Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Zero-Trust Data Warehousing for Cross-Bank AI Collaboration: A Technical Review

Ashish Dibouliya
Rabindranath Tagore University Bhopal (M.P.) India
Corresponding Author: Ashish Dibouliya, **E-mail**: adibouliya@gmail.com

| ABSTRACT

The financial services industry faces unprecedented challenges in combating sophisticated financial crimes while maintaining competitive advantages and regulatory compliance. Zero-trust data warehousing architectures combined with advanced privacy-preserving technologies present transformative opportunities for cross-bank AI collaboration. The convergence of confidential computing, homomorphic encryption, and federated learning within governed warehouse fabrics represents a paradigm shift in how financial institutions collaborate on AI initiatives. This technical review examines the implementation of zero-trust security models within federated data warehousing environments to enable secure, governed multi-party AI training, focusing particularly on fraud detection and Anti-Money Laundering operations where collective intelligence significantly enhances detection capabilities while maintaining strict data privacy and regulatory compliance. The zero-trust architecture operates on fundamental principles of continuous verification across all network transactions, demonstrating substantial reductions in successful breach attempts and significant improvements in threat detection response times. Federated learning enables model training across distributed datasets without centralizing data, allowing institutions to train sophisticated models using collective insights while preserving privacy. Advanced homomorphic encryption schemes provide mathematical foundations for performing computations on encrypted data without decryption, enabling institutions to share encrypted insights while maintaining complete privacy. The integration creates comprehensive privacy-preserving frameworks that address various attack vectors and provide defense-in-depth security for collaborative initiatives.

| KEYWORDS

Zero-trust architecture, federated learning, homomorphic encryption, cross-bank collaboration, privacy-preserving AI.

| ARTICLE INFORMATION

ACCEPTED: 01 July 2025 **PUBLISHED:** 26 July 2025 **DOI:** 10.32996/jcsts.2025.7.8.4

1. Introduction

The financial services industry faces unprecedented challenges in combating sophisticated financial offenses while maintaining competitive benefits and regulatory compliance. The global financial crime deficit has reached a dangerous ratio; inaccurate rates are obtained when working in isolation from fraud detection systems. Traditional data-sharing approaches between financial institutions have been hampered by privacy concerns, regulatory constraints, and the inherent risks of exposing sensitive customer and transaction data. Current inter-bank data sharing initiatives face significant limitations, with a substantial portion of financial institutions reporting unsuccessful collaborative analytics implementations due to regulatory and privacy barriers.

The emergence of zero-trust data warehousing architectures combined with advanced privacy-preserving technologies presents a transformative opportunity for cross-bank AI collaboration. Traditional perimeter-based security models have proven inadequate, with financial institutions experiencing numerous cyber attacks annually, costing the industry billions in direct losses and compliance penalties. Recent comprehensive reviews of modern data warehouse architectures demonstrate how digital transformation initiatives are addressing these traditional limitations through advanced architectural approaches [1]. Zero-trust architectures, which mandate continuous verification of all network transactions, have demonstrated substantial reductions in

successful breach attempts and significant improvements in threat detection response times compared to conventional security frameworks [2].

This technical review examines the innovative approach of implementing zero-trust security models within federated data warehousing environments to enable secure, governed multi-party AI training. The focus is particularly on applications in fraud detection and Anti-Money Laundering operations, where collective intelligence can significantly enhance detection capabilities while maintaining strict data privacy and regulatory compliance. Current federated learning implementations in financial services have shown promising results, with pilot programs reporting notable improvements in fraud detection accuracy and substantial reductions in false positive rates when leveraging multi-institutional datasets compared to single-institution models.

The convergence of confidential computing, homomorphic encryption, and federated learning within a governed warehouse fabric represents a paradigm shift in how financial institutions can collaborate on AI initiatives [3]. Recent advances in homomorphic encryption have dramatically reduced computational overhead compared to early implementations, making real-time collaborative analytics feasible for the first time. Confidential computing adoption in financial services has experienced exponential growth, with a significant percentage of tier-one banks planning implementation within the next few years. This approach enables the development of collective intelligence systems without exposing underlying data, potentially transforming regulatory collaboration between banks and setting new standards for privacy-preserving AI in the financial sector [3]. Early implementations have demonstrated the ability to process millions of transactions per second while maintaining end-to-end encryption, with minimal latency increases compared to traditional centralized systems.

