Science, Society and Policy Research

https://socsci-policy.science

Evaluating Compliance Readiness with Responsible AI Regulation in Financial Technology Firms

Yan-Tung Ip*, Carol Lee

School of Journalism and Communication, Chinese University of Hong Kong, Hong Kong, Hong Kong SAR, China

Corresponding author: yan.t.ip@cuhk.edu.hk

Abstract

The rapid integration of artificial intelligence within the financial technology sector has necessitated the development of rigorous regulatory frameworks aimed at ensuring ethical, transparent, and fair algorithmic decision-making. This paper provides a comprehensive evaluation of compliance readiness among financial technology firms through the application of difference analysis. As regulatory bodies globally transition from voluntary ethical guidelines to binding legal mandates, organizations face significant operational and technical challenges in aligning their existing technological infrastructures with emerging responsible artificial intelligence regulations. By utilizing difference analysis, this study systematically maps current institutional practices against anticipated regulatory requirements, identifying critical discrepancies in areas such as algorithmic transparency, bias mitigation, and automated accountability mechanisms. The findings reveal a persistent gap between high-level policy commitments and granular technical implementation, particularly regarding the interpretability of complex machine learning models utilized in credit scoring and algorithmic trading. Furthermore, this research highlights systemic vulnerabilities in data governance protocols that impede comprehensive compliance. The insights derived from this analysis provide actionable strategies for financial technology firms to proactively re-engineer their compliance architectures. Ultimately, this paper contributes to the broader academic discourse on regulatory technology by establishing a standardized methodological framework for quantifying compliance readiness in rapidly evolving regulatory landscapes.

Keywords: Responsible Artificial Intelligence; Difference Analysis; Financial Technology; Regulatory Compliance; Algorithmic Transparency

1. Introduction

1.1 The Rise of Artificial Intelligence in Financial Technology

The financial technology ecosystem has undergone a profound transformation over the past decade, driven largely by the exponential advancement and deployment of artificial intelligence and machine learning technologies. Traditional financial institutions and agile technology startups alike have leveraged these sophisticated computational models to optimize a wide array of operational processes, ranging from automated customer service and fraud detection to high-frequency algorithmic trading and dynamic credit risk assessment [1]. The utilization of complex neural networks, natural language

processing algorithms, and ensemble learning techniques has enabled these firms to extract actionable insights from vast, unstructured datasets at unprecedented speeds. Consequently, artificial intelligence has become the foundational infrastructure upon which modern financial services are built, offering unparalleled efficiency, hyper-personalization, and predictive accuracy [2].

However, the pervasive integration of these technologies has also introduced a novel class of systemic risks into the global financial architecture. The inherent complexity and opacity of advanced machine learning models, often described as black boxes, pose significant challenges to traditional mechanisms of financial oversight and risk management [3]. In applications such as credit scoring, the inability to clearly articulate the rationale behind an algorithmic decision can lead to severe socioeconomic consequences, including the perpetuation of historical biases and the systematic disenfranchisement of vulnerable demographic groups [4]. Furthermore, the financial sector is inherently sensitive to systemic shocks; the deployment of correlated algorithmic trading strategies across multiple institutions can amplify market volatility and precipitate cascading liquidity crises. As these risks become increasingly apparent, stakeholders across the financial ecosystem are recognizing that the unconstrained proliferation of artificial intelligence is fundamentally incompatible with the principles of financial stability and consumer protection [5].

1.2 The Imperative of Responsible AI Regulation

In response to the multifaceted risks associated with algorithmic deployment, international regulatory bodies and national legislative assemblies have initiated comprehensive efforts to establish binding frameworks for responsible artificial intelligence. These regulatory paradigms aim to enforce strict standards regarding algorithmic transparency, fairness, accountability, and data privacy [6]. Unlike previous waves of digital regulation, which primarily focused on data protection and cybersecurity, emerging responsible artificial intelligence regulations directly target the internal mechanics of algorithmic decision-making processes. Authorities are increasingly demanding that financial technology firms provide empirical evidence demonstrating that their models are not only accurate but also equitable, robust against adversarial manipulation, and interpretable by human overseers [7].

