ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Decentralized AI for Secure Multi-Party Computation

Ohm Patel

USA

ABSTRACT

In the modern digital world, large-scale data and the analytic processing of the data make privacy-preserving computation even more critical. SMPC is a cryptographic protocol used to compute a function over the inputs of multiple parties such that the other party's input is unknown. This then provides for computing in parallel with other participants, without requiring a coordinator, which, in today's privacy-conscious world, is beneficial in avoiding using a central authority in data-entrusted activities. In a nutshell, a decentralized AI approach is based on distributed computing principles and the blockchain to create a solid architecture for SMPC implementation. In this manner, decentralized AI eliminates several drawbacks of data centralization, such as single points of failure and data breaches. SMPC and decentralized networks are the foundation of the privacy-preserving ML, where sensitive data train models without revealing the data points. Specifically, the growing necessity for protecting data with the help of laws like the GDPR and CCPA enhances SMPC's application in decentralized AI. Blockchain technology extends this implementation by having additional qualities of having an unchangeable record and consensus mechanisms that guarantee computation reliability and openness. However, scalability, ITY, computational cost, and system compatibility are drawbacks to integrating decentralized AI and SMPC. Solving these needs more be a continuous effort in the search for cryptographic techniques in communication, network design, and protocol formation. The combination of decentralized AI and SMPC presents a new and revolutionary way of multi-party computation through data privacy and access to cooperation and innovation in sectors such as health, finance, and supply chain. With the development of technology, these intelligent computing applications of decentralized AI and SMPC will continue to develop and open up new areas for efficient and secure data usage.

***Corresponding author**

Ohm Patel, USA.

Received: May 02, 2022; **Accepted:** May 09, 2022; **Published:** May 24, 2022

Keywords: Secure Multi-Party Computation (SMPC), Decentralized AI, Privacy-Preserving Computation, Homomorphic Encryption, Differential Privacy, Blockchain Technology, Federated Learning

Introduction

The need for private computation is evident in the modern world, with the abundance of data and the resulting performance of analyses. SMPC, Secure Multi-Party Computation, would be an improved cryptographic technique meant to facilitate the execution of a function on different inputs from different parties without revealing the inputs. Using this type of paradigm makes computation occur in an orchestral manner without relying on a central point that would cause concern about the privacy of sensitive information in extensive data operations. Based on decentralized computing and blockchain principles, Decentralized AI is an appropriate solution for applying SMPC. This means that through the distribution of the control and management of data, decentralized AI reduces the vulnerability of being precipitated by single-point failures and the vulnerability of being hacked, as is evident in the recent Centralised Data Breaches. Based on the WoT decentralized networks and SMPC protocols, privacy-preserving machine learning is achieved by using sensitive data to train models while protecting individual information.

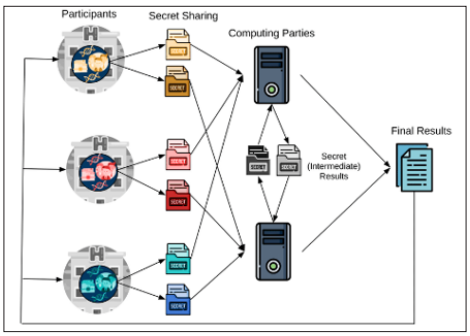

Figure 1: Secure Multi-Party Computation Architecture

Another reason that can be considered is the need to significantly protect data and its information content as the use of decentralized AI increases. The GDPR and the CCPA are among the regulations that require strict compliance in safeguarding individuals' information. Considering the above regulations, SMPC offers a reasonable method to accomplish computations that do not violate users' privacy. Further, the concept of decentralization has evolved even with the extension of blockchain technology in implementing these networks. In a distributed framework of AI, the reliability of the blockchain's computations and consensus mechanisms guarantee the ledger's security and reliability. Smart contracts, inherent to the blockchain, enforce secure computation through automation, boosting the need and application of SMPC.

However, when it comes to the integration of decentralized AI and SMPC, certain factors need to be revised. One of the significant challenges is scalability, as cryptographic operations can be time-consuming and have a significant cost. Furthermore, the ability to integrate multiple systems and protocols is also critical to achieving widespread adoption. Solving these obstacles necessitates continuous advancements in mathematical algorithms, developing efficient networks, and creating regular international dashboards.

Integrating decentralized AI with SMPC is a paradigm shift in secure multi-party computation transit. This approach ensures data privacy and promotes distributed innovation in numerous sectors, such as healthcare, finance, and supply chain. It should be noted that as technologies develop further, demands for decentralized AI and SMPC will only grow. Their potential will, in particular, create new possibilities for the effective use of data while maintaining the preservation of user privacy.

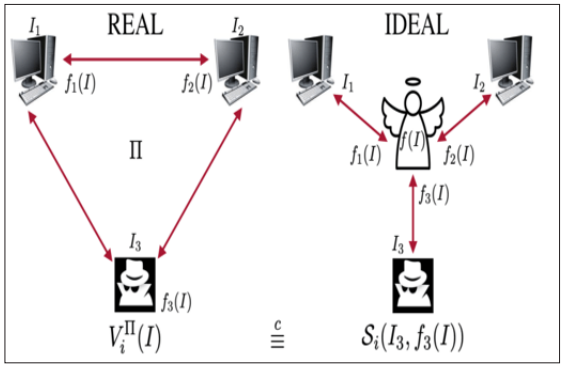

Figure 2: Real and Ideal Paradigms for Secure Multi-Party Computation

Fundamentals of Secure Multi-Party Computation (SMPC)

Overview and History of SMPC

SMPC, or Secure Multi-party computation, is a branch of cryptography that allows the execution of a function on inputs from multiple parties without revealing the said inputs to other parties. Andrew Yao originally defined the notion of SMPC. He was subsequently discovered in Yao's Millionaires' Problem, where two millionaires want to know who is richer without fully revealing each other's money. Its rich content helped to establish SMPC protocols and contributed to further progress in the theoretical and practical development of the field. After Yao presented the SMPC problem, many protocols and methods have been proposed in the literature to improve the efficiency and security of the SMPC. The need for SMPC has increased with the rise in the usage of private computations in areas like secure voting, private and collaborative data analytics, and machine learning. The initial works and studies in SMPC were developed by Goldreich, Micali, and Wigderson suggested that SMPC schemes applicable to any function are possible with enough computational assets [1].

