International Journal of communication and computer Technologies, Vol. 12, No. 2 , 2024 (pp. 31-39) IJCCTS
RESEARCH ARTICLE WWW.IJCCTS.ORG

Secure Computing Protocols without Revealing the Inputs to Each of the Various Participants

Shefer Roper,* Plessner Bar

Samuel Neaman Institute for Advanced Studies in Science and Technology Technion, Technion City, Haifa 32000, Israel

Keywords:
Cryptography;
Homomorphic Encryption;
Multi-Party Computation (MPC);
Privacy;
Secure Protocols

Corresponding Author Email: shefroop@techunix.technion.ac.il

DOI: 10.31838/IJCCTS.12.02.04

Received: 13.07.24

Revised: 11.08.24

Accepted: 22.09.24

Abstract

This work focuses on analyzing cryptographic protocols through which two or more parties can compute functions of their joint inputs without divulging their inputs in their raw form which is a building block of SMPC. Due to the security one gets to protect the data in the computations SMPC allows participants to engage in the computations while protecting the data it is used in fields such as finance, healthcare and data analytics whereby data is sensitive. The subject of the study is approaches for introducing security into the examined protocols to guarantee their correctness while preserving user privacy, through the use of such tools as homomorphic encryption, secret sharing, and zero-knowledge technology. We consider various security configurations, such as semi-honest and malicious security, to understand how vulnerable these protocols are to feasible attacks or data exposure. Also, important issues, such as scaling and computational complexity, are discussed where we give solutions for minimizing communication cost and time in the context of big data applications. The outcome indicates that carrying out secure and practical SMPC with strong security assurances is feasible, irrespective of performance requirements of various actual-world application scenarios. This work is relevant to the current state of the art in cryptography and provides new protocols enabling sensitive computations for real privacy-preserving applications in the modern digital environment.

How to cite this article: Roper S, Bar P (2024). Secure computing protocols without revealing the inputs to each of the various participants. nternational Journal of communication and computer Technologies, Vol. 12, No. 2, 2024, 31-39

Introduction

In the modern technologically advanced world there is a demand for information safety during its processing and analysis. Secure multi-party computation (SMPC) has become a revolutionary approach for solving the privacy problems in collaborative data analysis. This exciting development enables two or more parties to collaboratively compute on a function of the inputs of each of them without actually revealing those inputs. It is relevant to fields as diverse as finance or medicine to help organizations gain competitive insights from their data while preserving the privacy of individuals. Picking up further from that, this extensive tutorial introduces itself to the concept of SMPC and its basics and development. It considers the main elements of SMPC systems and analyses how they may be implemented in different sectors. It also contrasts SMPC with other approaches to privacy preservation, such as homomorphic encryption and block chain technology. Also, it speaks about the legal and the ethical issues related to the implementation of SMPC. Finally, by the end of the interventions, readers will have developed tremendous insights into what SMPC is and how it is likely to look like in the near future as it determines the future of data Privacy and collaborative computation.[1]

Fundamentals of Secure Multi-Party Computation

Secure multi-party computation or SMPC is an innovative cryptographic method that allows the various parties to process data together without compromising the data information. This approach has risen to the challenge of being able to calculate mathematical functions on information that cannot be shared but must be combined. SMPC is a set of cryptographic protocols used to solve the problem of preserving privacy and correctness of the computation carried out simultaneously by multiple parties.