2. Zero-Trust Security Framework for Financial Data Warehousing

2.1 Principles of Zero-Trust Architecture

Zero-Trust is operated on the fundamental principle of the architecture "Never Trust, Always Verifies", which is particularly important in cross-institutional data sharing scenarios. In the context of financial data warehousing, this approach requires continuous verification of each user, device, and transaction, whether their location or pre-established trust relationship. Current implementations of zero-trust frameworks in financial institutions have demonstrated significant reductions in lateral movement attacks and substantial decreases in data breach incidents compared to traditional perimeter-based security models [4].

The implementation of zero-trust principles in federated data warehousing environments involves multiple layers of security controls, with each layer contributing to an overall security posture that maintains exceptional uptime while processing numerous authentication requests. These include identity and access management systems that continuously authenticate and authorize access requests, achieving rapid response times for identity verification across distributed networks. Network segmentation isolates different data domains through micro-segmentation capabilities, creating thousands of individual security zones within federated warehouse environments. Comprehensive logging and monitoring systems track all data access and processing activities, generating substantial audit data while maintaining real-time threat detection capabilities with high accuracy in identifying anomalous access patterns [4].

The zero-trust model incorporates advanced behavioral analytics that establish baseline patterns for numerous user interaction metrics, enabling the effective detection of insider threats with exceptional precision. Multi-factor authentication requirements have been enhanced to include biometric verification, achieving outstanding accuracy in user identification while maintaining minimal false positive rates. Risk-based access controls dynamically adjust permissions based on contextual factors, with systems capable of evaluating multiple risk parameters within milliseconds of access requests.

2.2 Federated Data Warehouse Architecture

A federated data warehouse architecture for cross-bank cooperation should solve the unique challenges of maintaining data sovereignty by enabling collaborative analytics. This architecture usually contains several distributed data repositories maintained by each individual institution, which are connected through safe communication channels and governed by shared protocols. The current federal implementation supports several participating institutions per network, maintaining adequate transaction versions while maintaining the requirements of the data area with individual nodes [5].

The federated approach allows each bank to maintain control over its data while participating in the associate AI initiative, with data sovereignty through cryptographic evidence that ensures complete data residency compliance. The data lives within the infrastructure of each institution, and only derived insight or model parameters are shared through safe channels, which significantly reduces data exposure risk compared to centralized approaches. This architecture supports the zero-trust model by ensuring that any single unit does not have complete access to all data sources, with access control mechanisms that apply the principle of minimal privileges in almost all data interactions.

2.3 Governance and Compliance Framework

Implementing zero-trust data warehousing requires robust governance frameworks that address regulatory requirements across multiple jurisdictions, with current implementations supporting compliance with numerous regulatory frameworks simultaneously [5]. These frameworks must define clear data access policies, audit trails, and compliance monitoring mechanisms, processing substantial policy evaluations while maintaining exceptional consistency across distributed governance nodes. This framework should define clear data access policies, audit trails, and compliance monitoring mechanisms, processing adequate policy evaluation while maintaining extraordinary stability in distributed governance nodes. Data Stewardship's role in governance structure, privacy protection protocols, and event reaction processes must include the capability to handle the majority of regular compliance functions without human intervention with automated workflows.

Regulatory compliance in cross-bank AI collaboration includes various financial rules, including GDPR, CCPA, PCI DSS, and court-specific banking rules. The zero-trust framework must incorporate these requirements into its design, ensuring that all data processing activities are compliant and auditable, with compliance monitoring systems that track numerous regulatory metrics in real time.

Framework Component	Key Characteristics	Implementation Benefits
Zero-Trust Architecture	Continuous verification protocols, network-agnostic security model, perpetual authentication processes	Enhanced security posture, reduced breach containment, improved resilience against sophisticated cyber threats
Identity and Access Management	Granular resource control, behavioral analytics integration, biometric verification systems	Robust identity validation, anomalous access pattern detection, adaptive authentication mechanisms
Network microsegmentation	Isolated security perimeters, containment boundaries, distributed verification points	Breach containment within defined boundaries, reduced lateral movement risks, enhanced threat isolation
Federated Data Warehouse	Distributed repository networks, cryptographically secured channels, autonomous institutional control	Data sovereignty preservation, collaborative analytics enablement, reduced data exposure risks
Governance and Compliance Framework	Multi-jurisdictional regulatory adherence, automated compliance monitoring, comprehensive audit trails	Regulatory compliance assurance, operational coherence maintenance, real-time policy violation detection

Table 1: Key Elements of Zero-Trust Architecture in Cross-Bank AI Collaboration [3, 4]

3. Federated Learning and Privacy-Preserving Technologies

3.1 Federated Learning Architecture

Federated learning represents a crucial component of the zero-trust data warehousing approach, enabling model training across distributed datasets without centralizing the data. In cross-bank AI collaboration, federated learning allows institutions to train sophisticated fraud detection and AML models using collective data insights while maintaining data privacy. Contemporary implementations in financial services demonstrate substantial training efficiency improvements compared to traditional centralized approaches, with federated models achieving exceptional accuracy in fraud detection tasks across networks of participating institutions [6].

