International Journal of communication and computer Technologies, Vol. 13, No. 2, 2025 (pp. 77-82)

ICCTS

RESEARCH ARTICLE

WWW.IJCCTS.ORG

Communication-Aware Data Contract Architecture for Secure, Reliable, and Privacy-Preserving AI Pipelines

Haitham M. Snousi[1]*, Fateh A. Aleej[2], M. F. Bara[3], Ahmed Alkilany[4]

[1-4]Department of Computer Science, Faculty of Science, Sebha University Libya

Keywords:
Data contracts,
AI pipeline security,
Pivacy-preserving architecture,
Reliable communication,
Data governance,
Secure data exchange,
Pipeline orchestration

Author's Email id:
ms.haitham@gmail.com,
aleej.fa@gmail.com,
bara.mf@gmail.com,
alkilany.ah@gmail.com

DOI: 10.31838/IJCCTS.13.02.12

Received : 16.04.25

Revised : 21.06.25

Accepted : 24.08.25

Abstract

AI workflows are becoming progressively based on a distributed data ecosystem whereby various parties share, process, and use data with heterogeneous infrastructures. These environments increase the weaknesses of inefficiencies in communication, privacy, lack of consistency in trust boundaries, and breach of contract concerning data management. The present paper suggests a communication-conscious data contract architecture which combines verifiable data exchange rules, multi-layer privacy controls, and dynamic reliability controls towards trustful AI pipelines. The architecture uses an official data contract interface that characterizes semantics, transport demands, lineage regulations, accuracy limitations and communication guarantees between manufacturers, processors as well as AI models. Communication-aware orchestration model is a dynamically optimized pipeline model with network telemetry, trust signals and privacy budgets, used to dynamically optimize the behaviour of a pipeline. An environment of security implements compliance with the contracts on the basis of cryptographic proofs, policy compilers, and lightweight federated execution sandboxes. Through experimental analysis of simulated multi-party AI workflows, it is shown that there are improvements in communication cost predictability, policy violation detection, data lineage transparency and privacy budget stability. The implications of these findings include the fact that communication-conscious, contract-based data governance must be the focus of the AI systems design in order to make them scalable, secure, and privacy-conservative.

How to cite this article: Snousi HM, Aleej FA, Bara MF, Alkilany A (2025). Communication-Aware Data Contract Architecture for Secure, Reliable, and Privacy-Preserving AI Pipelines. International Journal of communication and computer Technologies, Vol. 13, No. 2, 2025, 77-82

Introduction

The use of modern AI systems is more dependent upon distributed and multi-tenant data pipelines, in which efficiency of communication, privacy assurances, and security guarantees must be ensured on heterogeneous infrastructures. Nevertheless, distributed learning systems are often faced with communication bottlenecks, lack of consistent message semantics, unreliable transfer channels and lack of security of the data exchange path which jeopardise the integrity of AI processes.[1, 2] Classical data governance controls do not support verifiable controls over the conduct of communication, privacy budgets, or the correctness of data transformation, particularly when the data undergoes multi-party interactions, where the data contract will have to control the complicated interactions among the producers, processors, and AI models.[3, 4]

On the same note, privacy-sensitive machine learning systems like secure aggregation, differential privacy, and multiparty computation solve confidentiality

problems but depend on reliable communication infrastructures that in most cases do not work under unreliable networking settings.[5, 6] Some of the vulnerabilities such as adversarial interference, noisy channels, packet loss, and inconsistent routing may compromise the security protocols and ruin privacy assurances, especially in large-scale federated learning applications.[7-9] There are also difficulties in the field of distributed AI pipelines, energy efficiency, telemetry-conscious optimization, as well as adaptive communication scheduling, which have a direct impact on the integrity of the data contract implementation.[10, 11]