Basic Principles and Protocols

The foundation of SMPC is to let different parties compute a unified function on their inputs and, at the same time, prevent more information leakage than what can be learned from the output of this function. It is done through cryptographic methods that ensure that inputs are kept secret and the computation is correct. A critical computation method used in SMPC is Yao's Garbled Circuits, which enables two parties to compute the result of a boolean circuit with the other's unknown inputs. Another necessary protocol is the Secret Sharing Scheme. Shamir presented in 1979, where the secret is split into shares and admitted to participants not only certain members can regenerate the secret. It is one of the schemes applied in SMPC to make secure input sharing among the parties involved. Moreover, concepts such as Oblivious Transfer (Rabin, 1981) and Zero-Knowledge Proofs enable parties to communicate while preserving their private inputs.

Applications of SMPC

The fields of use of SMPC are numerous and can be applied virtually in any field as the need for private computations increases. Secure voting systems are one of the most common applications of SMPC; the technique helps to add up the vote without deciphering personal options, thus preserving the voters' anonymity and the elections' sanctity [2]. SMPC is also used in privacy-preserving data mining and machine learning, enabling organizations to jointly analyze the data without compromising each other's information [3]. Regarding health and medical information, through SMPC, functions such as statistical analysis can be carried out on different data sets, which may be collected from different institutions without necessarily showing the patient's identity [4]. Financial services also find applications in SMPC where, through the joint control of fraud activity in banking systems that originate from user transactions, the actual data from customers is not shared [5]. Another interesting subject is the use of SMPC in decentralized networks and technologies such as blockchain. Another application of blockchain's innovative contract technology is to employ SMPC for implementing otherwise confidential agreements. This might include multiple financial transactions involving multiple parties or private bidding [6]. Combining SMPC with the decentralized network improves the security and privacy of the applications, making it compulsory to construct secure and trustless systems.

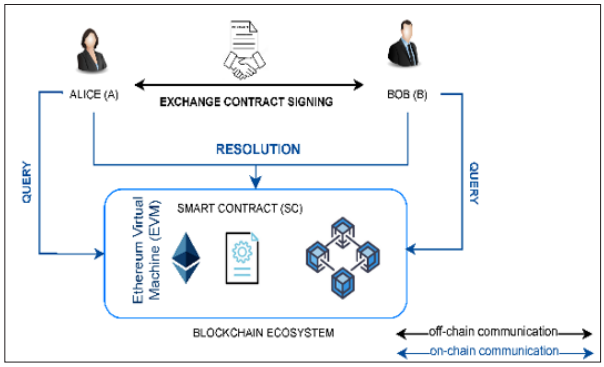

Figure 3: A Hard-Timeliness Blockchain-Based Contract Signing Protocol

SMPC is a robust cryptographic protocol that solves the increasing demand for private information computation in different fields. By facilitating the computation of functions on their inputs while preserving the inputs' privacy, SMPC offers the framework for secure cooperation and analysis. Enhancing newly developed and existing SMPC protocols and their applications presents this area as the key to safe and secure data sharing in a networked globe.

Privacy-Preserving Machine Learning Techniques

It is crucial to identify privacy-preserving machine learning (PPML) as the process that allows the use of sensitive data to train machine learning models while preserving the participants' privacy.

Homomorphic Encryption

Homomorphic encryption (HE) is the computation of data in an encrypted format without decrypting it and then encrypting it

again when ready. Organized by Rivest, Adleman, and Dertouzos in 1978, HE has been established progressively to incorporate a broader range of operations on encrypted content. The first approach developed was Gentry's fully homomorphic encryption (FHE) in 2009, which enables one to perform any calculation on encrypted data. This notion has enabled subsequent studies in data analysis and data-based sciences like machine learning. HE is most effective under situations in which data has to be secure such as data concerning health or finance. For instance, secure GWAS can be done by employing HE, where the raw genetic data analyses can be done without revealing the data [7]. HE still needs to be more costly in terms of computational complexity and current schemes' efficiency hinders them from being primarily used [8]. Progress in furthering cryptographic research is reducing the inefficiency characteristic of HE, making the environment viable enough for practical use.

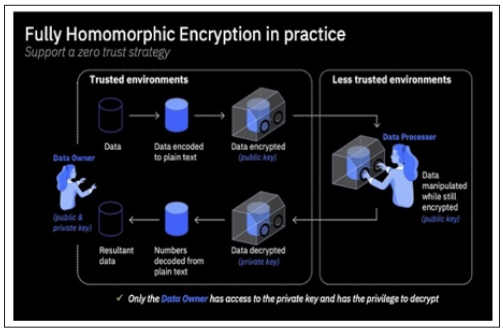

Figure 4: Fully Homomorphic Encryption

Differential Privacy

Differential privacy (DP) offers a theoretical concept to state that adding or removing a single record will not considerably influence a query, which helps protect the privacy of individuals [9]. This technique introduces noise into the data or the query results to prevent anyone from deducing anything about any particular individual and simultaneously arrives at the right macro-conclusion. A widely known DP application is the application of differential privacy by the US Census Bureau as respondent confidentiality measures for the 2020 Census [10]. Many firms like Apple and Google also use DP to gather data to improve users' privacy [11]. Although we can observe that DP offers good guarantees in terms of privacy, the objective complexity arises from the trade-off between the two: adding noise can reduce data usability while excluding it can harm privacy. New ways practiced in DP techniques keep on solving these difficulties. For instance, LDP, an improvement of DP, enables the users to apply functions to their data before sending them to the server, increasing privacy yet again [12]. This approach proves very productive in distributed environments where data is obtained from many places.