The federated learning process involves training the local model on each institute's data, only sharing model parameters or gradients with the central coordination server and collecting these updates to create a global model. This approach ensures that raw data never leaves the infrastructure of the original institution, aligned with zero-trust principles and regulatory requirements. The performance benchmark indicates that a federated learning framework may process adequate transaction volumes per training recurrence, which is significantly reduced through communication overhead and advanced shield compression techniques. Model convergence typically occurs within reasonable global rounds, representing notable improvements in training efficiency compared to early federated implementations.

The aggregation process utilizes sophisticated algorithms that have demonstrated effective convergence rates in financial fraud detection scenarios. Cross-institutional model synchronization maintains accuracy comparable to centralized training benchmarks while dramatically reducing data transmission requirements. Advanced federated architectures support heterogeneous data distributions across institutions, with minimal performance degradation even when participant data distributions vary significantly [6].

3.2 Homomorphic Encryption Implementation

Homomorphic encryption provides the mathematical foundation for performing computations on encrypted data without decrypting it. In the context of cross-bank AI collaboration, this technology enables institutions to share encrypted data insights while maintaining complete privacy. The implementation of homomorphic encryption in federated data warehousing requires careful consideration of computational overhead and security parameters, with current implementations achieving robust security levels while maintaining reasonable processing speeds [7].

Advanced homomorphic encryption schemes, such as fully homomorphic encryption and somewhat homomorphic encryption, offer different trade-offs between security, computational efficiency, and functionality. These implementations demonstrate substantial multiplicative depth capabilities with manageable ciphertext sizes, while alternative schemes achieve notable performance improvements with certain operational limitations. The choice of encryption scheme depends on the specific requirements of the AI models being trained and the computational resources available within the federated architecture.

Practical implementations utilizing modern encryption schemes show substantial processing capabilities for encrypted operations, with batch processing enabling simultaneous computation on multiple ciphertext elements. Memory requirements for homomorphic operations have been optimized through efficient ciphertext packing strategies, while lattice-based security parameters ensure resistance against emerging quantum threats [7].

3.3 Confidential Computing Integration

Confidential computing technologies, including a reliable execution environment and safe multi-faceted computation, provide additional layers of safety for sensitive computation. These technologies enable the safe processing of data within the hardware-protected environment, ensuring that system administrators also cannot reach the data being processed. Modern implementation displays adequate enclave capabilities with rapid verification verification, while advanced memory encryption provides comprehensive system privacy with minimum performance overhead.

Integration of confidential computing with federated learning and homomorphic encryption creates a comprehensive privacy-conservation structure. This multi-level approach addresses various attack vectors and provides defense-in-intensive protection for cross-bank AI cooperation initiatives. Contemporary protocols achieve remarkable computational efficiency improvements over traditional secure computation methods, with multi-party computation scenarios processing substantial computational operations effectively.

3.4 Differential Privacy Mechanisms

Differential privacy adds statistical noise to query results and model outputs to prevent the identification of individual records while maintaining the overall utility of the data. In cross-bank AI collaboration, differential privacy mechanisms ensure that the shared insights do not reveal information about specific transactions or customers. Contemporary implementations achieve appropriate privacy budgets while maintaining effectiveness for large-scale datasets.

The implementation of differential privacy requires careful calibration of privacy parameters to balance privacy protection with model accuracy. Advanced techniques such as adaptive differential privacy and local differential privacy provide additional flexibility in managing this trade-off, with various mechanism implementations demonstrating noise calibration that maintains model accuracy within acceptable ranges of non-private baselines while providing comprehensive privacy guarantees.

