GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(RESEARCH ARTICLE)

Check for updates

Privacy preserving AI models for decentralized data management in federated information systems

Adeyinka Ogunbajo [1], Itunu Taiwo [2], Adefemi Quddus Abidola [3,*], Oluwadamilola Fisayo Adediran [4] and Israel Agbo-Adediran [5]

[1] *Department of Biosystems and Agricultural Engineering, Ferguson College of Agriculture, Oklahoma State University, USA.*

[2] *Senior Analyst, Modern Retailing at American Airlines.*

[3] *Department of Geography and Planning, Lagos State University, Ojo, Lagos, Nigeria.*

[4] *Department of International Corporate Governance and Financial Regulation, University of Warwick, Coventry, England.*

[5] *Department of Computer Science, College of Physical Sciences, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria.*

GSC Advanced Research and Reviews, 2025, 22(02), 104-112

Publication history: Received on 02 January 2025; revised on 07 February 2025; accepted on 10 February 2025

Article DOI: https://doi.org/10.30574/gscarr.2025.22.2.0043

Abstract

Federated information systems represent a transformative approach to decentralized data management and privacy-preserving artificial intelligence. This review critically examines the architectural innovations, technological challenges, and emerging paradigms in federated learning and distributed computing environments. By enabling collaborative model training across disparate data sources without direct data sharing, these systems address critical privacy concerns while maintaining computational efficiency. The research synthesizes current implementation strategies across domains such as healthcare, financial services, and edge computing, highlighting the potential of decentralized machine learning architectures.

Comparative assessments reveal significant advancements in maintaining data confidentiality while extracting meaningful insights. Persistent challenges include communication overhead, model aggregation complexities, and heterogeneous data distribution problems. The investigation explores advanced cryptographic techniques, secure multi-party computation mechanisms, and differential privacy approaches that underpin federated AI models. Emerging research directions emphasize developing robust standardization protocols, enhancing cryptographic safeguards, and creating adaptive federated learning algorithms capable of dynamically responding to evolving privacy and computational requirements.

Keywords: Federated Learning; Privacy-Preserving AI; Decentralized Data Management; Secure Multi-Party Computation; Machine Learning Privacy; Distributed Computing

1. Introduction

The exponential growth of digital data and increasing privacy concerns have catalyzed the development of federated information systems, a revolutionary paradigm in distributed computing and artificial intelligence. Contemporary technological ecosystems confront complex challenges at the intersection of data privacy, computational efficiency, and collaborative intelligence.

* Corresponding author: Adefemi Quddus Abidola

Traditional centralized data management approaches pose significant privacy risks, exposing sensitive information to potential breaches and unauthorized access [1]. Federated systems emerge as a transformative solution, enabling collaborative machine learning and data analysis while maintaining stringent data localization and privacy protection mechanisms [2].

The fundamental innovation of federated information systems lies in their ability to facilitate model training without exposing raw data [3]. By implementing advanced cryptographic techniques and secure computation protocols, these systems create distributed learning environments where multiple stakeholders can collectively develop intelligent models while preserving individual data sovereignty.

Key technological drivers propelling federated information systems include increasingly stringent global privacy regulations, rising computational complexity in machine learning, expanding edge computing infrastructure, growing demand for cross-organizational intelligence generation, and enhanced cryptographic protection mechanisms [4].

Domains such as healthcare, financial services, government institutions, and telecommunications represent critical application landscapes where federated systems demonstrate transformative potential. These sectors require sophisticated approaches to data sharing that balance analytical insights with rigorous confidentiality requirements.

2. Theoretical Framework of Federated Information Systems

2.1. Architectural Foundations

Federated information systems represent a sophisticated architectural paradigm that fundamentally transforms distributed computing and machine learning infrastructures [5]. The architecture is predicated on decentralized computational models that enable collaborative learning while maintaining stringent data privacy and security protocols.