Federated Learning

FL is the technology whereby many learning partners contribute to building a model without using the primary dataset of the other participants. Instead, each participant downloads the model on their local dataset and only sends the model update to other participants [13]. This approach makes it possible to keep sensitive data stored on the local storage devices in the device to cut on the vielen of data theft and boosting on privacy. FL has been deployed in several applications effectively, for instance, in Google's Gboard where it is deployed to enhance the predictive text models without drilling down into the user's data [10]. Moreover, FL also achieves decentralization, which means it does not need a central place to store data, reducing various risks associated with data accumulation. However, there are several issues in FL, including communication overhead, model heterogeneity, and privacy issues when exchanging model updates. Specific methods such as secure aggregation and differential privacy can be incorporated into FL to improve privacy protection in FL. Future work in federated optimization algorithms is also being conducted to address specific concerns regarding efficiency and scalability [3].

Secure Federated Learning

Secure federated learning (SFL) integrates conventional FL with different cryptographic solutions to provide a higher level of protection. SFL also ensures that the raw data, model updates, and any computations performed in between are not leaked. This is achieved through applying different methods, such as secure multiparty computation (SMPC) and homomorphic encryption, which are also frequently used in SFL. Selene, Mohassel, and Zhang introduced SecureML, which relies on SMPC to perform the machine learning scheme on encrypted data [14]. This helps to ensure that the model updates are ascertained without exposing anyone's data or intermediate results. SecureML has been tested in many scenarios, especially where data security is of utmost importance, like the area of health and finance. SFL solves many of the problems of traditional FL because it offers better privacy guarantees. Nevertheless, it creates other computational and communication overheads by using cryptographical procedures. Current studies focus on enhancing all the parameters related toto SFL protocols to improve their efficiency and applicability at a large scale [10].

Decentralized Networks and Blockchain

Overview of Decentralized Networks

Decentralized networks are distributed systems where the individual nodes work autonomously and perform the train central hub's transferred functions that allow cooperation. This architecture improves system stability by eliminating the singularity point of control that may trigger significant scale failures and attacks. In this network structure, the nodes work cooperatively to ensure that data is legitimate and gets circulated; hence, the network is protected from failure and other unlawful activities. This model is very different from centralized systems and is far more reliable since a system does not have a single vulnerable point through which the entire network is vulnerable [15]. Some of these mechanisms include a distributed hash table (DHT), which is used to search for data in the network; other mechanisms use consensus algorithms to make all the nodes agree on the state of a given network. Some examples include peer-to-peer (P2P), such as Bit torrent, and distributed databases, such as Apache Cassandra. The concept of decentralization has been inherent throughout the evolution of the new digital age's main building block, blockchain technology, laying the foundation for the secure and transparent nature of the immutable ledger system.

Blockchain Technology for Decentralization

Blockchain is a perfect example of decentralized networks using cryptographic technologies and distributed consensus algorithms to develop a digital ledger. It was launched in 2008 by Satoshi Nakamoto, with the Bitcoin cryptocurrency commonly known as BTC. It has since been adopted for many applications besides being a currency [16]. A blockchain, therefore, contains a blockchain that is a series of blocks that holds a record of transactions. Cryptography connects these blocks; thus, changing previous information without the network's consensus becomes almost impossible. The decentralized operation of a blockchain is made possible by consensus algorithms such as the Proof of Work

(PoW) or the Proof of Stake (PoS) in approving the transaction and introducing new blocks to the blockchain. The PoW employed by Bitcoin needs the nodes to provide complicated numbers to solve mathematical problems so that only nodes with significant computational power can append blocks. In contrast, validators that PoS chooses for supporting acts based on the number of tokens they own and are willing to put in "stake," thus encouraging energy efficiency and scalability.

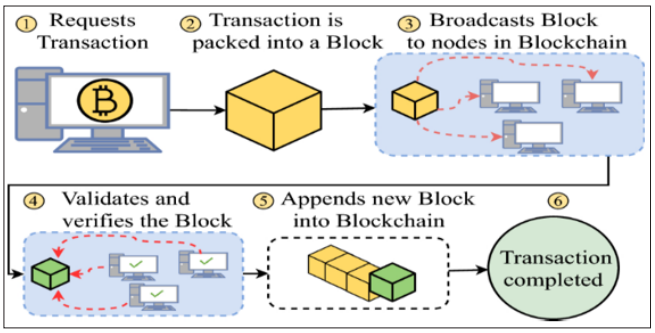

Figure 5: Blockchain for Decentralization of Internet

Use Cases of Blockchain in SMPC

Integrating blockchain technology into SMPC can bring a tremendous improvement in that it offers a record of all the computed results and guarantees that all the members are sticking to the rules and guidelines of the computation. SMPC makes it possible for many parties to compute the same function of their respective inputs while the information input is kept confidential and never revealed to other parties while computing a function. This is desirable in large scenarios such as collaborative data analysis and privacy-preserving machine learning. This utilization of blockchain runs in the realm of SMPC to apply, for example, transactional data analysis to identify fraud by involving several institutions without sharing customer data. For example, in the Enigma project, blockchain is employed to decentralize data and protect computation, including the decryption of data and the performance of computations, and ensuring the computations encrypted are authorized. A good example is the use of blockchain technology in the Field of Health care where patient data is shared mutually for research purposes and other collaborations without compromising on the privacy of the patient [6]. In supply chain management, integrating blockchain technology with SMPC will enable a transparent and secure tracking system for goods. Every link in a supply chain can independently certify the accuracy and reliability of transactions and not disclose the company's data. Its advantages include strengthening trust and optimizing supply chains, risky fraud and counterfeiting instances.

