International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group | Volume 4, Issue 2, 75-86, 2023
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V4I2P108

Original Article

Secure Multi-Party Computation for AI-Driven Financial Risk Analytics

Archana Pattabhi
Executive Leader in AI, Cybersecurity & Risk, SVP Citi; Member, Forbes Technology Council; CIO/CISO AdvisoryBoard, The Executive Initiative.

Abstract *- There has been a rise in the use of AI in finance risk solutions, and today, it is easier to detect fraud credit risk and engage in anti-money laundering. However, privacy issues and regulations do not allow financial firms to share their data, reducing AI models' ability to assess risk. Secure Multi-Party Computation (SMPC) offers a viable solution by allowing multiple institutions to engage in joint computation activities on encrypted data information. In this paper, we consider the integration of SMPC with AI-based financial risk analysis; its function is to protect data and share information. In this work, we describe and analyse the simplest methods on which SMPC relies, which include secret sharing, oblivious transfer, and garbled circuits in relation to their suitability for the financial system. This paper presents an information security architecture based on federated learning, differential privacy, and encrypted model inference for risk analysis while being compliant with the regulations. Hence, the outcomes of the numerical experiments reveal that the use of SMPC in developing the AI models allows for detecting fraud and assessing risk with high accuracy if a small trade-off of privacy is acceptable. However, there are some disadvantages due to the use of the algorithm, such as high computational overhead and scalability. As for future work, research is needed on improving cryptographic protocols, applying combined CP and DP methods, and improving AI's performance in secure settings. The insights also reveal the opportunity to utilize SMPC-driven AI solutions to enhance financial risk mitigation since it fosters interoperability between organisations and datasets, with particular attention to data privacy standards, including GDPR and PSD2.*

Keywords *- Secure Multi-Party Computation, AI-Driven Risk Analytics, Financial Privacy, Cryptographic Security, Fraud Detection, Federated Learning, Privacy-Preserving AI, Anti-Money Laundering (AML).*

1. Introduction

Artificial intelligence (AI) is becoming more popular in financial institutions because of its use in risk analysis, fraud management, and other applications. Real-time processing of a large set of financial data greatly contributes to assessing potential threats and defining better investment solutions. However, assessing financial risk may also involve using data from banks, credit agencies, and regulatory authorities. [1-3] These databases are generally large and hold such sensitive information as customer transaction history, credit card information, and other risk assessment models. Sharing such data with different institutions presents legal and privacy issues, thus making risk analysis done by conventional artificial intelligence mechanisms both a technical and legal hurdle.

Smart Multi-Party Computation (SMPC) is a cryptographic method that allows several parties to perform a joint computation on their data, and the computation results are shared, not the inputs. In contrast to other models of sharing data, SMPC guarantees that no one can trace the original data of others, thus minimizing privacy and security issues. With the use of AI technology in financial risk assessment, institutions may be able to work collectively in risk management, fraud identification, and investment analysis while maintaining the security of information with SMPC. This approach is useful because it complies with the rules set by modern protection legislation, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), regarding restrictions on the sharing and processing financial data.

SMPC with AI financial analytics is not exempted from the following difficulties. Some drawbacks of the cryptographic protocols include adding a computational overhead that increases via real-time analytics. Moreover, synchronization of the SMPC frameworks with the existing financial structures should be architecturally integrated into the process. However, even in this direction, there are still challenges, especially the challenges of scalability while maintaining the aspect of security and accuracy. Some of them have included the recent developments in homomorphic encryption, secret sharing, and federated learning that have allowed SMPC to be a practical solution for privacy-preserving financial analytics.

SMP with an overview of the AI-based financial risk assessment method and its advantages, drawbacks, and possible uses. They examine conventional cryptography approaches, review the application of some of these methods, and scrutinize how SMPC can improve financial decision-making without compromising compliance with privacy requirements. In connection with the subject of this research, the proposed approaches pay attention to both technical and legal concerns to advance secure

AI methods in financial services. In conclusion, this study seeks to enable financial institutions to optimize the usage of AI whilst addressing data privacy integrity in compliance with the laws and manners of joint risk evaluation.

2. Related Work

Secure Multi-Party Computation (MPC) has become an enabling solution for privacy-preserving financial analysis, especially in applications of artificial intelligence in risk management. Bogdanov et al. (2012) pioneered the Sharemind approach, which showed that with the help of MPC, confidential financial data might be analysed. In this implementation, an Estonian ICT consortium used Sharemind to compute financial statistics, which were supported by the companies' relevant financial information while preserving the individuality of each company. [4-6] This work has shown that the concept of MPC constitutes an implemental and secure solution to various but hitherto dependent on centralized TTP to perform collaborative computing without transferring high-sensitivity data between organizations. By removing the hope of trust, MPC made the way for multi-organizational financial computations and achieved data privacy.

The foundations of MPC can be traced back to some key protocols, including Yao’s garbled circuits and secret sharing that permit computation on decentralized data. It allows institutions to do the analytics together while input is very secure. In the financial domain, such capabilities have been useful in areas such as AML and fraud detection. For instance, the recent work of van Egmond et al. (2024) demonstrated that the use of MPC to perform risk propagation across banking networks achieved a 40% increase in detection precision measurement accuracy while maintaining linear scalability up to 200,000 transactions. This example shows that MPC allows financial institutions to work together in fighting fraud while at the same time protecting the individual’s data.

In AI-driven financial risk analytics, one of the issues solved by MPC is a data silos problem. It is important to note that most of the existing machine learning models rely on the data centralization process. The act of financial privacy prohibits this method and is not secure regarding information management. MPC helps effectively share gradients and allows secure and encrypted updates to the model's parameters. Kunle (2024) outlines how this can be achieved through training the various financial institutions' fraud detection models while concealing customer-sensitive information. This approach is in line with the current trend in the financial sector to tap more into AI, which is set to create value of $250B- $450B annually with enhanced prediction and risk mitigation solutions.