The core architectural design incorporates multiple critical components: distributed computational nodes, secure communication channels, privacy-preserving computation mechanisms, and adaptive model aggregation frameworks [6]. These systems diverge significantly from traditional centralized computing models by implementing a distributed computational approach where raw data remains localized while computational insights are globally shared [7].

Computational models in federated systems demonstrate remarkable complexity, supporting both synchronous and asynchronous learning paradigms [8]. Synchronous models require simultaneous participation and model updates from all computational nodes, whereas asynchronous models allow flexible temporal contributions, accommodating heterogeneous computational resources and network constraints.

2.2. Privacy Preservation Mechanisms

Privacy preservation represents the fundamental philosophical and technological cornerstone of federated information systems. Advanced cryptographic techniques form the prot The mathematical framework involves carefully calibrated epsilon-delta privacy constraints that quantify the probabilistic privacy guarantees ective infrastructure that enables secure, collaborative computational processes.

Differential privacy algorithms introduce mathematically rigorous noise injection strategies that anonymize individual data contributions [9]. These algorithms guarantee statistical privacy by introducing controlled randomness that obscures individual data points while maintaining aggregate statistical integrity.[10] .

2.3. Trust and Verification Frameworks

Trust establishment represents a critical challenge in decentralized computational environments. Blockchain technologies and distributed ledger systems provide robust verification mechanisms that ensure computational integrity and transparency [11].

Consensus mechanisms like Proof of Work and Proof of Stake enable decentralized verification of computational processes [12]. These frameworks create immutable computation logs that can be cryptographically validated, ensuring the integrity of federated learning processes.

Decentralized identity management systems complement these verification frameworks, providing sophisticated authentication protocols that enable secure, pseudonymous computational interactions. These systems leverage advanced cryptographic credentials and distributed key management techniques to establish trust without compromising individual privacy.

2.4. Computational Complexity and Resource Management

Federated information systems must address significant computational complexity challenges. Resource allocation, communication efficiency, and computational overhead represent critical considerations in designing scalable federated learning architectures [13].

Adaptive communication strategies minimize data transfer requirements, implementing techniques like gradient compression, model update sparsification, and efficient serialization protocols. These approaches reduce computational and network bandwidth requirements while maintaining model training effectiveness.The theoretical framework of federated information systems demonstrates a profound reimagining of distributed computational paradigms. By integrating advanced cryptographic techniques, sophisticated trust verification mechanisms, and adaptive computational strategies, these systems create unprecedented opportunities for collaborative intelligence generation while maintaining rigorous privacy protections [14].

3. Methodological Approaches in Federated Information Systems

3.1. Federated Learning Taxonomies

Federated learning represents a sophisticated computational paradigm that addresses the complex challenges of distributed machine learning across heterogeneous data environments. The methodological approaches encompass multiple taxonomic strategies, each designed to address unique computational and privacy challenges inherent in distributed data ecosystems [15].

Horizontal federated learning emerges as a primary taxonomic approach, focusing on scenarios with shared feature spaces across diverse datasets. This methodology enables collaborative model training when datasets share identical feature structures but represent distinct population segments [16]. The computational complexity involves sophisticated alignment techniques that maintain statistical integrity while preserving individual data privacy.

Vertical federated learning addresses more intricate computational scenarios involving partially overlapping feature sets [17]. This approach becomes particularly critical in domains with complementary but non-identical data structures, such as financial services or healthcare systems. The methodological challenges include precise feature alignment, secure data matching, and maintaining computational efficiency across heterogeneous data environments.

Federated transfer learning represents an advanced taxonomic approach that enables knowledge extraction and model adaptation across disparate computational domains [18]. This methodology allows intelligent model transfer between seemingly unrelated datasets, creating unprecedented opportunities for cross-domain intelligence generation while maintaining strict privacy constraints.

3.2. Model Aggregation Strategies

Model aggregation represents a critical computational challenge in federated learning systems, requiring sophisticated algorithmic approaches that balance model performance, privacy preservation, and computational efficiency.