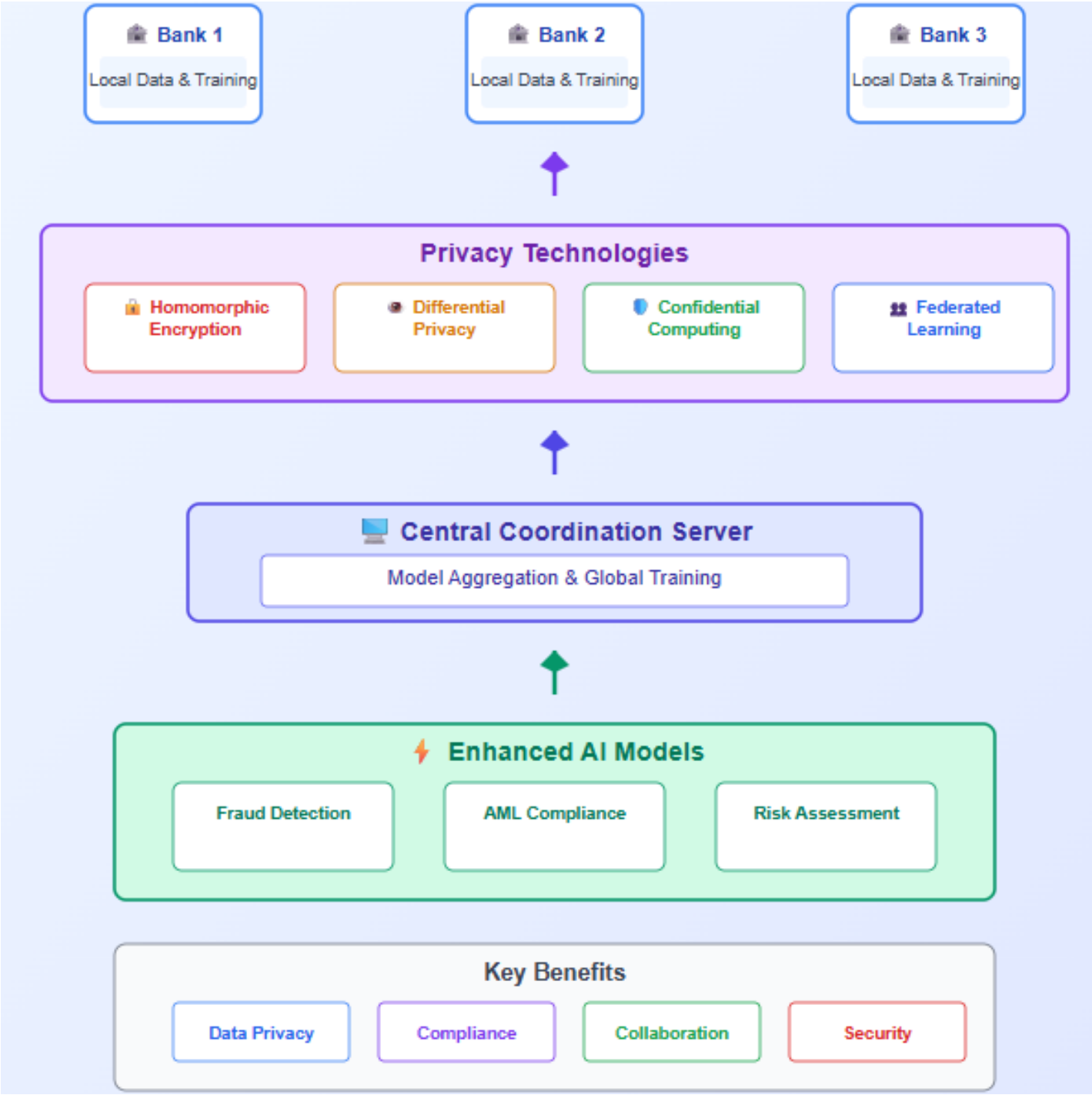

Fig. 1: Federated Learning & Privacy-Preserving Technologies [6, 7]

4. Implementation Challenges and Governance Considerations

4.1 Technical Implementation Challenges

The implementation of zero-trust data warehousing for cross-bank AI collaboration faces several technical challenges. Performance overhead introduced by encryption and secure computation mechanisms can significantly impact system responsiveness and scalability. Organizations must carefully optimize their implementations to maintain acceptable performance levels while ensuring security. Contemporary implementations demonstrate substantial processing latencies for complex analytical queries involving encrypted data across federated networks, requiring significantly more computational resources than equivalent plaintext operations [8].