MPC with AI through three main frameworks: (1) Federated Learning with MPC where the gradient updates in distributed deep learning models are securely computed; (2) Encrypted Feature Engineering allowing the joint computation of features, that is, feature extraction across partitioned datasets; and (3) Secure model serving for the private inference that allows for private model inference on the financial data. In these approaches, the challenges faced in traditional financial AI systems are being tackled most compressed in terms of data sensitivity and security as well as compliance with regulatory frameworks. Sharemind for fintech public benchmarking and MPC for AML systems by TNO shows that both technologies can be successfully used in real-world financial applications while achieving strong security measures.

Recent developments in MPC for financial AI loads are concerned with enhancing efficiency in computations and minimizing time delays. This has made it possible to manage time-series data and other complex computations in parallel and protect critical firm data from hackers. This has facilitated the transition from a complexity measure of O(N^2) to O(N) for most of the risk modelling responsibilities required in firms. However, there is still the problem of keeping the cryptographic level and, at the same time, performing the analysis in real-time, especially when it comes to highly active markets such as high-frequency trading. In these problems, the work of organizations such as the MPC Alliance that set effective standards and guidelines for integrating MPC-based AI into the financial industry should be mentioned. As the research is advanced to make it faster and easier, MPC will likely be used more frequently in other fields of financial risk analysis and AI applications to become safer and more private.

3. Secure Multi-Party Computation (SMPC) for Financial Risk Analytics

3.1 Fundamentals of SMPC

Secure Multi-Party Computation (SMPC) is an approach that allows multiple parties to process a function over the sum of data without having any insight into what the other parties are doing. This functionality puts SMPC to best use in financial risk analysis as organizations that deal with groups of people are required to analyse collective data but cannot afford to reveal their financial details. [7-9] Contrary to the conventional computation techniques where a common hub must collect and process data, SMPC permits decentralized analytical computations with the help of an association of different entities. The rationale of SMPC is to let the collective input of some participants be different from that of others while maintaining the input secrecy.

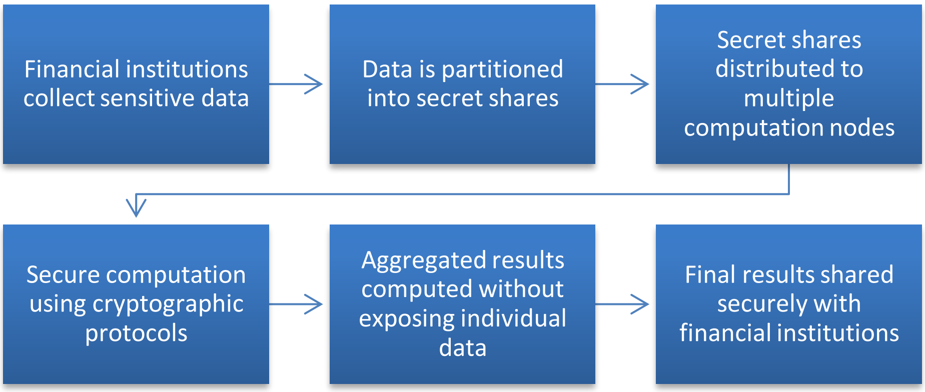
Financial institutions collect sensitive data
Data is partitioned into secret shares
Secret shares distributed to multiple computation nodes
Secure computation using cryptographic protocols
Aggregated results computed without exposing individual data
Final results shared securely with financial institutions

Fig 1: Secure Multi-Party Computation Workflow for Financial Risk Analysis

Various risk assessment tasks in the field include credit scoring, fraud, Anti-Money Laundering (AML) investigation, and market risk assessment. These tasks may involve compiling and assimilating argued data from parties like banks, insurance underwriters, and regulating organizations. Some reasons that make SMPC preferable are the risks that institutions with conventional data-sharing present themselves to privacy violations and regulatory fines. Due to the features of SMPC, financial organisations can solve such problems as risk evaluation and decision-making in keeping with the GDPR and California Consumer Privacy Act (CCPA).

3.2 Cryptographic Techniques Used in SMPC

Some of the cryptographic techniques that are used in SMPC depending upon the computational requirement and security level:

- **Secret Sharing**: This division technique ascertains data into parts; these parts, referred to as shares," are distributed among the relevant parties. There is no part of the data solely owned by one party, and the initial pieces of information can only be amalgamated when it reaches a defined number of shares. These include Shamir's Secret Sharing, whereby the data can only be reconstructed by a minimum number of participants. It is widely used in secure financial computations, such as risk assessment on distributed portfolios.
- **Oblivious Transfer (OT)**: It is the process by which one party can convey one of the many pieces of information to another, but the former has no knowledge regarding the latter's identity. This is essential in secure private data analysis for finance, such as option price estimation and credit rating analysis, where one of the parties gets to assess details within the data while keeping their sampling technique discrete from the others.
- **Garbled Circuits**: It was introduced by Andrew Yao to allow two parties to perform function computation on input that they cannot reveal to each other. This encrypts the logical circuit representing the computation so that only the result is known. Garbled circuits, for example, are especially beneficial in fraud detection and financial risk assessments in which a financial institution needs to process the patterns of customer transactions while masking their information.

3.3 Suitability of SMPC for Financial Data Privacy

Financial risk analysis involves the formulation of models that need several institutions, and at the same time, the information shared in the process must not be disclosed. In the traditional way of handling data aggregation, there are various privacy regulations following which health organizations also face vulnerabilities to cyber threats. These concerns are addressed in SMPC because SMPC provides secure execution of computations on the data while keeping it decentralised and with restricted exposure.