The fundamental concept of SMPC is to allow the parties to perform computations on sensitive data whereby the input data that each of the parties submits to the computation is concealed from the other participating parties. Sprivate computation specifies the capacity to jointly compute a particular function using several computing parties without disclosing their data by applying cryptographic methods such as secret sharing, encryption, and zero-knowledge proofs. This creates a vast opportunity as all entities could analyze the data before arriving at some decisions without necessarily compromising the security of the data (Figure 1).[2-5]

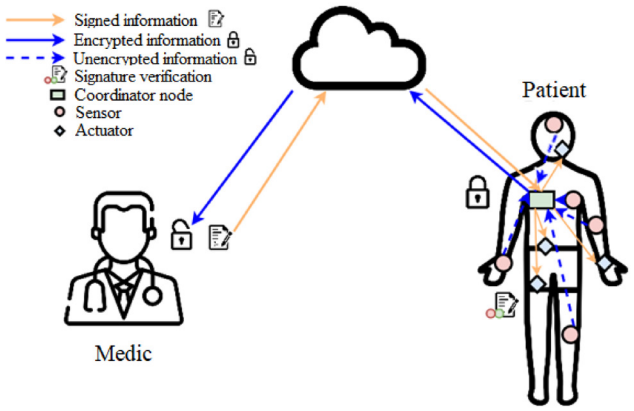

Fig. 1:Fundamentals of Secure Multi-Party Computation

SMPC has design objectives, which include, but are not limited to, the following, protecting the identity of an individual input during computation. This is done through some strategies such as the secret sharing and encryption. Secret sharing techniques divide the inputs in such a manner that no one of the parties can restore the original data with the help of others. Also, data confidentiality is safeguarded with the help of the encryption method to preserve data in computations and exchanges between parties. This is because through the use of SMPC, the inputs and the intermediate results that are produced do not go through the hands of any other party, they are encrypted to ensure that leakage of sensitive information is addressed.[6]

1.1 Mathematical foundations

SMPC's computational theory is based on cryptography; the technique applied to facilitate secure computing. One of them is an additive secret sharing that based on separating a value, which is to be protected, into a number of random pieces called "secret shares." For example, a value of $100,000 can be split into three secret shares: Of course, these variations are blank, but they could range from $20,000 to $30,000 to $50,000. One or more secret shares in a given DSM contain no information regarding the original value but collectively they unveil it.

This concept of secret sharing is normally used to ensure that data is protected even when it is being used. In SMPC protocol, the participants locally add their values together and aggregate the result together to generate the final result. This operation enables the computation that is safe and sound where no input can be disclosed from the party that supplied it.

Security models

As noted earlier, due to the participation of several parties who collude to provide incorrect information to the system a threat by Adversaries is posed to SMPC protocols that for correctness and integrity of computations are designed. Through techniques including the zero-knowledge proofs and secure commitment schemes SMPC is capable of identifying different forms of attacks including manipulation of results, cheating, and even attempts at gaining excessive information of other's inputs.

The security requirements for SMPC protocols ar' stringent and can be classified according to the behavior of the potential adversaries. Two main types of security models exist:

- Semi-Honest (Passive) Security: This model expects that the corrupted parties want to accumulate information but do not violate the given protocol. It offers a somewhat lower degree of security assurance; however, it helps avoid accidental information disclosure between cooperating parties and form the basis for more secure models.
- Malicious (Active) Security: In this model, the adversary is allowed to behave unfaithfully to the protocol execution with the intention to cheat. It is possible in this model to achieve very high security with protocols that hold the privacy of all honest parties intact, and the correctness of the output while assuming presence of other malicious ones.

Evolution of SMPC Protocols

The development of secure multi-party computation (SMPC) protocols has been an exciting journey that has taken several decades, which has had its fair share of milestones and accomplishments. This progression

has brought growth for SMPC from being a theoretical model to being an actual method for considering privacy issues in collaborative data processing.[7]

Early approaches

The original ideas for SMPC were presented with the inception of mental poker in the late 1970s, a cryptographic notion that aimed at emulating game playing across distances without involving a third trusted entity. This early work has laid the foundation of special purpose protocols that is more suited for particular functions.. Nonetheless, the problem is that it was Andrew Yao who gave formal thoughts on secure two-party computation in the early 1980s and solved the so-called Millionaires' Problem. Yao's contributions consist of the Garbled Circuits Protocol which is still used in most efficient applications of SMPC to date (Table 1).