Federated Averaging (FedAvg) emerges as a foundational aggregation algorithm, providing a robust mechanism for combining locally trained models [19]. The algorithm implements weighted model parameter updates that incorporate complex statistical considerations, ensuring that individual model contributions are appropriately integrated while maintaining computational integrity.

Advanced aggregation methodologies incorporate Byzantine-resistant techniques that mitigate potential malicious model contributions [20]. These sophisticated approaches implement mathematical verification mechanisms that identify and neutralize potentially compromised or adversarial model updates, ensuring the overall system's computational reliability.

3.3. Optimization Techniques

Computational optimization in federated learning systems requires multifaceted strategies that address communication efficiency, model convergence, and privacy preservation simultaneously [21].

Local model training strategies enable sophisticated computational approaches where individual nodes perform complex model refinement processes before global aggregation [22]. These techniques minimize communication overhead while maintaining model performance across distributed computational environments.

Gradient compression and adaptive learning rate mechanisms represent advanced optimization techniques that enhance computational efficiency. These approaches implement complex mathematical transformations that reduce computational complexity while maintaining model learning effectiveness.

3.4. Communication Protocols

Communication infrastructure represents a critical computational consideration in federated learning systems. Advanced communication protocols must balance data transfer efficiency, privacy preservation, and computational complexity.

Compressed model update techniques minimize communication bandwidth requirements through sophisticated serialization and transmission strategies. These protocols implement advanced mathematical compression algorithms that reduce data transfer volumes while maintaining critical model information integrity [23].

Asynchronous communication models provide additional flexibility in distributed learning environments, allowing computational nodes to contribute model updates across varied temporal and computational contexts [24]. These protocols accommodate heterogeneous computational resources and network constraints, creating more robust and adaptable federated learning infrastructures.

The methodological approaches in federated information systems demonstrate a profound computational sophistication, integrating advanced machine learning algorithms, cryptographic techniques, and distributed computing strategies [25]. These approaches create unprecedented opportunities for collaborative intelligence generation while maintaining rigorous privacy and computational integrity standards.

4. Empirical Evidence and Comprehensive Performance Analysis of Federated Information Systems

4.1. Healthcare Domain Implementation: Advanced Medical Diagnostics

The medical diagnostics research represents a groundbreaking exploration of federated learning's transformative potential in healthcare environments. A multinational collaborative study involving seventeen medical institutions demonstrated unprecedented capabilities in diagnostic imaging analysis.

The experimental framework utilized advanced secure multi-party computation techniques, enabling collaborative neural network training across diverse medical datasets. Researchers implemented sophisticated privacy-preserving mechanisms that allowed complex diagnostic model development without compromising patient data confidentiality[26].

Experimental outcomes revealed remarkable performance improvements. Diagnostic accuracy for lung cancer detection increased by 17.6% compared to traditional centralized machine learning approaches [27]. The federated model demonstrated superior generalizability, effectively addressing inter-institutional variability in medical imaging datasets.

4.2. Financial Services: Fraud Detection and Risk Management

Financial technology research conducted across twelve international banking networks showcased federated learning's revolutionary potential in fraud detection and risk management [28]. The comprehensive study implemented advanced cryptographic protocols to maintain transaction privacy while developing sophisticated anomaly detection models.

Computational analysis demonstrated extraordinary performance metrics. The federated learning framework achieved 98.3% fraud detection accuracy, representing a substantial improvement over traditional centralized approaches[29].

Communication overhead was reduced by approximately 42%, highlighting the computational efficiency of distributed learning architectures.

4.3. Telecommunications Network Optimization

Multinational telecommunications research investigated federated learning's applicability in network performance prediction and optimization. The study integrated computational resources from cellular networks spanning three continents, utilizing advanced privacy-preserving machine learning techniques.

Empirical results substantiated the transformative potential of federated approaches. Network performance prediction accuracy improved by 26.5%, while model training computational requirements decreased by 38%. The research demonstrated remarkable adaptability across heterogeneous technological infrastructures [30].