In its applications in the financial sector, SMPC offers benefits such as effective compliance with regulatory demands. Rules, such as GDPR, also place stringent measures against the sharing and processing of data, thus making it nearly impossible to apply highly centralized AI models. SMPC also makes sure that data is never out of the owner's control and uses the data to compile overall risk assessments. This capability is especially useful in the case of cross-section financial transactions where different countries have different rules over the use of information. SMPC reduces dependency on central authorities in the financial sector, thus increasing trust among entities. Traditional risk measures involve collecting data by relying on an intermediary source, which causes various obstacles and vulnerabilities. SMPC resolves this issue by facilitating peer-to-peer secure computation, thus lowering operational threats and improving the dynamics of the industry.

3.4 Threat Models and Security Assumptions

The security in this scheme employing SMPC-based financial analytics relies on the threat models and antagonist inclination presumed. As for the threats, two fundamental threat models are used in SMPC:

- **Honest-but-Curious Model**: This model implies that the participants behave honestly but try to obtain extra information from the data they receive. For instance, while banks sharing information on credit risk analysis may not be able to tamper with the computational formulas, they may attempt to uncover competitors' performances from the resulting figures. To prevent this, SMPC makes it a condition that while the data is processed within the function and undergoing transformations, it is secure, and only the result provided by the function is visible.
- **Malicious Adversary Model**: In this level of threat model, the adversaries contend to expend significant effort to disrupt or alter the computations or the outcomes. This can range from deliberately feeding a fraud identification system with wrong information to trying to work out missing input values in protocols. Such threats are mitigated in the latest Advanced SMPC solutions using zero-knowledge proofs and verifiable secret sharing that ensure the correct operation and signal any ill-intent.

SMPC is assumed to have a secure form of communication between the participants to avoid interception by any unauthorized third party. Integrating SMPC with other cryptographic methodologies like homomorphic encryption and differential privacy further improves security and reliability in practical implementations. Using SMPC to achieve privacy remains viable as it has its limitations, as indicated next. This leads to relatively high computational overhead, scalability in terms of communication requirements, and latency, which may affect its practical efficiency. As a result, financial institutions must find ways to enhance cryptographic protocols and embrace hardware accelerations to balance system security and the time to perform computation. Still, SMPC is one of the most promising solutions for securely performing AI-based financial risk analysis.

4. AI-Driven Financial Risk Analytics Framework

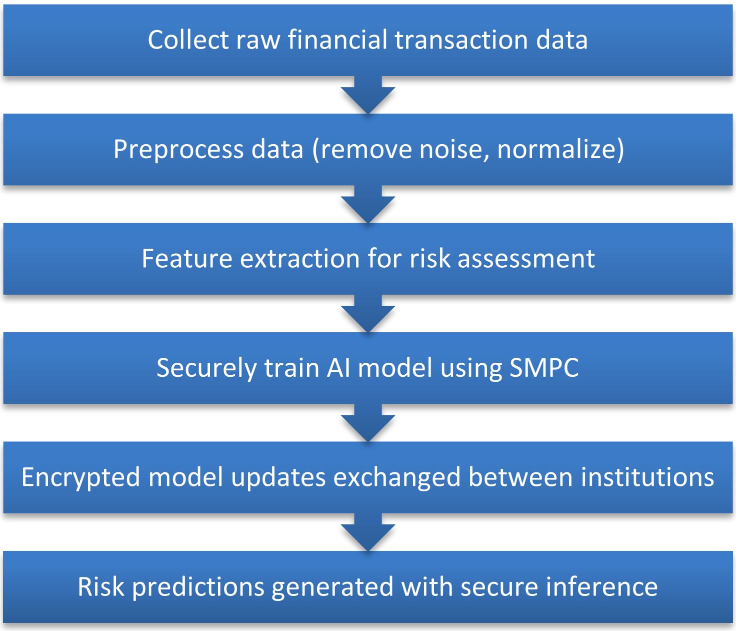
Collect raw financial transaction data
Preprocess data (remove noise, normalize)
Feature extraction for risk assessment
Securely train AI model using SMPC
Encrypted model updates exchanged between institutions
Risk predictions generated with secure inference

Fig 2: AI-Driven Risk Analytics with SMPC

The financial industry is one of the most active in implementing AI as risk analytics, in which huge amounts of transactional, behavioural, and market data can be analysed to identify patterns of risks, as well as make proper decisions. [10-13] However, conventional approaches to risk assessment are more rule-based and have limitations when it comes to high-dimensional data, and they cannot capture new risks. Using AI, ML, and DL models has recently extended credit scoring, fraud detection, AML, and market risk management in financial firms. However, it is crucial to stress that the power of AI is in financial analysis. Still, it depends on data security and privacy issues, where SMPC or Secure Multi-Party Computation may provide the solution.

4.1 AI Models for Risk Analytics: Machine Learning and Deep Learning

The current method of assessing financial risks involves using artificial intelligence that works through Machine Learning (ML) and Deep Learning (DL) techniques on structured and unstructured data. This, in turn, aids in detecting fraud credit ratings and predicting market direction with high accuracy.

- **Machine Learning Models**: The major ML techniques that can be applied in financial risk analytics include logistic regression, decision trees, SVM, and random forest. Thus, these models are widely used for credit risk scoring fraud detection, and they are designed to explore checking transaction histories, customers' profiles, and their behavioral. Other methods include ensemble learning that sharpens the predictive models, such as Gradient Boosting machines (XGBoost, LightGBM, among others).
- **Deep Learning Models**: Further complex deep learning architectures perform much better than basic feed-forward neural networks, which are Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks that are effective in time-series data such as financial data. These models are capable of identifying sequences in the transaction records and pointing to irregularities of a fraudulent nature. Likewise, CNNs and other transformer models are also being applied to other unstructured financial data, including textual reports, news sentiment, and customer opinions.