Afterwards, others, such as Oded Goldreich, Silvio Micali and Avi Wigderson extended Yao's work to the m-party computation. They proposed the GMW paradigm, specification transformation from a scheme for compounding multi-party computation protocols secure against passive/semi-honest adversaries into ones secure against active/ malicious adversaries. While initially viewed as costly due to high overheads, this approach was the gateway for the development of further improvements in SMPC.

Modern Advancements

More recent SMPC research concerns itself with optimizing the efficiency of the protocols it proposes, as proposed since the late 2007. These changes have caused more efficient protocols resulting in SMPC as a computation solution to real-world problems like distributed voting, private bidding and auctions, sharing of signature or decryption functions and private information retrieval. Danish Sugar Beet Auction is the practical successful model of SMPC, by doing an electronic double auction in January 2008. This case showed that with SMPC it is possible to work in real conditions and perform linear sharing of secrets while the communication between the Share owners is minimal.

SMPC protocols have also experienced improvements in the security model side in the modern day. While originally, the best semi-honest (passive) security model was assumed where corrupted parties collaborate to obtain more information while referring to the protocol description, recent advances in the field address the case of malicious (active) security. In this model, the opponents can errantly opt out of the protocol execution and aim to trick, which gives the need for additional security.

State-of-the-art Techniques

Recent years have revealed significant advancements in the techniques of SMPC to achieve heretofore unsolvable or considered very cumbersome tasks. Among the interesting accomplishments is the capacity to perform secure inference with Large Language Models (LLMs). As a result, researchers have shown that it is possible to perform inference operations on an encrypted version of a 13 billion parameter model using a combination of MPC servers with GPUs in a few seconds per token. Modern SMPC techniques also know the progress in some applications, including the convolutional neural network, the cloud implementation, and structure-aware private-set intersection. These developments have opened up new areas where SMPC can be applicable, they make SMPC suitable for various kind of computations while keeping data private.

Moreover, current advancements have considered tabular operations that are mass-usable; regular expressions for extensive text data; and enriching conventional machine learning algorithms. These solutions enable the protection of training data, queries, and models contingently on the application domain and efficiency expectations. Even as SMPC progresses, however, new problems for its researchers to solve are

Table 1: Comparison of Symmetric and Asymmetric Cryptographic Protocols

Protocol Type	Example Protocols	Key Characteristics	Use Cases	Strengths	Limitations
Symmetric	AES, DES, 3DES	Uses a single key for encryption and decryption	Data encryption at rest, VPNs	Fast, efficient for large data	Key distribution and management challenges
Asymmetric	RSA, ECC, El-Gamal	Uses a pair of public and private keys	Digital signatures, SSL/TLS, key exchange	High security, no key exchange problem	Slower, computationally intensive for large data

emerging in the form of how to handle new types of data such as image data, free text, and DNA sequences as well as faster processing. This progress is due to the adoption of new cryptographic protocols, parallelism and techniques of hardware acceleration that make SMPC a well suited solution for tackling the problem of privacy in the epoch of the big data and collaborative computing.[8]

Key Components of SMPC Systems

SMPC systems include several components which collectively provide the means for private multi-party computational operations. These components guarantee that several parties can freely compute a function but individually the input information is secret. Let's explore the essential elements of SMPC systems:

Input Sharing

The first step therefore in SMPC is to define the function for which the parties wish to jointly compute. There are inputs which are specific data of each participant and they cannot be disclosed during computation process. In order to achieve this, SMPC makes use of secure techniques for sharing secrets for distributing the inputs securely among the parties. Shamir's secret sharing is also one of the critical parts of this approach: the method that employs polynomial interpolation to split the secret in a way that only a predetermined number of the shares can recreate the original data. For example, using additive secret sharing, a value of $100,000 can be split into three randomly-generated pieces (or "secret shares"): It plans on raising $20,000, $30,000, and $50,000. Alone each share is absolutely meaningless with respect to the original data, but in aggregate they provided the reconstruction of the secret value.

