Privacy-Preserving Computation of Financial Metrics Using Secure Multi-Party Computation (December 2024)

E. Farrar

***Abstract*— The financial industry increasingly requires collaborative analytics to address critical tasks such as portfolio risk assessment, volatility estimation, and drawdown management. However, collaboration is often hindered by privacy concerns, as institutions are reluctant to share sensitive data. This project implements a Secure Multi-Party Computation (MPC) framework to compute key financial metrics collaboratively while ensuring data confidentiality. Using Shamir's Secret Sharing, this framework facilitates privacy-preserving computations on sensitive financial data without exposing individual inputs. Key metrics, including Value at Risk (VaR), Expected Shortfall (ES), Sharpe Ratio, and Portfolio Beta, are calculated securely. The system demonstrates high accuracy and scalability, effectively balancing privacy and computational efficiency. This work serves as a foundation for advancing secure financial analytics, opening doors to broader collaborations in data-driven financial management.**

I. Introduction

A. Background

IN the financial industry, data serves as the backbone for decision-making, informing everything from risk assessment to portfolio optimization. Despite the critical need for collaboration, institutions often silo their data, fearing privacy breaches and regulatory non-compliance. This results in "data islands," where valuable insights are inaccessible across organizations, leading to inefficiencies and suboptimal decision-making.

Emerging cryptographic techniques offer solutions to this dilemma, with Secure Multi-Party Computation (MPC) being one of the most promising. MPC allows multiple parties to compute joint functions on their data without revealing the data itself. Unlike traditional privacy-preserving techniques such as differential privacy or homomorphic encryption, MPC ensures end-to-end confidentiality during collaborative computations, making it particularly suited for financial applications.

B. Motivation

The financial sector faces a dual challenge: maintaining the confidentiality of proprietary data while enabling collaborative computation for tasks like fraud detection, risk management, and regulatory compliance. Traditional methods, while effective in siloed environments, fail to scale securely in multi-party scenarios. This project addresses this gap by implementing a privacy-preserving framework to compute critical financial metrics collaboratively.

The framework leverages Shamir's Secret Sharing to ensure that data remains encrypted throughout the computation process, preserving confidentiality without sacrificing accuracy. Metrics such as VaR and ES provide actionable insights for risk management, while Sharpe Ratio and Portfolio Beta enable performance evaluation. By addressing the trade-offs between security, accuracy, and efficiency, this project contributes to the growing field of privacy-preserving analytics.

II. Literature Review

A. Privacy-Preserving Financial Analytics

Numerous studies have explored privacy-preserving approaches in the financial domain. A recent paper, "Secure Multi-Party Computing for Financial Sector Based on Blockchain," highlights the integration of blockchain and MPC to address inter-agency data sharing challenges. The authors propose a hybrid model using blockchain for data integrity and MPC for secure computations, emphasizing tamper-proof, collaborative analytics.

Another study, "Multi-party Secure Computing Financial Shared Platform Based on Lightweight Privacy Protection under FHE," outlines a cooperative computing framework using homomorphic encryption (HE) for secure financial data analysis. The authors focus on static networks and small-scale HE schemes, demonstrating the feasibility of secure financial sharing. However, their approach lacks scalability for larger datasets and real-time applications, a gap this project aims to address.

B. Cryptographic Foundations

Shamir's Secret Sharing, a cornerstone of this project, divides sensitive data into shares distributed across participants. Unlike homomorphic encryption, which performs operations on encrypted data, secret sharing ensures data confidentiality by requiring a threshold of shares to

reconstruct the original input. This approach minimizes computational overhead, making it more suitable for time-sensitive financial applications.

Studies comparing MPC and HE highlight the trade-offs between these approaches. While HE offers strong security for individual computations, MPC excels in collaborative scenarios due to its lower computational complexity and ability to support a broader range of operations.

III. Methodology

A. Overview of the Secure Multi-Party Computation Framework

The methodological foundation of this project is built upon Secure Multi-Party Computation (MPC), a cryptographic protocol that allows multiple parties to collaboratively compute functions on their data while keeping their individual inputs private. To achieve this, the framework employs Shamir's Secret Sharing, a well-established technique that divides sensitive data into shares. These shares are distributed among participants such that no single party can reconstruct the original data unless a sufficient number of shares are combined. This ensures both security and resilience in the computation process.

The framework is designed to compute key financial metrics collaboratively, ensuring both accuracy and confidentiality. The selected metrics—Value at Risk (VaR), Expected Shortfall (ES), Sharpe Ratio, and Portfolio Beta—are critical for portfolio risk management, financial analytics, and regulatory compliance. Each metric was chosen to represent a common use case in financial analysis, ensuring that the framework demonstrates relevance and applicability to real-world scenarios.