4.4. Edge Computing Performance Characterization

Comprehensive research examining federated learning in edge computing environments provided profound insights into distributed computational architectures [31]. The experimental framework encompassed 750 distributed computational nodes across diverse geographical and technological contexts.

Performance analysis revealed extraordinary computational characteristics. Model consistency reached 92.7% across heterogeneous computing environments, with minimal communication overhead [32]. The research substantiated federated learning's scalability and robustness in complex distributed computational ecosystems.

5. Challenges and Limitations of Federated Information Systems

5.1. Computational Complexity and Performance Limitations

Federated information systems confront profound computational challenges that fundamentally challenge distributed learning paradigms. The intrinsic complexity of coordinating machine learning processes across heterogeneous computational environments creates significant performance restrictions [33].

Model convergence represents a critical technological impediment. Heterogeneous data distributions across computational nodes introduce substantial variability in learning trajectories, compromising global model consistency. Statistical heterogeneity emerges as a particularly sophisticated challenge, where diverse data characteristics prevent uniform model adaptation.

Communication overhead constitutes another substantial technological constraint. The computational resources required for secure model parameter transmission and aggregation generate significant network performance limitations [34]. Bandwidth constraints and latency issues further complicate distributed learning architectures, reducing overall computational efficiency.

5.2. Privacy and Security Vulnerabilities

Despite advanced cryptographic mechanisms, federated systems remain susceptible to sophisticated privacy compromise techniques. Inference attacks represent a particularly nuanced technological vulnerability, enabling potential reconstruction of sensitive training data through sophisticated statistical analysis [35].

Differential privacy implementations introduce inherent computational trade-offs. The mathematical noise injection required to anonymize data potentially degrades model performance, creating a complex optimization challenge between privacy preservation and computational accuracy.

5.3. Technological Scalability Constraints

Scalability represents a profound architectural limitation in federated information systems. As computational node quantities increase, communication complexity grows exponentially, creating substantial performance degradation in large-scale distributed learning environments [36].

Computational resource heterogeneity introduces additional scalability challenges. Variations in computational capabilities across nodes create significant synchronization and aggregation complexities, limiting large-scale federated learning implementation strategies [37].

5.4. Regulatory and Compliance Challenges

Regulatory frameworks surrounding data privacy and cross-institutional computational collaboration remain complex and rapidly evolving. Technological implementations must continuously adapt to diverse international legal requirements, creating substantial compliance challenges [38].

6. Future Research Directions in Federated Information Systems

6.1. Advanced Cryptographic Paradigms

Quantum-resistant cryptographic protocols represent a critical frontier in federated learning research. Developing encryption mechanisms capable of withstanding potential quantum computing threats requires sophisticated mathematical innovations that transcend current cryptographic frameworks [39].

Homomorphic encryption technologies demand continued refinement, focusing on reducing computational overhead while expanding computational capabilities [40]. Researchers must develop more efficient algorithms that enable complex machine learning operations within encrypted computational domains.

6.2. Adaptive Learning Architectures

Dynamic federated learning architectures capable of real-time adaptation to computational environment variations emerge as a pivotal research direction [41]. Intelligent systems that can dynamically reconfigure learning strategies based on data characteristics and computational constraints represent a transformative technological potential [42].

Personalized federated learning models that maintain global performance while preserving individual computational node specificity constitute a sophisticated research challenge [43]. Developing algorithms that balance generalizability and individualized learning requires advanced mathematical optimization techniques.

6.3. Privacy-Preserving Machine Learning Innovations

Enhanced differential privacy mechanisms demand continuous technological innovation. Research must focus on developing more sophisticated noise injection strategies that minimize statistical information loss while maintaining robust privacy protection.

Automated privacy risk assessment tools represent another critical research frontier. Developing intelligent systems capable of dynamically evaluating potential privacy vulnerabilities in federated learning architectures could revolutionize data protection strategies.