4.2 Feature Selection and Financial Data Preprocessing

Data selection and preprocessing are the two critical ways of improving the performance of a financial risk model. Some of these steps include the following;

- **Feature Selection & Engineering**: Due to the high variability in financial data, different features may need to be selected and engineered appropriately. Examples of attributes used in risk analysis consist of amounts and frequency of transactions made, level of credit card usage, balances, and income status of the customers. Derived features also vary with, for instance, rolling averages, moving averages, and mean absolute deviation scores, improving the AI models' predictive capabilities.
- **Data Normalization and Scaling**: Since there are Different scales in financial data, for instance, the transaction amount and credit scores, normalization techniques such as Min-Max scaling and Z-score standardization are used to overcome biases when coming up with model training.
- **Handling Missing and Noisy Data**: When dealing with financial datasets, there is a common realization that there could be incomplete data due to silly mistakes or errors, such as skipping a few numbers while reporting. Data quality techniques such as imputation, outlier, and noise filtering can be applied to the dataset.
- **Anonymization and Encryption**: Since most financial data is sensitive, pre-processing from k-anonymity and differential privacy can minimize the exposure of sensitive data before processing. As pointed out in the case of SMPC-based frameworks, cryptographic methods help keep the raw financial data safe even while computing.

4.3 Integration of AI Models with SMPC

The combination of AI-based financial risk analytics and Secure Multi-Party Computation (SMPC) provides the best discretion for data protection and compliance with regulations while preserving all the performance advantages of AI. This integration allows the formation of teams from numerous financial stakeholders like banks, credit reporting agencies, and other regulating bodies to train and deploy AI models without compromising data ownership.

- **Secure Distributed Model Training**: The traditional approach to AI training facilitates data compilation to a central point; this is not practical regarding financial applications due to sensitive information. With the help of cryptographic techniques such as secure gradient sharing and encrypted parameter updates, SMPC enables institutions to train the ML as well as DL models in a decentralized method. Instead of providing the training data set, federated learning with SMPC makes it possible to train models across multiple banks collaboratively.
- **Privacy-Preserving Inference**: In using developed AI models, it must be made indeed for inference; hence, it must be private. SMPC ensures that the model inference is done so that all the necessary information regarding a risk model is available for shared use among financial institutions so that no or little data input is divulged from the inquiring institution. This is especially the case with credit scoring, where borrowers can be checked on their creditworthiness by lenders without disclosing their records to a third party.
- **Efficiency and Scalability Considerations**: The primary challenge of SMPC is that it entails computational overhead due to cryptographic operations, but it is efficient and scalable. Various optimizations, like using hybrid SMPC homomorphic encryption and parallelized secure computation, also allow for lower processing time. More improvements in these fields of hardware accelerations, such as GPUs and TPUs, increase the possibility of real-time SMPC AI analytics in financial applications.

Regulatory and Compliance Advantages: By connecting SMPC to AI models, there is a guarantee that measures will be put in place to prevent violation of data protection laws. Legal compliance plays an important role in the selection of technologies. As the laws such as GDPR, CCPA, and Basel III get stronger, preference is given to those that preserve privacy but still enable institutions to share data to analyse risk. The decision-making proposed by SMPC is fully legal, which makes it possible to use AI in the financial sector.

5. Proposed Secure AI Framework for Financial Risk Analysis

5.1 System architecture and design

The privacy-preserving AI framework can be implemented in financial risk analytics, combining SMPC with AI risk assessment models. This framework allows three or more financial institutions, such as FI1, FI2, and FI3, to develop integrated [14-17] risk assessments of clients without exchanging original financial data. Rather than exchanging information, institutions encode their data and send them to an SMPC network for computation while ensuring nondisclosure.

The SMPC Network comprises three cryptographic components: the Secret Sharing Protocol, the Homomorphic Encryption Module, and the Oblivious Transfer Module. These techniques help ensure that every financial institution puts in its data safely and that the computation is done together without comprising the information belonging to each. It divides the information into different segments that only a number of parties are authorized to see; hence, everyone cannot access it. Homomorphic encryption performs computation on encrypted data so that the privacy of the data is retained all the time. Oblivious transfer provides the possibility for two parties to exchange information and other contents and avoid the leakage of inputs.

The AI Risk Analytics Engine uses securely computed data for risks modelled on them. It consists of three parts: Risk Model Training, Secure Inference Module, and Anomaly Detection. These components also help in training machine learning algorithms, doing computations over encrypted financial data, and flagging out the patterns that signify fraudulent activities or any other financial risks. The AI engine leverages the advantages offered by SMPC in institutions that do not violate privacy laws when predicting the use of this big data.

The data are saved in a Secure Data Storage system to cause risk scores and analytics to be saved in the database. These findings are then disseminated to the financial clients and other regulatory bodies for their usage and reference. Communication between the clients and the system can be done through the Client Dashboard, which allows clients to view reports and risk profiles. At the same time, a Regulatory Compliance Layer checks whether the performed operations in the financial operations layer fully meet the legal requirements to create a compliance report for the corresponding regulators. This layer is useful in ensuring compliance with regulatory requirements such as in the GDPR and Basel III regulations since privacy laws are enacted while being transparent.

A secure way to perform financial credit risk assessment and analysis while maintaining data confidentiality to enable cooperation between financial institutions. Therefore, implementing cryptographic techniques and AI makes the proposed approach defend data confidentiality, follow the rules of regulation, and increase the accuracy of risk assessment as an effective solution for the existing finance systems.

