Secure Multi-Party Computation Overview Page

Introduction to Secure Multi-Party Computation

This page explains what Secure Multi-Party Computation (SMPC) is, how it protects sensitive information, and why it's important for financial services.

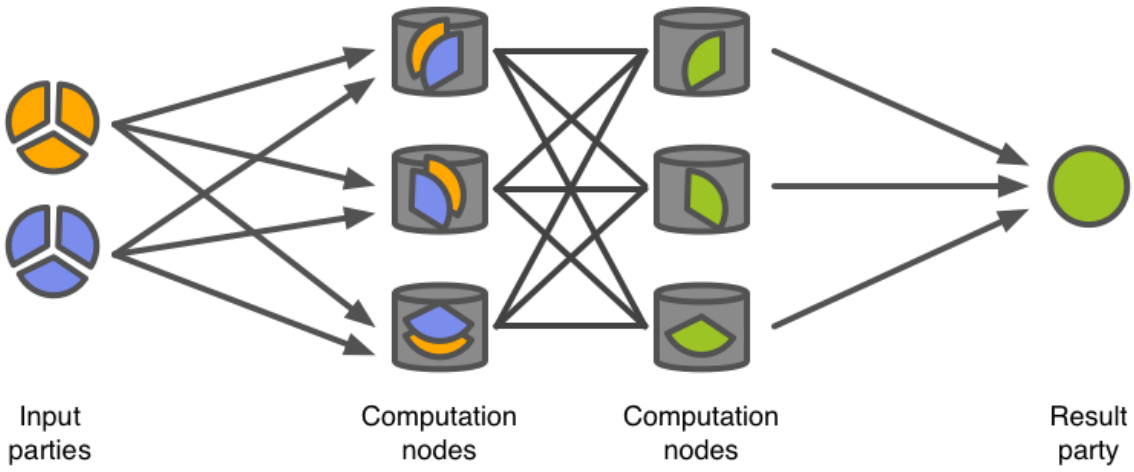
You'll learn about its key benefits, real-world applications, and how leading companies are using it to ensure privacy while enabling secure collaboration.

What is Secure Multi-Party Computation (SMPC)?

Definition: Secure Multi-Party Computation (SMPC) is a cryptographic technique that allows multiple parties to compute a function over their inputs while keeping those inputs private. This means that the parties involved in the computation can get the result without revealing their individual data to each other.

In financial services, SMPC allows institutions to collaborate on data analysis without sharing sensitive information.

SMPC Process Flow



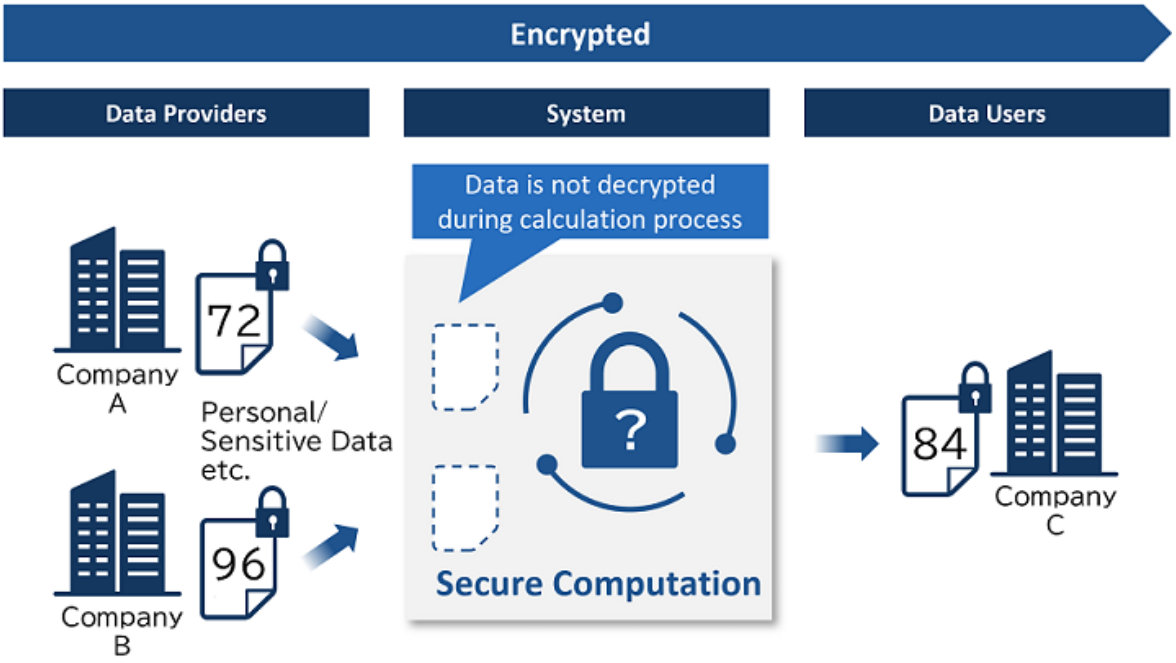
How Secure Multi-Party Computation Works