Secure Computation

Upon data security and data encryption, what actually carries out the computation is the real distributed system. This stage mean that the parties compute the value of the desired function with full cooperation but without disclosure. In the course of the secure computation phase, a number of cryptographic methods are applied to guarantee privacy and protection throughout the process.

For instance, in a situation where three colleagues would like to add their common hourly wage without revealing each of their wages, each of the participants would complete local summations on his/her secret shares. They would then exchange partial of results with other parties so that the final result can be computed together, but nobody knows the inputs that were put in.

The security models within the SMPC protocols can be implemented with reference to two security models: the semi-honest (passive) and the malicious (active). If the corrupted parties collude to obtain information while rejecting outside information, then the attacked model is the semi-honest model. The adversary model on the other hand, has the assumption that an opponent could change or decide to act in anyway they like provided that they are cheating.

Output reconstruction

The last aspect of SMPC systems is the process of reconstruction of the output of the computation. At this stage, the parties get an answer of some computation done by all parties put together with no other information of the input values from other parties rather than getting some aggregated value (Figure 2).

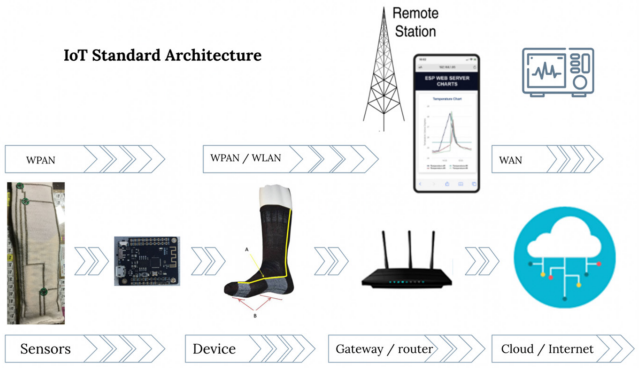

Fig. 2. Output reconstruction

Moving on with the salary example, an average hourly wage for the company would be disclosed while no single participant's salary would be disclosed. This process guarantees accuracy and at the same time each party's input does not reveal the other party's input. To reconstruct the output securely, SMPC systems mainly utilize some techniques such as; majority filtering. On some instances, a complete binary tree is created out of quorums each of which includes some parties and where root quorum collects the output of a circuit. This output is then processed and passed down through the chain using majority filtering in which each party will compute the majority of all messages received from the parent quorum to arrive

at the correct output. These key components jointly contribute to realize secure multi-party computation so that multiple parties can work on the computation of analysis results on sensitive datasets without leaking out individual sensitiveness. In this way, the SMPC systems give a promising tool for privacy-preserving in a range of domains starting from finance for instance, or healthcare, to machine learning as a service [9].

SMPC in Practice

The concept of secure multi-party computation is no longer an abstract thought exercise but a real world idea, used in many disciplines. This section focuses on the current adoption, the applications, the case studies and real-world performance analysis of SMPC systems.

Real-world implementations

Currently, the integration of SMPC has spread across many fields, where it plays an important role in the field of financial operation, medical researches, and digital assets. It was in the last 2 years of the 2010s that digital asset custodians started relying on SMPC to protect digital assets. This application has a profound influence on the blockchain-effecting area and the private key of Web3 wallet can be divided (sharded among multiple parties). To perform any function, certain minimum number of participant keys have to be used making the environment more secure from other malicious invasions. One interesting realisation of the method can be found in the context of cryptocurrency wallets. Web3 wallets backed by MPC are employed by the custodians to protect the assets and to confirm transactions. While in traditional multisig wallets, the multiple private keys are used to sign a transaction, in MPC wallet, the single key is broken into several subparts and each is given to the custodian. This approach ensures security complementary to the flexibility needed in signing of transactions.