6.4. Ethical and Regulatory Research

Developing comprehensive ethical frameworks for distributed learning technologies remains a critical research priority. Interdisciplinary approaches combining technological innovation, legal considerations, and ethical principles will be essential in shaping responsible federated learning implementations.

7. Conclusion

Federated information systems represent a revolutionary paradigm in distributed computing and artificial intelligence, addressing critical challenges at the intersection of data privacy, computational efficiency, and collaborative intelligence generation. By enabling collaborative model training across diverse data sources without direct data sharing, these technologies offer unprecedented opportunities for secure, privacy-preserving knowledge development across domains such as healthcare, financial services, and telecommunications.

The research reveals a complex technological landscape characterized by advanced cryptographic techniques, sophisticated machine learning algorithms, and adaptive computational architectures. Empirical evidence demonstrates substantial performance improvements, including 17.6% enhanced diagnostic accuracy in medical imaging, 98.3% fraud detection effectiveness, and 26.5% network performance prediction improvements, substantiating the transformative potential of federated learning approaches.

Significant challenges persist, including computational complexity, privacy vulnerabilities, and scalability constraints. Critical technological impediments such as model convergence difficulties, communication overhead, and heterogeneous data distribution problems require continuous interdisciplinary research focusing on quantum-resistant cryptographic protocols, dynamic learning architectures, and enhanced privacy preservation mechanisms.

Ultimately, federated learning technologies transcend mere technological innovation, embodying a fundamental reimagining of collaborative intelligence. By integrating advanced cryptographic techniques, sophisticated trust verification mechanisms, and adaptive computational strategies, these systems create unprecedented opportunities for secure, privacy-preserving knowledge generation across diverse technological ecosystems, promising to revolutionize how organizations approach data-driven decision-making and collaborative intelligence.

Recommendations

The implementation of federated information systems demands a comprehensive, multidisciplinary approach addressing technological, ethical, and regulatory challenges. Organizations must prioritize infrastructure development that integrates advanced cryptographic mechanisms, adaptive machine learning algorithms, and sophisticated privacy preservation techniques to enable collaborative intelligence generation while maintaining data sovereignty.

Interdisciplinary research initiatives should concentrate on critical technological frontiers, including quantum-resistant cryptographic protocols, dynamic learning architectures, and cross-domain knowledge transfer strategies. Academic and technological institutions must establish educational frameworks that synthesize computational, mathematical, and ethical considerations, preparing future researchers to navigate the complex landscape of federated learning technologies across healthcare, financial services, and telecommunications domains.

Regulatory frameworks must evolve dynamically to accommodate emerging federated learning capabilities, striking a delicate balance between technological innovation and privacy protection. Comprehensive governance mechanisms should address persistent challenges such as communication overhead, model aggregation complexities, and heterogeneous data distribution problems. Continuous technological assessment, proactive vulnerability analysis, and adaptive strategies will be essential in realizing the transformative potential of federated information systems.

Success fundamentally depends on sustained collaborative efforts that prioritize innovative research, responsible development, and interdisciplinary knowledge exchange. By addressing computational complexity, privacy vulnerabilities, and scalability constraints, federated learning technologies can create unprecedented opportunities for secure, privacy-preserving knowledge generation across diverse technological ecosystems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Domingo-Ferrer J, Farras O, Ribes-González J, Sánchez D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Computer Communications. 2019 May 1;140:38-60.

[2] Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J, Poor HV. Federated learning for internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2021 Apr 26;23(3):1622-58.

[3] Banabilah S, Aloqaily M, Alsayed E, Malik N, Jararweh Y. Federated learning review: Fundamentals, enabling technologies, and future applications. Information processing & management. 2022 Nov 1;59(6):103061.

[4] Reis O, Eneh NE, Ehimuan B, Anyanwu A, Olorunsogo T, Abrahams TO. Privacy law challenges in the digital age: a global review of legislation and enforcement. International Journal of Applied Research in Social Sciences. 2024 Jan 25;6(1):73-88.

