

Fostering AI and Data Governance

SafeLiShare ConfidentialAI™ governs the full lifecycle of your AI models with single source of truth

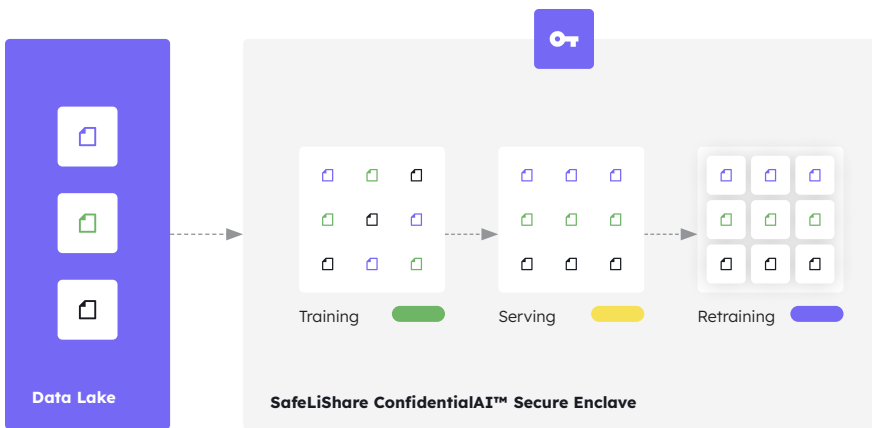
AI governance is important for controlling, predicting, and following AI regulations and ethics. It also helps build confidence, especially during economic uncertainty. Through automating monitoring and documentation of data sources, models, metadata, and workflows, it provides useful information for audits and addresses the concerns of stakeholders, organizations, and customers.

This SafeLiShare ConfidentialAI™ solution brief outlines the use of secure enclave to protect important data in model development, training, serving, and retraining. The solution provides tamper-proof security compliance and improves transparency and data custodianship tracking. SafeLiShare ConfidentialAI™ also helps identify potential risks throughout the model's lifecycle.

Gartner®

80% of organizations seeking to scale digital business will fail because they do not take a modern approach to data governance.

Source



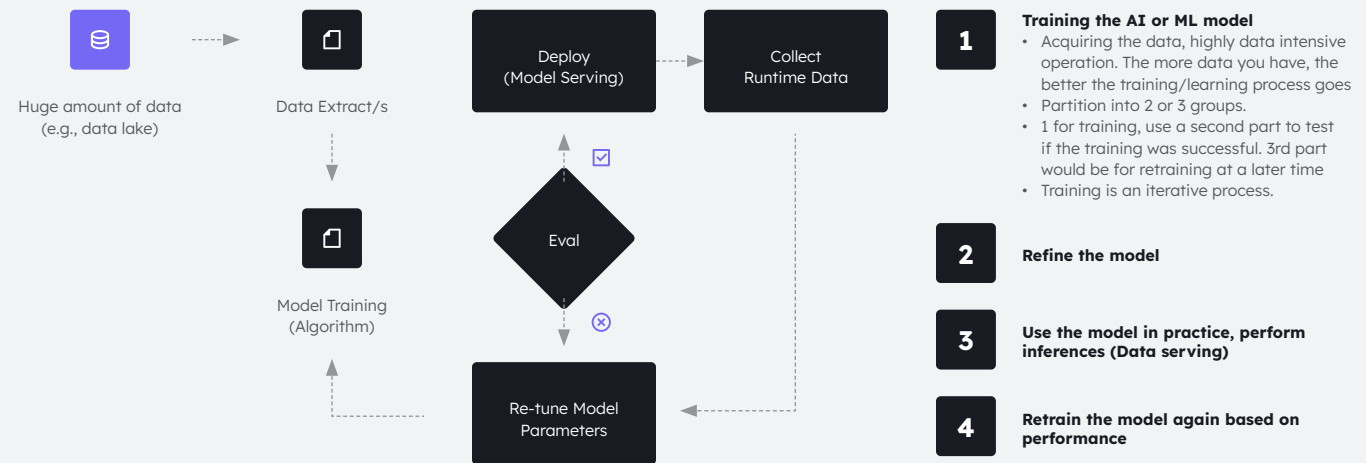
Adopting artificial intelligence can be challenging for many organizations. These challenges include limited access to the right data, manual processes that introduce risk and limit scalability, and the use of multiple unsupported tools in building, deploying, and monitoring models. Additionally, many platforms and practices are not optimized for AI, making it difficult to deliver transparent, explainable, and trusted AI decisions that comply with ethical standards and regulations. To meet these challenges, organizations need AI governance that can operationalize AI, manage risk, and provide scalability while complying with growing AI regulations.

AI & Data Governance: Driving Responsible and Auditable Enterprise Insights

SafeLiShare ConfidentialAI™ is a data governance platform designed for the AI era, created from scratch to support responsible AI workflows with all types of data. It includes all necessary components to establish a tamper-proof and auditable model management process, documenting model training, development, post-deployment, retraining, and model monitoring workflows, all with the goal of achieving scalability through simplicity. This new SafeLiShare ConfidentialAI™

solution automates the security with advanced encryption across the AI/ML lifecycle so data science teams can focus on other tasks, rather than model documentation. Data science leaders and model validators benefit from always having an accurate, up-to-date view of their models. Businesses benefit from the ability to scale and deliver auditable, explainable outcomes free from harmful bias and drift.