SMPC allows different parties to jointly compute a function while keeping their inputs private. Here's how it works:

1. **Step 1**: Each party inputs its private data into the computation.
2. **Step 2**: The computation is split into smaller steps, with each party only computing its own part.
3. **Step 3**: The intermediate results are exchanged in an encrypted form.
4. **Step 4**: The result is obtained without any party ever seeing the other parties' private data.

This ensures that each party can contribute to the computation without compromising the privacy of their data, making SMPC a valuable tool in finance.

SMPC Process Diagram



Example of averaging numbers provided by data providers

Benefits of Secure Multi-Party Computation in Financial Services

SMPC offers several key advantages for financial institutions:

1. **Data Privacy**: Ensures that sensitive financial data remains private throughout the computation process.
2. **Collaboration Without Data Sharing:** Institutions can collaborate securely on tasks like fraud detection.
3. **Regulatory Compliance:** SMPC helps meet privacy regulations like GDPR and CCPA.
4. **Improved Security**: Reduces the risk of data breaches since the data remains encrypted and private during computations.
5. **Increased Trust**: Facilitates secure collaboration between different organizations, increasing trust while preserving confidentiality.

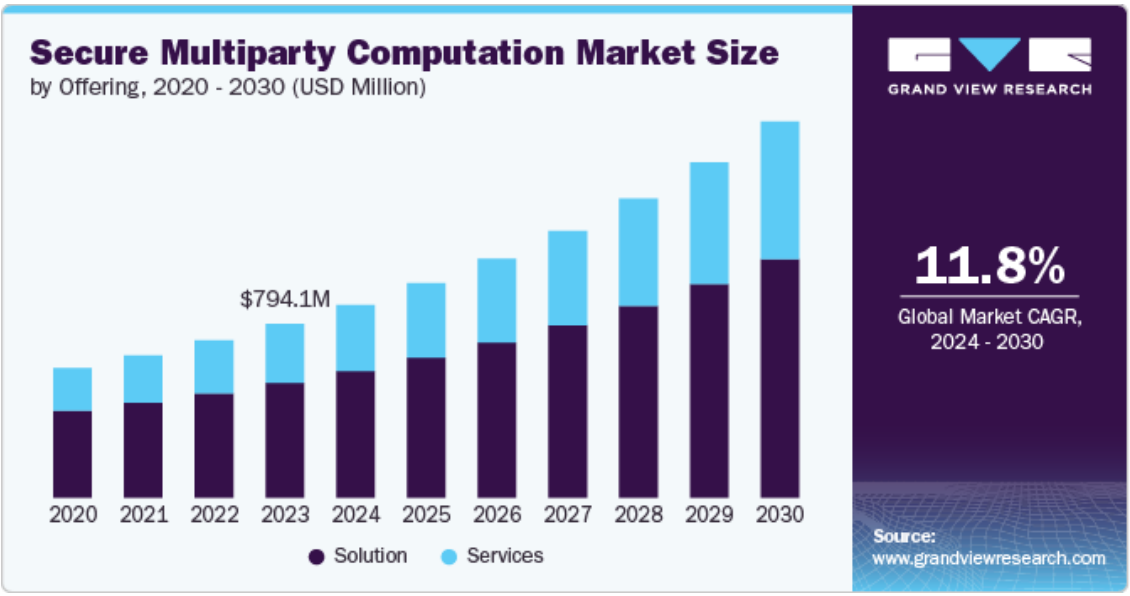
SMPC Benefits and Downsides Infographic

Market Trends and Adoption of Secure Multi-Party Computation

As data privacy regulations grow stricter, financial institutions are adopting SMPC to ensure compliance while collaborating securely. SMPC is gaining traction in industries where multiple entities need to compute data without revealing sensitive information.