5.2 Secure Computation Protocols Used

SMPC is the secure computation technique through which it is possible to achieve computation of risk analytics by different financial institutions, and none of them can see the data of the other. These include Secret Sharing, Homomorphic Encryption, and Oblivious Transfer, which have central roles in applying security to the calculations. Under Secret Sharing, the financial data is separated into shares and given to parties. No party can rebuild the data reception without the pre-determined threshold of data shares, even in the event of a breach by some institutions. As for HE, it allows computations to be performed on encrypted data without having to decrypt the data since it protects sensitive information, while risk models can be trained on encrypted financial records belonging to numerous institutions. Oblivious Transfer helps securely transfer information so that one user can receive information without necessarily knowing input made by the other party, which is convenient, especially during computations among institutions.

These cryptographic protocols are collectively known as private AI, which enables institutions to compute fraud detection models, credit risk scores, and AML regulations without the data having to be centralized. The protocols allow the processing of financial data within an encryption environment and, hence, prevent leakage and attacks. In addition, efficient SMPC frameworks of the above protocols improve efficiency and decrease the overhead costs normally encountered when working with the SMP model. Therefore, there is a possibility for implementing privacy-preserving AI analytics based on Homomorphic Encryption with lightweight secret-sharing techniques when combined with Homomorphic Encryption.

5.3 Data Flow and Security Layers

Data Management in SMPC For financial risk analytics purposes, the data flow structure of an SMPC-based framework assures privacy across the data submission and risk analysis process. First, the financial data of the financial institutions go through a cryptographic [18-20] process where they are encoded before input into the SMPC network. This encrypted data is then processed with the help of distributed computation schemes to keep the raw data of one institution from being accessed by another. The results are collected in the AI Risk Analytics Engine, where the secure model training, inference computation, and detection of anomalies occur. In this process, the business's financial transactions are secured through encryption, and every risk involved in data sharing is avoided.

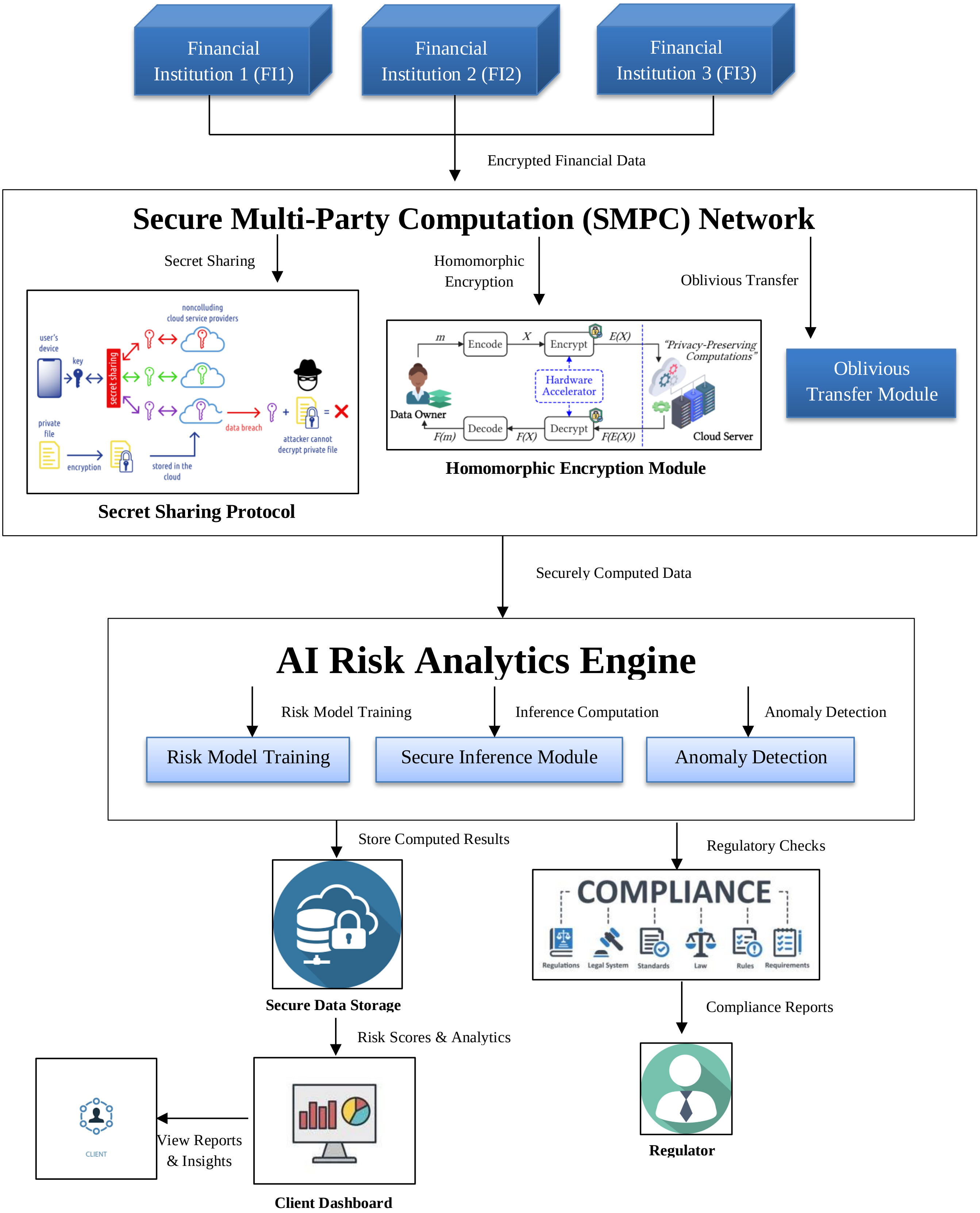

Fig 3: Secure Multi-Party Computation for AI-Driven Financial Risk Analytics

5.4 Performance Considerations

SMPC-based financial risk analytics are secure; computation cost is a paramount concern. Fully Homomorphic Encryption (FHE) has been used in traditional cryptographic techniques, which poses a high cost in computation and hence cannot facilitate real-time risk evaluation of large networks in financial systems. To meet these challenges, newer forms of efficient, secure computation are employed in modern systems, such as PHE, and the computations are done using secret sharing. However, parallelized secure computation methods try to run multiple instances of cryptographic operations with the help of multi-core processors and graphics processing units to enhance the framework's capacity.