The transition from abstract ethical principles to concrete legal mandates represents a critical inflection point for the financial technology sector. Firms are now required to embed compliance mechanisms directly into the lifecycle of artificial intelligence development, necessitating a fundamental paradigm shift in how algorithms are designed, trained, tested, and deployed [8]. This regulatory shift imposes significant compliance burdens, as organizations must bridge the historical divide between their data science teams, who prioritize predictive performance, and their legal and compliance departments, who prioritize risk mitigation and regulatory adherence [9]. The failure to proactively address these regulatory demands exposes firms to substantial legal liabilities, punitive financial sanctions, and severe reputational damage, underscoring the urgent need for robust compliance readiness assessment methodologies.

1.3 Research Objectives and Scope

The primary objective of this research is to comprehensively assess the compliance readiness of financial technology firms facing emerging responsible artificial intelligence regulations through the application of difference analysis. Difference analysis, a methodology traditionally utilized in software engineering and organizational change management, provides a structured approach for identifying and quantifying the variances between an existing baseline state and a desired target state [10]. By adapting

this methodological framework to the context of regulatory technology, this study aims to systematically uncover the structural, procedural, and technological discrepancies that hinder comprehensive compliance.

To achieve this overarching objective, the research focuses on several specific sub-goals. First, it seeks to map the specific technical requirements mandated by emerging regulations against the current operational capabilities of financial technology firms [11]. Second, it aims to categorize the identified discrepancies across multiple dimensions, including algorithmic explainability, data governance, and automated auditing mechanisms. Finally, the research endeavors to synthesize these findings into actionable strategic recommendations, enabling organizations to systematically remediate compliance gaps and build resilient, ethically aligned artificial intelligence infrastructures. The scope of this study encompasses a diverse cross-section of financial applications, providing a holistic perspective on the industry-wide challenges of responsible artificial intelligence integration [12].

2. Literature Review and Regulatory Background

2.1 Evolution of Artificial Intelligence in Financial Services

The academic literature documenting the integration of artificial intelligence within financial services reveals a distinct evolutionary trajectory, characterized by alternating periods of technological unbridled enthusiasm and subsequent regulatory recalibration. Early adoption phases were dominated by deterministic expert systems and rule-based algorithms designed to automate routine back-office processes and enhance transactional efficiency [13]. However, the advent of deep learning and the proliferation of big data catalyzed a paradigm shift, enabling the development of probabilistic models capable of autonomous pattern recognition and adaptive decision-making. Scholars have extensively documented how these advanced models have revolutionized credit underwriting, dynamic pricing, and quantitative trading, fundamentally altering the competitive dynamics of the financial sector [14].

Despite these technological advancements, researchers have increasingly highlighted the latent risks associated with the uncritical adoption of complex machine learning models in high-stakes financial environments. The literature on algorithmic fairness has consistently demonstrated that models trained on historical financial data often inherit and amplify pre-existing societal biases, leading to discriminatory outcomes in lending and insurance pricing [15]. Furthermore, the extensive body of research on model interpretability has underscored the tension between predictive accuracy and algorithmic explainability. As financial technology firms deploy increasingly sophisticated neural architectures, their ability to provide coherent, human-understandable justifications for specific algorithmic decisions diminishes, directly conflicting with established consumer protection norms and regulatory expectations [16].

2.2 Global Landscape of Responsible Artificial Intelligence Regulation

The regulatory response to the challenges posed by artificial intelligence in the financial sector has evolved rapidly, transitioning from voluntary corporate guidelines to comprehensive legislative frameworks. Academic analyses of the global regulatory landscape highlight a convergence around several core principles of responsible artificial intelligence, notably transparency, fairness, privacy, and human oversight [17]. Various jurisdictions have adopted distinct regulatory architectures to operationalize these principles. For instance, some regulatory bodies have pursued a horizontal, risk-based approach, categorizing artificial intelligence systems based on their potential to cause societal

harm and imposing stringent ex-ante conformity assessments on high-risk applications, such as those used for credit scoring and biometric identification [18].

Conversely, other regulatory authorities have favored a sectoral approach, embedding responsible artificial intelligence requirements into existing financial supervisory frameworks. These agencies have issued detailed guidelines mandating that financial institutions establish comprehensive model risk management protocols, encompassing rigorous validation, continuous performance monitoring, and explicit board-level accountability [19]. The academic discourse emphasizes that regardless of the specific regulatory architecture, the overarching objective is to compel organizations to internalize the externalities associated with algorithmic decision-making. However, researchers also point out that the fragmentation of global regulatory frameworks presents significant compliance challenges for multinational financial technology firms, which must navigate a complex mosaic of overlapping and occasionally conflicting legal requirements [20].