Case Studies

It is also important to highlight several examples that show how SMPC is used in practice to solve certain problems. An example of this is Jana system created out of Galois Inc., in collaboration with several universities and companies. Jana offers an MPC secured database to execute a Private Data as a Service (PDaaS) application for relational data. This system is unique among encrypted databases as it encrypts all data even during processing, in contrast to today's encrypted databases that, at the very least, bring data into the clear for processing. Another example is Sharemind, MPC-secured database system, designed by Cybernetica, Estonian-based company. Among those problems it is important to note, that Sharemind is aimed at solving questions connected with data sharing and computation and at the same time providing clients with the opportunity of cooperation in the sphere of analysis of data, however preserving their privacy. First beginning in Denmark in 2009, Partisia has been the first company to employ SMPCs for pure commercial purposes. They were first used in auctions; it was also the first large-scale utilization of SMPC in the now famous sugar beet auction. Today, Partisia act again as a commercial marketplace targeting SMPC covering from research and development to market in the field of design.

Performance analysis

Recent developments in SMPC protocols have increased their potential efficiency to the level at which they can be considered useful in practice. For example, it has been shown that running inference operations on an encrypted 13 billion parameter model in MPC servers with GPUs is possible to do in only a few seconds per token (Table 2).

In certain applications, there has also been heightened performance levels recorded recently. The researchers performing a GWAS implementation using

Table 2: Cryptographic Protocols for Secure Communication

Protocol Name	Type (Symmetric/ Asymmetric)	Key Features	Common Applications	Security Level
TLS (Transport Layer Security)	Asymmetric, then Symmetric	Secure communication over the internet	HTTPS, VPNs, secure email	High, widely used in web security
IPsec (Internet Protocol Security)	Symmetric/Asymmetric	Secures internet communication at the network layer	VPNs, secure data transfer	High, commonly used for VPNs and secure networks

Protocol Name	Type (Symmetric/ Asymmetric)	Key Features	Common Applications	Security Level
PGP (Pretty Good Privacy)	Asymmetric	Used for secure email encryption and digital signatures	Email encryption, file encryption	High, used for personal and corporate security
SSH (Secure Shell)	Asymmetric, then Symmetric	Provides secure remote access to network devices	Remote server management	High, widely used for system administrators
Kerberos	Symmetric	Network authentication protocol for secure identity verification	Authentication in distributed systems (e.g., Active Directory)	High, commonly used in enterprise environments

SMPC noted that it has reduced total runtime to similar network usage. Smaller P values and lesser degrees of freedom justify expectation of increased efficiency: A million-individual study using SMPC-based GWAS could be expected to be finished in approximately 3 weeks, whereas earlier accounts reported that the process would take 3 months. Likewise, in a scenario of drug-target interaction (DTI) prediction through SMPC, scholars noted nearly reduced code by 2-3 times more than the four times faster execution time, and more than half of the network usage. Such enhancements mean a lot in terms of realistic practice sessions, which could lead to trimming down of training time to below one day, from the current four days.

Nonetheless, the results are still dependent on the particular usage and the increased intricacy of some of the algorithms. For example, in metagenomic binning task, SMPC implementation required 18.5 hours to do classification which in a normal run requires less than 10 second. This is a performance difference primarily due to overhead of the computational aspects particular to the MPC setting such as Bloom filters. However, there are still many opportunities for development of SMPC application in practice and new fields of secure computation. Thus, as new knowledge is being accumulated and application of implementations is being optimized, SMPC is gradually getting a chance to become the key enabler of privacy-preserving analytics and cooperation.[10-11]]

Privacy-Preserving Data Analysis with SMPC

Secure multi-party computation (SMPC) is a promising technique that has recently received significant attention since it allows multiple parties to perform computations on sensitive data and not disclose anything about their data to others. This has proved to be very useful in different fields such as statistics, machine learning and handling large volumes of data.

Statistical Computations

Specifically, SMPC enables performing statistical computations on several distributed datasets while preserving the original datasets' confidentiality. A well known fallacy of reasoning is the fallacy found in the scenario such as two millionaires wanting to puzzle out who among them is richer than the other while not disclosing the level of their affluence. This concept also applies to more complicated cases like summing or averaging, medians or any other form of averaging from different submissions received from two or more parties (Figure 2).