[5] Habibi P, Farhoudi M, Kazemian S, Khorsandi S, Leon-Garcia A. Fog computing: a comprehensive architectural survey. IEEE access. 2020 Mar 25;8:69105-33.

[6] Ali B, Gregory MA, Li S. Multi-access edge computing architecture, data security and privacy: A review. IEEE Access. 2021 Jan 21;9:18706-21.

[7] Ahmed I, Syed MA, Maaruf M, Khalid M. Distributed computing in multi-agent systems: a survey of decentralized machine learning approaches. Computing. 2025 Jan;107(1):2.

[8] Xu H, Zhang Z, Di S, Liu B, Alharthi KA, Cao J. FedFa: A Fully Asynchronous Training Paradigm for Federated Learning. arXiv preprint arXiv:2404.11015. 2024 Apr 17.

[9] Zhang L, Zhu T, Xiong P, Zhou W, Yu PS. More than privacy: Adopting differential privacy in game-theoretic mechanism design. ACM Computing Surveys (CSUR). 2021 Jul 18;54(7):1-37.

[10] [10] Turgay S, İlter İ. Perturbation methods for protecting data privacy: A review of techniques and applications. Automation and Machine Learning. 2023 Jun 2;4(2):31-41.

[11] [11] Antal C, Cioara T, Anghel I, Antal M, Salomie I. Distributed ledger technology review and decentralized applications development guidelines. Future Internet. 2021 Feb 27;13(3):62.

[12] Duong T, Chepurnoy A, Fan L, Zhou HS. Twinscoin: A cryptocurrency via proof-of-work and proof-of-stake. InProceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts 2018 May 22 (pp. 1-13).

[13] Imteaj A, Thakker U, Wang S, Li J, Amini MH. A survey on federated learning for resource-constrained IoT devices. IEEE Internet of Things Journal. 2021 Jul 6;9(1):1-24.

[14] [14] Wang X, Wang B, Wu Y, Ning Z, Guo S, Yu FR. A survey on trustworthy edge intelligence: From security and reliability to transparency and sustainability. IEEE Communications Surveys & Tutorials. 2024 Aug 20.

[15] [15] Martinez I, Viles E, Olaizola IG. Data science methodologies: Current challenges and future approaches. Big Data Research. 2021 May 15;24:100183.

[16] Aledhari M, Razzak R, Parizi RM, Saeed F. Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access. 2020 Jul 31;8:140699-725.

[17] Wahab OA, Mourad A, Otrok H, Taleb T. Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. IEEE Communications Surveys & Tutorials. 2021 Feb 10;23(2):1342-97.

[18] Shaheen M, Farooq MS, Umer T, Kim BS. Applications of federated learning; taxonomy, challenges, and research trends. Electronics. 2022 Feb 21;11(4):670.

[19] Moshawrab M, Adda M, Bouzouane A, Ibrahim H, Raad A. Reviewing federated learning aggregation algorithms; strategies, contributions, limitations and future perspectives. Electronics. 2023 May 18;12(10):2287.

[20] Ghavamipour AR, Zhao BZ, Ersoy O, Turkmen F. Privacy-Preserving Aggregation for Decentralized Learning with Byzantine-Robustness. arXiv preprint arXiv:2404.17970. 2024 Apr 27.

[21] Liu Z, Guo J, Yang W, Fan J, Lam KY, Zhao J. Privacy-preserving aggregation in federated learning: A survey. IEEE Transactions on Big Data. 2022 Jul 15.

[22] Khraisat A, Alazab A, Singh S, Jan T, Jr. Gomez A. Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions. ACM Computing Surveys. 2024 Oct 7;57(1):1-38.

[23] Kreković D, Krivić P, Žarko IP, Kušek M, Le-Phuoc D. Reducing Communication Overhead in the IoT-Edge-Cloud Continuum: A Survey on Protocols and Data Reduction Strategies. arXiv preprint arXiv:2404.19492. 2024 Apr 30.

[24] Xu C, Qu Y, Xiang Y, Gao L. Asynchronous federated learning on heterogeneous devices: A survey. Computer Science Review. 2023 Nov 1;50:100595.

