International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 12-No.1 (2026) pp. 247-254
http://www.ijcesen.com

ISSN: 2149-9144

Copyright © IJCESEN

Research Article

Establishing Robust Data Governance Structures for Artificial Intelligence Deployment in Financial Institutions: A Compliance and Trust Perspective

Yogesh Kumar*

Süleyman Citi, USA
* **Corresponding Author Email:** reachkumaryogesh@gmail.com - **ORCID:** 0000-0002-9907-7550

Article Info:

DOI: 10.22399/ijcesen.4756
Received : 03 November 2025
Revised : 28 December 2025
Accepted : 08 January 2026

Keywords

Data Governance,
Artificial Intelligence,
Banking,
Compliance,
Trust

Abstract:

The adoption of Artificial Intelligence in the banking industry has the potential to deliver significant benefits, but it also poses new challenges in terms of data governance. This article explores the importance of effective data governance frameworks for ensuring the integrity, security, and ethical use of data in AI implementations within the banking sector. It highlights the regulatory landscape, including the General Data Protection Regulation and the California Consumer Privacy Act, and the financial implications of non-compliance. The article discusses key principles of data governance for AI in banking, such as establishing clear policies, ensuring data quality, implementing access controls, and addressing data privacy and security concerns. It also emphasizes the importance of ethical considerations and the need for rigorous testing and monitoring of AI models. The article further examines best practices for integrating AI into existing data governance frameworks, including conducting risk assessments, establishing dedicated governance structures, defining roles and responsibilities, and investing in staff training. Finally, it underscores the importance of transparency and accountability in building trust among stakeholders and fostering a positive perception of AI adoption in the banking industry.

1. Opening Context: Where Banking Meets Artificial Intelligence

1.1 How AI Transforms Financial Institution Operations

Banking establishments currently witness a significant technological shift through Artificial Intelligence, substantially modifying how operations function, customers receive services, and organizations handle risks. AI technologies permit financial organizations to streamline complex procedures, craft personalized customer interactions, spot fraudulent activities with greater precision, and make well-informed lending choices using sophisticated data examination [1]. Incorporating AI within banking operations indicates a major shift touching numerous aspects of financial services, ranging from customer-facing activities to internal risk handling and regulatory compliance functions. Machine learning algorithms analyze enormous transactional data quantities in real-time, spotting patterns that human analysts would miss, and producing insights driving organizational strategic choices [2]. However, this technological progress brings substantial responsibilities, demanding that banking establishments build AI implementations on solid foundations featuring thorough data governance, ethical frameworks, and regulatory compliance.

1.2 New Data Governance Obstacles in AI Deployment

Banking organizations implementing AI systems face complicated data governance obstacles reaching well past standard data management issues. The data-heavy nature of AI algorithms demands organizations gather, handle, and store massive amounts of confidential customer details, raising vital questions about data quality, origins, privacy safeguards, and security protocols [1]. Standard banking systems show fairly transparent and verifiable data movements plus decision-making processes, whereas AI models often work as complex computational frameworks, making it hard for governance teams to grasp how outputs get produced or confirm regulatory compliance and

ethical standards matching. The difficulty grows through the changing nature of machine learning models, which constantly adjust by processing fresh data, possibly straying from initial specifications and bringing unexpected risks [2]. Banking establishments must tackle data origin questions, confirming training datasets hold representative qualities and stay clear of biases that could produce discriminatory results, while keeping the flexibility needed for innovation within quickly changing technological settings.

1.3 Research Aims, Coverage, and Analytical Approach

This examination provides a complete analysis of data governance frameworks built specifically for AI deployment within banking sectors, focusing on regulatory compliance guarantees and stakeholder trust maintenance. The investigation covers regulatory environment analysis, core data governance principles for AI systems, model creation and monitoring practices, and best methods for bringing AI into established governance frameworks [5]. The research method used combines recent academic publications, industry reports, and regulatory guidance documents to build a thorough understanding of obstacles and solutions tied to AI governance in banking. By merging insights from various sources and studying practical implementation factors, this analysis offers banking professionals, risk managers, and compliance officers practical guidance for creating strong governance frameworks supporting responsible AI adoption while encouraging innovation and competitive advantage within progressively digital financial services settings.

