Secure Multi-Party Computation Research Report

Privacy Technology for Financial Intelligence

Trimester 3, 2023

Introduction 3
A. Background 3
B. Objective 3
Secure Multiparty Computation (SMPC) overview 3
C. Secure Multi Party Computation methodology 4
Use cases of Multi Party Computation 5
Advantages of Secure Multiparty Computation 6
Limitations of Secure Multiparty Computation 6
Application in Financial Crime 7
How can it help increase collaboration to combat financial crime 7
SMPC and Federated Learning 7
References 8

Introduction

Background

In the current days organizations are increasingly concerned about data security and data privacy from various aspects, this includes collecting and retaining sensitive personal information, processing this information in internal and external environments where other users may access it, and sharing this information with other parties. Many of commonly implemented solutions do not provide strong protection from data theft and privacy disclosures. Risk management professionals and regulatory bodies becoming more concerned about privacy and security of data used for multiple purposes. Compliance to privacy regulations such as the US State of California Consumer Privacy Act (CCPA), the EU General Data Protection Regulation (GDPR) and other emerging regulations around the world require techniques for secure processing of sensitive data. In this report delves into one of the common privacy technologies to preserve data privacy called Secure Multi Party Computation (SMPC), with the focus on the application of it in Financial Intelligence realm. It will also evaluate its advantages and limitations and will explore some of the real-world applications of this method in tackling Financial Crime.

Objective

- Understand SMPC method and its applications in general.
- Investigate the applications and benefits of SMPC in financial intelligence area.

Secure Multiparty Computation (SMPC) overview

Secure Multiparty Computation (SMPC) is a technique that allows multiple parties to collaborate on getting a specific output from a function over their individual inputs while maintaining those input in secret and not revealing them.

SMPC start to be theorised as mathematical and cryptographical concepts in 1982 with the so-called Millionaires' Problem, however Companies institutions and organizations have only started utilizing MPC in real-world scenarios in the last fifteen years or so. in 1986 by Andrew Yao so called Garbled Circuits. They both introduce two party computation which later was followed by Multi Party Computation[1]. The computation and implementation of SMPC became plausible in mid 2000s with the first practical use of SMPC was to calculate sugar beet market prices in Denmark, keeping the farmers' private data confidential (Maxwell, 2020, p.13).

In 2011, as part of an efficiency improvement effort, Cybernetica's Sharemind PMC solution was utilized by the Estonian Association of Information Technology and Telecommunications. This application enabled 17 companies to confidentially process their financial performance metrics without revealing sensitive data, completing the task in just two minutes (Maxwell, 2020, p.13). In 2016, CSIRO's Data61 was established to advance Australia's strategic data-centric projects and later create the 'Confidential Computing' platform. This platform integrates distributes machine learning with homomorphic encryption and secure multiparty computing, enabling the analysis of combined datasets while keeping the data secure at its source. Data61 confirmed that the encrypted computations yielded results as accurate as those processed without encryption (Maxwell, 2020, p.13).

[1] Introduced by Goldreich, Micali and Widgerson 1987

Secure Multiparty Computation (SMPC) also has been used as a cryptographic technique that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. This is achieved through the use of cryptographic protocols that enable secure computation without revealing the individual inputs. The core principles of MPC include privacy-preserving collaborative computation, secure communication channels, and the prevention of any individual party from learning more than it should.

Secure Multi Party Computation methodology

Over the past three decades, many different techniques have been developed for creating SMPC protocols with different elements, and for different settings. One of the common SMPC protocols is called "Secret Sharing" which is built upon a zero-trust system by allowing mutually distrustful parties to conduct secret sharing.

In secret sharing, first introduced by Adi Shamir[2], data is divided into shares that are themselves random, but when combined (for example, by addition) recover the original data. SMPC relies on dividing each data input item into two or more shares and distributing these to compute parties. The homomorphic properties of addition and multiplication allow for those parties to compute on the shares to attain shared results, which when combined produce the correct output of the computed function. To perform the shared computation required for SMPC, all participating compute parties follow a protocol : a set of instructions and intercommunications that when followed by those parties implements a distributed computer program.