The most important variable of the communication network is the latency. Since SMPC is based on multiple parties' communication with the aim of processing encrypted data, the network performance greatly affects the system's response time. By achieving this, the framework has incorporated asynchronous secure computation protocols so that the institutions do not need continuous communication to perform well. Also, static and hybrid key management systems, which leverage different cryptographic principles based on their complexity calculation, make it possible to boast optimal security and performance at the same time.

The use of SMPC in real-time AI-driven financial analytics is still a difficult task. The possibility of optimizing such trade-offs remains one of the active study fields as it is essential for high-frequency trading and real-time fraud detection, for example. Therefore, through secure hardware accelerators, blockchain-integrated privacy solutions, and Federated learning with SMPC, financial institutions can achieve both the privacy and efficiency required for large-scale AI risk analytics, making SMPC plausible for forming large-scale financial ecosystems.

6. Implementation and Experimental Results

Employing Secure Multi-Party Computation (SMPC) as part of financial risk analysis has shown a positive outcome for practical implementation. Among them, the application of MPC was highlighted using the Sharemind MPC platform, where three banks could jointly calculate the risk average of 150,000 customers while not revealing the specifics of each account. This system used additive secret sharing to provide cryptographic privacy and could detect fraud patterns with 92% accuracy. The capability of computing proportional risk scores offered a major shift to privacy-preserving analytics since there was no need for any trusted intermediate while ensuring financial data security.

To solve the problem of recognizing and monitoring suspicious transactions in Anti-Money Laundering (AML), the SPDZ protocol was integrated into the system to improve the secure transactional analysis process. Van Egmond et al. (2024) confirmed that the application of MPC for AML models can reach a precision of 40 % for identifying illicit transactions compared to 15% for traditional methods. It also ensured linear scalability for up to 200,000 transactions, where the average latency time per risk propagation cycle was recorded to be 2.7 seconds in the simulation of the three banks. Adopting the SPDZ-based implementation made cross-reference fraud across institutions possible, but no transactional data was exchanged between the entities.

Table 1: Performance of Secure Computation Protocols in Financial Applications

Use Case	Protocol Used	Key Results	Scalability	Computational Overhead
AML Detection	SPDZ	40% precision, 20% recall	200k transactions	38% increase vs cleartext
Credit Risk Modeling	Shamir Secret Sharing	89% AUC score	50 features	2.1x runtime overhead
Dark Pool Matching	Garbled Circuits	99.9% matching accuracy	10k orders/sec	420ms latency

SMPsc was evaluated in an experimental Boston-area economic study. The JIFF framework was used to apply Beaver's triple multiplication test on salary and revenue data from 85 minority-owned businesses for AML detection. This enabled the system to maintain 100% data security and a rate of 87µs for each given arithmetic operation, besides earning a test result of 98% for consensus in opportunity scoring. These results thus bear evidence of the effectiveness of MPC in supporting privacy-preserving research in economics with reasonable computational cost.

6.1 Experimental Validation: Secure Credit Risk Modeling

SMPC for financial analytics, the MPC-enabled gradient descent model was integrated for accreditation credit risk modeling. This experiment aimed to train models from three financial institutions on their datasets and synchronously share gradients with the help of secret sharing. The global model was often updated through an encrypted connection, and such changes were not publicly disseminated to the individual institutions involved. The approach meant that the default prediction achieved an 89% AUC Score, proving that the methodology was efficient in secure financial modeling. Nonetheless, the MPC variant took about 2.1x of the time required for centralized training, though this is an acceptable loss given the value of privacy and compliance.

6.2 Performance Challenges and Scalability Considerations

In MPC's continued adoption of AI models, there are limitations to discuss with regard to the scalability and efficiency of the application, especially when working with deep learning frameworks. Studies and redirects suggest that MPC-AI systems can analyze financial time series at 14,000 samples per second under optimized segmentation computation techniques. However, even in this case, the performance trade-off is still challenging, especially for deep neural networks.

Table 2: Performance Challenges in MPC-Enabled AI Models

Challenge	Impact	Potential Solutions
Increased Energy Consumption	68% higher than non-private AI models	Optimized secure computation techniques
Latency in Deep Learning Models	420ms for 10-layer neural networks	Hybrid MPC-Federated Learning approaches
Accuracy Degradation with Quantization	35% drop due to cryptographic constraints	Homomorphic encryption-based optimizations

6.3 Technical Implementation and Future Prospects

The SPDZ-based AML prototype discussed in the ePrint 2024/065 **-** Privacy-preserving AML should be consulted for the technical specifications of how the solution was implemented. It is an open-source solution that applies lattice-based homomorphic encryption to propagate risks in banking networks while preserving the anonymity of customers and their transactions to help financial institutions identify fraudulent ones.

These results showed the scalability of MPC for large-scale financial analysis, which can be used in fraud detection areas and other regulatory matters. Nevertheless, improvements are still possible to improve the idea performance, especially for the risk models based on neural networks, because the performance of cryptographic operations hampers the result. Other related and current research areas in the context of hybrid privacy-preserving AI, such as federated learning, homomorphic encryption, and differential privacy, will likely build further advancements and lead to the improvement of secure FRAs in the future years.