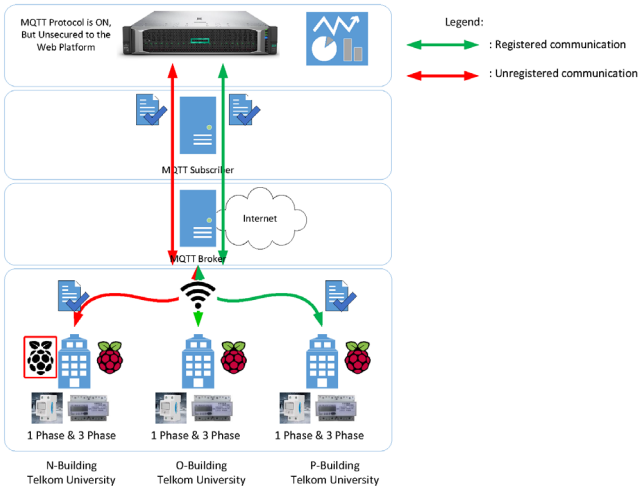

Fig. 2: Privacy-Preserving Data Analysis with SMPC

For example, in a practical use, SMPC helped to process secret salary information by collaborating the Boston employers. This served to make summary statistics possible without compromising on the

individual salary details of any party for the outside world. Such implementations show the applicability of SMPC in handling privacy issues in collaborative data analysis.

Machine Learning Applications

The combination of SMPC and machine learning has provided possible ways of performing private data analysis. Most machine learning methods always necessitate the need to collect huge data in order to forecast with some level of reliability that is usually invasive to privacy. This SMPC solves this problem by allowing different parties to train and leverage machine learning models collaboratively and securely without any party revealing its inputs to the others. An example of this application is a pooled study that was conducted with the contribution of the University of Pennsylvania and nine other institutions. Employing a method called federated learning, which is based on SMPC, they trained a machine learning model for the diagnosis of MRI scans of brain tumor patients. This approach allowed making the differentiation between healthy and malignant brain tissue without exchanging patient's records between institutions. Nevertheless, it is crucial to mention that the effectiveness and, especially, the possibility of SMPC's practical implementation with ML are still the topics for further investigation. The latter means that the choice of the protocol and the security model can significantly affect computation time and the number of participants in the protocol can affect the computation time notably if the number increased from 2 to 3 and more significantly if the transition from semi-honest to malicious security is made.

Big data processing

Due to the steadily increasing amount of data, the use of SMPC in the processing of big data is quite logical. However, current SMPC algorithms often have poor scalability with respect to the amount of data, and thus their application to big data is not easy. To tackle this problem, researchers proposed several solutions that complement SMPC with other methods to enhance scalability. One such approach is illustrated in a query compiler called Conclave that speeds up data analysis by converting queries to a mix of data-parallel, local cleartext, and small SMPC steps. This mode of operation enables the overall system to process datasets that may be between three and six orders of magnitude greater than what is addressable with existing SMPC frameworks independently.

Conclave offers most benefits for relational analytics queries, it is designed to keep SMPC's end-to-end security without relying on the cryptographic SMPC for all operations. Indeed, Conclave can perform other steps outside of SMPC when the parties trust others with some portions of the data, thus enhancing scalability through applying new hybrid MPC-cleartext protocols. Such enhancement in SMPC for big data analysis brings about practicality to obtain privacy-preserving data analysis in different fields such as healthcare, finance, and research. In the future, as research in this domain unfolds, SMPC will be utilized to analyze even large datasets, while preserving privacy at a higher level.

SMPC vs. Other Privacy-Preserving Technologies

SMPC is one of the many privacy-preserving techniques developed to preserve data privacy while facilitating concurrent analysis. In this section, the author contrasts SMPC with other popular methods and analyses the advantages and shortcomings of each.