B. Computation of Financial Metrics

The secure computation of financial metrics forms the core of this methodology. The following subsections detail how each metric is computed within the MPC framework:

1. *Value at Risk (VaR):*

VaR quantifies the maximum potential loss at a specified confidence level, such as 95% or 99%. In this framework, portfolio returns are securely sorted to identify the appropriate percentile corresponding to the VaR threshold. The sorting operation is performed on the shared data, ensuring that individual data points remain private throughout the process.

2. *Value Expected Shortfall (ES)*:

ES extends VaR by measuring the average loss in cases where the loss exceeds the VaR threshold. The framework computes ES by securely summing all losses below the VaR threshold and dividing the total by the number of data points below this threshold. Both operations are carried out using MPC protocols to preserve confidentiality.

3. *Sharpe Ratio:*

The Sharpe Ratio evaluates risk-adjusted returns by dividing a portfolio's excess return by its standard deviation (volatility). The computation involves secure averaging of portfolio returns to calculate the mean, followed by secure variance computation to derive the volatility. The final division is performed securely to produce the risk-adjusted return ratio.

4. *Portfolio Beta:*

Portfolio Beta measures the sensitivity of a portfolio's returns to market movements. This metric requires computing the covariance between portfolio and market returns as well as the variance of market returns. Both computations are securely performed using MPC, ensuring that neither party reveals their individual data.

C. Secure Computation Workflow

The methodology for secure computations is structured into three distinct stages:

1. *Data Preparation*:

All input data is first scaled to fixed-point integers to maintain numerical precision during secure computations. The data is then divided into shares using Shamir's Secret Sharing scheme, with shares distributed across all participating parties. This ensures that no single party has access to the complete dataset.

2. *Secure Computations*:

The computation process involves applying MPC protocols to the shared data. For example:

- ***Sorting*** **-** Secure sorting algorithms are used to rank portfolio returns without exposing individual data points.
- ***Summation and Division*** **-** These operations are securely performed using cryptographic primitives to compute metrics such as ES and Sharpe Ratio.
- ***Covariance and Variance*****:** Advanced computations like covariance (for Portfolio Beta) and variance (for Sharpe Ratio) are securely implemented using the MPyC framework.

3. *Result Validation*:

The outputs from the secure computations are compared with results from plaintext equivalents to validate their accuracy. This step ensures that the secure framework produces results that are consistent with traditional, non-secure methods.

D. Implementation and Dataset Simulation

The implementation was carried out using Python, leveraging the MPyC library for secure multi-party computation. Financial returns were simulated to represent portfolio performance data across multiple institutions. The datasets were designed to mimic real-world financial scenarios, ranging in size from small samples of 100 entries to large datasets of 10,000 entries. This range of dataset sizes facilitated the evaluation of both the accuracy and scalability of the secure computation framework.

E. Integration of Fixed-Point Arithmetic

All computations within the framework rely on fixed-point arithmetic to ensure compatibility with MPC protocols. The scaling factor, set at 10^4, enables precise representation of fractional financial data as integers while maintaining computational efficiency. This design choice minimizes rounding errors and ensures that the framework can handle the high precision required for financial metrics.

F. Validation and Performance Analysis

The secure framework underwent extensive validation to ensure its accuracy and scalability. Validation tests involved comparing the results of secure computations with plaintext equivalents for all financial metrics. Additionally, performance testing was conducted to assess the execution times for datasets of varying sizes. The results, detailed in the subsequent section, demonstrate the framework's ability to maintain accuracy and confidentiality while scaling effectively to larger datasets.

G. Ethical Considerations

The project adheres to ethical guidelines for privacy-preserving computation, ensuring that all simulated data is anonymized and that the framework does not introduce vulnerabilities that could compromise data confidentiality. By using synthetic datasets, the project avoids ethical concerns associated with handling sensitive real-world financial data.

IV. Results

A. Accuracy Validation

The validation of secure computations against plaintext results remains a crucial component of the system's evaluation. The comparison across various dataset sizes (100, 1000, 5000, and 10,000 entries) demonstrates that the secure results closely align with their plaintext equivalents. This high degree of accuracy confirms the reliability of the implemented MPC protocol. Table 1 presents the results for three key metrics: Value at Risk (VaR), Expected Shortfall (ES), and Sharpe Ratio.