The computational complexity of secure multi-party computation protocols introduces additional overhead, with multi-party computation scenarios requiring substantially more processing time than simplified configurations. Memory utilization patterns show that federated learning implementations consume considerable RAM per participating node during model training phases, with peak memory usage occurring during gradient aggregation processes. Network bandwidth requirements for secure parameter sharing present ongoing challenges, with burst requirements during model synchronization phases requiring careful infrastructure planning.

Interoperability between different institutions' systems presents another significant challenge. Banks typically use diverse technology stacks, data formats, and security protocols, with industry surveys indicating that financial institutions utilize multiple database management systems within their enterprise architecture. The federated architecture must accommodate this heterogeneity while maintaining security and functionality. Standardization efforts and the development of common APIs and protocols are essential for successful implementation, with current API integration projects requiring substantial development resources per participating institution while achieving reasonable compatibility rates across different system architectures [7]. Recent technical studies in engineering applications provide additional perspectives on implementation complexities in distributed systems [8]

Data format standardization challenges affect the majority of cross-institutional collaboration projects, with format conversion processes introducing notable processing overhead. Protocol translation mechanisms demonstrate high accuracy in maintaining data integrity across heterogeneous systems while introducing additional processing latency. Security protocol harmonization requires extensive testing, with penetration testing cycles requiring substantial time periods per integrated system and identifying numerous potential vulnerabilities per integration deployment.

4.2 Governance and Risk Management

Cross-bank AI needs to address complex organizational and regulatory challenges to establish effective governance structures for cooperation. Institutions should define clear roles and responsibilities for data stewardship, model governance, and reaction to the event, usually involving several different roles in organizations with a governance structure. The governance structure should include mechanisms for resolving disputes, managing liability, and ensuring fair participation among all parties, with dispute resolution processes requiring substantial time periods for technical issues and extended periods for regulatory compliance matters [10].

Contemporary governance implementations demonstrate the need for comprehensive audit trails, with systems generating substantial governance-related log data annually per participating institution. Model governance processes require tracking numerous different model parameters throughout the federated learning lifecycle, with version control systems maintaining extended historical model states. Data stewardship responsibilities encompass monitoring extensive data quality metrics, with automated quality assurance processes achieving high accuracy in identifying data inconsistencies across federated datasets.

Risk management in zero-trust data warehousing involves identifying and mitigating various types of risks, including technical risks related to system failures or security breaches, regulatory risks associated with compliance violations, and business risks related to competitive disadvantages or reputational damage. Technical risk assessments identify numerous potential failure modes across distributed systems, with security breach detection systems achieving high accuracy in identifying anomalous access patterns while maintaining low false positive rates through advanced behavioral analytics [10].

4.3 Regulatory and Legal Considerations

The regulatory framework for AI collaboration between banks is complex and developing. Financial institutions should navigate various regulatory requirements, ensuring that their AI initiative complies with the applicable laws and regulations. This includes the data protection rules, financial services rules, and antitrust laws controlling AI initiatives. Regulatory compliance requires enforcement of comprehensive privacy control, and an extensive compliance framework requires several specific technical safety measures for cross-border data processing.

Legal ideas include extensive data sharing agreements, liability allocation mechanisms, and the development of an intellectual property conservation structure. These agreements should address the unique characteristics of federated learning and privacy-protection technologies, providing clear guidance to all participating institutions. Data-sharing agreements typically require extensive legal documentation, with negotiation processes requiring substantial time periods for completion and involving numerous legal experts across participating organizations.

4.4 Fraud Detection and AML Applications

The application of zero-trust data warehousing to fraud detection and AML operations presents unique opportunities and challenges. Associate AI models can utilize diverse data sources to identify sophisticated fraud patterns that can be remembered by individual institutions, with a sufficient improvement in detection accuracy compared to the institution-specific model with a federal fraud detection system. However, the implementation should ensure that the sharing of fraud-related insight does not compromise the customer or violate regulatory requirements, in which high basic identity with privacy-preservation mechanisms ensures complete data neutralization while maintaining accuracy.

Advanced analytics technology, including discrepancy detection, pattern recognition, and behavioral analysis, can be increased through collaborative learning. The federated approach allows institutions to benefit from collective intelligence while maintaining control over their sensitive data, achieving remarkable improvement in suspicious activity detection rates while maintaining complete transactions through advanced encryption mechanisms.