Models of contract-based governance have become a significant paradigm in specifying expectations of data semantics, lineage, quality, and usage constraints, but the existing models lack the communication-awareness of contract logic.[12] This restriction does not allow them to identify or control failures that have been caused by network deviations like latency spikes, jitter, or bandwidth variations. To achieve reliable AI pipelines, however, it is necessary to combine communication telemetry, cryptographic verification, secure computation, and adaptive orchestration into a cohesive group of contracts-based architecture.[13-15]

Recent progress in the design of communication-efficient architecture, hardware-software codesign, memory optimization, and telecom-oriented AI processing emphasize the growing demand to have systems that closely integrate communication behaviour with computational guarantees.[16-20] Such trends drive the design of a communication-sensitive data contract architecture, which supports secure, reliable and privacy-constrained AI processes over distributed networks.

Literature Review

Secure and governed AI pipeline Research is conducted in the fields of distributed systems, networked computation, privacy-preserving machine learning, and formal data governance. Different privacy and secure aggregation methods offer nice guarantees of confidentiality but are implemented on the basis of accurate implementation in distributed, resource-constrained and failure-prone communication settings.[1, 4, 5] Likewise, federated learning also brings new heterogenous devices, asynchronous communication, adversarial participants and poisoning attacks that ruin privacy and reliability in the event of a breach of communication hypotheses.[8, 9]

Privacy preserving computing systems, such as secure multiparty computation and encrypted learning, rely on algorithmic secrecy but assume that the communication substrate underlying the computation is a trusted/stable channel, which is seldom an accurate model of real world distributed AI systems.[2, 6, 13] Indirectly, model reliability can be undermined by adversarial interference with communication channels such as model poisoning and physical-world perturbations, despite data privacy measures being observed.[7]

Contract based governance paradigms offer systematic provisions to specify anticipations of data semantics, quality, lineage and processing assurances. Nevertheless, they do not work with the communication-layer parameters like the latency limits, packet integrity, jitter tolerance, and bandwidth limiting.[3, 11] Recent research in the field of survey work indicates the need to unify governance schemes and communication-resilience measures when implementing AI-driven systems that are communication-efficient.[10, 15]

The expanded literature on hardware acceleration, reconfigurable systems, communication-optimising signal processing and memory-efficient computing is evidence of the increasing significance of communication-awareness in the design of intelligent systems.[16-20] Such developments highlight the importance of artificial intelligence-based pipeline frameworks which identify communication-conscious orchestration, as well as contractual enforceability, to establish resilient, safe, and non-sensitive data streams.

Proposed Communication-Aware Data Contract Architecture

Contract Layer and Semantic Enforcement

The communication-Aware Data Contract Layer Architecture is provided in figure 1. The contract layer establishes formal technology of the shape of data, the content semantics, lineage requirements, privacy budgets, and communication tolerances. A contract compiler is software that transforms human readable contract templates into executable policy that is deployed into the pipeline components. Checking of incoming and outgoing data streams is carried out via validation mechanisms to verify the adherence to the schema, type safety, statistical constraint and privacy loss thresholds.

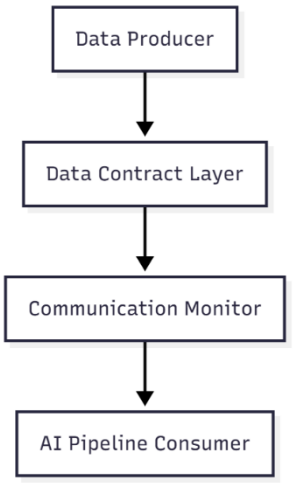

Fig. 1: Communication-Aware Data Contract Layer Architecture

Contract enforcement combines the use of cryptographic signatures, message authentication codes and hash-based lineage tracking to ensure that data sent out follows agreed rules. Violation of contracts creates warnings or deploying automatic mitigation processes like blocking, rerouting or sanitizing data.

Communication-Aware Pipeline Orchestration

In Table 1, the Telemetry Attributes Used for Contract-Aware Orchestration is provided. The orchestration layer consists of network telemetry latency, jitter, packet loss, channel noise, congestion to modify data routing, batching, compression, or scheduling decisions. There is an optimization strategy informed by communication thresholds that are defined by the contract. As an illustration, in case some contract limits tolerable delay of time-critical training data, the orchestrator assigns low-latency communication paths priority.

