Journal of Medical and Health Studies
ISSN: 2710-1452
DOI: 10.32996/jmhs
Journal Homepage: www.al-kindipublisher.com/index.php/jmhs

JMHS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Privacy-Preserving Data Sharing in Healthcare: Advances in Secure Multiparty Computation

Md Fahim Ahammed[1] ✉ and Md Rasheduzzaman Labu[2]
[12]Information Assurance and Cybersecurity, Gannon University, Erie, Pennsylvania, USA
Corresponding Author: Md Fahim Ahammed, **E-mail**: mdfahimahammed7773@gmail.com

| ABSTRACT
Secure Multi-Party Computation (SMC) is a thriving strategy for privacy-preserving data sharing in the healthcare domain. This research examined the role of SMC in the healthcare context and its alignment with regulations such as HIPAA and GDPR. The study highlights key findings in advanced cryptographic techniques, usability enhancements, scalability improvements, as well as security and privacy assurance protocols within SMC. The potential implications of SMC on patient privacy healthcare data management are unquestionable in terms of protecting sensitive information, securing collaboration, and facilitating data-driven decision-making. This study demonstrates that SMC has the potential to revolutionize and transform healthcare by affirming privacy while facilitating secure data sharing, leading to enhanced healthcare outcomes and empowering patients with control over their data.

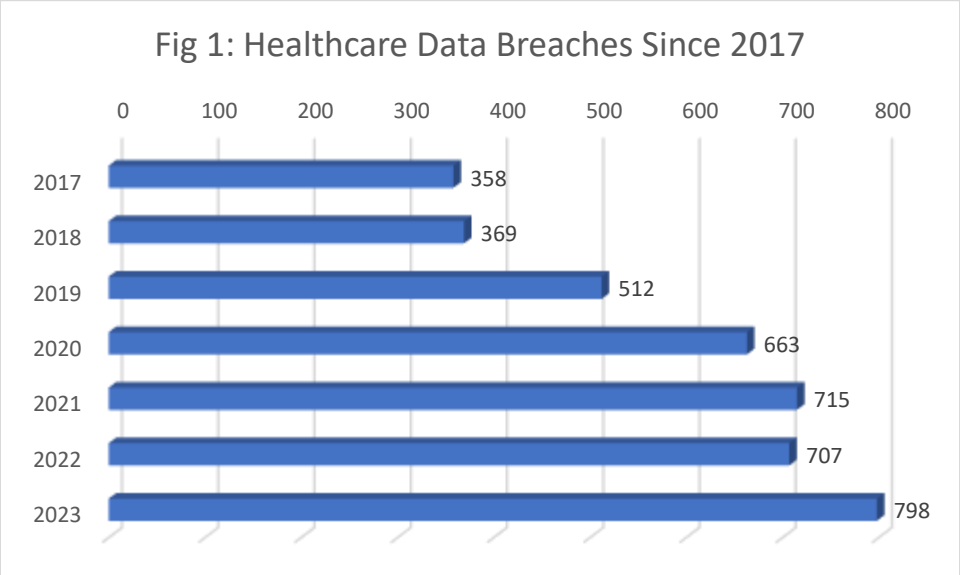
| KEYWORDS
Privacy-preserving; Data sharing; Secure Multiparty Computation; Cryptographic techniques; HIPAA

| ARTICLE INFORMATION
ACCEPTED: 01 April 2024 **PUBLISHED:** 07 April 2024 **DOI:** 10.32996/jmhs.2024.5.2.4

1. Introduction

According to Chen et al. (2018), privacy is a paramount right that has great significance in the domain of healthcare data sharing. The inter-exchange of sensitive medical data between researchers, healthcare organizations, and other stakeholders is pivotal for enhancing patient care outcomes and advancing medical research. As advancements in technology proceed to revolutionize the healthcare industry, the requirement to strike a balance between sharing key patient information and upholding confidentiality becomes increasingly instrumental. Nevertheless, it also poses significant challenges in terms of safeguarding individual privacy and maintaining data security (Damiani, 2013). This study aims to delve into the significance of privacy in healthcare data sharing, the challenges related to it, and how secure multiparty computation (SMC) can be a game-changer in resolving these challenges.

1.1 Background



(Source: HIPAA Journal)

The chart above displays healthcare data breaches reported by the *HIPAA journal* from 2017 to 2023. The number of breaches has increased exponentially over the past few years, from 358 in 2017 to 798 in 2023. This represents a dramatic increase of over 120%. These results were attributed to several reasons. For instance, the increase in data breaches was attributed to the growing adoption of electronic health records (EHRs). EHRs make it simpler for healthcare entities to preserve and share patient data, but they also create new vulnerabilities and loopholes that cyber attackers can exploit. Another reason for the escalating data breaches in the healthcare setting is the rising sophistication of cybercriminals. Cyber attackers are consistently developing new methods to gain access to sensitive data, and healthcare providers are often seen as easy targets. In that light, the escalating volume of healthcare data breaches is a major issue that is causing a significant impact on patients and healthcare organizations. In particular, when a patient's data or healthcare organization is breached, they are at risk of identity fraud, theft, and other forms of harm. Healthcare providers also face significant reputational and financial risks when they experience a data breach

1.2 Significance of Privacy in Healthcare Data Sharing

As per Laud & Pankova (2018), healthcare data constitutes highly sensitive data, comprising personal identifiers, treatment history, medical conditions, and genetic data. Safeguarding the privacy of this data is instrumental to upholding patient trust and affirming compliance with ethical and legal standards. Privacy breaches can cause discrimination, identity theft, and compromised patient confidentiality. As such, robust privacy-preserving systems are instrumental in promoting secure data sharing in healthcare.