Smart Contracts for Secure Computation

Smart contracts are digital contracts that automatically execute the agreed terms. Used in a blockchain environment, these contracts self-execute and self-verify the contract terms while doing away with mediators. Smart contracts can be effectively used in SMPC to enforce and execute computation rules to the agreed standards. Smart contracts and SMPC can be combined to ensure that parties can securely perform computations without the help of an intermediary; for instance, in decentralized finance (DeFi), smart contracts can facilitate all the financial operations and investments, for example, computing the interest rate and executing the related and subsequent fund transactions while being very secure and accurate. Also, in situations of many offers, smart contracts can safely determine the winners within auctions, and the participants' offers will not be disclosed to anyone [17].

Decentralized networks and blockchain allow the adoption of a more massive and practical approach to increasing the security and transparency of Secure Multi-Party Computation. By utilizing blockchain's low-level properties like non-editable and distributed consensus features with the help of smart contracts, numerous fields can adopt secure collaborative computer computations with privacy and accurate data.

Cryptographic Techniques in SMPC

Secret Sharing Schemes

Secret Sharing Schemes are elementary to SMPC since they enable sharing secrets with the parties in the computation. The two initial approaches in this field are Shamir's Secret Sharing (1979) and Blakley's Scheme (1979). Shamir proposed using polynomial interpolation over a finite field such that the original secret is divided and distributed so that only a specific subset of participants can recreate the original secret. On the other hand, Blakley's method applies geometrical dimensions where the secret is a point in a k-dimensional space while every share is a hyperplane passing through the point [18]. These schemes guarantee that no person can arrive at the secret without assistance from other individuals; this makes SMPC secure for use in areas such as voting and data analysis.

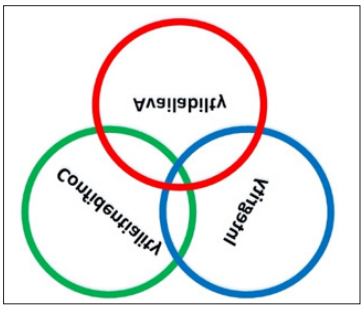

Figure 6: Overview of Blakley's Secret Sharing Scheme

Zero-Knowledge Proofs

Zero-knowledge proofs (ZKPs) is a technique that allows a prover to provide the verifier with the assurance of the statement's truth without disclosing additional details [1]. This cryptographic protocol is fundamental to SMPC since it means that the parties can convince other parties of possession of specific information while at the same time not revealing the information. Goldreich, Micali, and Wigderson generalized this idea to the case of several parties in order to carry out computations in which all inputs are kept private. They are often implemented in the field of blockchain technology to allow for the verification of a transaction's legitimacy without compromising the contents of the transaction itself. This property is used to protect data from others in a decentralized system and to strengthen the security aspect of the shared calculations.

Figure 7: Zero-knowledge proofs

Oblivious Transfer

Oblivious Transfer (OT) is a complete and intellectual protocol introduced by Rabin, which works in such a way that a sender sends one of the many pieces of information to the receiver. However, the sender needs to know what the receiver has received information. It remains a building block of most SMPC protocols since it allows for the communication of sensitive information with anonymity. Rabin's OT (1981) and Even-Goldreich-Lempel's OT (1985) offer different ways to attain the obliviousness property in this area. OT is essential in protocols such as Yao's Garbled Circuits in which it is helpful in the exchange of the cryptographic keys required in the evaluation of the circuits. The efficiency of using OT in preserving privacy and security is thus the reason why OT has been widely used in multi-party computations, especially in areas that demand high security.

Garbled Circuits

Garbled Circuit is one of the most significant protocols in SMPC proposed in the mid-1980s by Andrew Yao known as Yao's Garbled Circuits. This method enables two parties to compute a function over the inputs held by each of them without either party learning the inputs of the other party. It involves presenting the function as a boolean circuit and encrypting all the gates so that only the inputs intended to decrypt the gates of the circuit can do so. Garbled Circuits have been expanded and optimized over the years, such as the Fairplay system by Malkhi, Nisan, Pinkas, and Sella in 2004 and then later by Pinkas, Schneider, and Zohner in 2014 to improve computational overhead and scalability. This technique is essential to two-party computations. It has been generalized to n-Party computations, whereby secure collaborative computations in numerous disciplines ranging from data mining to financial computations are practicable.

Secure Multi-Party Computation is based on cryptographic protocols, including Secret Sharing Schemes, Zero-Knowledge Proofs, Oblivious Transfer, and Garbled Circuits. They allow for collaborative computations while preserving the privacy of individual computations for the participants. By employing these protocols, SMPC supports various privacy-preserving use cases from different domains, ranging from secure voting to private data analysis or Decentralized Finance. Further developments and refinements of these methods are imperative for tackling the problems of scale, speed, and compatibility of SMPC and inspire more extensive use and more robust protection of users' privacy in the context of the growing reliance on big data.

Challenges in Decentralized AI for SMPC

Scalability Issues

To the best of our knowledge, this is one of the first works that needs to address scalability as a significant concern while integrating a decentralized AI scheme with SMPC. SMPC protocols generally include intricate cryptographic calculations that substantially impact complex processes. For instance, Yao's Garbled Circuits and Secret Sharing schemes, which are at the base of many SMPC solutions, include complex computations and significant communication costs that are proportional to the participants' number and the functions performed [18]. The complexity and response time may skyrocket as the network grows, which makes it challenging to keep the efficiency in large applications. Improving SMPC protocols' scalability means improvimprovingcryptographic methods and searchisearching new algorithms that could positively impact the overall overhead at a given security level. Ben-Or, Goldwasser, and Wigderson' have pointed out some positive attempts at increasing scalability by more efficient multiparty computation strategies, but the existing strategies present several viable challenges.

Latency and Performance

This application involves decentralized intelligent machines using SMPC that experience latency, and performance issues are a critical factor. As the requirement for privacy and security arises, mainly where several people need to communicate over the same channel, it leads to delays, which impact the system's ability. For example, Oblivious Transfer and Zero-Knowledge Proofs are vital to preserving privacy and security, although they come with high latency and computational overhead. This can be very challenging, especially in applications whereby the response must meet a specific schedule. Experiments by Cramer, Damgård, and Nielsen have tried to solve these performance problems by designing new efficient cryptographic protocols; however, the need to balance security, privacy, and efficiency constitutes a significant challenge. More studies should be conducted on enhancing the network and constant work on understanding and using parallel processing algorithms to decrease latency when using SMPC in decentralized AI systems.

