, 2019, pp. 30–33, doi: 10.1109/I2CACIS.2019.8825044.
[4] Baker S. B., Xiang W., and Atkinson I., (2017) Internet of things for smart healthcare: Technologies, challenges, and opportunities, *IEEE Access*, vol. 5, pp. 26521–26544, 2017, doi: 10.1109/ACCESS.2017.2775180.
[5] Balasundaram A., Routray S., Prabu A., Krishnan P., Malla P. P., and Maiti M., (2023) Internet of things (IoT)-based smart healthcare system for efficient diagnostics of health parameters of patients in emergency care, *IEEE Internet Things J.*, vol. 10, pp. 18563–18570, 2023, doi: 10.1109/JIOT.2023.3246065.
[6] Cai Q., Wang H., Li Z., and Liu X., (2019) A survey on multimodal data-driven smart healthcare systems: Approaches and applications, *IEEE Access*, vol. 7, pp. 133583–133599, 2019, doi: 10.1109/ACCESS.2019.2941419.
[7] Cui Q., Ding Z., and Chen F., (2024) Hybrid Directed Hypergraph Learning and Forecasting of Skeleton-Based Human Poses, *Cyborg Bionic Syst.*, vol. 5, Art. no. 0093, 2024, doi: 10.34133/cbsystems.0093.
[8] Du M., Li Z., Bian L., Randriamahazaka H., and Chen W., (2025) Two-dimensional materials van der Waals assembly enabling scalable smart textiles, *Mater. Sci. Eng. R Rep.*, vol. 163, Art. no. 100915, 2025, doi: 10.1016/j.mser.2024.100915.
[9] Gardašević G., Katzis K., Bajić D., and Berbakov L., (2020) Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare, *Sensors*, vol. 20, Art. no. 3619, 2020, doi: 10.3390/s20133619.
[10] He W., Zhu J., Feng Y., Liang F., You K., Chai H., and Wang W., (2024) Neuromorphic-enabled video-activated cell sorting, *Nat. Commun.*, vol. 15, Art. no. 10792, 2024, doi: 10.1038/s41467-024-55094-0.
[11] Hossain M. K. and Thakur V., (2024) A performance management framework for smart health-care supply chain based on Industry 4.0 technologies, *J. Glob. Oper. Strateg. Sourc.*, vol. 18, pp. 285–306, 2024, doi: 10.1108/JGOSS-12-2022-0123.
[12] Hu F., Yang H., Qiu L., Wei S., Hu H., and Zhou H., (2025) Spatial structure and organization of the medical device industry urban network in China: Evidence from Specialized, Refined, Distinctive, and Innovative firms, *Front. Public Health*, vol. 13, Art. no. 1518327, 2025, doi: 10.3389/fpubh.2025.1518327.
[13] Ibrahim Y., Abdel-Malek M. A., Azab M., and Rizk M. R., (2025) Privacy-preserved mutually-trusted 5G communications in presence of pervasive attacks, *Internet Things*, vol. 30, Art. no. 101491, 2025, doi: 10.1016/j.iot.2025.101491.
[14] Ijaz M., Li G., Wang H., El-Sherbeeny A. M., Moro A Y., Lin L., Koubaa A., and Noor A., (2015) Intelligent fog-enabled smart healthcare system for wearable physiological parameter detection, *Electronics*, vol. 9, Art. no. 2015, 2020, doi: 10.3390/electronics9122015.
[15] Istepanian R. S. and Al-Anzi T., (2018) m-Health 2.0: New perspectives on mobile health, machine learning and big data analytics, *Methods*, vol. 151, pp. 34–40, 2018, doi: 10.1016/j.ymeth.2018.05.015.
[16] Kandeel M., (2024) Revolutionizing Healthcare: Harnessing the Power of Artificial Intelligence for Enhanced Diagnostics, Treatment and Drug Discovery, *Int. J. Pharmacol.*, vol. 20, pp. 1–10, 2024, doi: 10.3923/ijp.2024.1.10.
[17] Khalid U., Chen L., Khan A. A., Chen B., Mehmood F., and Yasir M., (2025) A smart facial acne disease monitoring for automate severity assessment using AI-enabled cloud-based internet of things, *Discov. Comput.*, vol. 28, Art. no. 12, 2025, doi: 10.1007/s10791-025-09503-7.
[18] Khan M. and Hossni Y., (2025) A comparative analysis of LSTM models aided with attention and squeeze and excitation blocks for activity recognition, *Sci. Rep.*, vol. 15, Art. no. 3858, 2025, doi: 10.1038/s41598-025-88378-6.
[19] Kumar A., Gupta R., Kumar S., Dutta K., and Rani M., (2025) Securing IoMT-based healthcare system: Issues, challenges, and solutions, in *Artificial Intelligence and Cybersecurity in Healthcare Cyber Physical Systems*, R. Agrawal, P. S. Rathore, G. G. Devarajan, and R. R. Divivedi, Eds. Beverly, MA, USA: Scrivener Publishing LLC, 2025, pp. 17–56, doi: 10.1002/9781394229826.ch2.
[20] Lakshmi S. G., Lalitha C. N., Lavanya S., Vijaya L. S., and Sri-Lakshmi P. S., (2025) IOT-enabled cloud solutions for reliable health monitoring, in *Emerging Trends in Computer Science and Its Application*, Boca Raton, FL, USA: CRC Press, 2025, pp. 278–282, doi: 10.1201/9781003606635-45.