2. Regulatory Environment and Compliance Demands

2.1 Major Regulatory Framework Summary

The regulatory setting controlling AI deployment in banking has grown into a detailed and complex landscape, with frameworks like the General Data Protection Regulation and the California Consumer Privacy Act setting strict demands for how financial establishments gather, handle, and safeguard customer data. These regulations place major obligations on banking organizations, covering demands to get clear consent for data handling activities, offer transparency about personal information use, let customers access and remove their data, and put in place fitting technical and organizational steps guaranteeing data security [3]. Where AI and data privacy regulations meet creates specific obstacles, as the GDPR holds provisions for algorithmic decision-making, giving people rights to get explanations for automated choices notably affecting them, practically demanding banks create explainable AI systems offering meaningful insights into decision-making processes. Past general data protection laws, banking regulators worldwide create AI-specific guidance tackling issues like model risk handling, algorithmic fairness, and machine learning system governance [5]. Financial establishments must work through this changing regulatory setting while keeping operational efficiency and competitive standing, demanding sophisticated governance frameworks adjustable to shifting demands across various jurisdictions.

2.2 Banking-Focused Regulatory Factors and Compliance Effects

Banking regulators have recognized that AI systems bring unique risks to financial stability, consumer safeguards, and market soundness, leading to the creation of sector-focused guidance and supervisory standards. These banking-focused demands often reach past general data protection laws to tackle concerns like model validation, stress evaluation, governance supervision, and likelihood for AI systems to increase systemic risks or create fresh weaknesses in financial markets [3]. Regulators want banks to keep thorough documentation of AI models, holding detailed records of data sources, training methods, performance measurements, and validation steps, letting supervisors judge whether establishments properly handle AI-related risks. The financial and reputation effects of failing to comply are major, with regulatory fines for data protection violations climbing into hundreds of millions of dollars and banks possibly facing limits on AI system deployment abilities if they cannot show adequate governance and risk handling abilities [5]. Moreover, failing to comply wears down customer trust, harms brand reputation, and brings competitive drawbacks in markets where consumers increasingly care about data privacy and algorithmic fairness matters, making strong compliance frameworks not just regulatory needs but strategic requirements for lasting success.

3. Core Principles of Data Governance for AI in Banking

3.1 Building Clear Data Governance Guidelines and Standards

The basis of successful AI governance in banking establishments lies in thorough data governance guidelines and standards offering clear direction for data gathering, handling, and use throughout AI lifecycles. These guidelines must tackle basic questions about data ownership, stewardship duties, quality demands, keeping periods, and allowed uses, building unified frameworks directing organizational choices [1]. Banks need particular standards for AI training data, holding demands for dataset representation, minimum sample amounts, data freshness, and documentation of data origins letting practitioners grasp information sources and features feeding models. The guidelines should build clear governance processes for approving fresh AI projects, stating criteria projects must meet before moving from creation to production, and listing ongoing monitoring and reporting demands guaranteeing continued compliance with institutional standards [8]. Successful governance guidelines strike a balance between offering enough structure guaranteeing consistency and handling risks while keeping sufficient flexibility, fitting the varied AI use cases banks may chase, from customer service chatbots to intricate credit risk models.

3.2 Data Quality Handling, Access Restrictions, and Security Structures

Data quality stands as a vital factor of AI system performance, as machine learning models basically rely on accuracy, completeness, consistency, and timeliness of training data, making strong quality handling processes crucial for successful AI deployment. Banks must build organized methods for data quality checking, holding automated validation tests, regular data profiling work, anomaly spotting tools, and fixing workflows tackling identified quality problems before hurting model performance or producing wrong outputs [1]. Access restriction tools play equally vital roles in AI governance, guaranteeing sensitive data used in model creation and deployment stays reachable only to authorized staff with legitimate business needs, while keeping detailed audit records documenting data access patterns covering staff, timing, and purposes. The security structure for AI systems must tackle unique weaknesses tied to machine learning, holding likelihood for adversarial attacks trying to change model behavior, data poisoning attacks damaging training datasets, and model inversion attacks looking to pull sensitive details from trained models [8]. Banks need deployment of defense-in-depth plans mixing technical controls covering encryption, access handling, and network separation with organizational steps covering security awareness training, incident response steps, and regular security checks confirming protective measure success.