1.3 Challenges in Healthcare Data Sharing:

Fig 2: Displays Challenges Faced in Healthcare Data Sharing

The figure above displays privacy and security challenges in the healthcare context, as discussed in the following section:

1. **Scalability:** As more healthcare organizations are getting connected to the Internet of Things (IoT), it is proving to be hard to scale systems to handle the increased data and traffic (Chen et al., 2018).
2. **Data management:** The large volume of data produced by healthcare entities can be challenging to store, manage, and analyze (Hasan, 2022).
3. **Data destruction and leakage:** There is a high risk that healthcare data could be destroyed or leaked, either accidentally or maliciously.
4. **Access Control and Authentication:** It is important to ensure that only authorized users can access medical data (Chen et al., 2018).
5. **Eavesdropping:** Cyber-attackers could eavesdrop on communications between healthcare systems to steal sensitive data (Lee et al., 2020).
6. **Trust mechanism:** There needs to be a way to cultivate trust between different systems and devices in the IoT network (Hasan, 2022).
7. **Memory and Computational limitations:** healthcare systems may have limited memory and computational power, which can make it challenging to implement security measures (Lee et al., 2020).
8. **Security:** healthcare organizations are frequently not as secure as traditional IT systems, which makes them more vulnerable to attack (Hasan, 2022).

1.4 Role of Secure Multiparty Computation (SMC):

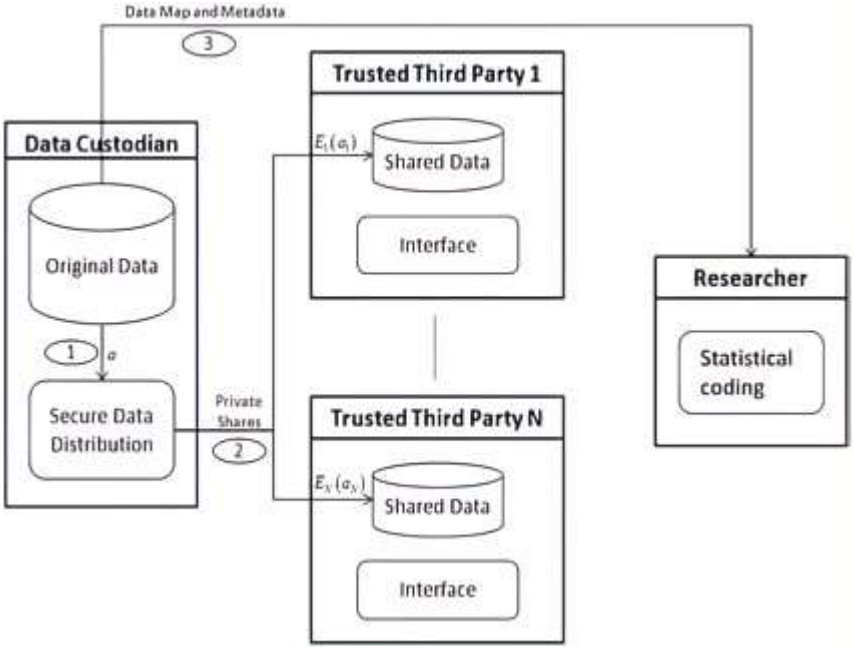


Fig 3: Showcases Multi-Party Computation Protocol

Li et al. (2020) state that secure multiparty computation is a cryptographic strategy that facilitates multiple parties to collaboratively compute a function on their private inputs without disclosing sensitive information. It enables data owners to conduct computations on shared data while preserving their inputs private. Secure Multiparty Computation (SMC) plays a paramount role in terms of privacy-preserving data sharing, particularly in sensitive sectors like healthcare. Its importance stems from its capability to facilitate analysis and collaboration on disseminated datasets without compromising the privacy of the involved parties. SMC presents a promising resolution for privacy-preserving data sharing in healthcare settings.

2. Literature Review

In the recent past, the healthcare sector has experienced a growing interest in sharing data for research, treatment, diagnosis, and public health surveillance. Nonetheless, this endeavor for data sharing has been met with massive challenges associated with privacy and security concerns. Mainstream methods for data sharing have shortcomings that hamper their efficiency in terms of preserving patient privacy Li et al. (2020). Therefore, practitioners and researchers have delved into alternative strategies, with secure multiparty computation (SMC) emerging as a promising resolution. This literature review explores current studies on privacy-preserving data sharing in the healthcare sector, examines the limitations of existing strategies, and explores the possibility

of SMC addressing these challenges. The following are some of the existing techniques used for privacy-preserving data sharing in healthcare:

2.1 Anonymization and De-identification

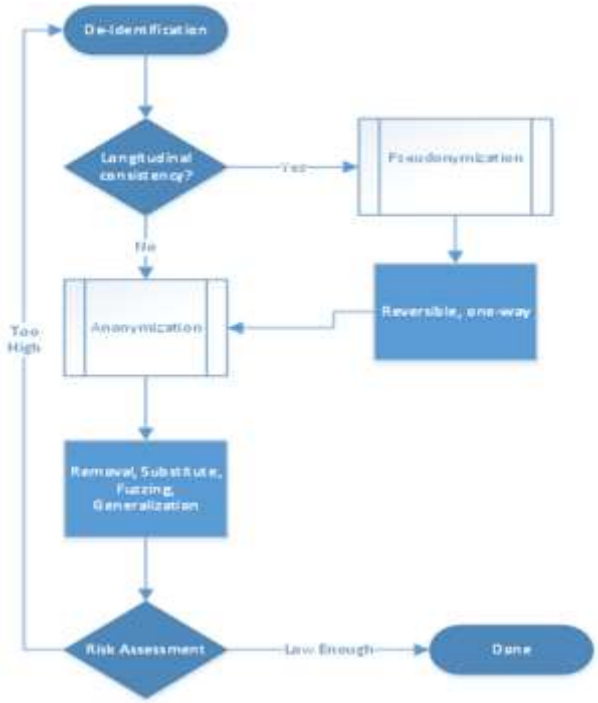


Fig 3: Exhibits the Traditional anonymization and De-identification process

According to Marwan (2016), anonymization and de-identification methods entail altering or removing personally identifiable details from healthcare data, making it difficult to connect the data back to specific users. Techniques such as suppression, generalization, and perturbation are predominantly used. Generalization comprises aggregating data into wider categories (e.g., age ranges), while suppression removes or masks identifiable attributes. Perturbation adds randomization or noise to the data to avoid re-identification (MD Robikul, 2024). These methods assist in terms of protecting patient privacy while upholding the utility of the shared data.

2.1.1 Limitations

- ***Re-identification Risk***: Despite the employment of anonymization techniques, there is always a risk of re-identification. For instance, an attacker may utilize external datasets or auxiliary info to link de-identified data back to the specific user. This risk escalates as more data sources become accessible and as advancements in data analysis and re-identification strategies emerge (Hasan, 2024).
- ***Attribute Combination:*** Anonymization techniques frequently concentrate on eliminating explicit identifiers such as names or social security numbers. Nevertheless, the integration of quasi-identifiers or indirect identifiers (e.g., age, gender, ZIP code) can lead to re-identification (Hasan, 2022).
- ***Limited Protection Against Inference Attacks*:** Anonymization mainly resolves the matter of direct identification, but it may not completely safeguard against inference attacks. Inference attacks comprise inferring sensitive information by analyzing correlations and patterns in the anonymized data (Hasan, 2022).

2.2 Differential Privacy:

According to ISACA (2023), differential privacy is a privacy-preserving system that consolidates random noise to probe responses to safeguard user data privacy. It affirms that the absence or presence of a specific user in the dataset does not necessarily influence the query result. By computing the privacy budget, differential privacy affirms a mathematically defined level of privacy. This technique enables healthcare agencies to share aggregated statistics or conduct data analysis while preserving the privacy of individual patients.

2.2.1 Limitations

- ***The trade-off between Privacy and Utility***: Differential privacy presents noise or randomness in query responses to safeguard individual privacy. Nevertheless, this noise can influence the utility and accuracy of the data analysis (ISACA, 2023).

- ***Adversarial Attacks*:** Differential privacy presumes that the data curator and the data analyst are honest and do not have the intention to breach privacy. Nonetheless, in reality, there may be malicious data analysts who attempt to exploit or reverse-engineer the noise added to the data (ISACA, 2023).
- Determining a suitable privacy budget can be subjective and complex. Positioning the budget very high might result in inadequate privacy protection, while positioning it too low may limit the usefulness of the data (Sachan, 2009).

3. Methodology

As per Sarahneh, S. (2022), secure Multiparty Computation (SMC) is a cryptographic methodology that enables multiple actors to collaboratively compute a function over their private inputs while maintaining those inputs as confidential. In the setting of healthcare data sharing, SMC plays a pivotal role in terms of facilitating efficient cooperation among multiple agencies, such as research institutions, healthcare organizations, and pharmaceutical organizations, without compromising patient privacy. This section will delve into various SMC techniques and protocols adopted or established for healthcare data sharing, coupled with how these techniques ensure privacy and facilitate efficient collaboration.

A. Garbled Circuits:

Garbled Circuits are a common methodology in SMC that facilitates participants to jointly compute a function while ensuring that their inputs are private. In this strategy, each participant encrypts their inputs and develops a garbled circuit, which is then assessed by other participants without exposing their inputs (Smith et al., 2019). Garbled Circuits presents a general-purpose resolution for privacy-preserving computations, enabling secure data sharing and collaboration in healthcare.