[21] Li W., Chai Y., Khan F., Jan S. R. U., Verma S., Menon V. G., Kavita F., and Li X., (2021) A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system, *Mob. Netw. Appl.*, vol. 26, pp. 234–252, 2021, doi: 10.1007/s11036-020-01700-6.

[22] Magara T. and Zhou Y., (2024) EMAKAS: An efficient three-factor mutual authentication and key-agreement scheme for IoT environment, *Cyber. Secur. Appl.*, vol. 3, Art. no. 100066, 2025, doi: 10.1016/j.csa.2024.100066.

[23] Nguyen D. C., Pham Q.-V., Pathirana P. N., Ding M., Seneviratne A., Lin Z., Dobre O., and Hwang W.-J., (2022) Federated learning for smart healthcare: A survey, *ACM Comput. Surv.*, vol. 55, pp. 1–37, 2022, doi: 10.1145/3501296.

[24] Pham T. P. T. and Huang M. C., (2025) Exploring the relationship between nursing professional values and job satisfaction in Vietnam, *Nurs. Pract. Today*, vol. 12, no. 1, pp. 55–64, 2025, doi: 10.18502/npt.v12i1.17525.

[25] Qi K., (2025) Advancing hospital healthcare: Achieving IoT-based secure health monitoring through multilayer machine learning, *J. Big Data*, vol. 12, Art. no. 1, 2025, doi: 10.1186/s40537-024-01038-w.

[26] Rahman A., Debnath T., Kundu D., Khan M. S. I., Aishi A. A., Sazzad S., Sayduzzaman M., and Band S. S., (2024) Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities, *AIMS Public Health*, vol. 11, Art. no. 58, 2024, doi: 10.3934/publichealth.2024004.

[27] Ridoy M. J. I. and Abdullah C. A., (2021) AI-driven threat intelligence and cybersecurity performance in US organizations: Examining the roles of adoption, system complexity, and workforce expertise, *Bus. Soc. Sci.*, vol. 1, no. 1, 1–8, 2021, doi: 10.25163/business.1110777.

[28] Ridoy M. J. I. and Akhir A., (2025) Smart transportation solutions using AI to optimize traffic flow and reduce urban congestion for improved urban mobility, *Int. J. Orange Technol.*, vol. 7, no. 2, pp. 116–123, 2025, doi: 10.31149/ijot.v7i2.5707.

[29] Ridoy M. J. I. and Islam A., (2025) Integrating machine learning into financial systems to improve risk management and economic stability, *J. Knowl. Learn. Sci. Technol.*, vol. 4, no. 4, pp. 119–126, 2025, doi: 10.60087/jklst.vol4.n4.013.

[30] 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, *J. Primeasia*, vol. 3, no. 1, pp. 1–8, 2022, doi: 10.25163/primeasia.3110776.

[31] Salman M., Munawar H. S., Latif K., Akram M. W., Khan S. I., and Ullah F., (2022) Big data management in drug-drug interaction: A modern deep learning approach for smart healthcare, *Big Data Cogn. Comput.*, vol. 6, Art. no. 30, 2022, doi: 10.3390/bdcc6010030.