2.3 Difference Analysis as an Evaluation Mechanism

Difference analysis has emerged as a robust methodological tool for assessing organizational readiness in the face of complex regulatory transformations. Rooted in systems theory and gap analysis, this approach involves a rigorous, systematic comparison between an organization's current operational baseline and the normative requirements stipulated by external regulatory mandates [21]. In the context of technology compliance, difference analysis extends beyond superficial policy reviews to encompass a granular examination of technical infrastructures, data pipelines, and algorithmic architectures. Scholars have successfully utilized difference analysis to evaluate compliance readiness for data protection regulations, demonstrating its efficacy in identifying structural deficiencies and guiding remediation efforts [22].

The application of difference analysis to responsible artificial intelligence regulation represents a novel and critical frontier in regulatory technology research. Given the highly technical nature of emerging algorithmic mandates, traditional compliance auditing techniques, which often rely on manual documentation reviews and qualitative self-assessments, are fundamentally inadequate [23]. Difference analysis, conversely, facilitates a quantitative and technically grounded evaluation. By defining precise metrics for evaluating algorithmic fairness, transparency, and robust data governance, difference analysis enables researchers and compliance officers to objectively measure the distance between existing technological capabilities and the stringent demands of emerging regulatory frameworks, thereby providing an empirically rigorous foundation for strategic compliance planning [24].

3. Methodology for Difference Analysis in FinTech

3.1 Analytical Framework Design

The methodology employed in this study is anchored in a comprehensive difference analysis framework specifically tailored to the unique technical and regulatory dynamics of the financial technology sector. The initial phase of the framework design involved the systematic deconstruction of emerging responsible artificial intelligence regulations into discrete, measurable technical requirements. This process required a multidisciplinary synthesis, translating abstract legal principles such as algorithmic fairness and transparency into concrete engineering specifications and operational protocols [25]. The resulting regulatory baseline served as the normative target state against which the internal practices of the sampled financial technology firms were evaluated.

The analytical framework was structured around three primary pillars of compliance evaluation. The first pillar focused on algorithmic interpretability and explainability, assessing the extent to which firms possessed the technical capability to generate coherent, human-understandable explanations for automated financial decisions. The second pillar centered on bias mitigation and algorithmic fairness, evaluating the robustness of the statistical techniques employed by organizations to detect, quantify, and remediate discriminatory patterns within their training data and model outputs. The third pillar examined data governance and provenance, analyzing the integrity of the data pipelines used to fuel machine learning models and the mechanisms in place to ensure compliance with stringent data privacy mandates [26].