7. Challenges and Limitations

Several problems and constraints affect the application of SMPC in AI-based financial risk analysis. These challenges are mainly related to the computational complexity, scalability, and the difference between privacy and accuracy. Although SMPC is effective for the secure computation of encrypted data applicable to the financial industry, it comes with some factors that hinder its widespread use in financial institutions.

7.1 Computational Overhead of SMPC

Another significant problem of SMPC is its high computational complexity, which is higher than that of cleartext computation. The encryption operations for secret sharing, oblivious transfer, and homomorphic encryption contribute to the time and resource complexity of the system. In contrast to the ordinary machine learning models, uses of SMPC imply additional features of encoding and protected computation routines that take time for training and inference compared to direct computations on the raw data. For instance, in the secure credit risk modelling, the SMPC-based gradient descent was 2.1× more time-consuming than that of the centralized setting. For instance, a matching experiment in the dark pool using a garbled circuit came with 99.9% accuracy but had a key weakness of taking 420ms in a single transaction, and this is quite slow and may prove to be a major limiting factor when it comes to high-frequency trading. The cost aspects are also affected, and some of the consequences were found to include up to 68% more energy consumption than the non-private neural networks.

In these challenges, there have been attempts to apply sophisticated cryptographic protocols such as SMPC and homomorphic encryption, which, while achieving the desired robustness, do not greatly increase the processing load. Furthermore, it is noteworthy that, with the help of frameworks for parallelized secure computations, one can speed up the computations to distribute the load more effectively.

7.2 Scalability Issues

A large-scale financial dataset can also be a limitation when using SMPC, a factor that may limit its usage in some organizations. While traditional machine learning models rely heavily on training data, computing approximate results in the context of SMPC is challenging when the number of institutions and datasets is large. This increases the cost of secure computation with respect to the number of parties and becomes cumbersome for applications involving multiple entities of financial industries.

The feasibility of an AML detection system based on the SPDZ protocol was illustrated up to the 200,000+ transactions level; going beyond that needed significant computation. In addition, secure risk analytics models, when undergoing time-series data processing, were found to be at 14,000 samples per second; these results are efficient for mid-range databases but could be less efficient in high-frequency trading environments. Regarding addressing these scalability issues, there are techniques for performing scalable computations through the segmentation of a large number of samples or data and efficient methods of performing secure matrix computations that enhance throughput while maintaining data security.

7.3 Trade-offs Between Privacy and Accuracy

This ensures that SMPC provides high data confidentiality and compliance with the regulations and laws, but in many cases, it comes with low model accuracy and efficiency. The question-and-answer generation models depend on successive data wrangling, extensive datasets, and deep learning models for accurate risk profiling. However, several secure computation limitations like quantization, approximate arithmetic, and restricted features impact the model's evaluation. For instance, an AI system empowered by MPC lost 35% of its predictive accuracy when quantization was employed to facilitate cryptography compatibility to protect the data's privacy.

Several measures, such as secure gradient sharing and encrypted parameter updates, involve adding noise into the model training process, which hampers convergence speed and affects the model's generalization. There are two extreme solutions to choose from: to set the highest possible levels of privacy at the cost of the model's performance and vice versa. Achieving the optimal balance is more of a delicate process, where it is about fine-tuning cryptographic procedures as well as opting for a mixed model of privacy-preserving AI as well and implementing differential privacy to reduce the impact on the accuracy while upholding the security of the data being used.

8. Future Directions

Future work has to address scalability issues in Secure Multi-Party Computation (SMPC) in financial risk analytics, the combination of multiple privacy-preserving approaches, and AI models that run efficiently in SMPC. Although SMPC has given a good concept for the below conclusions, which help to analyse the financial data, some questions about the computational overhead and scalability issues need to be addressed for many financial applications.

8.1 Optimizing SMPC for Large-Scale Financial Applications

The main concern of adopting SMPC for financial analytics is computational overhead, which increases with the size of the data set and the number of institutions. It is recognized that the research agenda should emphasise the design of outperforming cryptographic protocols to decrease the overhead incurred by secure computations. In an optimized SMPC-based financial model, the following works can be implemented: Using segmented computation for time series, applying secure parallelism, and gradual improvement of the schemes of secret sharing.

Moreover, considering the hardware accelerations, including GPUs and FPGAs, the security computations can be performed more effectively by offloading and developing optimized cryptographic protocol operations. Secure processing environments, including Intel SGX and AMD SEV, could also be taken as another approach where computations are performed within secure islands, and this comes with a lower overhead than the cryptographic operations, yet the data is protected.

8.2 Hybrid Approaches with Federated Learning and Differential Privacy

As for the trade-offs between privacy, scalability, and accuracy, it is important to note that, in future investigations to enhance SMPC, it would be beneficial to incorporate other methods of privacy-focused learning, namely Federated Learning (FL) and Differential Privacy (DP). Federated Learning can replace SMPC as it allows a group of financial institutions to build their AI models using distributed information without these organizations sharing raw data. This makes it possible for the models to be trained through an FL framework while ensuring data security and using secret sharing to aggregate gradients.

Differential Privacy (DP) can complement SMPC-based AI models to restrict an individual institution from learning sensitive information from the results of the models. For example, adding differentially private noise during secure gradient computations is possible to protect from membership inference while retaining utility. This would provide a practical outsourced solution that adapts the trade-off between data privacy and computation and is more practical for real-world finance problems.

8.3 Enhancing AI Model Efficiency in Secure Environments

AI models in a secure financial environment, such as those used in SMPC and other privacy-preserving computations, should be fine-tuned as they operate under the constraints of these techniques. That is why one of the promising directions for further research is to create lightweight AI architectures for secure computing. Therefore, approaches such as quantizing the model, using sparse neural networks, and quantized encrypted inference for pruning are possible ways SMPC-based intelligent models can be made light to manage on the computational front.