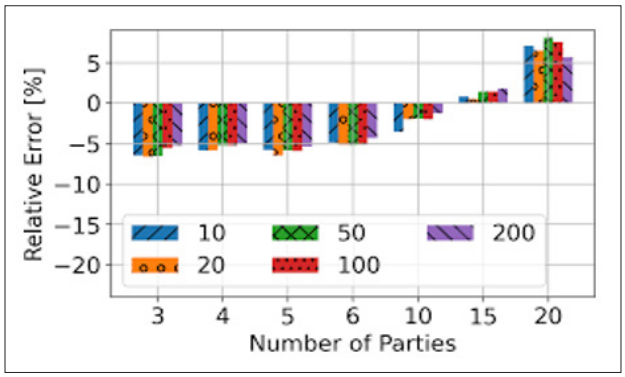

Figure 8: Network Traffic of SMPC Protocols

Security Vulnerabilities

Owing to poor encoding, there is also a likelihood of security vulnerability in SMPC protocols being another major challenge. It is clear that the objective of SMPC is to make sure that neither participant gets to know anything beyond what can be inferred from the output, and yet there are still sources of insecurity here that emanate from implementation and side-channel. For example, differential attacks that take advantage of differing amounts of time required to perform computation or energy consumption may reveal information. Besides, compliance with all the necessary rules without including a virus is also essential in protecting the computation from interference. The absence of a standardized solution in SMPC constructs and the absence of any predetermined simple solution for coordinating committee structures has been examined by Lindell and Pinkas, and the simple export of security models is only the beginning of security with constant validation and verification tests requiring constant improvement [5]. The critical research directions include implementing SMPC protocols and enhancing the protocols' robustness against advanced attacks.

Interoperability

System and protocol integration for decentralizing AI and SMPC has been deemed crucial, given that the two models would require compatibility with several other systems and protocols. The problem is that the different organizations and SMPC platforms can employ different standards and technologies to implement solutions, which hampers smooth integration. To effectively

achieve interoperability, one has to set up common standards and protocols that can be utilized across all sectors. Goldwasser and Bellare state that it is more significant to stress the compatibility between various systems for developing cryptographic protocols. Moreover, the need to ensure these standards reduce the security and efficiency of the SMPC protocols should be emphasized. The finite view of security and the lack of a unifying theory for its implementation is one of the significant problems in this area of study. Their attempts to make the frameworks more interoperable, such as the work done by Canetti et al. on universally composable security is an attempt to deal with this challenge. However, it could be challenging to harmonize many systems to ensure the proper functionality of SMPC and keep high-security levels [19]. Solving the issues related to scalability, latency, and performance, exhaustive security threats that affect decentralized AI, and the integration of SMPC is essential. Further study and innovation on these topics based on the principles laid by conventional cryptography scholars are an urgent necessity in order to propel decentralized Artificial Intelligence systems to a new efficiency level.

Case Studies and Real-world Applications

Healthcare Data Sharing

In the healthcare industry, there is a critical concern about how data will be helpful while protecting patients' privacy rights. SMPC enables the analysis of multiple patients' records by several institutions without compromising the patient's privacy due to the sharing of records. For example, SMPC permits hospitals to conduct cooperative genetic studies; while combining the data of several patients can make results more accurate, patient data will not be disclosed to third parties. One example is the safe GWA, which enables researchers to work with the genetic data statistical tests are applied to without revealing personal information [16]. This capability is essential in the context of the work since data leakages in the specific sector lead to legal and ethical ramifications.

Financial Services

SMPC can help the financial sector to allow secure exchange of data among competitors for analysis, such as banks, financial institutions, etc. By adapting SMPC protocols, these institutions can identify fraudulent activities while maintaining the concealment of their sensitive information from other institutions. For instance, the Fairplay system presented by Malkhi, Nisan, Pinkas, and Sella shows that SMPC can be used in computing privacy-preserving models, enabling banks to securely share risk and fraud detection models. This is especially helpful in light of imposing demands concerning data protection and safety such as the rules of the Sarbanes Oxley Act say. Furthermore, the fact that data can be analyzed collectively by many people where details of some of the analyses might be withheld further strengthens and stabilizes financial-related systems.

Collaborative Data Analysis

It was pointed out that SMPC can yield benefits in virtually any advanced collaborative data analysis spanning different domains. For instance, firms in ventures or doing market research can apply SMPC to share data without revealing strategic data. The Sharemind framework introduced by Bogdanov, Laur, and Williamson in is a real-life solution that can be used to implement SMPC and then forward the computations to handle the data safely among multiple parties. This framework has been used in similar cases and situations, such as privacy-preserving data mining for two or more organizations that want to analyze large data sets without infringing on each other's privacy. The high efficiency and security that SMPC offers make it a suitable option for use in organizations and groups where data privacy is paramount.

Supply Chain Management

Both flow of product and security and transparency are essential factors in SCM aiming to mitigate fraud cases. Blockchain technology and SMPC offer a highly reliable solution for these needs. For example, Kamvar, Schlosser, and Garcia-Molina explore using distributed peer-to-peer networks for information exchange, which can also be applied to supply chain systems. According to blockchain's distributed and tamper-proof list, supply chain members can confirm the additional and unalterable parameters of transactions without sharing sensitive information. This integration assures that all the concerned parties shall access a clear and checkered record of the movement of goods, thus increasing the level of trust amongst the members and minimizing fraud cases. Furthermore, SMPC enables the safe transmission of sensitive information, such as pricing and supplier details, within the prescribed chain among the authorized authorized parties, enhancing the supply chain's security.