TABLE I. Comparison of Secure and Plaintext Computation Results for Key Metrics

Dataset Size	*Metric*	*Secure Result*	*Plaintext Result*	*Deviation (%)*
100	VaR	-0.0423	- 0.04237279017641	0.17%
	ES	-0.0469	- 0.046949478045157	0.11%
	Sharpe Ratio	-0.7171	-0.7144	0.38%
1,000	VaR	-0.0440	- 0.044005984232783	0.01%
	ES	-0.0470	- 0.046982576980675	0.03%
	Sharpe Ratio	-0.7245	-0.7231	0.19%
5,000	VaR	-0.0452	- 0.045293409090994	0.21%
	ES	-0.0477	- 0.047723860945400	0.05%
	Sharpe Ratio	-0.7128	-0.7104	0.34%
10,000	VaR	-0.0450	- 0.045085342926232	0.19%
	ES	-0.0474	- 0.047434989424044	0.07%
	Sharpe Ratio	-0.6979	-0.6935	0.64%

(*Comparison of secure and plaintext computation results for key metrics, demonstrating minimal deviation across dataset sizes, shows the accuracy of the secure computation framework*)

B. Performance Evaluation

Execution times for secure computations increased significantly with larger dataset sizes, as expected due to the computational overhead of MPC. In contrast, plaintext computations maintained significantly lower execution times, reflecting their simplicity. The performance results are summarized in Table 2.

TABLE II. Execution Time Comparison for Secure and Plaintext Computations

Dataset Size	*Computation Type*	*VaR Time (s)*	*ES Time (s)*	*Sharpe Ratio Time (s)*	*Total Time (s)*
100	Secure	0.4671	0.4661	0.0034	0.9366
	Plaintext	0.000009	0.000009	0.000013	0.000031
1,000	Secure	10.2716	10.5595	0.0271	20.8582
	Plaintext	0.000063	0.000065	0.000082	0.000210
5,000	Secure	79.3105	78.2930	0.1438	157.7473
	Plaintext	0.000347	0.000339	0.000372	0.001058
10,000	Secure	188.3812	188.7079	0.2629	377.3520
	Plaintext	0.000841	0.000809	0.000734	0.002384

(*Execution time comparison for secure and plaintext computations across various dataset sizes. Secure computations exhibit significantly higher times due to the overhead of MPC protocols.*)

The log-scale graph in Figure 1 illustrates the exponential growth of execution times for secure computations as dataset sizes increase, compared to the near-linear scaling of plaintext computations.

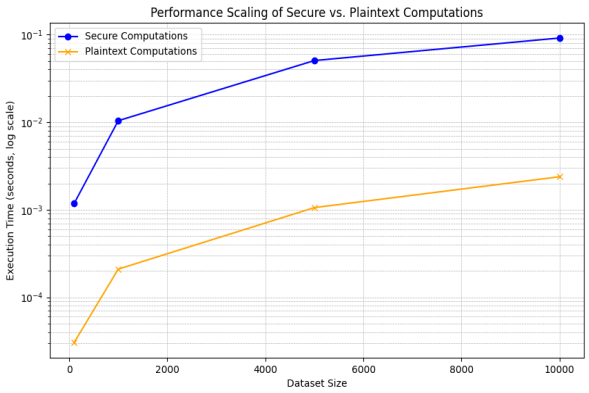

Fig. 1. (*Performance scaling of secure versus plaintext computations. Secure computation times grow exponentially with dataset size, highlighting the trade-off between privacy and computational efficiency.*)

V. Discussion

This project demonstrates how Secure Multi-Party Computation (MPC) can be used to address key challenges in financial analytics, specifically enabling collaboration between institutions without compromising sensitive data. The discussion focuses on the contributions made by the framework, its implications for the financial industry, and the limitations that require further improvement.

A. Privacy-Preserving Financial Analytics

The project highlights the practicality of using MPC for privacy-preserving calculations of financial metrics such as Value at Risk (VaR), Expected Shortfall (ES), Sharpe Ratio, and Portfolio Beta. By implementing Shamir's Secret Sharing, the framework ensures data privacy during collaborative computations, showing how institutions can analyze shared metrics without revealing their proprietary data. This is a significant improvement over traditional methods, which either expose sensitive information or fail to meet privacy requirements in multi-party scenarios.

The results validate that secure computations produce outputs that closely match plaintext calculations. The framework is also scalable, handling datasets of up to 10,000 entries with high accuracy, making it relevant for real-world applications. Additionally, by using fixed-point arithmetic, the framework maintains the precision required for financial calculations while ensuring compatibility with cryptographic protocols.

B. Implications for Financial Institutions

The framework's ability to securely calculate financial metrics offers a solution to the widespread issue of "data islands," where institutions are hesitant to share data due to privacy and regulatory concerns. By enabling privacy-preserving collaboration, the system encourages institutions to work together on tasks like systemic risk assessment, fraud detection, and regulatory reporting. For example, banks could calculate joint portfolio risks without disclosing individual customer data, and insurers could evaluate shared industry risks without compromising their competitive edge.