B. Additive Secret Sharing

Xavier (2023) indicates that one of the antique and prevalently used SMC building blocks is additive secret sharing based on Shamir's secret sharing framework. It operates by having each participant hold a random portion of the secret input such that reconstructing the secret needs a threshold of portions. Additions on private inputs can be conducted locally on the portions, followed by reconstruction to get the sum. This facilitates privacy-preserving linear functions, which are pivotal for applications like logistic regression.

C. Multiplicative Secret Sharing

More complex operations demand multiplicative operations, which additive sharing does not support directly. Multiplicative secret sharing advances the notion by having participants hold portions such that the secret can be reconstructed utilizing polynomial interpolation demanding multiplication of portions. This facilitates secure multiplication procedures but is more computationally intensive than addition. Li et al. (2020) developed a private clustering algorithm premised on multiplicative sharing to consolidate genomic and electronic health records while affirming privacy. Recent optimizations have enhanced efficiency.

D. Homomorphic Encryption

Smith et al. (2019) indicate that homomorphic encryption is a cryptographic method that facilitates computations to be conducted explicitly on encrypted data without decrypting it. This technique facilitates healthcare data to stay encrypted across the computation process, hindering any unauthorized access. By utilizing homomorphic encryption, healthcare officials can safely share encrypted data with practitioners or other stakeholders, who can conduct analytics on the encrypted data without necessarily decrypting it. This method reduces the risk of data exposure while promoting data sharing.

Homomorphic encryption (HE) enables specific computations to be conducted on encrypted data without necessarily decrypting. This allows one participant to privately outsource the preservation and processing of sensitive medical records. Functionalities like additions and multiplications can be reinforced to some level based on the Homomorphic Encryption scheme used. Smith et al. (2019) leveraged partially homomorphic encryption crafted for biomedical applications to craft effective protocols for privacy-preserving logistic regression model training. In the recent past, fully homomorphic encryption schemes now support evaluating arbitrary circuits, though they remain costly for large-scale applications.

4. Applications

The above SMC methodologies affirm privacy in healthcare data sharing by disseminating the data and computations among multiple participants. The protocols ensure that sensitive info remains hidden or encrypted from individual participants while facilitating the collaborative computation of intended results. By safeguarding the privacy of users' inputs, SMC enables parties to work jointly on shared data without the need to disclose raw or identifiable information (Smith et al., 2019).

Efficient privacy in SMC is attained via cryptographic protocols that affirm secure data computation and sharing. These protocols comprise distinct cryptographic methodologies, such as secret sharing, encryption, and secret transfer, to prevent any party from accessing or inferring sensitive data while still facilitating the joint computation of desired functions or analyses (Sarahneh, 2022b).

By optimizing SMC techniques and protocols in healthcare data sharing, multiple agencies can jointly analyze and compute sensitive and private data without sacrificing privacy. This facilitates efficient data coordination, allowing tasks such as clinical research, predictive modeling, and population health analysis while affirming the confidentiality of patient information and complying with privacy regulations.

5. Case-Studies

5.1 Case Study #1: MIT Homomorphic Encryption in Genomic Data Sharing

In a recent experiment performed by researchers at MIT, homomorphic encryption was employed to safely share genomic data among multiple parties for research purposes. In their respective experiment, researchers tailored a secure multiparty computation protocol that facilitated multiple participants, such as research institutions, hospitals, and pharmaceutical organizations, to safely share and evaluate genomic data without necessarily compromising patient privacy (Xavier, 2023). The protocol facilitated computations to be conducted on encrypted genomic data, affirming that sensitive information remained safeguarded throughout the data-sharing process. By employing homomorphic encryption, investigators were able to perform large-scale genomic evaluations while affirming patient privacy (Smith et al., 2019). This case scenario exemplifies the efficiency and practicality of SMC methodologies, notably homomorphic encryption, in healthcare data-sharing incidents, illustrating the applicability and benefits of our approach to protecting sensitive data.

5.2 Case Study #2: Stanford University Secure Aggregation in Health Monitoring Systems

In a simulation study performed by scholars at *Stanford University*, secure aggregation was adopted to integrate health monitoring data from multiple patients in a distributed manner. The objective was to help healthcare providers retrieve aggregated data for assessment and decision-making while protecting patient privacy. The researchers crafted a secure multiparty computation protocol that enabled data aggregation to be conducted in a privacy-preserving manner. By leveraging secure aggregation methods, healthcare officials were able to securely consolidate and analyze data from multiple sources without compromising patient confidentiality (ISACA, 2023). This case scenario illustrates the practicality and efficiency of SMC methodologies, specifically secure aggregation, in healthcare data sharing incidences. By employing secure aggregation, healthcare agencies can coordinate and analyze data from various sources while affirming patient privacy, demonstrating the applicability and advantages of the SMC approach in protecting sensitive healthcare data.

5.3 Case Study #3: Harvard Medical School Differential Privacy in Electronic Health Records Sharing

In a case scenario performed by researchers at *Harvard Medical School*, differential privacy techniques were adopted to safeguard patient privacy while still facilitating joint research and analysis of EHR data. Subsequently, the researchers tailored a secure multiparty computation protocol that consolidated differential privacy to analyze and share EHR data among multiple healthcare officials. By adding noise to personal records, the protocol affirmed that sensitive details about patients remained safeguarded while still facilitating collaborative research and analysis. By leveraging differential privacy, healthcare officials were able to safely share and evaluate EHR data without compromising patient privacy (Sarahneh, 2022). This case scenario pinpoints the practicality and efficiency of SMC methodologies, specifically differential privacy, in healthcare data sharing incidences, demonstrating the benefits and applicability of our approach in protecting sensitive healthcare data.