These case studies further highlight the versatility of SMPC in different fields across the economy. In care, it opens up collaborative research possibilities while preventing patients' identifiers from being exposed. In financial services it improves the prevention of fraud and more ways of evaluating the level of risk without violating the client's rights to confidentiality. Organizations are helped through SMPC in terms of collaborative data analysis since they securely obtain insights from the shared data. Finally, regarding supply chain management, SMPC, in conjunction with blockchain, fosters high transparency and security, which play an essential role in SCM. The consistent developments and integration of SMPC will pave the way to even more creative uses, thus placing significant importance on its role in attaining data protection and safety in a connected world.

Future Trends in Decentralized AI and SMPC

Advances in Cryptographic Methods

The future of SMPC is likely driven partly by the improvement in cryptographic techniques. Advancements in homomorphic encryption, for instance, are expected to bring computations on encrypted data closer to reality. Significant work has been done to develop fully homomorphic encryption that will enable computations to be made on encrypted messages with the help of work by Gentry [20]. However, the problem of high computational cost remained an issue. Further developments like the BGV scheme by Brakerski, Gentry, and Vaikuntanathan in the year 2011 have aimed at enhancing these processes as they introduced more efficient possibilities for the execution of homomorphic encryption that might open the pathway toward its more pragmatic application in decentralized AI In the same way, advances in multi-party computation protocols such as the SPDZ protocol offer strong reference models for secure computation and therefore enhance the feasibility and flexibility of SMPC applications [21].

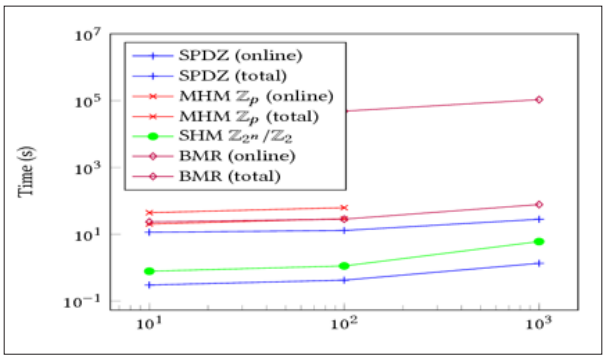

Figure 9: Generalizing the SPDZ Compiler for Other Protocols

Integration with IoT Devices

Another emerging practice involves extending SMPC with the Internet of Things (IoT). Given that many IoT devices will be continuously producing massive amounts of data, there is a rising concern about how to process such data in a safe and personalized manner. In this context, it remains evident that SMPC can hold significant potential regarding IoT devices' data confidentiality while maintaining the data's collaborative work suitability. Other published works, like Li et al, have discussed the integration of IoT with SM to improve the security and privacy of the collected data. Using SMPC in IoT could help compute data collected from smart homes, healthcare gadgets, and industrial sensing devices where privacy is a significant concern. However, some of these are as follows:" challenges in the implementation of SMPC due to the incurred computational and communication overhead in the resource-limited IoT devices [4].

Potential for Quantum Computing

Quantum computing can be seen as a threat or an opportunity for SMPC. On the one hand, quantum computers threaten to render many of today's commonly used cryptographic protocols insecure by utilizing Shor's algorithm that factors large integers within an efficient time. However, quantum also provides brand-new cryptography methods that may improve SMPC. Quantum key distribution (QKD), as proposed by Bennett and Brassard in 1984, allows for generating fresh keys that are protected against any computational attack and form the basis for building quantum-safe SMPC protocols. Furthermore, analysis of quantum homomorphic encryption in Dulek, Schaffner, & Speelman, 2016 may point to secure quantum computations on big data, innovative to Decentralized AI and SMPC [22].

Emerging Standards and Protocols

It is necessary to set up new standards and protocols to encourage the use of SMPC technologies and enable communication between them. Interoperability is the capability of one SMPC implementation to interact with other SMPC implementations. Since different implementations can use their techniques, standards must be set so that different SMPC implementations can securely communicate with each other. The standardization work completed by the ISO and NIST in the field of cryptography remains the blueprint for any attempts at SMPC standardization. For example, ISO/IEC 29192-1:2012 describes lightweight cryptographic primitives for resource-constrained environments, which can be used in SMPC in the context of IoT. Besides, novelties like the Fairplay protocol for secure function evaluation give a development of protocols that can be applied for specific domains in SMPC [5]. These standards will similarly continue to evolve and be adopted, thus enabling the integration of SMPC into various industries for secure and private computational subsections in decentralized Artificial Intelligence.

As future directions to the development of decentralized AI and SMPC, enhanced cryptographic techniques, the fusion with the IoT devices, quantum computing, and reassessment of the proven norms and measures indeed have a promising future, these advancements will improve the potential of SMPC in terms of versatility, stability, and connectivity to enter more areas of the economy and contribute to collaborative creation while protecting data privacy.

Comparative Analysis of SMPC Frameworks

Comparative Study of Existing Frameworks

Frameworks for SMPC include Sharemind, VIFF, and SPDZ, developed to cater to the growing demand for secure computations. Sharemind, described by Bogdanov et al, is considered as employing a set of tools and techniques for solving real-life problems of secure computations in conditions of cooperation [16]. It operates on a three-computation model of the parties to improve efficiency and security. Some of the successful usages of Sharemind are Privacy-preserving data mining and statistical analysis, which make this tool preferable in academic and industrial environments. Other than the SMPC protocols, Damgård et al, introduced the Virtual Ideal Functionality Framework (VIFF), which generalizes the traditional SMPC protocols [20]. The architecture of VIFF enables asynchronous computations, which is necessary for real-world applications of the latencies of the network and proven delays in the communication channel. It allows the researcher to develop personal methods and test different cryptographic methods to improve the framework. SPDZ (Speedz) by Damgård, Pastro, Smart, and Zakarias is another technology for secure computations that concentrates on pre-processing and offline phases to achieve the best result. In particular, SPDZ aims to group computations, allowing performing massive calculations and thus suitable for large-scale machine learning and big data [21]. The current cryptographic primitives in the framework facilitate high security while the protocols designed are lightweight.