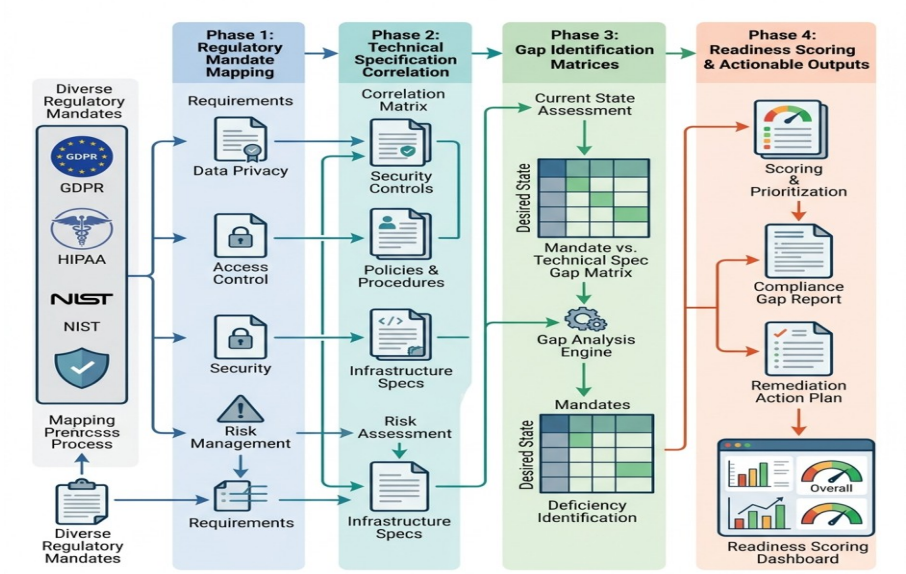

Figure 1: Comprehensive Schematic of Compliance Difference Analysis Workflow

3.2 Data Collection and Sampling Strategy

To ensure the empirical validity and industry-wide applicability of the difference analysis, a rigorous data collection and sampling strategy was implemented. The study utilized a purposive sampling technique to select a diverse cohort of financial technology firms operating across various sub-sectors, including digital lending, algorithmic trading, automated wealth management, and fraud detection. The inclusion criteria required that participating firms actively utilize machine learning models in core business processes that directly impact consumers or financial markets. This diverse sample provided a comprehensive cross-section of the varying levels of technological maturity and compliance awareness present within the industry [27].

Data acquisition was conducted through a multi-tiered approach. Initially, extensive reviews of internal corporate documentation were performed, encompassing model risk management policies, data governance charters, and algorithmic development guidelines. This documentary analysis provided insights into the theoretical compliance postures of the organizations. Subsequently, structured technical audits and interviews were conducted with key personnel, including chief data officers, machine learning engineers, and regulatory compliance directors. These interactions were designed to probe beyond superficial policy statements, extracting granular details regarding the actual algorithms deployed, the specific bias mitigation tools utilized, and the practical challenges encountered during the implementation of responsible artificial intelligence protocols [28].

3.3 Evaluation Metrics and Gap Identification Procedures

The core of the difference analysis involved the application of standardized evaluation metrics to systematically quantify the discrepancies between the regulatory target state and the observed operational baseline. For each technical requirement identified in the analytical framework, a standardized scoring rubric was utilized. This rubric evaluated compliance readiness on a continuous scale, ranging from complete absence of capability to full, automated technical integration. For example, regarding algorithmic explainability, a firm relying solely on post-hoc interpretation methods for black-box models would receive a lower readiness score compared to a firm proactively designing inherently interpretable models for high-risk applications [29].

The gap identification procedure synthesized these individual metric scores to construct a comprehensive compliance readiness profile for each participating organization. Advanced clustering techniques and comparative statistical analyses were employed to identify pervasive industry-wide deficiencies and isolate structural vulnerabilities. The methodology placed particular emphasis on identifying hidden technical debt related to compliance. This involved uncovering instances where firms had achieved superficial adherence through manual workarounds or isolated policy updates, but lacked the fundamental architectural integration necessary to sustain compliance under continuous regulatory scrutiny. The output of this procedure provided a highly granular, empirically supported map of the specific technical and procedural hurdles that financial technology firms must overcome to achieve genuine regulatory alignment.

4. Results of Compliance Readiness Assessment

4.1 Current Baseline of Responsible Artificial Intelligence Compliance

The application of the difference analysis framework yielded extensive empirical data detailing the current compliance baseline across the sampled financial technology organizations. The results indicate a significant divergence between high-level executive commitments to responsible artificial intelligence and the reality of ground-level technical implementation. While a vast majority of the firms possessed formal ethical guidelines and had established dedicated artificial intelligence governance committees, the technical audits revealed profound structural deficiencies in operationalizing these principles within the software development lifecycle. Many organizations continue to treat regulatory compliance as a retroactive administrative task rather than a core engineering requirement that must be embedded from the initial stages of model design.

One of the most critical findings pertains to the pervasive reliance on highly complex, uninterpretable machine learning architectures, particularly deep neural networks and extreme gradient boosting algorithms, for critical financial decisions such as credit underwriting and risk assessment. The assessment revealed that while these models often demonstrated superior predictive accuracy on historical datasets, the vast majority of firms lacked the sophisticated explainability infrastructure required to meet emerging regulatory demands for algorithmic transparency. The utilization of standard post-hoc explanation techniques was frequently found to be technically insufficient, producing inconsistent or overly generalized explanations that fail to satisfy the rigorous evidentiary standards expected by regulatory supervisory bodies.