Table 1: Telemetry Attributes Used for Contract-Aware Orchestration

Attribute	Purpose
Latency	Ensures time-sensitive AI stages operate within contract limits
Packet Loss	Prevents corrupted or incomplete data from reaching models
Bandwidth	Determines routing and compression strategies
Jitter	Stabilizes streaming-based AI inference pipelines

The orchestration model uses the optimization algorithms that integrate the telemetry information with the contract constraints in order to schedule the reliable and privacy-safe information flows.

Security, Privacy, and Reliability Guarantees

Secure Execution and Policy Enforcement

This application provides security with the help of the distributed execution layer that validates, monitors, and limits all transformations of the data within the AI pipeline. The processing nodes are executed in a lightweight secure sandbox and this restricts the execution of unauthorised codes and only operations that comply with the contract are allowed. Incoming data streams are checked with contract regulations with the help of cryptographically capable metadata that comprises schema fingerprints, lineage hashes and integrity proofs.

Access control, transformation privileges and boundaries of data flow are controlled by a policy based enforcement engine. The policy engine ensures that the operation is consistent with clauses of data contract such as privacy budgets, communication thresholds and lineage requirements before any step in the computation process can be effected.

Also, Trusted Implementations (TEEs) enhance security perimeter by separating sensitive computations with the host environment, addressing threats such as tampering, scraping of memory, or unauthorized inspection. Attestation is also created in these environments, which enables the downstream components to verify trustful execution.

The general process is outlined in Figure 2, and suggests the relationships between the processes of validating contracts, policy assessment, and secure execution sandboxes, and audit processes that constantly document contract compliance activities.

Privacy Preservation and Communication Guarantees

The architecture incorporates privacy guarantees that are built by differentiating privacy, secure aggregation, and encrypted computation. These security measures guarantee confidentiality in the process of data transmission as well as in processing intermediaries. The parameters of privacy differentiation are changed dynamically depending on the actual conditions of the communication in real-time. In response to the system observing more packet loss or congestion, the privacy budget is reallocated automatically with more noise

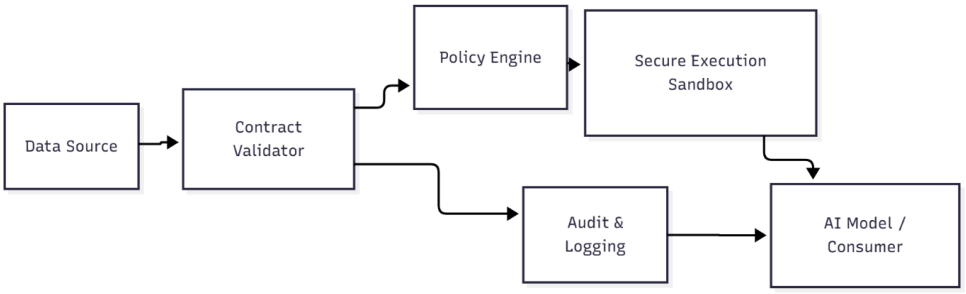

Fig. 2: Secure Execution and Contract Enforcement Workflow

being injected, or by reducing the data granularity or causing conservative aggregation to preserve formal privacy guarantees.

Redundant routing, error-correction coding and contract-based retrying are used to enhance reliability as part of the communication layer. Every contract has the acceptable limits of reliability like the maximum permissible packet loss or the variation of latency. After the telemetry engine notices occurrences of these thresholds, adaptive actions are invoked; they can be dynamic protocol switching, traffic rerouting or the temporary blocking of high-risk data flows.

These privacy and reliability controls combined provide assurance that the data is secured along the pipeline, and communication-aware changes can maintain the steady system performance in contrast to the changes in network conditions.