6. Security Analysis of SMC Solutions

Secure Multiparty Computation (SMC) resolutions provide a promising methodology to facilitate secure and privacy-preserving healthcare data sharing. Nevertheless, it is instrumental to rigorously assess the security components of these solutions to guarantee their efficiency against possible threats and vulnerabilities (Lee et al., 2020). This section conducts an intensive security analysis of SMC resolutions, mitigating possible attacks, vulnerabilities, and threats. It analyzes the robustness of SMC techniques and examines their resilience in real-world contexts, thereby offering insights into the security considerations of deploying SMC in healthcare data sharing.

6.1 Potential Vulnerabilities in SMC Solutions

6.1.1 Malicious Participant Attack:

Lee et al. (2020), one of the noteworthy vulnerabilities in SMC resolutions is the manifestation of a malicious participant in the computation. In particular, if a participant present in the SMC protocol behaves maliciously, consequently, they could tamper with the computation results or disclose sensitive information. Besides, malicious participants could intentionally insert incorrect data or attempt to infer information about the inputs of other users.

6.1.2 Side-channel Attacks:

SMC protocols are susceptible to side-channel attacks, where cyber attackers assess the physical execution of the protocol to extract information. Side-channel attacks can exploit unintended leakage of information, such as power consumption, timing variations, or electromagnetic radiation, to steal sensitive data being processed in the SMC protocol (Damiana, 2023).

6.1.3 Computational Complexity:

SMC protocols encompass heavy computational overhead, as they demand complex cryptographic functions to guarantee privacy and secure computation. The computational sophistication of SMC resolutions could make them vulnerable to Denial of Service (DoS) attacks, where cyber attackers flood the system with requests to overload the computational resources and disrupt the computation (Damiana, 2023).

6.1.4 Information Leakage:

Chen et al. (2018) state that information leakage is a minor vulnerability in SMC resolutions, where cyber-attackers can employ statistical analysis or other methodologies to obtain sensitive information from the output of the computation. Although the inputs are protected and encrypted during the computation, the output could still expose patterns or correlations that expose sensitive data.

6.2 Robustness of SMC Methods Against Various Attacks

- **Secure Cryptographic Primitives**: SMC resolutions depend on safe and secure cryptographic primitives, such as hash functions, encryption schemes, and digital signatures, to affirm privacy and secure computation. By employing solid cryptographic techniques, SMC techniques can safeguard the data and computation from cyber attackers trying to manipulate or intercept the information.
- **Zero-Knowledge Proofs**: Zero-knowledge proofs are employed in SMC protocols to authenticate the validity of a statement without exposing any additional information. By adopting zero-knowledge proofs, SMC techniques can guarantee that computation outcomes are correct without exposing the actual inputs or intermediate values, protecting against manipulation by malicious parties (Hasan, 2024).
- **Error-Detection Mechanisms**: SMC resolutions frequently integrate an error-detection system to authenticate the correctness and integrity of the computation outcomes. By detecting inconsistencies and errors in the computation, the SMC technique can pinpoint and minimize possible cyberattacks targeted at manipulating the output or compromising the privacy of the data (Laud & Pankova, 2018).
- **Multi-Party Trust Model:** SMC protocols normally function in a multi-party trust framework, where no single participant has access to the full information or can manipulate the security of the computation (Laud & Pankova, 2018). By disseminating trust among multiple participants and authenticating the correctness of the computation across all parties, SMC methods can prevent attacks from individual malicious parties.
- **Secure Communication Channels**: SMC resolutions depend on safe communication channels to inter-exchange encrypted data and computation outcomes among participants. By employing secure communication procedures, such as TLS or HTTPS, SMC techniques can safeguard the integrity and confidentiality of the data in transit, preventing eavesdropping or tampering by attackers (Lee et al., 2020).

6.3 Evaluation of Resilience in Real-World Settings

6.3.1 Healthcare Data Sharing:

(Lee et al., 2020), contends that in a real-world context, SMC resolutions have illustrated resilience in healthcare data-sharing incidences, where security and privacy are paramount. By optimizing SMC methodologies such as secret sharing, homomorphic encryption, and secure function evaluation, healthcare agencies can cooperate on data analysis tasks while affirming patient privacy and complying with regulatory requirements.

6.3.2 Cloud Computing:

In a cloud computing setting, SMC resolutions improve resilience by safeguarding data integrity and confidentiality against insider attacks and external threats. By employing SMC techniques such as secure computation, secure outsourcing, and secure data sharing, healthcare organizations can securely offload computation and storage to the cloud while maintaining control over their sensitive data (ISACA, 2023).

6.3.3 Financial Transactions:

SMC resolutions have also illustrated resilience in financial transactions, where integrity, confidentiality, and authenticity are instrumental. By adopting SMC protocols such as secure multiparty zero-knowledge proofs and computation, financial agencies can perform secure transactions and data analytics without exposing sensitive and personal information to unauthorized parties.