Table 1: Baseline Compliance Discrepancy Dimensions

Regulatory Dimension	Observed Industry Baseline	Required Regulatory Target	Primary Technical Discrepancy
Algorithmic Explainability	Retroactive post-hoc analysis	Proactive, verifiable	Lack of mathematically

Regulatory Dimension	Observed Industry Baseline	Required Regulatory Target	Primary Technical Discrepancy
		interpretability	rigorous explanation generation
Bias Detection and Mitigation	Manual, ad-hoc statistical sampling	Continuous, automated fairness auditing	Absence of integrated debiasing algorithms in production
Data Provenance Tracking	Fragmented siloed databases	Immutable, end-to-end audit trails	Insufficient metadata capture during model training
Dynamic Performance Monitoring	Periodic quarterly reviews	Real-time drift detection and alerting	Inadequate infrastructure for live concept drift analysis

4.2 Identification of Critical Discrepancies

The difference analysis highlighted severe discrepancies in the methodologies employed for bias detection and mitigation. The results demonstrated that most organizations currently evaluate algorithmic fairness through rudimentary statistical analyses of model outputs, often utilizing narrowly defined, static definitions of fairness. This approach is profoundly inadequate for addressing the complex, intersectional biases that can manifest within high-dimensional financial data. Furthermore, the technical audits showed a near-total absence of automated, continuous fairness monitoring systems deployed in live production environments. This reliance on manual, periodic audits creates significant windows of vulnerability during which models can silently drift and propagate discriminatory outcomes without immediate detection.

Additionally, the analysis uncovered systemic vulnerabilities in fundamental data governance and provenance protocols. Emerging responsible artificial intelligence regulations emphasize the absolute necessity of maintaining comprehensive, immutable audit trails detailing the specific datasets utilized for model training, testing, and validation. However, the assessment revealed that many financial technology firms operate with fragmented data architectures, severely hindering their ability to trace the lineage of model inputs with the precision required by regulatory mandates. This lack of robust data provenance not only impedes the validation of model integrity but also significantly complicates the forensic investigation of algorithmic failures, thereby elevating the overall compliance risk profile of the organization.

Table 2: Aggregated Readiness Scores by Firm Category

Firm Category	Explainability Readiness (0-100)	Fairness Integration (0-100)	Data Provenance (0-100)	Overall Compliance Score
Algorithmic Trading	32.5	45.0	78.5	52.0
Digital Lending	48.0	55.5	65.0	56.1
Wealth Management	65.5	60.0	72.0	65.8
Fraud Detection	41.0	50.5	80.5	57.3

5. Discussion and Conclusion

5.1 Strategic Implications for Financial Technology Firms

The empirical evidence generated through this difference analysis carries profound strategic implications for the financial technology sector. The fundamental conclusion drawn from the data is that superficial policy adjustments and reliance on rudimentary compliance tools are entirely insufficient to meet the rigorous technical demands of emerging responsible artificial intelligence regulations. Financial technology firms must initiate comprehensive architectural re-engineering efforts to integrate automated compliance mechanisms directly into their core computational infrastructures. The persistent inability to mathematically guarantee algorithmic fairness and provide robust model interpretability represents a severe existential risk, not merely a minor regulatory hurdle. Organizations

that fail to address these structural discrepancies will face compounding technical debt, leading to restricted market access, severe legal penalties, and the catastrophic erosion of consumer trust.

To effectively navigate this transition, organizations must fundamentally restructure their internal operational paradigms. The historical siloing of data science, legal, and risk management departments must be dismantled in favor of cross-functional teams capable of translating complex regulatory mandates into precise algorithmic constraints. Furthermore, firms must urgently prioritize strategic investments in advanced regulatory technology solutions, particularly focusing on the development of inherently interpretable machine learning models and the deployment of continuous, automated fairness monitoring pipelines. The competitive landscape of the financial technology sector is rapidly shifting; future market dominance will be determined not solely by predictive accuracy, but by the demonstrable capacity to deploy sophisticated artificial intelligence systems that are provably secure, profoundly transparent, and strictly compliant with global regulatory standards.