Differential privacy

Differential privacy is mathematical approach in which a small amount of randomness or noise is added to the data to obscure an individual's contribution. This technique has received a lot of acceptance in the market, and big firms such as Google and Apple incorporate it in their systems. While in SMPC we concerned with the input data and make sure it is private during the computation, DP guarantees that the outcome of a data analysis contains no information about specific individuals. However, at the same time, differential privacy is one of those techniques that provides a measure of privacy. It also clearly defines how much information on the given person can be derived from the analysis results. This makes it particularly useful in cases when it is required to post summary statistics or machine learning models. However, there is one concern for differential privacy. The added noise can cause problems when there are not large amount of data available to help to balance out the true signal and noise. Further, decision regarding the level of noise to be added (privacy budget) is equally hard and perhaps could need expertise in the domain.

Federated learning

Federated learning can be defined as: Federated learning is a distributed approach to machine learning where several parties cooperate to train a model with

a central objective and simultaneously keep their raw data private. Instead, each party builds its local model from its own data and transfers only gradients to a central server for accumulation. A strength of this technique relates to the issue of scalability inherent in SMPC computation since it minimizes the information exchange between the involved parties. Federated learning is especially advantageous in situations where data can only remain at their source because of various restrictions. However, federated learning lacks robust privacy protection on its own. Whereas raw data themselves are still remained local, model parameters that are shared across models could potentially cause the leakage of data information. To this, it has been suggested that federated learning should be implemented alongside other techniques of data protection which include differential privacy or SMPC.

Homomorphic Encryption

Homomorphic encryption (HE) is an encryption technique which enables computation to be made on encrypted data without first having to decrypt the data. Its most important property makes it usable for such computations when to be outsourced to untrusted parties while the data stay secure. As with SMPC, HE has some similarities with it because it also allows computation on private data safely. However, HE centers on situations, where one party has an incentive to protect data from an untrusted compute provider, whereas SMPC is primarily aimed at multiple parties who share data and want to compute a joint function.

This is a major benefit of HE since the data is encrypted all the time, thus giving good security assurances. However, HE suffers from great computational cost, which renders it unrealistic for many applications, and especially for those that involve complex computations or big data sets. Instead, SMPC is more liberal which can solve a broader spectrum of computations effectively at the cost of certain level of communication complexity. w SMPC it is also possible to get stronger security assurance against the collusion among the parties in the network under the assumption that the honest participants form some fraction of the total.

Legal and Ethical Considerations in SMPC

Tomorrow's SMPC applications will present a litany of legal and ethical challenges that organisations will need to meet: as established in the paragraphs above, there are few areas into which SMPC is not relevant, and has not the potential to make a significant impact; these applications will open up a variety of legal and ethical questions which organisaitons apllied or impacted by SMPC will need to answer. The findings also show that both the facilitators and inhibitors of SMPC have enormous implications for compliance regulation, data protection legislation, and ethics.

Regulatory Compliance

SMPC presents a useful solution for organizations to be on the right side of the laws while ensuring they secure their information. With the use of the SMPC based on key generation and management system, CISOs stands to benefit from better data protection, compliance, and risk management. This approach has already found a lot of popularity among large corporations, such as financial, pharmaceutical, automobile companies, etc. SMPC has numerous benefits in terms of supporting organizations in meeting data protection legislation, including the GDPR and HIPAA. These regulations sometimes prevent the distribution of data sets even to authorized agencies that may needs them. The decentralized analytics provided by SMPC make it possible to perform combination analyses of many datasets while keeping all the individual inputs secure, which makes it possible to solve the problems set by current regulations.

Data Protection Laws

The act that has been adopted by the European Union on this has been the GDPR which goes a long way in protecting personal data. It is designed to enhance the protection of human individual rights and citizen's rights as well as ease doing business by providing legal frameworks for organizations and government bodies in the digitized markets. The GDPR has provided unified law to remove legal disparity in different national frameworks in order to avoidextraneous bureaucracy. Accordingly, SMPC can be used by the organization that falls under the GDPR to serve the purpose of data protection regulation and still perform the necessary computation without the leakage of data. This alignment has given rise to new source of control for SMPC and engendered new form of trust proprio to inter-organisational data sharing.