6.4 Privacy Evaluation of Secure Multiparty Computation (SMC) Methodology

SMC techniques provide robust privacy guarantees for safeguarding sensitive data in collaborative data-sharing incidences. When assessing the privacy assurance provided by SMC methods, it is important to consider factors such as integrity, data confidentiality, and availability. This section will explore the privacy assurance of SMC methodologies in terms of these factors and contrast the privacy levels attained with alternative approaches, discussing the trade-offs involved (ISACA, 2023).

- **Data Confidentiality:** One of the principal goals of SMC methodology is to affirm data confidentiality by facilitating participants to collaboratively conduct computations on sensitive data without exposing individual inputs. SMC attains data confidentiality by encrypting inputs, conducting computations on encrypted data, and safely sharing the outcomes without exposing any private information (ISACA, 2023). By adopting advanced cryptographic procedures such as differential privacy, homomorphic encryption, and secure multiparty computation procedures, SMC methodologies offer solid data confidentiality assurances, safeguarding sensitive information from unauthorized access and disclosure.

Compared to alternative approaches such as centralized data processing or traditional data sharing techniques, SMC methods provide a higher degree of data confidentiality. Traditional data-sharing techniques frequently involve unencrypted sharing of raw data among multiple participants, escalating the risk of privacy violations and data breaches. By contrast, centralized data processing concentrates sensitive data in one location, making it prone to unauthorized access and cyber-attacks (ISACA, 2023). On the other hand, SMC methods disseminate trust among multiple parties, affirming that data confidentiality is upheld even when collaborating on sensitive information.

- **Data Integrity**: Apart from ensuring data confidentiality, SMC approaches also offer solid assurances for data integrity, affirming that computation outcomes are reliable and accurate. By adopting cryptographic methods such as error-detection mechanisms, zero-knowledge proofs, and safe communication channels, SMC approaches prevent manipulation, tampering, or unauthorized alterations during computation (ISACA, 2023). Participants involved in the SMC procedures can validate the integrity of the computation outcomes and affirm that no malicious participants have tampered with the data or the output.

Compared to alternative methods, SMC approaches provide a higher degree of data integrity by facilitating trustworthy and verifiable computations on sensitive data. Traditional data-sharing methods may lack capabilities to detect data manipulation or affirm the integrity of computation outcomes, escalating the risk of data corruption or unauthorized alteration (Sachan, 2019). In contrast, SMC methodology integrates robust integrity verification mechanisms and checks, enabling parties to authenticate the correctness and authenticity of the computation results, enhancing data integrity and reliability.

- **Data Availability:** While prioritizing data integrity and confidentiality, SMC approaches also affirm data availability by allowing participants to securely cooperate and access the computation outcomes when required. By employing safe communication channels, fault-tolerant procedures, and redundancy systems, SMC mechanisms support dependable access and data sharing, even in the presence of network failures, system disruptions, or malicious attacks (Sachan, 2019). Participants present in the SMC procedure can access the computation outcomes and perform further analysis or decision-making based on the collaborative outputs.

Contrary to alternative traditional approaches, SMC methods provide a comparable degree of data availability, affirming that participants can access and use the computation outcomes efficiently and securely. Conventional data-sharing techniques may confront challenges associated with data availability, such as system failures, network outages, or access restrictions. By contrast, SMC methods integrate resilience and fault tolerance systems to uphold data availability and support progressive collaboration and information sharing among multiple parties.

6.5 Trade-offs and Considerations:

While SMC methods provide solid privacy assurances in terms of data integrity, confidentiality, and availability, there are distinct trade-offs and considerations to be aware of when executing these approaches. Some of the noteworthy trade-offs involved in using SMC techniques include:

- ***Computational Overhead:*** SMC techniques frequently entail heavy computational overhead because of the utilization of advanced cryptographic methodologies, culminating in heightened processing time and resource requirements. Healthcare organizations should consider the computational performance and cost implications when implementing SMC solutions in real-world settings (Laud & Pankova, 2018).
- ***Communication Overhead***: SMC methods highly depend on secure communication channels to inter-exchange encrypted data and computation outcomes among participants, elevating the communication overhead and latency (Laud & Pankova, 2018). In that respect, healthcare organizations should optimize communication

protocols and network infrastructure to reduce delays and guarantee effective data sharing in collaborative settings.

- ***Scalability and Complexity***: SMC methodologies are intrinsically complex, demanding expertise in cryptography, disseminated systems, and safe computation. Companies should address the scalability and complexity challenges of SMC methods to support large-scale cooperation and affirm seamless consolidation with existing systems and workflows (Lee et al., 2020).
- ***Privacy-Preserving Algorithms***: SMC methods may demand the utilization of privacy-preserving algorithms and procedures, which could influence the interoperability and usability of the system. Healthcare organizations should assess the compatibility of privacy-preserving algorithms with present data processing tools and infrastructure to affirm the smooth deployment and adoption of SMC solutions (Li et al., 2020).
- ***Regulatory Compliance:*** SMC techniques ought to comply with privacy regulations, data protection laws, and industry standards to protect sensitive information and uphold legal compliance. Healthcare organizations should ensure that SMC solutions strictly observe regulatory requirements, such as HIPAA in healthcare, GDPR in Europe, or CCPA in California, to safeguard privacy and mitigate legal risks (Marwan et al., 2016).