Pros and Cons of Different Frameworks

It is important to note that each SMPC framework has specific strengths and weaknesses. At the same time, Sharemind stands out for its functionality and relatively simple implementation. The three parties' computation model may offer satisfactory levels of security while maintaining efficiency for many real-world use cases. However, Sharemind's requirement of a particular number of parties could be viewed as a limitation in the given scheme in cases where more diverse configurations are essential for the parties. The main strength of VIFF is the adaptability and the practical parallel computations, especially asynchronous ones, which are essential in the distributed occurrence. That is advantageous for users because they can quickly implement and assess a new protocol, and the solutions can enhance the sphere of safe computations. On the negative side, we notice that the performance of VIFF can be negatively influenced by latency and delay in the network communication, thus making it unsuitable for use in areas requiring a low latency.

Compared with the other methods, described above, SPDZ is effective, scalable, and particularly suitable for computations at large numbers of participants. Its pre-processing phase has been well optimized to consume as little online time as possible; therefore, it is suitable where much time is needed. However, the protocol of SPDZ is somewhat complex and, therefore, may

be challenging to implement and may take much effort and or professional input to implement successfully. As such, the first two phases or steps involve overhead that may not be ideal for all applications.

Performance Benchmarks

For the benchmarking of the SMPC framework, there is a need to perform benchmarking of the performance. It has also been verified that Sharemind is suitable for problems that do not require significant computation, presenting reasonable security and performance. For instance, Laud showed that Sharemind could perform private statistics computations effectively with reasonable efficiency and other measures in different experiments. While BitTorrent's throughput at the VIFF site is relatively stable, the throughput at the remainder of the networks fluctuates based on the current conditions. Damgård et al, described how VIFF performs well in asynchronous scenarios, but at the same time, they discovered that the communication overhead significantly impacts the protocol. This makes VIFF suitable for research and development and likely inefficient for real-time use. From the previous session, it has been indicated that SPDZ has been benchmarked comprehensively for its adequacy in performing large-scale mathematics. Much has been said regarding the framework's efficiency for extensive data processing and machine learning tasks with relatively small online computation time. Damgård et al, demonstrated that SPDZ outperforms other secure computing protocols in linear algebra and similar computations to prove that secure computing environments lend themselves to high-performance computing.

Each of Sharemind, VIFF, and SPDZ has its own strengths and weaknesses and faces unique difficulties. Sharemind is operational and easy to use, VIFF is diverse and creative, and SPDZ is effective and can be expanded. The framework selection depends on the characteristics of the particular application, namely the number of parties, the necessity of using delayed calculations, and the computational demands of the task.

Ethical and Regulatory Considerations

Ethical Implications of SMPC

It is crucial to state that SMPC application in different domains raises numerous ethical concerns. First and foremost, it is essential to note that data minimization, one of the fundamental principles of ethical data processing, is implicitly compliant with SMPC. It enables the parties to evaluate functions over their inputs so that they reveal nothing about the inputs themselves. However, the ethical concern continues beyond minimizing data collection and processing. When implementing SMPC, care should be taken so that the results do not perpetuate the biases seen in the data. For example, when using SMPC to compare data from different hospitals for analysis, it has to consider fairness concerning the proportionate representation of different groups and guarantee that its outcomes are not detrimental to equality in healthcare delivery [4]. Moreover, strict moral requirements state that the continual use of SMPC cannot turn into an instrument of monitoring or unauthorized data collection. The example of potentially illicit data collection through SMPC creates a central ethical quandary that requires appropriate regulation, regulation standards, and action protocols.

Regulatory Compliance and Legal Issues

Something that one must consider in the application of SMPC is regulatory conformity. This increases or guarantees data privacy and protection demands in different regions. For instance, the GDPR in the EU and the CCPA in the United States. With SMPC, compliance can be achieved since people are confident computations can be made without exposing raw data points, and this fits the GDPR's data protection by design and by default principles. However, the legal status of SMPC is unclear, and there are some contingencies regarding its application and implementation under the current laws. For example, items like the right to explanation under GDPR, which recommends that all automated decisions ought to be explicable to people, may present challenges to SMPC executions, especially when the computation process is deliberately concealed to enhance the privacy of the process. Furthermore, in the case of cross-border data transfers to SMPC, they have to meet the laws of the country of the transfer as well as the country of destination, which can be a challenge due to the variance of different countries. These regulations mean that legal compliance must be appropriately understood alongside forming SMPC processes that are sufficiently adaptable to the fluctuation in legal standards.

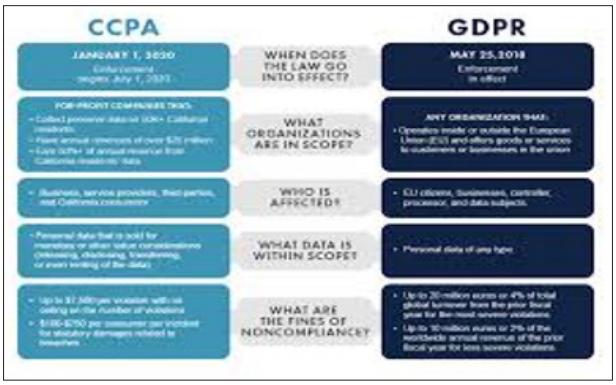

Figure 10: The Difference between CCPA and GDPR for Businesses

Data Ownership and Consent

Ownership of Personal Data and consent are significant factors in the Moral operation of SMPC. Even though SMPC mechanizes the processes, it does not mean data ownership can be unclear, and data subjects' consent is not required. However, the peer-to-peer paradigm can lead to rather challenging issues concerning the separation of ownership when utilizing SMPC, as data is distributed among multiple parties but encrypted simultaneously. Understanding and defining who possesses the data inputs and outputs of the SMPC process and how this right is exercised is therefore very essential. Also, to get informed consent from the data subjects, the subjects should be made to understand how their data will be processed, the benefits and risks of the SMPC, and their rights concerning their data. This is especially relevant in sectors like the health and financial sectors, where data subjects require magnanimous confidence in the data protection process adopted by an organization. Furthermore, the consent has to be continuous and allow the withdrawal of consent, which, in terms of SMPC, is technically complex. To overcome such challenges, a robust consent management system and regimes of ownership and usage rights to the data are needed.