5.2 Concluding Remarks and Future Trajectories

In conclusion, this study has successfully applied a difference analysis methodology to quantitatively evaluate the compliance readiness of financial technology firms facing emerging regulations governing responsible artificial intelligence. By systematically mapping current operational baselines against anticipated regulatory target states, the research has highlighted critical, industry-wide vulnerabilities in algorithmic explainability, automated bias mitigation, and rigorous data provenance tracking. The findings clearly demonstrate that while awareness of responsible artificial intelligence principles is high, the practical technical implementation remains dangerously underdeveloped, exposing the sector to significant regulatory and systemic risks.

Future academic research should focus on developing standardized, open-source technical frameworks that facilitate the automated auditing of complex financial algorithms. Expanding the scope of difference analysis to encompass real-time, dynamic regulatory changes across multiple international jurisdictions will be essential for creating adaptive compliance strategies. Additionally, longitudinal studies tracking the remediation efforts of financial technology firms over time will provide valuable insights into the efficacy of different organizational approaches to regulatory alignment. Ultimately, ensuring the responsible integration of artificial intelligence in finance requires a continuous, collaborative effort between technologists, regulatory bodies, and academic researchers to build financial systems that are simultaneously innovative, highly efficient, and fundamentally equitable.

References

1. Zhang, Y.; Joe, I. The Optimized Deployment of Service Function Chain Based on Deep Reinforcement Learning Algorithm. In Proceedings of the International Conference on Machine Learning, Pattern Recognition and Automation Engineering, Singapore, 7–9 August 2024; ACM: New York, NY, USA, 2024; pp. 24–28.

2. Foerster, J.N.; Farquhar, G.; Afouras, T.; Nardelli, N.; Whiteson, S. Counterfactual Multi-Agent Policy Gradients. In Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence (AAAI 2018), New Orleans, LA, USA, 2–7 February 2018; AAAI Press: Palo Alto, CA, USA, 2018; pp. 2974–2982.

3. Nguyen, T.T.; Nguyen, N.D.; Nahavandi, S. Deep Reinforcement Learning for Multiagent Systems: A Review of Challenges, Solutions, and Applications. IEEE Trans. Cybern. 2020, 50, 3826–3839.

4. Chen, A.C.H.; Jia, W.-K.; Hwang, F.-J.; Liu, G.; Song, F.; Pu, L. Machine Learning and Deep Learning Methods for Wireless Network Applications. EURASIP J. Wirel. Commun. Netw. 2022, 2022, 115.

5. Latreche, S.; Bellahsene, H. A Comprehensive Survey on 6G: Enabling Technologies, Key Applications, and Future

Challenges. Frankl. Open 2026, 15, 100559.

6. Sun, A.; Wu, P.; Jin, S.; Jiao, F. Deep Reinforcement Learning-Driven Multidomain Resource Allocation for Integrated Sensing, Communication, and Computing. In Proceedings of the Eighth International Conference on Artificial Intelligence and Pattern Recognition (AIPR 2025), Quanzhou, China, 19–21 December 2025; Tian, H., Ed.; SPIE: Bellingham, WA, USA, 2025; p. 239.

7. Bagdasaryan, E.; Veit, A.; Hua, Y.; Estrin, D.; Shmatikov, V. How To Backdoor Federated Learning. In Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics; PMLR: Cambridge, MA, USA, 2020; pp. 2938 –2948.

8. Li, S.; Fang, B. AI Development Strategies in Countries Around the World. In Artificial Intelligence Security and Safety; Fang, B., Ed.; Springer Nature: Singapore, 2025; pp. 51–84.

9. Lee, T.H.; Kim, J. Hybrid PPO–DQN for Multi-Objective Adaptive Cruise Control in Eco-Driving: Reward Shaping Toward Safety and Sustainability (Student Abstract). In Proceedings of the AAAI Conference on Artificial Intelligence, Singapore, 20–27 January 2026.

10. Pandya, S.; Srivastava, G.; Jhaveri, R.; Babu, M.R.; Bhattacharya, S.; Maddikunta, P.K.R.; Mastorakis, S.; Piran, M.J.; Gadekallu, T.R. Federated Learning for Smart Cities: A Comprehensive Survey. Sustain. Energy Technol. Assess. 2023, 55, 102987.

11. Ozdalga, E.; Ozdalga, A.; Ahuja, N. The smartphone in medicine: A review of current and potential use among physicians and students. J. Med. Internet Res. 2012, 14, e128.