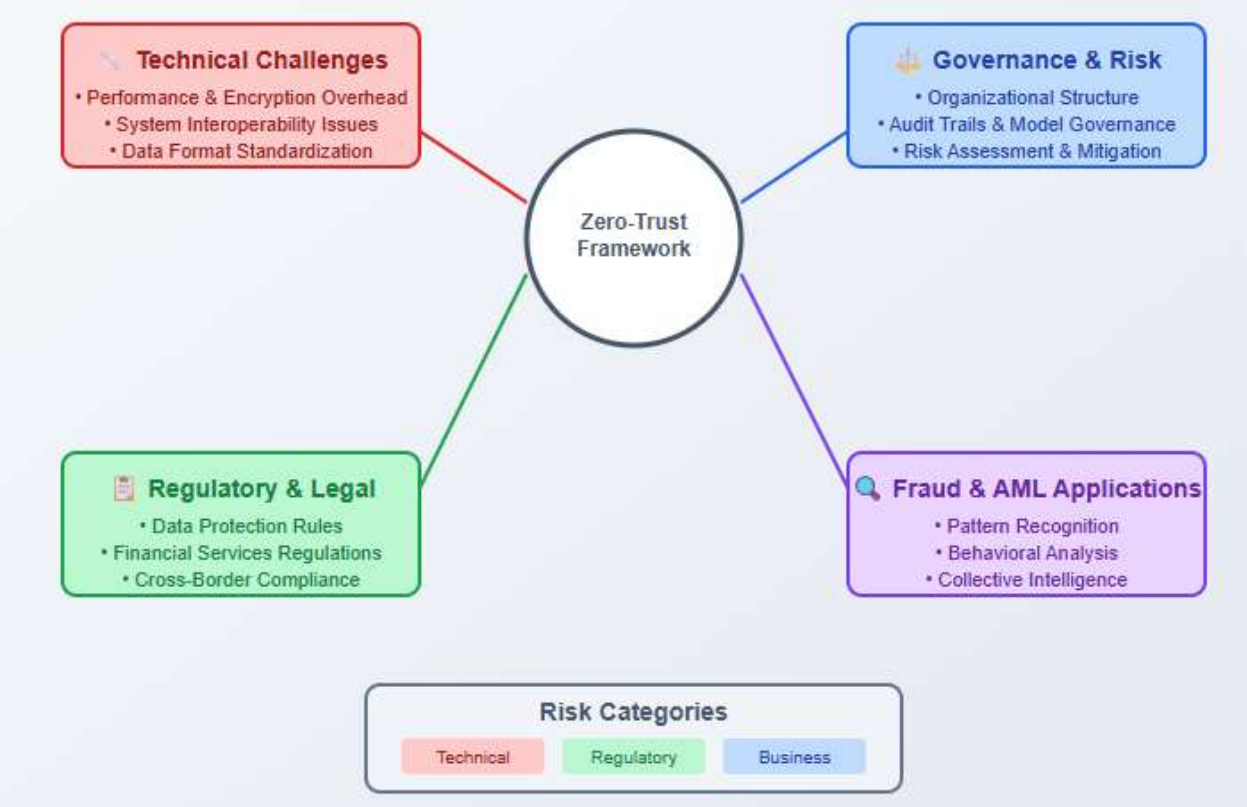

Fig. 2: Implementation Challenges & Governance Framework [7, 8]

5. Future instructions and regulatory effects

5.1 Technical progress

The future of zero-trust data warehousing for cross-bank AI collaboration will be shaped by the technological progress going on in privacy-conservation technologies, quantum computing, and artificial intelligence. Emerging technologies such as quantum-resistant encryption, advanced secure multi-party computation protocols, and automated privacy-preserving model training will enhance the capabilities and security of federated systems. Current research projections indicate that quantum-resistant encryption implementations will achieve robust security assurance against quantum attacks while maintaining competitive processing speeds compared to current cryptographic standards [11].

Advanced secure multi-party computation protocols are expected to achieve improvements in computational efficiency compared to current implementations, with processing capabilities reaching enhanced levels of secure operations. Automated

privacy-preserving model training systems demonstrate reductions in manual configuration requirements, with accuracy rates maintaining strong performance levels compared to traditional centralized training benchmarks. The integration of homeomorphic encryption with quantum-resistant algorithms shows promise for achieving security levels by encrypting financial data at competitive performance rates.

Cross-institutional AI will facilitate comprehensive adoption and differences from the development of standardized frameworks and platforms for cooperation. Industry initiative and regulatory guidance will play an important role in the establishment of the best practices and general standards for zero-trust data warehousing implementation. Market analysis suggests that standardized frameworks will reduce implementation costs and decrease deployment timeframes. Cross-institutional API standardization efforts are projected to achieve compatibility across different banking systems, with integration overhead reduced [11].