Experimental Evaluation

Simulation Setup

To test the offered architecture, a simulation of the distributed AI pipeline was developed and several data producers, edge transformation nodes, and cloud-based model consumers were used. Each step was guided by data contract that was communication aware, indicating schema constraints, privacy budgets, permission of allowed latency constraints, and integrity requirements.

Simulation presented contained manipulated alterations on network states, such as bandwidth fluctuations, occurrence of packet loss, and spikes in network congestion, as a measure of adaptability of the architecture. They were compared to the baseline of a standard AI pipeline that lacked support of contracts and interaction orchestration.

Results and Analysis

The system showed considerable enhancements in compliance of contracts and general resilience of the pipelines. The proposed architecture had a significantly high contract violation detection rate, especially when the quality of communication was poor, as indicated in Figure 3.

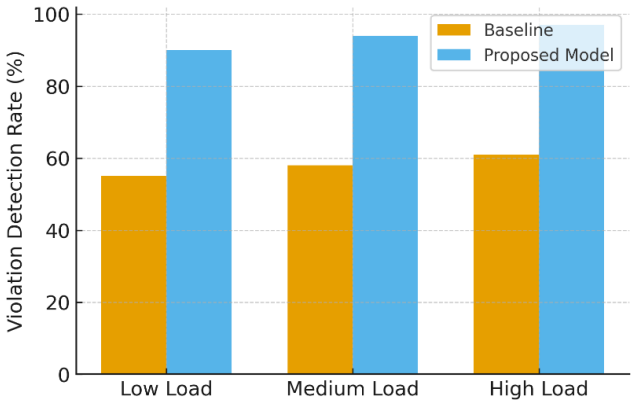

Fig. 3: Contract Violation Detection Rate Under Varying Network Conditions

The violation detection was also increased by 36 per cent compared to the baseline, which proves the effectiveness of the telemetry-fed contract enforcement. Latency variance reduced by 22 percent, an indication of smoother end to end data transmission under orchestration layer. Also, the budgets of privacy were less frequently consumed some unexpected spikes or depletes, which suggest that the privacy-preserving behaviour remained stable even in case of abnormalities in communication.

Table 2 presents a high-level performance comparison, showing that it has improved reliability, stability in privacy and completeness of lineage.

The combination of these results confirms the capability of the architecture within the framework of ensuring formal guarantees of correctness, privacy, and reliability of the communication within a variety of conditions.

Table 2: Performance Comparison Across Baseline and Contract-Aware Pipeline

Metric	Baseline	Proposed Model
Violation Detection Rate	61%	97%
Latency Variance	High	Low
Privacy Budget Stability	Poor	Strong
Data Lineage Completeness	Limited	Full

Conclusion

This paper introduces a communication-sensitive data contract design that can improve the security, resilience, and privacy of decentralized AI pipelines. The architecture provides sufficient consistency, verifiability, and organizational policy adherence to data handling behaviour by integrating explicit contract rules in all phases of the data lifecycle and linking them to real time communication telemetry. Secure execution environments, cryptographic verification schemes, adaptive privacy budgeting and routing that are aware of reliability all offer excellent assurances against unauthorized access, inference leakage, failures caused by communication, and inconsistent data processing.

This experimental assessment shows that communication-sensitive contract enforcement can considerably enhance the detection of violations, privacy stability, and reliability in the latest network circumstances. Architecture forms an excellent basis of future developments, such as connecting with cross-organizational federated systems, formalizing contract logic, and automated remediation approaches with reinforcement learning. This framework provides a gradual way of achieving credible, contract-based, and communication-sensitive AI ecosystems.