12. Charani, E.; Castro-Sánchez, E.; Moore, L.S.; Holmes, A. Do smartphone applications in healthcare require a governance and legal framework? It depends on the application! BMC Med. 2014, 12, 29.

13. Hoang, D.T.; Huynh, N.V.; Nguyen, D.N.; Hossain, E.; Niyato, D. Deep Reinforcement Learning for Wireless Communications and Networking: Theory, Applications and Implementation, 1st ed.; Wiley: Hoboken, NJ, USA, 2023.

14. Wang, Y.; Lei, J.; Shang, F.; Li, Y. A Comprehensive Survey of Multi-Agent Deep Reinforcement Learning for Wireless Spectrum Management. Neurocomputing 2025, 653, 131236.

15. Bereketeab, L.; Zekeria, A.; Aloqaily, M.; Guizani, M.; Debbah, M. Energy Optimization in Sustainable Smart Environments with Machine Learning and Advanced Communications. IEEE Sens. J. 2024, 24, 5704–5712.

16. Omidshafiei, S.; Pazis, J.; Amato, C.; How, J.P.; Vian, J. Deep Decentralized Multi-Task Multi-Agent Reinforcement Learning under Partial Observability. In Proceedings of the 34th International Conference on Machine Learning (ICML 2017), Sydney, Australia, 6–11 August 2017; PMLR: New York, NY, USA, 2017; Volume 70, pp. 2681–2690.

17. Lim, W.Y.B.; Luong, N.C.; Hoang, D.T.; Jiao, Y.; Liang, Y.-C.; Yang, Q.; Niyato, D.; Miao, C. Federated Learning in Mobile Edge Networks: A Comprehensive Survey. IEEE Commun. Surv. Tutor. 2020, 22, 2031–2063.

18. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge Computing: Vision and Challenges. IEEE Internet Things J. 2016, 3, 637–646.

19. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.

20. Batty, M.; Axhausen, K.W.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart Cities of the Future. Eur. Phys. J. Spec. Top. 2012, 214, 481–518.

21. Mahmood, A.; Abdallah, A.M.; Baharom, B.B.; Habilah, A.S.K. Ensuring Satellite Operational Integrity: A Power Budget Analysis for Next Generation Satellites. IEEE Access 2025, 13, 44901–44911.

22. Li, Y.; Chang, Y.; Fukawa, K.; Kodama, N. Reinforcement Learning-Based Cognitive Radio Transmission Scheduling in

Vehicular Systems. In Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 20–23 June 2023; pp. 1–5.

23. Pessoa, L. (2008). On the relationship between emotion and cognition. Nature Reviews Neuroscience, 9(2), 148–158.

24. Zendejo, D. S., & Escalona, R. S. (2025). Analysis of best practices compliance and transparency for diamond open access journals. Revista de Comunicacion de la Seeci, 58, e903.

25. Ferrag, M.A.; Friha, O.; Kantarci, B.; Tihanyi, N.; Cordeiro, L.; Debbah, M.; Hamouda, D.; Al-Hawawreh, M.; Choo, K.-K.R. Edge Learning for 6G-Enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses. IEEE Commun. Surv. Tutor. 2023, 25, 2654–2713.

26. Scott, W.R. Constructing an analytic framework I: Three pillars of institutions. In Institutions and Organizations, 2nd ed.; SAGE Publications: Thousand Oaks, CA, USA, 2001; pp. 47–70.

27. Rashid, T.; Samvelyan, M.; Schroeder de Witt, C.; Farquhar, G.; Foerster, J.N.; Whiteson, S. QMIX: Monotonic Value Function Factorisation for Deep Multi-Agent Reinforcement Learning. In Proceedings of the 35th International Conference on Machine Learning (ICML 2018), Stockholm, Sweden, 10–15 July 2018; PMLR: New York, NY, USA, 2018; Volume 80, pp. 4295–4304.

28. Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. Corporate Reputation Review, 10(3), 163–176.

29. Kim, S.Y.; Swann, W.L.; Weible, C.M.; Bolognesi, T.; Krause, R.M.; Park, A.Y.S.; Tang, T.; Maletsky, K.; Feiock, R.C. Updating the Institutional Collective Action Framework. Policy Stud. J. 2022, 50, 9–34.