3.3 Ethical Factors and Model Transparency Demands

The ethical aspects of AI in banking reach past legal compliance to cover broader questions of fairness, accountability, and social duty, shaping how financial establishments create and use intelligent systems. Banks must tackle the likelihood for AI models to continue or grow existing biases found in historical data, producing discriminatory results affecting protected groups unfairly in areas covering credit choices, insurance pricing, or fraud spotting [8]. Tackling these concerns demands active efforts in spotting and reducing bias throughout AI lifecycles, holding careful study of training data for possible bias sources, testing models for unequal impact across demographic groups, and putting in place fairness limits stopping models from producing discriminatory outputs even when such results might boost overall accuracy measurements. Model transparency and explainability stand as vital parts of ethical AI governance, as stakeholders, covering regulators, customers, and internal oversight functions, need an understanding of how AI systems reach conclusions to confirm proper operation and match with institutional values [1]. Banks progressively adopt explainable AI methods offering insights into model behavior, covering feature importance study, counterfactual explanations, and visualization tools helping non-technical stakeholders grasp factors driving AI choices, building trust and permitting meaningful oversight of automated systems.

4. AI Model Creation, Evaluation, and Oversight

4.1 Thorough Testing Methods and Bias Spotting Plans

The creation of AI models for banking uses thorough testing methods reaching past standard software quality checks to tackle unique obstacles posed by machine learning systems, holding probabilistic nature, sensitivity to input data features, and likelihood for unexpected behavior in edge situations. Wide-ranging testing frameworks should cover various aspects of model performance, including holding accuracy measurements, judging how well models reach intended goals, robustness evaluation, checking performance under different stress situations and data spreads, and stability study, looking at whether models produce consistent results when given similar inputs [4].

Bias spotting stands as an especially vital part of AI testing in banking, given the likelihood for models to produce discriminatory results, breaking fair lending laws and harming vulnerable populations, demanding establishments put in place organized methods for spotting and measuring bias across protected features covering race, gender, age, and ethnicity. Banks should use various bias spotting methods, holding statistical parity study comparing results across demographic groups, individual fairness checks judging whether similar people get similar treatment, and a causal study looking at whether protected features influence model choices either straight or through proxy variables [2]. The testing process must tackle likelihood for models to show different performance features across different customer segments, guaranteeing AI systems keep acceptable accuracy and fairness levels for all populations served rather than optimizing for majority groups at minority cost.

4.2 Ongoing Oversight, Validation, and Risk Evaluation Structures

Once AI models move into production settings, ongoing oversight becomes crucial for guaranteeing continued performance as expected without straying from initial specifications as data spreads change over time or external conditions shift. Banks need establishment of wide-ranging oversight frameworks tracking various aspects of model performance, holding prediction accuracy, decision spreads, processing times, error rates, and different fairness measurements judging whether models keep fair treatment across demographic groups [4]. These oversight systems should hold automated alerting tools notifying relevant stakeholders when performance measurements stray from acceptable ranges, permitting quick response to possible problems before causing notable harm or regulatory breaches. Model validation stands as a vital governance control offering independent judgment of whether AI systems fit intended purposes, with validation teams looking at model design picks, testing methods, performance features, and risk handling frameworks to guarantee meeting institutional standards and regulatory expectations [2]. Risk evaluation structures for AI systems must consider a wide range of possible failure types and bad consequences, including direct impacts of wrong predictions, systemic effects of widespread model use, reputation risks tied to algorithmic bias or privacy breaches, and strategic risks of falling behind competitors in AI abilities. Banks should run regular risk evaluations, judging these different aspects and informing choices about risk reduction plans, model use limits, and fitting levels of human oversight for different AI uses.