The formal description of SMPC as described by (Zhao et. al. 2019, 358) is as follows "two or more P_i $(i = 1, . . ., n)$ with private inputs x_i in a distributed computing environment wish to jointly and interactively compute an objective functionality $f(x_1, x_2, . . ., x_n) = (y_1, y_2, . . ., y_n)$ based on their private inputs. Once the computation is complete, each party P_i should obtain its own corresponding output y_i without acquiring any other information". In order words the objective of SMPC is to facilitate a group of independent data owner who may not trust each other to compute a function that depends on all private inputs without revealing their individual private inputs.

C. Zhao et al. / Information Sciences 476 (2019) 357–372

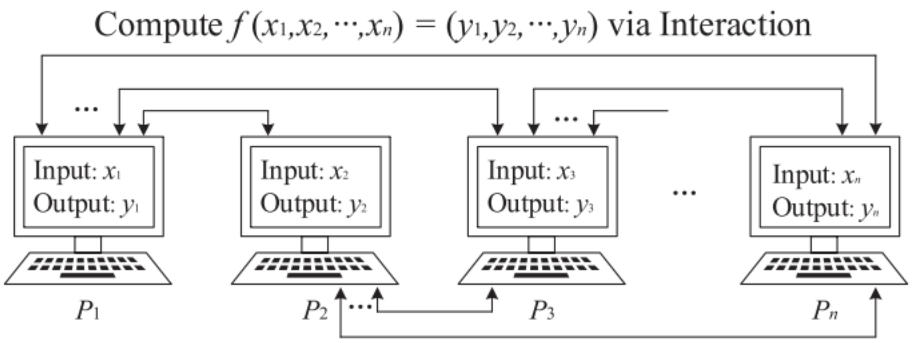

Fig. 1. Diagram of Secure Multi-Party Computation.

To get an idea of how the multiparty computation works, we explain it through an example. Imagine we need to analyse current salaries of various careers in the health care industry. Salaries are usually

[2] See for detail Shamir, A. (1979) How to Share a Secret. Communications of the ACM, 22, 612-613. http://dx.doi.org/10.1145/359168.359176

private information, so it is important that individuals and companies not have to share this private information. However, by studying the average salaries of various fields, you are hoping to get a sense of where the health care industry may see a higher rate of growth in the years to come.

For this example, say you are interested in the salaries of registered nurses who work in intensive care units. Nurse A's salary is $100K. In additive secret sharing, the multiparty computation protocols split this $100K into three randomly generated shares: $40K, $35K, and $25K. Nurse A then keeps one of these secret shares ($40K) for herself and distributes one secret share each to Nurse B ($35K) and Nurse C ($25K).

The salaries of Nurse B and Nurse C follow the same multiparty computation protocol. When the secret sharing is completed, each person holds three secret shares: one from Nurse A's salary, one from Nurse B's, and one from Nurse C's.

At this point, all three nurses have contributed their personal information, yet no nurse is able to determine the exact salary of any other nurse. Therefore, the data remains private.

Use cases of Multi Party Computation

Title	**Breaking Bad Actors**	**Data share Team**	**Secret Computers**	**TNO Multi-Party Computation for AML (MPC4AML) Proof of concept**
Sector	Banking and financial services	Banking and financial services	Banking and financial services	Banking and financial services
Objective	a solution, using multi-party computation, to allow the real-time assessment of outbound and inbound payments to identify mismatches between account names or other risk factors.	a solution, using multi-party computation, that creates a system where financial institutions can upload encrypted data about a customer and receive predefined information about that customer from other institutions.	a solution, using secure multi party computation, to identify suspicious transaction networks across multiple institutions in order to identify patterns that an individual institution would not see.	risky money (originated from cash deposit or cryptocurrencies) is transferred via multiple bank accounts from different banks to obfuscate money laundering. The research question is: How can banks more effectively detect money laundering by collaborative transaction analysis, while respecting privacy?
Information revealed	Able to match payments without revealing private data	Participants upload encrypted data via secure API, several computations done, and results given to banks based on set of pre-agreed	No personal data is revealed only encrypted secret shares are exchanged amongst participants in a company	The secure analysis uses transaction data, but only the bank accounts' (risk-score based) associations with suspected 'risky money' transactions are revealed

		queries. No private data is revealing		
Participants	Partisia, Sedicii, Goldman Sachs, Ex Ante Advisory, UBS and Deloitte	Cybernetica, Data Miner, RBS, Societe Generale and PWC	Inpher, Goldman Sachs, Standard Chartered and Eversheds	3 organizations: TNO, ABN AMRO (bank), Rabobank (bank)
Type of data	Transaction data	Transaction data	Transaction data	Synthetic data