4 Stages of AI/ML Process



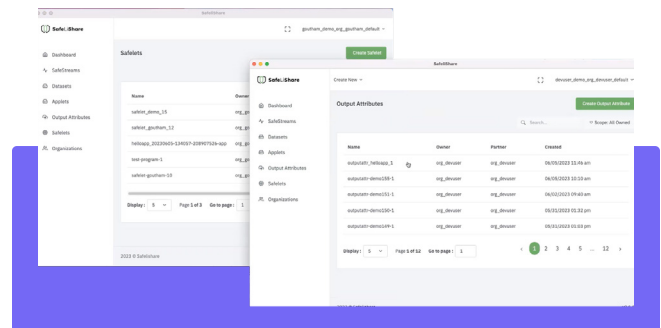
Continuous Security and Compliance

SafeLiShare ConfidentialAI™ solution increases the accuracy of predictions by identifying how AI is used and where retraining is indicated within the secure enclave that supports bringing compute to data or data to compute without de-identification on the real data.

Model risk management is also guaranteed with airgap-ed isolation and encryption in execution to identify, manage, trace, and report on risk and compliance initiatives at scale.

Centralized Workflow Management

Ease of use dashboards in SafeLiShare ConfidentialAI™ provides clear, concise customizable results that enable a robust set of secure enclave stream, or SafeLiShare SafeStream, enhance federated collaboration and drive AI and data regulatory compliance across multiple regions and geographies.



Centralized Workflow Management

Ease of use dashboards provide clear, concise customizable results that enable a robust set of secure enclave stream, or SafeLiShare SafeStream, enhance federated collaboration and drive AI and data regulatory compliance across multiple regions and geographies.

Encryption in use with Zero Trust

SafeLiShare delivers the data governance platform for the AI era. Upon entering secure enclaves where all algorithms and data are encrypted to generate models with privacy enforcement from the single source of truth in cloud TEE.

Non deidentified input and output data

In the process of removing or obfuscating personally identifiable information (PII) from data sets, the challenges of re-identification risk, attribute leakage, data accuracy & quality, biased prediction, and legal & regulatory compliance can result in inefficient AI modeling. SafeLiShare provides stronger privacy guarantees with secure enclaves for multi-party computation while maintaining data utility and model performance. Encrypted output data generated by models that can only be decrypted by predetermined consumer(s).

Model confidentiality

When multiple non-trusting parties are involved in AI workflows or model training, ensuring model confidentiality becomes a significant concern. With SafeLiShare AI & data governance solution, algorithms and data can be provided by different non-trusting parties.

Data quality

To fully utilize the value of data and freshness of the data, it is essential that it be trustworthy. Poor-quality data with bad masking process can have negative consequences.


Harden the delivery of your own Large Language Model (LLM)


Use secure enclave to perform secure model serving as the GPT-like generative AI or LLM model can be trained outside the enclave. The LLM is encrypted and deployed in a TEE. The input question to the LLM is encrypted.


Drive AI auditability for stakeholders


Real-time and customizable dashboards are utilized for data management and stakeholder collaboration throughout AI workflows.


The advantages of implementing AI and data governance:

 **Implement AI and data governance**
The origin of datasets, models, associated metadata, and pipelines are traced and documented on a large scale.

 **Implement responsible AI to mitigate potential risks**
The AI models are monitored for fairness, bias, and drift, which will automatically detect the need for correction.

 **Protect against regulations at scale**
To ensure fairness, transparency, and accuracy of machine learning models in production, it is recommended to use protections and validation.

 **Utilize collaborative and automated tools**
to enhance efficiency and improve the visibility of the AI lifecycle.

 **Efficiently develop strategic planning for AI implementation.**
Optimize effectiveness by achieving equilibrium between individuals, procedures, and artificial intelligence advancements.

Gartner

41% of organizations had experienced an AI privacy breach or security incident. ID G00778428



Summary

In the AI and ML model lifecycle, whether generative AI or responsible AI, the cost of poor data quality can be substantial, impacting various aspects of an organization's operations, finances, compliance, and reputation. Therefore, ensuring data accuracy without de-identification, completeness, and consistency is essential to mitigate these costs and drive better business outcomes. SafeLiShare delivers a combination of technical measures, policies, and templates to safeguard the models and data, including:

Attribute-based access control (ABAC)

ABAC allows for fine-grained access control by considering multiple attributes rather than relying solely on user roles or group memberships.

Data encryption

Encrypt AI/ML model data when in transit, at rest and in execution. This protects the confidentiality and integrity of the data, preventing unauthorized access or tampering during computation within cloud chip-set privacy enforcing environment.

Secure and encrypted storage and transmission

Store and transmit AI/ML model and data through secure channels and protocols. Utilize industry-standard PKI encryption and secure transfer mechanisms to protect against unauthorized interception or tampering.

Tamper-proof logging and auditing

Support robust logging and auditing mechanisms to track and monitor access to AI/ML models and data. This enables organizations to detect and investigate any suspicious activities, maintain accountability, and support forensic analysis if needed.

Compliance with regulations

Ensure FIPS 140-2 Level 3 and 4 compatible compliance with relevant data protection and privacy regulations, such as GDPR, CCPA, or industry-specific regulations.

By implementing these measures, organizations can establish robust access controls for AI/ML models and data, protecting them from unauthorized access, ensuring data privacy, and maintaining the integrity and confidentiality of the information. For more information on SafeLiShare AI & data governance solution, visit [SafeLiShare website](#) or email ai@safelishare.com.



About SafeLiShare

In an era when data has become the product for many enterprises, and faces increased scrutiny due to tightening global regulations, SafeLiShare was founded with a vision to provide application specific access to data. All operations on data by applications are made visible, auditable, and trackable. Multiple governance policies can be enforced simultaneously. Powered by confidential computing technology, policies drive compliance and governance throughout an enterprises' multiple business functions, data domains, and even across to external business partners engendering a new class of business models based on ownership of data and applications.