5. Optimal Methods for AI Integration into Data Governance Structures

5.1 Running Wide-Ranging Risk Evaluations and Building Governance Frameworks

The merging of AI into existing data governance structures begins with wide-ranging risk evaluations carefully judging possible dangers and weaknesses tied to particular AI use cases, thinking about factors covering the sensitivity of data being handled, the possible impact of wrong choices, the complexity of model design, and the amount of automation in decision-making processes. These risk evaluations should use organized methods categorizing AI uses based on risk profiles, permitting establishments to apply fitting governance controls matching scrutiny and oversight levels to sizes of possible consequences [3]. High-risk uses covering credit decisioning or fraud spotting systems deserve more intensive governance processes, holding rigorous validation steps, frequent oversight, and senior management supervision, while lower-risk uses covering marketing recommendation engines may work with lighter governance arrangements. Building dedicated AI governance frameworks stands as optimal practice for guaranteeing these systems get fitting attention and skill, with leading banks making specialized committees or councils bringing together representatives from risk handling, compliance, technology, legal, and business units to offer coordinated oversight of AI projects [5]. These governance bodies typically take on duties covering reviewing and approving fresh AI projects, building institutional standards for model creation and use, watching production system performance, and guaranteeing AI activities match with broader strategic goals and risk appetite statements.

5.2 Stating Roles, Duties, and Putting Resources into Staff Growth

Successful AI governance demands clear marking of roles and duties across organizations, guaranteeing accountability for different parts of AI creation, use, and oversight are clearly assigned and grasped by all parties. Banks should build formal accountability structures pointing to particular people or teams as owners for different AI-related functions, holding model creation, data handling, risk judgment, validation, oversight, and compliance [3]. The structure should make clear

decision-making powers, escalation steps, and reporting relationships, ensuring transparency about duties and permitting efficient coordination among different parties involved in AI projects. Putting resources into staff training and ability growth programs stands as a vital success factor for AI governance, as successful oversight of these systems demands staff across organizations to grow fresh skills and knowledge, possibly absent from standard banking skills [5]. Training programs should fit different audiences, with technical staff getting education on AI creation optimal practices, fairness factors, and interpretability methods, while business leaders learn about AI abilities and limits, governance demands, and strategic factors, and oversight functions covering audit and compliance growth skills in AI risk judgment and oversight methods. Banks successfully building internal AI understanding make stronger governance settings where stakeholders engage in informed talks about AI projects, spot possible problems before escalation, and make sound judgments about fitting use of these powerful yet intricate technologies.

5.3 Stakeholder Involvement and Creating Transparency for Trust

Stakeholder involvement and communication plans play vital roles in creating trust and acceptance for AI systems in banking, as customers, regulators, employees, and the broader public hold legitimate worries about how these technologies may affect their interests and well-being. Banks should grow active communication methods explaining how AI gets used, benefits offered, safeguards in place guarding against misuse or harm, and how stakeholders can exercise rights or raise worries about AI systems [3]. Transparency stands as a cornerstone of trust-building work, with leading establishments publishing AI principles statements expressing commitments to responsible creation and use, making tools for customers to grasp when interacting with AI systems, and offering channels through which people can request human review of automated choices notably affecting them. Creating transparency and trust through governance practices demands establishments to move past mere compliance with legal demands toward a more thorough embrace of ethical principles and stakeholder expectations [5]. This holds in place practices covering algorithmic impact checks, judging possible consequences before using AI systems, building ethics review boards, judging proposals from values-based views, making feedback tools permitting stakeholders to report worries about AI behavior, and showing accountability by looking into problems quickly and taking corrective action when problems are spotted. Banks succeeding in creating trust around AI make competitive advantages by marking themselves as responsible technology stewards, attracting customers valuing ethical business practices, and positioning themselves favorably with regulators viewing them as partners in promoting beneficial innovation.

Table 1: *AI Applications and Benefits in Banking Operations [1, 2]*

AI Application Area	Primary Function	Key Benefits	Implementation Complexity
Customer Service	Chatbots and Virtual Assistants	Enhanced response time, reduced operational costs, and availability around the clock	Medium
Fraud Detection	Transaction Monitoring Systems	Real-time threat identification, reduced false positives, and pattern recognition	High
Credit Risk Assessment	Automated Lending Decisions	Improved accuracy, faster processing, and comprehensive data analysis	High
Personalized Banking	Recommendation Engines	Tailored product offerings, increased customer satisfaction, and cross-selling opportunities	Medium
Regulatory Compliance	Automated Reporting Systems	Reduced compliance costs, improved accuracy, and real-time monitoring	High
Trading Operations	Algorithmic Trading Platforms	Market pattern analysis, rapid execution, optimized portfolio management	Very High