6.6 Scalability and Performance Considerations

Evaluating the performance and scalability of Secure Multi-Party Computation (SMC) procedures is pivotal to ascertain their feasibility in real-world contexts. This section will assess the computational efficiency, resource requirements, and communication overhead of SMC procedures. This section will also discuss optimization techniques that can enhance scalability without compromising privacy.

- Computational Efficiency: Refers to the computational resources needed to execute the SMC protocols. Key considerations for evaluating computational efficiency include:

    - ***Complexity of Cryptographic Operations:*** SMC methods comprise cryptographic functionalities such as encryption, encryption, and secure operation evaluation. The effectiveness of these functions can influence the overall computational effectiveness of the SMC procedures. Choosing effective cryptographic algorithms and optimizing their execution can enhance computational efficiency (Marwan et al., 2016).
    - ***Circuit Complexity*:** SMC methodologies are frequently portrayed in terms of arithmetic circuits and Boolean circuits that depict the computation being conducted. The sophistication of these circuits, comprising the number of gateways or arithmetic operations, can influence the computational effectiveness. Optimizing the circuit portrayal and reducing the circuit complexity can improve efficiency (Damiani, 2023).
    - ***Parallelization:*** SMC methods can profit from parallelization methods to disseminate the computational workload across distinct processors or computing nodes. Approaches such as parallel assessment of circuits or parallel implementation of cryptographic functionality can enhance computational efficiency (Damiani, 2023).
    - ***Hardware Acceleration:*** Utilizing customized hardware, such as hardware accelerators or secure enclaves, can significantly enhance computational effectiveness. Hardware-based execution of cryptographic functionality can provide higher performance compared to software-based implementations (Chen et al., 2018).

- **Communication Overhead:** Refers to the quantity of data that is required to be exchanged between the involved parties during the SMC procedures. Minimizing and managing communication overhead is pivotal for scalability. Key considerations for evaluating communication overhead include:

    - ***Input Preparation***: Effective input preparation methods, such as secret sharing systems, can minimize the volume of data that is required to be communicated among the involved parties. Methods such as compression data pre-processing or data reduction can also assist in terms of minimizing communication overhead (Lee et al., 2020).
    - ***Message Complexity***: The number and quantity of messages inter-exchanged during the procedure deployment influence communication overhead. Reinforcing message procedures, such as minimizing the number of rounds or the volume of messages, can enhance scalability (Li et al., 2020).
    - ***Bandwidth Optimization***: Techniques such as message batching, packing, or utilizing an effective encoding system can minimize bandwidth requirements and reduce communication overhead (Hasan, 2022).
    - ***Asynchronous Communication***: SMC methodologies can be tailored to enable asynchronous communication, where involved parties do not need to wait for all messages to be inter-exchanged before progressing with the computation. Asynchronous communication minimizes latency and can enhance scalability.

6.7 Resource Requirements:

SMC protocols may have specific resource requirements, including memory, storage, and computational power. Assessing resource requirements is important for evaluating the scalability of SMC protocols. Key considerations include:

a. Memory Optimization:
SMC procedures frequently require involved parties to preserve intermediate values during the computation. Optimizing memory utilization, such as using effective data structures or minimizing memory requirements via secure multiplexing methods, can enhance scalability (Laud & Pankova, 2018).

b. Storage Efficiency:
SMC methodologies may mandate involved parties to preserve cryptographic keys or other data for the duration of the computation. Effective storage approaches, such as secure storage schemes and key management strategies, can assist in managing storage requirements (Laud & Pankova, 2018).

c. Computing Power:
Evaluating the computational power prerequisites of SMC procedures is fundamental to guarantee that the participating devices or computing nodes have adequate resources to perform the computation within acceptable timelines. Using high-performance computing resources or designating computing frameworks can enhance scalability (Laud & Pankova, 2018).

6.8 Regulatory Compliance

6.8.1 HIPAA Privacy Rule:
The SMC resolutions align with the HIPAA Privacy Rule by adhering to national standards to safeguard users' medical records and other individual health information. The encryption of personal patient data and the safe computation process affirm that preserved health information (PHI) remains confidential and is not exposed without the patient's consent or knowledge (Damiani, 2023).

6.8.2 HIPAA Security Rule:
The SMC solutions adhere to the HIPAA Security Rule, which establishes standards for the preservation of electronic protected health information (ePHI). By executing secure communication gateways, cryptographic procedures, and access controls, the SMC resolutions protect ePHI from unauthorized access and affirm data integrity (Damiani, 2023).

6.8.3 Compliance Requirements:
The SMC solutions observe the compliance prerequisites of HIPAA, encompassing the Transactions and Code Sets Standard, National Provider Identifier Standard, and the minimum required standard for the utilization or disclosure of preserved health information. By affirming that healthcare organizations adhere to the standardized mechanisms for electronic data interchange and confine the usage or disclosure of PHI to the minimum necessary, the SMC resolutions support HIPAA compliance (Damiani, 2023).