Based on the ethical and regulatory aspects, ethical data management, legal compliance, and data ownership are issues related to SMPC. Solving these problems is essential for proper SMPC utilization, which improves data protection and security while preserving ethical and legal requirements.

Conclusion

The decentralized AI and SMPC combination is a significant leap in privacy-preserving data analysis. Distributed AI overcomes issues related to data centralization and single points of failure with the help of distributed computing and blockchain technologies. Due to the latest data security challenges, SMPC helps at least two parties to compute functions on their input data co-operatively to keep the input data secret. The need for SMPC for privacy-respecting computations could be seen in the fact that regulatory compliance has emerged from strict standards such as the GDPR and CCPA. However, scalability, computational complexity, and compatibility must be addressed to improve results and widespread application. Current cryptographic techniques, such as homomorphic encryption and differential privacy, and new learning approaches, such as federated learning, provide a solid foundation for enhancing the efficiency of SMPC. Integrating these technologies' applications is expected to transform many industries, such as healthcare, finance, and supply chain, by providing a secure co-creation environment. Thus, as research progresses, the areas of decentralized AI and SMPC will remain promising for new methods of improving the efficiency of secure data utilization and privacy and trust in the use of data, a value that is likely to grow in the future as data becomes an even more significant commodity in an ever more digital society.

References

1. Ben-Or M, Goldwasser S, Wigderson A (1988) Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. Proceedings of the twentieth annual ACM symposium on Theory of computing.
2. Cramer R, Gennaro R, Schoenmakers B (1997) A Secure and Optimally Efficient Multi-Authority Election Scheme. Eurocrypt 103-118.
3. Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan HB, et al. (2017) Practical Secure Aggregation for Privacy-Preserving Machine Learning. ACM Conference on Computer and Communications Security (CCS) 1175-1191.
4. Bost R, Popa RA, Tu S, Goldwasser S (2015) Machine learning classification over encrypted data. Network and Distributed System Security Symposium https://eprint.iacr.org/2014/331.pdf.
5. Ben-David A, Nisan N, Pinkas B (2008) FairplayMP: A system for secure multi-party computation. Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS) 257-266.
6. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: Using Blockchain for Medical Data Access and Permission Management. In 2016 2nd International Conference on Open and Big Data (OBD) 25-30.
7. Ayday E, Raisaro JL, Hubaux JP (2013) Privacy-preserving processing of medical data with homomorphic encryption. IFIP Advances in Information and Communication Technology 405: 62-74.
8. Bos JW, Lauter K, Naehrig M (2014) Private predictive analysis on encrypted medical data. Journal of Biomedical Informatics 50: 234-243.
9. Dwork C, McSherry F, Nissim K, Smith A (2006) Calibrating noise to sensitivity in private data analysis. In Theory of cryptography conference Springer, Berlin, Heidelberg 265-284.
10. Abowd JM (2018) The US Census Bureau Adopts Differential Privacy. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining 2867-2867.
11. Erlingsson U, Pihur V, Korolova A (2014) RAPPOR: Randomized aggregatable privacy-preserving ordinal response. In Proceedings of the 2014 ACM SIGSAC conference on computer and communications security 1054-1067.
12. Duchi JC, Jordan MI, Wainwright MJ (2013) Local privacy and statistical minimax rates. In 2013 E 54th Annual Symposium on Foundations of Computer Science 429-438.
13. Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan BH, et al. (2017) Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security 1175-1191.
14. Mohassel P, Zhang Y (2017) SecureML: A System for Scalable Privacy-Preserving Machine Learning. IEEE Symposium on Security and Privacy 19-38.
15. Baran P (1964) On Distributed Communications Networks. IEEE Transactions on Communications Systems 12: 1-9.
16. Bogdanov D, Laur S, Willemson J (2008) Sharemind: A Framework for Fast Privacy- Preserving Computations. ESORICS 192-206.
17. Brandt F (1983) Cryptographic Protocols: Zero Knowledge, Blind Signatures, and Coin Flipping.
18. Blakley GR (1979) Safeguarding cryptographic keys. Proceedings of the National Computer Conference 48: 313-317.
19. Canetti R, Lindell Y, Ostrovsky R, Sahai A (2002) Universally composable two-party and multi-party secure computation. Proceedings of the thiry-fourth annual ACM symposium on Theory of computing 494-503.
20. Gentry C (2009) Fully homomorphic encryption using ideal lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC) 169-178.
21. Damgård I, Pastro V, Smart N, Zakarias S (2012) Multiparty computation from somewhat homomorphic encryption. Advances in Cryptology – CRYPTO 2012. Lecture Notes in Computer Science 643-662.
22. Dulek Y, Schaffner C, Speelman F (2016) Quantum homomorphic encryption for polynomial- sized circuits. Advances in Cryptology – CRYPTO 2016. Lecture Notes in Computer Science 9816: 3-32.
23. Acquisti A (2010) The Economics of Personal Data and the Economics of Privacy https://kilthub.cmu.edu/articles/journal_contribution/The_Economics_of_Personal_Data_and_the_Economics_of_Privacy/6471989?file=11901470.
24. Bennett CH, Brassard G (1984) Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175-179.
25. Binns R (2012) A Theory of Political Accountability in the Age of Data-Driven Governance.
26. Brakerski Z, Gentry C, Vaikuntanathan V (2011) Fully homomorphic encryption without bootstrapping. Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS) 309-325.
27. Floridi L (2016) The Fourth Revolution: How the Infosphere is Reshaping Human Reality.