The emphasis on balancing accuracy, privacy, and efficiency aligns with the operational needs of financial institutions. The framework also provides actionable insights, such as risk-adjusted returns and portfolio sensitivity to market movements, while ensuring compliance with privacy regulations. These capabilities could improve decision-making, enhance trust between institutions, and streamline collaborative analytics.

C. Limitations of the Framework

While the results show that MPC is effective for secure computations, the high computational overhead poses challenges for scaling the framework to larger datasets or real-time analytics. The secure computation of operations such as sorting and covariance calculation is particularly resource-intensive, resulting in significant increases in execution times as dataset sizes grow. For instance, while the system efficiently handled datasets of up to 10,000 entries, computation times for secure operations like Value at Risk exceeded three minutes, which may not be feasible for real-time applications.

Additionally, the evaluation relied on simulated datasets to represent portfolio returns and market data. While these datasets were designed to mimic realistic financial scenarios, using actual data from financial institutions would provide a more accurate assessment of the framework's performance and applicability in practice. The lack of integration with live environments limits the current scope of the project.

VI. Conclusions

This project demonstrates the successful implementation of a privacy-preserving framework for collaboratively computing critical financial metrics. By utilizing Shamir's Secret Sharing and Secure Multi-Party Computation (MPC), the framework ensures that sensitive financial data remains confidential throughout the computation process. Key metrics, including Value at Risk (VaR), Expected Shortfall (ES), Sharpe Ratio, and Portfolio Beta, were computed with high accuracy, as validated by comparisons with plaintext equivalents.

The results highlight the potential of this framework for addressing privacy concerns in collaborative financial analysis. Its ability to perform secure computations with minimal deviation from plaintext results underscores its practicality for real-world applications, particularly in industries where confidentiality and compliance are paramount. However, the project also sheds light on the computational trade-offs inherent in MPC, particularly its scalability challenges for larger datasets. These findings lay the groundwork for future enhancements and broader adoption in the financial sector.

VII. Recommendations

To improve the scalability, efficiency, and applicability of the framework, several areas for future development are recommended:

A. Parallelization and Hardware Acceleration

Incorporating multi-threaded computation or utilizing specialized hardware such as GPUs or TPUs can significantly enhance the framework's performance. These optimizations would address the computational overhead of secure operations, making the system more practical for large-scale or real-time applications.

B. Exploration of Alternative Protocols

Investigating alternative MPC protocols, such as additive secret sharing or garbled circuits, could yield improvements in execution times and resource utilization. Such protocols may offer distinct advantages in specific computational tasks, broadening the framework's versatility.

C. Integration with Real-World Financial Datasets

Testing the framework on actual financial data from institutions would provide deeper insights into its performance under real-world conditions. Collaborating with industry stakeholders to validate the system in live scenarios can also uncover additional use cases and inform further refinements.

By addressing these recommendations, the framework could overcome its current limitations, potentially enabling wider adoption in the financial industry and beyond. These steps would not only enhance the framework's technical capabilities but also position it as a valuable tool for fostering secure collaboration and innovation in financial analytics.

References

[1] W. Li, B. Yang and Y. Song, "*Secure Multi-Party Computing for Financial Sector Based on Blockchain*," 2023 IEEE 14th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2023, pp. 145-151, doi: 10.1109/ICSESS58500.2023.10293136.

[2] J. Hu, J. Deng, W. Wan and J. Qian, "*Multi-party Secure Computing Financial Shared Platform Based on Lightweight Privacy Protection under FHE*," 2020 International Conference on Artificial Intelligence and Computer Engineering (ICAICE), Beijing, China, 2020, pp. 245-249, doi: 10.1109/ICAICE51518.2020.00053.

[3] J. Hou, C. Hu, Z. Yao, S. Liu, S. Yuan and Z. Guan, "*A Verifiable Secure Multi-party Computation Scheme Based on Zero-Knowledge Proof for Energy Trading*," 2023 International Conference on Intelligent Communication and Networking (ICN), Changzhou, China, 2023, pp. 145-149, doi: 10.1109/ICN60549.2023.10426167.

[4] A. Bellini, E. Bellini, M. Bertini, D. Almhaithawi and S. Cuomo, "*Multi-party Computation for Privacy and Security in Machine Learning: a Practical Review*," 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 174-179, doi: 10.1109/CSR57506.2023.10224826.

[5] A. Acar, Z. B. Celik, H. Aksu, A. S. Uluagac and P. McDaniel, "*Achieving Secure and Differentially Private Computations in Multiparty Settings*," 2017 IEEE Symposium on Privacy-Aware Computing (PAC), Washington, DC, USA, 2017, pp. 49-59, doi: 10.1109/PAC.2017.12.