Source: Maxwell, N (2020) '*Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime'*

Source: 2019 Global AML and Financial Crime TechSprint: https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint

Advantages of Secure Multiparty Computation

Secure Multiparty Computation enables to reduce the risk if data leak and privacy disclosure. Some of the key advantages of this method are as the following:

- **Privacy control**: SMPC methods ensure the data and privacy of participants remain private. It allows the parties to still perform the activity that is required though processing of data with SMPC, while their individual information is kept unrevealed. Whilst some other techniques such as encryption method like obfuscation try to protect data, they are still prone to attacks and the risk of data leakage, whereas SMPC is more effective in eliminating the risk of data being accessed by a malicious party.

- **Collaborative analysis**: SMPC allows multiple parties or organisations perform an analysis or detection on sensitive information jointly while their own information is not shared to other parties. This will enable broader cross organisation collaboration to achieve mutual benefit and outcome and gain conclusive cross organisation insights.

- **Versatile application**: SMPC protocols can be utilised in various use cases and scenarios. This includes data sharing across industries to detect financial crime and Money Laundry activities, health care data sharing, market clearing and betting products and compliance reporting.

- **Accuracy**: Computations can be carried out accurately on the combined data without compromising privacy, which is beneficial for sensitive data analysis.

- **Regulatory Compliance**: It can help organisations comply with data protection regulations by processing data without revealing it.

Limitations of Secure Multiparty Computation

Despite its potential, various barriers hinder SMPC adoption by institutions:

- **Complexity**: Implementing SMPC protocols is complex and require significant expertise in cryptography. It also requires additional architectural components to support the requirements of the privacy preserving protocols
- **Performance**: SMPC can be computationally intensive and slower than traditional computations, particularly as the number of parties involved increases. This has hindered these methods to be very practical in some of the use cases.
- **Scalability**: Large-scale applications of SMPC can be challenging due to the increased computational and communication overhead.

- **Cost**: due to the high complexity and high computational power that is required to implement the SMPC, it is still considered to involve high processing and implementation cost.

Application in Financial Crime

Financial Crime refers to illegal acts committed by an individual or a group of individuals to obtain a financial gain. These crimes are typically characterized by deceit or a breach of trust and are motivated by money, property, or services. Financial crime, ranging from fraud such as identity theft to large-scale operations like money laundering—estimated at around $2 trillion annually by the UNODC[3]—disproportionately affects vulnerable populations, underscoring the urgency for implementing privacy-preserving technologies to counteract these crimes.

Financial institutions combat financial crime by monitoring transactions, and adhering to AML rules, but they are constrained by privacy concerns, data breach risks, and stringent regulatory compliance, hindering the free exchange of information. Data-sharing can enhance the detection of crimes and predictive analytics to prevent financial crimes. Privacy-preserving technologies such as Secure Multiparty Computation (SMPC) enable financial institutions to share data crucial for fighting financial crime without compromising individual privacy. SMPC facilitate secure collaboration, allowing institutions to pool data, identify patterns, and address potential threats collectively while adhering to privacy regulations and protecting sensitive information.

How can it help increase collaboration to combat financial crime

SMPC can play a critical role in allowing financial institutions to collaborative on financial intelligence activities, where they can aim to identify patterns and anomalies indicative of financial crime without compromising confidential data. When it comes to fraud detection and prevention, SMPC helps financial institutions, regulatory bodies, and law enforcement agencies to collaborate on comprehensive data analysis to detect financial crime without violating regulatory requirements. Some of the areas that organisations can leverage SMPC to combat financial crime are as the following:

- **Transaction Monitoring and Fraud Detection:** Financial institutions can collaborate through SMPC to identify patterns of suspicious transactions across their customer bases or to interact on a targeted activity for investigation. Each party can contribute to sharing information about potentially suspicious transactions, and the joint computation helps the detection of the overall trends without compromising the privacy of individual customer data

- **Customer onboarding and Due Diligence**: SMPC can contribute to customer in boarding and customer due diligence processes. Financial institutions often do not get visibility of the activity of their customers in other banks or institutions. This can hinder them from knowing the history of the potential financial criminal activity of the customer in other places. Leveraging SMPC, they can jointly assess the risk associated with new customers without sharing sensitive information with each other directly.