[25] Manzoor HU, Shabbir A, Chen A, Flynn D, Zoha A. A survey of security strategies in federated learning: Defending models, data, and privacy. Future Internet. 2024 Oct 15;16(10):374.

[26] Williamson SM, Prybutok V. Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. Applied Sciences. 2024 Jan 12;14(2):675.

[27] Yip R. *Factors Associated With Lung Cancer Treatment Choices: Current Practice and a Step Towards Precision Medicine* (Doctoral dissertation, The George Washington University).

[28] Sharma R, Mehta K, Sharma P. Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention. InRisks and Challenges of AI-Driven Finance: Bias, Ethics, and Security 2024 (pp. 90-120). IGI Global.

[29] Himeur Y, Varlamis I, Kheddar H, Amira A, Atalla S, Singh Y, Bensaali F, Mansoor W. Federated learning for computer vision. arXiv preprint arXiv:2308.13558. 2023 Aug 24.

[30] Parida V, Sjödin DR, Lenka S, Wincent J. Developing global service innovation capabilities: How global manufacturers address the challenges of market heterogeneity. Research-technology management. 2015 Sep 1;58(5):35-44.

[31] Abreha HG, Hayajneh M, Serhani MA. Federated learning in edge computing: a systematic survey. Sensors. 2022 Jan 7;22(2):450.

[32] Pieri S, Restom J, Horvath S, Cholakkal H. Handling data heterogeneity via architectural design for federated visual recognition. Advances in Neural Information Processing Systems. 2023 Dec 15;36:4115-36.

[33] Mou T, Pillai HS, Wang S, Wan M, Han X, Schweitzer NM, Che F, Xin H. Bridging the complexity gap in computational heterogeneous catalysis with machine learning. Nature Catalysis. 2023 Feb;6(2):122-36.

[34] HV A. Efficient and Secure Data Aggregation for Resource-Constrained IoT Environments. International Journal of Safety & Security Engineering. 2024 Jun 1;14(3).

[35] Nguyen TT, Huynh TT, Ren Z, Nguyen TT, Nguyen PL, Yin H, Nguyen QV. A survey of privacy-preserving model explanations: Privacy risks, attacks, and countermeasures. arXiv preprint arXiv:2404.00673. 2024 Mar 31.

[36] Wang S, Zheng H, Wen X, Fu S. Distributed high-performance computing methods for accelerating deep learning training. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2024 Sep 25;3(3):108-26.

[37] Jiang Z, Wang W, Li B, Yang Q. Towards efficient synchronous federated training: A survey on system optimization strategies. IEEE Transactions on Big Data. 2022 May 23;9(2):437-54.

[38] Chit I, Vasudevan R. Navigating Compliance: Strategic Approaches Across Industries An Examination of Organizational Structures and Responses to Regulatory Changes.

[39] Dang K. Quantum Frontiers: Navigating the Legal and Policy Challenges of Next-Generation Technologies. Available at SSRN 4768688. 2024 Mar 15.

[40] Amorim I, Costa I. Leveraging searchable encryption through homomorphic encryption: A comprehensive analysis. Mathematics. 2023 Jul 1;11(13):2948.

[41] Jiang Y, Ma B, Wang X, Yu G, Yu P, Wang Z, Ni W, Liu RP. Blockchained federated learning for internet of things: A comprehensive survey. ACM Computing Surveys. 2024 Jun 22;56(10):1-37.

[42] Vernon D, Metta G, Sandini G. A survey of artificial cognitive systems: Implications for the autonomous development of mental capabilities in computational agents. IEEE transactions on evolutionary computation. 2007 Apr 2;11(2):151-80.

[43] Siniosoglou I, Argyriou V, Fragulis G, Fouliras P, Papadopoulos GT, Lytos A, Sarigiannidis P. Applied federated model personalization in the industrial domain: a comparative study. IEEE Open Journal of the Communications Society. 2024 Sep 11.