- **Rising Demand**: More financial institutions are exploring SMPC for secure collaborations.
- **Regulatory Compliance**: Institutions are driven by the need to comply with privacy regulations like GDPR and CCPA.

SMPC Market Size Trends



How to Implement Secure Multi-Party Computation

Implementing SMPC in financial services involves the following steps:

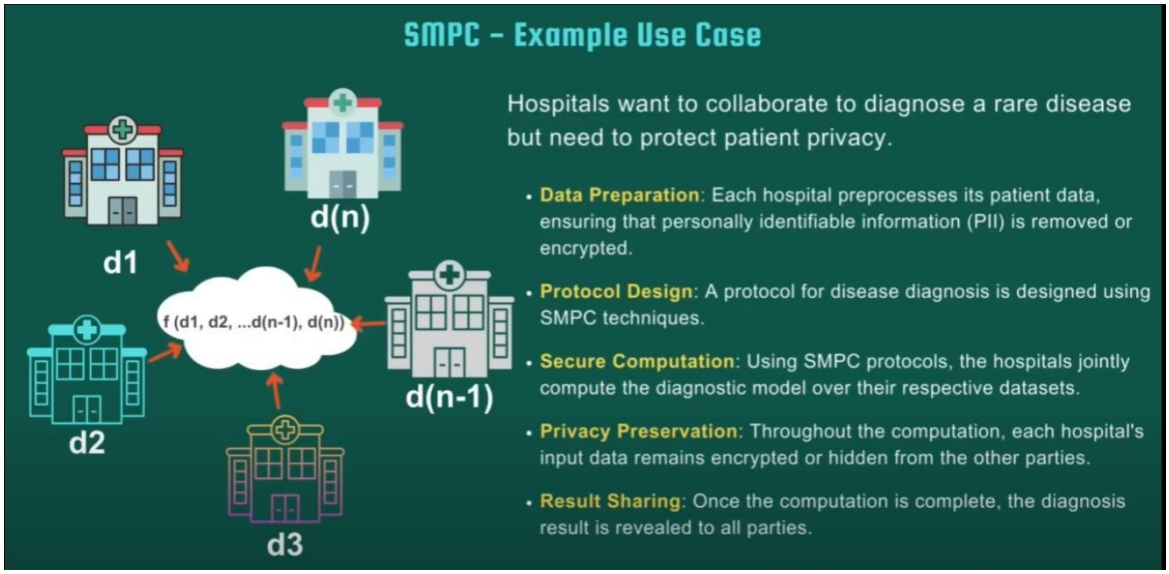
1. **Define the Data and Function**: Identify the sensitive data to be computed and the function to be performed.
2. **Distribute the Computation:** Split the task so each party only sees its own data.
3. **Encrypt Intermediate Results**: Ensure that intermediate results are encrypted and shared securely between parties.
4. **Finalize the Computation**: Compute the result without exposing individual data inputs.

Real-World Applications of Secure Multi-Party Computation in Finance

SMPC is particularly useful in financial services for scenarios where multiple institutions need to work together without exposing sensitive data. Some key applications include:

1. **Fraud Detection**: Enables banks to jointly detect fraud patterns without sharing customer data.
2. **Joint Risk Analysis**: Allows financial institutions to assess risks across different datasets without revealing proprietary data.
3. **Collaborative Credit Scoring**: Multiple banks can jointly compute credit scores while keeping individual data private.
4. **Anti-Money Laundering (AML)**: Institutions can collaborate on detecting suspicious transactions without sharing raw data.

SMPC Use Cases



Consumer Trust and Data Privacy

SMPC helps financial institutions maintain consumer trust by ensuring that their data remains private, even when collaborating with other organizations.

This is critical in today's landscape, where consumers expect their data to be handled with the highest level of security.

Companies Adopting Secure Multi-Party Computation

Several leading financial institutions and technology companies are adopting SMPC to enhance data privacy while enabling secure collaboration.

Companies such as JP Morgan, IBM, and Visa are using SMPC to protect sensitive data while performing joint computations with other institutions.

Brands who use SMPC

Summary

Secure Multi-Party Computation (SMPC) provides a robust solution for financial institutions that need to collaborate on data-driven tasks without compromising privacy. As data privacy regulations become more stringent, SMPC allows organizations to comply with regulations while preserving data security, making it an essential technology in the financial sector.