SMPC and Federated Learning

Federated Learning is a technique that enables a large number of users to jointly learn a shared machine learning model, managed by a centralized server, while the training data remains on user devices. That said, federated learning reduces data privacy risks. Privacy concerns still exist since it is possible to leak information about the training data set from the trained model's weights or parameters. Most federated learning systems use the technique of differential privacy to add noise to the weights so that

[3] United Nations: Office on Drugs and Crime. https://www.unodc.org/unodc/en/money-laundering/overview.html#:~:text=The%20estimated%20amount%20of%20money,Terrorist%20Financing

it is harder to reverse-engineer the individual data sets. Differential privacy reduces the risk but does not eliminate leakage from the data. The combination of differential privacy and cryptography can eliminate potential leakage in data reconstruction attacks. However, adding the randomness and noise can reduce the accuracy of the input data.

Secure Multiparty Computation can help keep the privacy without compromising data accuracy. With this approach the parties only learn the final output of the models without revealing their input. In this method the output of the locally trained models on each party's data, will be shared to construct a global model as input into that model.

This approach can help institutions to collaborate on utilising Machine Learning and AI capabilities for specific use cases such as Money Laundry and Financial Crime detection without compromising data privacy.

This approach is being touched on this paper as one of the use cases where SMPC can be utilised to further collaborate on enhancing Financial Intelligence capabilities and advancements. More details on the Federated Learning and Differential Privacy method are provided separately.

References

- Agahari, W. Ofe, H. and Reuver, M. (2022). *It is not (only) about privacy; How multi-party computation redines control, trust, and risk in data sharing.* Springer, 32, 1577-1602.
- Financial Conduct Authority (FCA). (2019) *2019 Global AML and Financial Crime TechSprint.* https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint
- Goldreich, O. Micali, S. and Wigderson (1987) *How to Play Any Mental Game –A Completeness Theorem for Protocols with Honest Majority,* Proceedings of the 19th Annual ACM Symposium on Theory of Computing. New York, pp. 218-229.
- IEEE Digital Privacy, *Application of Multiparty Computation* accessed November 2023. Applications of Multiparty Computation - IEEE Digital Privacy
- ISACA, *Privacy Preserving Analytics and Secure Multiparty Computation* accessed November 2023. Privacy-Preserving Analytics and Secure Multiparty Computation (isaca.org)
- Maxwell, N. (2020). *Innovation and discussion: Case studies of the use of privacy-preserving Analysis to tackle financial crime.* Future Intelligence Sharing (FFIS) research programme, Version 1.3.
- Nasdaq, *Multi-Party Computation Technology can ensure effective fraud detection*, accessed November 2023, Multi-Party Computation (MPC) Technology Can Ensure Effective Fraud Detection | Nasdaq
- Shamir, A. (1979) *How to Share a Secret*. Communications of the ACM, 22, 612-613. http://dx.doi.org/10.1145/359168.359176
- TNO innovation for life, Bundling forces in money laundering detection using MPC, accessed November 2023, Bundling forces in money laundering detection using MPC (tno.nl)
- Vaikkunth Mugunthan, A., Polychroniadou, A., Byrd, D., & Hybinette Balch, T. (2019) *SMPAI: Secure Multi-Party Computation for Federated Learning*, in Proceedings of the 33rd Conference on Neural Information Processing System (NeurIPS) 19 Workshop on Robust AI in Financial Services: Data, Fairness, Explainability, Trustworthiness, and Privacy, pp. 1-9, MIT press Cambridge, MA, USA.
- Veugen, T. (2022). *Secure Multi-party Computation and Its Applications,* accessed November 2023, Secure Multi-party Computation and Its Applications (springer.com)
- Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & Tan, Y.-a. (2018). *Secure Multi-Party Computation: Theory, Practice, and Applications*. Elsevier, 476, 357-372.