Ethical implications

As with any new practice, SMPC provides many advantages, it also poses some new ethical issues.

It generates the new kind of requirement the need to trust in the basic computations and indubious new forms of the data abuse. Companies need to clarify various ethical issues relating to SMPC, especially in high-risk fields, including medicine and finance.

Another factor of ethical concern is the possibility of the treatment of data sets that is enough to identify people again. Although de-identification and anonymization procedures have been implemented, they are now regarded as insufficient for foiling those intent on circumventing these procedures. Combined with differential privacy, SMPC gives a better approach in preventing any leakage of information specifically about individual records or datasets other than the intended and authorized information disclosure.

Conclusion

Secure multi-party computation is a robust concept that affects business organizations and their approach to managing sensitive data and performing complex computations in partnerships. It has become possible to solve new problems in such fields as finance, healthcare, and machine learning as it promised an opportunity for analyzing data together with maintaining privacy. With development in the work of SMPC, it is becoming less costly in terms of computational cost, and more feasible for the large-scale real-world use. Such progress is preparing the ground to expand the SMPC usage across different industries. Regarding the future, the further development of SMPC looks quite promising; new researches contribute to its development and correction of current shortcomings. With the ever-rising need to sustain privacy in a world that is rapidly embracing the use of data, SMPC has the potential of performing a middleman in the provision of data analysis while at the same time, the protection of privacy. In other for the goal and objectives of SMPC to be achieved to the optimal, certain legal and ethical implications should be considered as follows. In this regard, we can guaranty that this powerful technology is going to be used responsibly to influence the process of innovation but the same time to protect confidential data.

References

1. Peter, A., Tews, E. and Katzenbeisser, S., 2013. Efficiently outsourcing multiparty computation under multiple keys. IEEE transactions on information forensics and security, 8(12), pp.2046-2058.
2. Goldwasser, S., 1997, August. Multi party computations: past and present. In Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing (pp. 1-6).
3. Brandt, F., 2005, December. Efficient cryptographic protocol design based on distributed El Gamal encryption. In International Conference on Information Security and Cryptology (pp. 32-47). Berlin, Heidelberg: Springer Berlin Heidelberg.
4. Smart, N.P., 2003. Cryptography: an introduction (Vol. 3, p. 433). New York: McGraw-Hill.
5. Canetti, R., 2000. Security and composition of multiparty cryptographic protocols. Journal of CRYPTOLOGY, 13, pp.143-202.
6. Goldreich, O., 2003. Cryptography and cryptographic protocols. Distributed Computing, 16, pp.177-199.
7. Demmler, D., Schneider, T. and Zohner, M., 2015, February. ABY-A framework for efficient mixed-protocol secure two-party computation. In NDSS.
8. Chaum, D., Damgård, I.B. and Van de Graaf, J., 1988. Multiparty computations ensuring privacy of each party's input and correctness of the result. In Advances in Cryptology—CRYPTO'87: Proceedings 7 (pp. 87-119). Springer Berlin Heidelberg.
9. Naor, M. and Nissim, K., 2001, July. Communication preserving protocols for secure function evaluation. In Proceedings of the thirty-third annual ACM symposium on Theory of computing (pp. 590-599).
10. Canetti, R., Lindell, Y., Ostrovsky, R. and Sahai, A., 2002, May. Universally composable two-party and multi-party secure computation. In Proceedings of the thiry-fourth annual ACM symposium on Theory of computing (pp. 494-503).
11. Lindell, Yehuda, and Benny Pinkas. "An efficient protocol for secure two-party computation in the presence of malicious adversaries." In Advances in Cryptology-EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007. Proceedings 26, pp. 52-78. Springer Berlin Heidelberg, 2007.