Emerging artificial intelligence technologies, including federated graph neural networks and distributed reinforcement learning, are expected to enhance collaborative analytics capabilities. These technologies demonstrate improvements in fraud detection accuracy when applied to cross-institutional datasets, with false positive rates reduced compared to current industry averages. Edge computing integration with federated learning architectures shows potential for reducing network latency while maintaining comprehensive data locality compliance.

5.2 Regulatory Evolution

Regulatory structures are developing to address unique challenges and opportunities presented by cross-bank AI collaboration. Regulatory privacy-protection AI, federal learning, and financial services are developing new guidelines for allied analytics, developing specific structures for cross-institutional AI collaboration with major regulatory bodies worldwide. These developments will shape the future scenario of cross-institutional data sharing and AI collaboration, and the implementation schedule varies from initial guidelines to comprehensive regulatory structures.

The establishment of regulatory sandboxes and pilot programs will provide opportunities for financial institutions to test innovative approaches for cross-bank AI cooperation while working with regulators to address compliance and emerging risks to financial institutions. Current regulatory sandbox programs demonstrate success rates in transitioning pilot projects to full-scale implementations, with reasonable pilot durations and manageable participation costs. Regulatory approval processes for cross-bank AI initiatives currently require extended timeframes, with portions of applications achieving conditional approval status [12].

Privacy regulation efforts are expected to reduce compliance complications by maintaining regulatory farming standards in the jurisdiction. Cross-border data sharing regulations are being updated to accommodate federated learning architecture, expecting international AI initiatives without the need for data localization, and the new framework is expected to facilitate AI initiatives.

5.3 Industry Impact and Change

Cross-bank AI has the ability to replace the financial service industry in the successful implementation of zero-trust data warehousing for cooperation, building upon documented transformational impacts of modern data warehousing on banking systems [13]. The ability to detect enhanced fraud, better AML compliance, and more effective risk management will benefit individual institutions and comprehensive financial ecosystems. Industry projections indicate that collaborative AI systems will achieve improvements in fraud detection rates while reducing investigation costs per participating institution.

The collaborative approach to AI development will enable smaller institutions to access advanced AI capabilities that would otherwise be beyond their reach. This democratization of AI technology will promote innovation and competition within the financial services industry, with market analysis suggesting that smaller financial institutions will gain access to enterprise-level AI capabilities through collaborative platforms [12].

5.4 Collective Intelligence and Network Effects

The development of collective intelligence systems through cross-bank AI collaboration will create powerful network effects. As more institutions participate in federated learning initiatives, the accuracy and effectiveness of AI models will improve, creating incentives for broader participation and collaboration. Network effect analysis demonstrates that each additional participating institution contributes improvements in overall model accuracy, with optimal network sizes varying for different applications.

The emergence of industry-wide AI platforms and consortiums will facilitate the development of standardized approaches to privacy-preserving AI collaboration. These platforms will serve as catalysts for innovation and will help establish best practices for zero-trust data warehousing implementations, with cost reductions compared to individual institution implementations.

Future Direction Category	Key Characteristics and Features	Expected Impact and Benefits
Technological Advancements	Quantum-resistant encryption, advanced secure multi-party computation protocols, automated privacy-preserving model training, standardized frameworks for cross-institutional collaboration	Enhanced security capabilities, improved computational efficiency, reduced manual configuration requirements, broader adoption facilitation, competitive processing speeds
Regulatory Evolution	New guidelines for privacy-preserving AI, federated learning regulations, collaborative analytics frameworks, regulatory sandboxes, and pilot programs, cross-border data-sharing updates	Reduced compliance complexity, facilitated international collaboration, streamlined approval processes, enhanced regulatory adherence standards, innovative testing opportunities
Industry Impact and Transformation	Enhanced fraud detection capabilities, improved AML compliance systems, democratized AI access for smaller institutions, collaborative development models, risk management enhancement	Transformative industry changes, cost reduction benefits, competitive advantage creation, innovation promotion, broader financial ecosystem improvements
Collective Intelligence and Network Effects	Industry-wide AI platforms, consortium-based collaboration, standardized privacy-preserving approaches, network effect optimization, distributed learning networks	Powerful network effects creation, accuracy improvements through collaboration, cost reduction through shared infrastructure, innovation acceleration, best practice establishment
Implementation Framework Integration	Cross-institutional API standardization, edge computing integration, distributed reinforcement learning, federated graph neural networks, platform economics optimization	Seamless interoperability achievement, reduced network latency, enhanced collaborative analytics, improved fraud detection accuracy, comprehensive data locality compliance