Table 2: *Key Regulatory Frameworks for AI in Banking [3, 5]*

Regulatory Framework	Jurisdiction	Core Requirements	Data Subject Rights	Penalties for Non-Compliance

General Data Protection Regulation	European Union	Lawful processing, data minimization, purpose limitation, storage limitation	Access, rectification, erasure, portability, objection to automated decisions	Up to 4% of annual global turnover or 20 million euros
California Consumer Privacy Act	California, USA	Notice requirements, opt-out mechanisms, data deletion rights, and non-discrimination	Access, deletion, opt-out of sale, and non-discrimination	Up to 7,500 dollars per intentional violation
Banking Secrecy Act	United States	Customer identification, transaction monitoring, suspicious activity reporting	Limited disclosure rights	Civil and criminal penalties, license revocation
Payment Card Industry Data Security Standard	Global	Network security, cardholder data protection, vulnerability management	Breach notification rights	Fines up to 100,000 dollars per month, license suspension
Basel Committee Guidelines	International	Model risk management, governance frameworks, and stress testing requirements	Transparency in automated decisions	Regulatory restrictions, capital requirements

***Table 3**: Data Governance Policy Components for AI Systems [1, 8]*

Policy Component	Governance Objective	Key Elements	Responsible Party	Review Frequency
Data Ownership Framework	Define accountability for data assets	Owner identification, stewardship roles, decision rights	Chief Data Officer	Annual
Data Quality Standards	Ensure accuracy and completeness	Validation rules, accuracy thresholds, completeness metrics, and timeliness requirements	Data Quality Team	Quarterly
Data Retention Policy	Manage data lifecycle appropriately	Retention periods, archival procedures, and deletion protocols	Legal and Compliance	Annual
Data Access Controls	Protect sensitive information	Authorization levels, access approval workflows, and audit logging	Information Security	Semi-Annual
AI Model Approval Process	Gate inappropriate deployments	Risk assessment criteria, validation requirements, and approval authorities	AI Governance Committee	Annual
Training Data Standards	Ensure representative datasets	Sample size minimums, diversity requirements, bias assessment, and provenance documentation	Model Development Team	Per Project
Data Usage Restrictions	Prevent unauthorized purposes	Permitted use cases, prohibited applications, consent requirements	Legal Department	Annual

***Table 4:** AI Model Risk Assessment Matrix [2, 4]*

Risk Category	Risk Indicators	Potential Consequences	Risk Level Assessment	Mitigation Requirements

Prediction Errors	Accuracy degradation, increased false positives or negatives	Financial losses, customer dissatisfaction, and regulatory scrutiny	High if accuracy drops beyond 5%	Enhanced monitoring, model retraining, and human review
Data Drift	Distribution changes, feature shift, concept drift	Model obsolescence, incorrect decisions	High if detected drift exceeds threshold	Continuous data monitoring, adaptive learning, periodic retraining
Algorithmic Bias	Disparate impact, discriminatory patterns	Legal liability, reputation damage, and regulatory penalties	Critical for lending and credit decisions	Fairness audits, bias mitigation techniques, and diverse training data
Security Vulnerabilities	Adversarial attacks, unauthorized access, and data breaches	System compromise, data theft, and financial fraud	High for customer-facing applications	Security hardening, penetration testing, and access controls
Operational Failures	System downtime, processing delays, and integration issues	Service disruption, lost revenue, customer attrition	Medium to High based on criticality	Redundancy, failover systems, business continuity plans
Regulatory Non-Compliance	Policy violations, documentation gaps, approval lapses	Fines, operational restrictions, license revocation	Critical for all AI applications	Compliance monitoring, audit trails, and regulatory reporting
Reputational Damage	Public incidents, negative media coverage, customer complaints	Brand erosion, market share loss, stakeholder distrust	High for visible customer applications	Transparency initiatives, stakeholder communication, incident response

6. Conclusions

The successful deployment of Artificial Intelligence in banking basically relies on building strong data governance structures, guaranteeing compliance with regulatory demands while creating and keeping stakeholder trust. The meeting of AI and banking presents both tremendous opportunities and notable obstacles, demanding financial establishments to grow sophisticated methods for data handling, model oversight, and risk reduction, reaching well past standard governance practices. The regulatory setting keeps changing quickly, with frameworks covering GDPR and CCPA building strict demands for data safeguards while banking supervisors grow AI-focused guidance tackling unique worries about model risk, algorithmic fairness, and systemic stability. Banks must work through this intricate setting by putting in place thorough governance structures built on clear guidelines, rigorous data quality handling, strong access restrictions and security steps, and powerful commitments to ethical principles holding fairness, transparency, and accountability.