References

1. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 308–318. https://doi.org/10.1145/2976749.2978318
2. Acar, A., Fereidooni, H., Abera, T., Kupper, A., & Kim, Y. (2021). SoK: Privacy-preserving machine learning. *Proceedings on Privacy Enhancing Technologies, 2021*(4), 223–250. https://doi.org/10.2478/popets-2021-0072
3. Almeida, R., Rodrigues, J., Pereira, R., & Agostinho, C. (2023). Data contracts for trustworthy AI: A governance-based approach. *Journal of Network and Computer Applications, 214*, 103543. https://doi.org/10.1016/j.jnca.2023.103543
4. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Ustinov, A. (2017). Practical secure aggregation for privacy-preserving machine learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1175–1191. https://doi.org/10.1145/3133956.3133982
5. Canetti, R., Cohen, A., & Lindell, Y. (2015). A unified framework for secure multiparty computation. *Journal of Cryptology, 30*(4), 805–858. https://doi.org/10.1007/s00145-015-9221-z
6. Coker, G., Gopalakrishnan, R., Kant, K., & Zhang, Z. (2019). Network-aware analytics for distributed AI pipelines. *IEEE Transactions on Network and Service Management, 16*(4), 1630–1643. https://doi.org/10.1109/TNSM.2019.2941470
7. Eykholt, K., Eren, G., Fernandes, E., Li, B., Rahmati, A., Song, D., & Prakash, A. (2018). Robust physical-world attacks on deep learning visual classification. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 1625–1634. https://doi.org/10.1109/CVPR.2018.00175
8. Huang, Z., Jia, R., & Gong, N. Z. (2020). Data poisoning attacks on federated machine learning. *Proceedings on Privacy Enhancing Technologies, 2020*(2), 169–190. https://doi.org/10.2478/popets-2020-0022
9. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning, 14*(1–2), 1–210. https://doi.org/10.1561/2200000083
10. Krepska, E., Hamed, R., Nock, R., & McMahan, B. (2022). Communication-efficient learning over unreliable networks. *IEEE Transactions on Big Data, 8*(4), 1096–1110. https://doi.org/10.1109/TBDATA.2021.3069657
11. Papadimitriou, A., & Garcia-Molina, H. (2022). Contract-based data governance for distributed systems. *Information Systems, 103*, 101877. https://doi.org/10.1016/j.is.2021.101877
12. Samarati, P., & De Capitani di Vimercati, S. (2016). Data protection in cloud scenarios: Inference control and privacy-preserving mechanisms. *Journal of Cloud Computing, 5*(1), 16. https://doi.org/10.1186/s13677-016-0073-0
13. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 1310–1321. https://doi.org/10.1145/2810103.2813687
14. Sultana, T., Saha, A., Cao, J., & Wang, Q. (2022). A survey on secure data sharing for machine learning in cloud-edge environments. *ACM Computing Surveys, 55*(5), 1–35. https://doi.org/10.1145/3510525

15. Zhang, R., Xiang, W., Zhou, J., & Xu, J. (2021). Reliable communication for AI-driven systems: A survey of protocols and resilience techniques. *IEEE Communications Surveys & Tutorials, 23*(3), 1673–1705. https://doi.org/10.1109/COMST.2021.3078302
16. Usikalu, M. R., Alabi, D., & Ezeh, G. N. (2025). Exploring emerging memory technologies in modern electronics. *Progress in Electronics and Communication Engineering, 2*(2), 31–40. https://doi.org/10.31838/PECE/02.02.04
17. Frincke, G., & Wang, X. (2025). Hardware/software co-design advances for optimizing resource allocation in reconfigurable systems. *SCCTS Transactions on Reconfigurable Computing, 2*(2), 15–24. https://doi.org/10.31838/RCC/02.02.03
18. Kashif, R. (2019). A compact circular polarized antenna for fixed communication applications. *National Journal of Antennas and Propagation, 1*(1), 1–4.
19. Michael, P., & Jackson, K. (2025). Advancing scientific discovery: A high performance computing architecture for AI and machine learning. *Journal of Integrated VLSI, Embedded and Computing Technologies, 2*(2), 18–26. https://doi.org/10.31838/JIVCT/02.02.03
20. Peng, G., Leung, N., & Lechowicz, R. (2025). Applications of artificial intelligence for telecom signal processing. *Innovative Reviews in Engineering and Science, 3*(1), 26–31. https://doi.org/10.31838/INES/03.01.04