[32] Selem M., Jemili F., and Korbaa O., (2025) Deep learning for intrusion detection in IoT networks, *Peer-Peer Netw. Appl.*, vol. 18, Art. no. 22, 2025, doi: 10.1007/s12083-024-01819-3.

[33] Selna A., Othman Z., Tham J., and Yoosuf A. K., (2022) Challenges to using electronic health records to enhance patient safety, in a Small Island Developing State (SIDS) context, *Rec. Manag. J.*, vol. 32, pp. 249–259, 2022, doi: 10.1108/RMJ-03-2022-0008.

[34] Shama A. T. and 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*, vol. 5, no. 1, pp. 208–214, 2023. doi: 10.31149/ijefsd.v5i1.5799.

[35] Shama A. T., (2024) Third-Party Risk Management in API-Driven Ecosystems: Continuous Vendor Security Practices and Emerging Challenges, *American Journal of Technology Advancement*, vol. 1, no. 4, pp. 42–50, 2024. doi: 10.31149/ajta.v1i4.4322.

[36] Shama A. T., (2025) AI Governance Challenges in Banking: Model Explainability, Regulatory Compliance, and the Limits of Traditional Risk Management, *Business and Social Sciences*, vol. 3, no. 1, pp. 1–10, 2025. doi: 10.25163/business.3110901.

[37] Shama A. T., (2025) AI Governance Challenges in Banking: Model Explainability, Regulatory Compliance, and the Limits of Traditional Risk Management, *Business and Social Sciences*, vol. 3, no. 1, pp. 1–10, 2025. doi: 10.25163/business.3110901.

[38] Sikdar S. and Guha S., (2020) Advancements of healthcare technologies: Paradigm towards smart healthcare systems, in *Recent Trends Image Signal Process. Comput. Vis.*, vol. 1124, pp. 113–132, 2020, doi: 10.1007/978-981-15-2740-1_9.

[39] Taha K., (2025) Big Data Analytics in IoT, social media, NLP, and information security: Trends, challenges, and applications, *J. Big Data*, vol. 12, Art. no. 150, 2025, doi: 10.1186/s40537-025-01192-9.

[40] Taware R. D., Deshmukh A., Singh C., and Rathod N., (2025) Magnitude of data science & big data in fitness care, *AIP Conf. Proc.*, vol. 3162, Art. no. 020020, 2025, doi: 10.1063/5.0243796.

[41] Wang W., Bo X., Li W., Eldaly A. B. M., Wang L., Li W. J., Chan L. L. H., and Daoud W. A., (2025) Triboelectric Bending Sensors for AI-Enabled Sign Language Recognition, *Adv. Sci.*, vol. 12, Art. no. 2408384, 2025, doi: 10.1002/advs.202408384.

[42] Xiao X., Li Y., Wu Q., Liu X., Cao X., Li M., and Dai X., (2025) Development and validation of a novel predictive model for dementia risk in middle-aged and elderly depression individuals: A large and longitudinal machine learning cohort study, *Alzheimer's Res. Ther.*, vol. 17, Art. no. 103, 2025, doi: 10.1186/s13195-025-01750-6.

[43] Xie Q. and Ding Z., (2025) Provably secure and lightweight blockchain based cross hospital authentication scheme for IoMT-based healthcare, *Sci. Rep.*, vol. 15, Art. no. 6461, 2025, doi: 10.1038/s41598-025-90219-5.

[44] Zhang G., Song C., Yin M., Liu L., Zhang Y., Li Y., and Li C., (2025) TRAPT: A multi-stage fused deep learning framework for predicting transcriptional regulators based on large-scale epigenomic data, *Nat. Commun.*, vol. 16, Art. no. 3611, 2025, doi: 10.1038/s41467-025-58921-0.

[45] Zhao X. and Ge B., (2010) An indicator framework for assessing the readiness of hospital in the smart healthcare transformation, *IOP Conf. Ser. Earth Environ. Sci.*, vol. 1101, Art. no. 072010, 2022, doi: 10.1088/1755-1315/1101/7/072010.

[46] Zhou Z., Jin Y., Fu J., Si S., Liu M., Hu Y., Gan J., Deng Y., Li R., and Yang J., (2025) Smart wireless flexible sensing system for unconstrained monitoring of ballistocardiogram and respiration, *npj Flex. Electron.*, vol. 9, Art. no. 15, 2025, doi: 10.1038/s41528-025-00388-6.