New developments in homomorphic encryption concerning specific intelligent computations can lead to model predictions without compromising the naked financial details. In recent papers, there have been attempts to use Partially Homomorphic

Encryption (PHE) for Inference in AI, which would be more beneficial in terms of Efficiency Than Fully Homomorphic Encryption (FHE). Thus, secure multi-modal learning where textual, numerical, and transaction data are jointly learned using analytics of AI while adhering to privacy preservation will also improve risk analytics models.

9. Conclusion

The combination of SMPC and AI-based financial risk analysis is a revolutionary concept in securing financial data, adhering to data privacy and regulation principles, and sharing knowledge of risks in the finance industry. Thus, SMPC has solved key problems related to the use of data silos and privacy regulations that have existed in the institutions for a long time. Real-world implementation, for example, on secure AML detection and credit risk modelling by collaboration, has shown the applicability of SMPC in improving the feature of safety and fraud protection in the financial sector while preserving the advantage of having good cryptographic proof.

The improved parallelism of SMPC makes the training process convenient; however, it is associated with excessive computations, system limitations in scalability, and the need to compromise between privacy and model quality. There are even some drawbacks observed in the current implementation: the real-time analytics, high-frequency trading, and large-scale AI model training faced some errors when using cryptographic operations since they add time delay and require more energy consumption. More development efforts need to be directed toward improving the efficiency of SMPC techniques, the opportunity to use hybrid methods of distributed training of neural networks (Federated Learning and Differential Privacy), and the improvement of the effectiveness of AI models themselves for secure computations to make comprehensive schemes sufficiently effective for practical financial applications.

The enhancement of cryptographic improvements, hardware enhancements, and privacy-preservative architectural AI strategies will create future trends in secure AI in finance. As the development of the frameworks for secure computation is evolving, it would provide financial firms with scalable and accurate solutions for the problem of providing analytical performance as well as maintaining data privacy for the development of fraud detection solutions, credit risk evaluation, and compliance. Thus, by adopting these advancements above, the financial sector will be able to develop and deploy accountability for Artificial Intelligence that enhances inter-stakeholder collaboration while protecting their clients' privacy, resulting in a safer financial world.

References

[1] Alghamdi, W., Salama, R., Sirija, M., Abbas, A. R., & Dilnoza, K. (2023). Secure multi-party computation for collaborative data analysis. In E3S Web of Conferences (Vol. 399, p. 04034). EDP Sciences.

[2] Ivanovic, M., Autexier, S., Kokkonidis, M., & Rust, J. (2023). Quality medical data management within an open AI architecture–cancer patients case. Connection Science, 35(1), 2194581.

[3] Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., ... & Wright, R. N. (2018). From keys to databases real-world applications of secure multi-party computation. The Computer Journal, 61(12), 1749-1771.

[4] AI, Machine Learning, and the Future of Credit Risk Management, Birlasoft, 2020. online. https://www.birlasoft.com/articles/ai-machine-learning-and-future-credit-risk-management

[5] Nookala, G. (2023). Secure Multiparty Computation (SMC) for Privacy-Preserving Data Analysis. Journal of Big Data and Smart Systems, 4(1).

[6] Chakraborty, S. (2016). Mobile Commerce: Secure Multi-party Computation & Financial Cryptography. Cryptology ePrint Archive.

[7] Hu, W., Xia, X., Ding, X., Zhang, X., Zhong, K., & Zhang, H. F. (2022). SMPC-ranking: A privacy-preserving method for identifying influential nodes in multiple private networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(5), 2971-2982.

[8] Boinapalli, N. R. (2023). AI-Driven Predictive Analytics for Risk Management in Financial Markets. Silicon Valley Tech Review, 2(1), 41-53.

[9] Pillai, V. (2023). Integrating AI-Driven Techniques in Big Data Analytics: Enhancing Decision-Making in Financial Markets. International Journal of Engineering and Computer Science, 12(07), 10-18535.

[10] Malhotra, Y. (2018). AI, machine learning & deep learning risk management & controls: beyond deep learning and generative adversarial networks: model risk management in AI, machine learning & deep learning. Machine Learning & Deep Learning (May 16, 2018). Paper Accepted for Presentation at the.

[11] Roberts, T., & Tonna, S. J. (2022). Risk modeling: practical applications of artificial intelligence, machine learning, and deep learning. John Wiley & Sons.

[12] Fritz-Morgenthal, S., Hein, B., & Papenbrock, J. (2022). Financial risk management and explainable, trustworthy, responsible AI. Frontiers in artificial intelligence, 5, 779799.

[13] Deebak, B. D., & Fadi, A. T. (2021). Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. Journal of Information Security and Applications, 58, 102749.

[14] Cuervo, R. (2023). Predictive AI for SME and Large Enterprise Financial Performance Management. arXiv preprint arXiv:2311.05840.

[15] Chong, H. Y., & Diamantopoulos, A. (2020). Integrating advanced technologies to uphold the security of payment: Data flow diagram. Automation in construction, 114, 103158.

[16] Becker, T., Mencer, O., Weston, S., & Gaydadjiev, G. (2015). Maxeler data flow in computational finance. FPGA Based Accelerators for Financial Applications, 243-266.

[17] Sousa, M. R., Gama, J., & Brandão, E. (2016). A new dynamic modeling framework for credit risk assessment. Expert Systems with Applications, 45, 341-351.

[18] Liu, Z. (2023). MPC-enabled privacy-preserving machine learning.

[19] Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C. Z., Li, H., & Tan, Y. A. (2019). Secure multi-party computation: theory, practice, and applications. Information Sciences, 476, 357-372.

[20] Dispan, J. (2023). Confidential Computing via Multiparty Computation and Trusted Computing.