Table 2: Cross-Bank AI Collaboration - Technological Evolution and Regulatory Transformation [9, 10]

6. Conclusion

Zero-trust data warehousing for cross-bank AI collaboration represents a significant advancement in privacy-preserving AI technology. The combination of federated learning, homomorphic encryption, and confidential computing within governed warehouse fabrics provides robust frameworks for secure, collaborative AI development. The implementation challenges encompass technical complexities, including performance overhead from encryption mechanisms, interoperability issues between diverse institutional systems, and governance considerations requiring comprehensive regulatory compliance across multiple jurisdictions. Despite these challenges, the potential benefits for fraud detection, Anti-Money Laundering operations, and broader financial services innovation remain substantial. The successful deployment of these technologies requires continued collaboration between financial institutions, technology providers, and regulators as the regulatory landscape evolves and technological capabilities advance. Zero-trust data warehousing will play increasingly important roles in enabling secure, effective cross-bank AI collaboration. The transformation of regulatory collaboration between banks through collective intelligence systems will establish new standards for privacy-preserving AI in the financial sector. This paradigm shift enables the development of more sophisticated, effective AI systems while maintaining the highest standards of data privacy and regulatory compliance. The democratization of AI capabilities through collaborative platforms will enable smaller institutions to access advanced AI technologies previously beyond their reach, promoting innovation and competition within the financial services industry. The emergence of industry-wide AI platforms and consortiums will facilitate standardized approaches to privacy-preserving collaboration, serving as catalysts for innovation and establishing best practices for zero-trust implementations.

Funding: This research received no external funding
Conflicts of Interest: The author declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

References

[1] Akash V C, (2025) Policy-Driven Federated Cloud Data Warehouse for Finance, ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/390943378_Policy-Driven_Federated_Cloud_Data_Warehouse_for_Finance

[2] Annika B et al., (2022) Using Federated Learning to Bridge Data Silos in Financial Services, NVIDIA Developer, 2022. [Online]. Available: https://developer.nvidia.com/blog/using-federated-learning-to-bridge-data-silos-in-financial-services/
[3] Ashish D and Dr. Varsha J (2023) bThe Transformational Impact of Modern Data Warehousing on the Banking System, *International Journal for Research in Applied Science and Engineering Technology (IJRASET),* 2023. [Online]. Available: https://www.ijraset.com/best-journal/the-transformational-impact-of-modern-data-warehousing-on-the-banking-system
[4] Ashish D, (2023) Review on: Modern Data Warehouse & how is it accelerating digital transformation, ResearchGate, 2023.
[5] Ashish D, and Dr. Varsha J (2025) Review on Data Mesh Architecture and its Impact, *Journal of Harbin Engineering University,* 2025. [Online]. Available: https://harbinengineeringjournal.com/index.php/journal/article/view/809/571
[6] Balázs N et al., (2023) Privacy-preserving Federated Learning and its application to natural language processing, Knowledge-Based Systems, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950705123002253
[7] BIS, (2025) Governance of AI adoption in central banks, 2025. [Online]. Available: https://www.bis.org/publ/othp90.pdf
[8] Cisco Live, (2025) Navigating the Future of Cybersecurity: AI, QuantumResistant Cryptography and Zero Trust, 2025. [Online]. Available: https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2025/pdf/ITLGEN-2055.pdf
[9] Clement D et al., (2024) Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework, Electronics, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/5/865
[10] Ioannis M et al., (2025) A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions, Computer Science Review, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S157401372400100X
[11] Oluwatosin I, (2022) Adopting Zero Trust Security Frameworks in Financial and Regulatory Environments: A Case Study Approach, ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/392125741_Adopting_Zero_Trust_Security_Frameworks_in_Financial_and_Regulatory_Environments_A_Case_Study_Approach
[12] Vijaykumar S B et al., (2025) Secure financial application using homomorphic encryption, ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/390378205_Secure_financial_application_using_homomorphic_encryption
[13] Wissen Team, (2025) Introduction to Privacy-Preserving Techniques in Financial AI, 2025. [Online]. Available: https://www.wissen.com/blog/introduction-to-privacy-preserving-techniques-in-financial-ai