The core principles talked about the importance of building clear governance guidelines and standards offering direction while keeping flexibility, guaranteeing data quality through organized handling processes, putting in place fitting access restrictions and security structures guarding sensitive details, and tackling ethical factors holding bias spotting and model explainability. The rigorous evaluation and oversight of AI models stands as a vital governance control, demanding banks to put in place thorough validation steps, continuous performance oversight, and organized risk evaluations, spotting possible problems before causing notable harm. Optimal practices for merging AI into data governance structures include running complete risk evaluations, informing fitting governance arrangements, building dedicated governance frameworks with clear roles and duties, putting resources into staff training to create institutional abilities, and growing stakeholder

involvement plans, creating trust through transparency and accountability.

Looking toward what comes next, data governance for AI in banking will likely keep changing as technologies advance, regulatory structures mature, and societal expectations around responsible AI creation become more sophisticated. Banks putting resources into creating strong governance bases today will be better positioned to capitalize on AI opportunities while handling tied risks, making lasting competitive advantages through abilities to innovate responsibly. The path forward demands ongoing commitment to governance excellence, continuous learning and adjustment as the field changes, and genuine partnership among financial establishments, regulators, technology providers, and civil society to guarantee AI serves the interests of all stakeholders in the banking ecosystem. In the end, the success of AI in banking will be measured not only by efficiency gains and improved services permitted but also by the extent to which use occurs in ways that are fair, transparent, secure, and worthy of public trust.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Vinay Yandrapalli, "AI-Powered Data Governance: A Cutting-Edge Method for Ensuring Data Quality for Machine Learning Applications," IEEE Xplore, 18 April 2024. Available: https://ieeexplore.ieee.org/abstract/document/10493601

[2] Narayanage Jayantha Dewasiri, et al., "Chapter 13 Leveraging Artificial Intelligence for Enhanced Risk Management in Banking: A Systematic Literature Review," IEEE Xplore, 2024. Available: https://ieeexplore.ieee.org/document/10790827

[3] Nitin Sharma, "Generative-AI Governance Standards and Bank Performance: An IEEE/ISO Proposal and Its Economic Implications," Hampton Global Business Review, 23 October 2025. Available: https://hgbr.org/research_articles/generative-ai-governance-standards-and-bank-performance-an-ieee-iso-proposal-and-its-economic-implications/

[4] EY Global Banking & Capital Markets Team, "Model Risk Management for AI and Machine Learning," Ernst & Young (EY), 2023. Available: https://www.ey.com/en_us/insights/banking-capital-markets/understand-model-risk-management-for-ai-and-machine-learning

[5] Giriprasad Manoharan, "Data Governance Frameworks for AI Implementation in Banking: Ensuring Compliance and Trust," International Journal of Advanced Research in Engineering and Technology (IJARET), July 2024. Available: https://www.researchgate.net/publication/382073756_DATA_GOVERNANCE_FRAMEWORKS_FOR_AI_IMPLEMENTATION_IN_BANKING_ENSURING_COMPLIANCE_AND_TRUST

[6] Zaixin Song, et al., "Improved Multi-Stage Decoupling Space Vector Modulation for Asymmetrical Multi-Phase PMSM With Series Winding Connection," IEEE Access, 29 March 2022. Available: https://ieeexplore.ieee.org/document/9744562

[7] EY Risk Advisory Team, "Understanding Model Risk Management for AI/ML Models," Ernst & Young, 2023. Available: https://www.ey.com/en_us/insights/banking-capital-markets/understand-model-risk-management-for-ai-and-machine-learning

[8] Alejandro Barredo Arrieta, et al., "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," Information Fusion (Elsevier), 2020. Available: https://www.sciencedirect.com/science/article/abs/pii/S1566253519308103