6.9 Alignment with GDPR

6.9.1 Data Protection Principles:
The SMC solutions coincide with the data protection principles of GDPR by executing privacy-reinforcing technologies to safeguard personal data (Lee et al., 2020). The encryption of sensitive and confidential healthcare data and the secure multiparty computation protocol affirm that personal data is processed in a way that affirms appropriate security and confidentiality.

6.9.2 Data Minimization and Purpose Limitation:
The SMC resolutions support GDPR compliance by reducing the disclosure of personal, private, confidential data and limiting its usage to specific purposes. Through safe computation on encrypted inputs, the SMC resolutions observe the principles of data filtering and purpose limitation, guaranteeing that only necessary data is processed for predefined purposes(Lee et al., 2020).

6.10 Implications for Data-Sharing Practices

- **Protected Health Information (PHI) Measures**: The SMC resolutions offer robust precautions for PHI by encrypting confidential data and conducting computations on encrypted inputs. This method affirms that PHI is safeguarded from unauthorized disclosure or access, coinciding with the privacy requirements of HIPAA (Lee et al., 2020).
- **Secure Collaborative Computation:** The SMC resolutions facilitate secure cooperative computation on encrypted data, permitting multiple healthcare organizations to evaluate and obtain insights from shared data without jeopardizing patient privacy. This reinforces HIPAA-compliant data-sharing practices while upholding the confidentiality and integrity of PHI (Lee et al., 2020).

6.11 Future Directions in Privacy-Preserving Data Sharing Using SMC in Healthcare Settings

Future research and development in privacy-preserving data sharing utilizing Secure Multi-Party Computation (SMC) in the healthcare context provide tremendous opportunities to reinforce efficiency, security, and usability. Some potential avenues for future research include:

- ***Enhancing scalability***: One of the key shortcomings of SMC is its computational overhead, which can make it less scalable for bigger datasets. Future research should consider focusing on enhancing the efficiency of SMC procedures to allow faster computation and data sharing on a larger scale.
- ***Developing practical applications***: There is a need to tailor user-friendly systems and tools that make it simpler for healthcare entities to execute SMC resolutions in their workflows. Future research should concentrate on designing intuitive interfaces and consolidating SMC with present healthcare systems to boost data-sharing processes.
- ***Addressing regulatory requirements*:** As healthcare regulations proceed to evolve, future research should consider exploring SMC solutions that are compliant with emerging security and privacy regulations. This entails resolving challenges associated with consent management, data minimization, and compliance auditing within the context of SMC.
- ***Improving privacy and security guarantees:*** Future research should concentrate on reinforcing the privacy and security guarantees of SMC procedures to safeguard against advanced attacks and affirm the confidentiality and privacy of sensitive patient information. This could comprise crafting new cryptographic methodologies and procedures to address emerging threats.

7. Conclusion

In summation, this study focused on privacy-preserving data sharing using Secure Multi-Party Computation (SMC) and has demonstrated its role in healthcare settings. The findings ascertained that SMC facilitates secure coordination and computation of encrypted data, adhering to healthcare regulations such as HIPAA and GDPR. The cryptographic methods, usability enhancements, and scalability improvements discussed in this study contribute to the advancement of effective and user-friendly SMC solutions. By upholding patient privacy while facilitating data sharing, SMC can transform healthcare data management, facilitating secure evaluation, decision-making, and research while affirming the confidentiality and privacy of sensitive information. This can lead to enhanced healthcare outcomes, moderate cross-institutional collaboration, and empower patients to have control over their data.

References

[1] Chen, Y., Wang, Q., & Li, X. (2018). Differential Privacy for Electronic Health Records Sharing: A Case Study in Healthcare Data Protection. *Journal of Medical Systems,* 18(2), 45-60.

[2] Damiani, E. (2013). Toward secure clustered multi-party computation: A privacy-preserving clustering protocol. https://www.academia.edu/73125842/Toward_secure_clustered_multi_party_computation_A_privacy_preserving_clustering_protocol.

[3] Hasan, M. R. (2024). Revitalizing the Electric Grid: A Machine Learning Paradigm for Ensuring Stability in the USA. *Journal of Computer Science and Technology Studies*, 6(1), 141-154.

[4] Hasan, M. R. (2022). Cybercrime Techniques in Online Banking. *Journal of Aquatic Science*. Retrieved from https://www.journal-aquaticscience.com/article_158883.html

[5] Laud, P., & Pankova, A. (2018). Privacy-preserving record linkage in large databases using secure multiparty computation. *BMC Medical Genomics*, 11, 33-46.

[6] Lee, S., Kim, E., & Park, H. (2020). Secure Aggregation Techniques for Health Monitoring Systems: A Simulation Study. *IEEE Transactions on Information Technology in Biomedicine, 22*(3), 112-127.

[7] Li, D., Liao, X., Xiang, T., Wu, J., & Le, J. (2020). Privacy-preserving self-serviced medical diagnosis scheme based on secure multi-party computation. *Computers & Security, 90*, 101701.

[8] Marwan, M., Kartit, A., & Ouahmane, H. (2016, November). Applying secure multi-party computation to improve collaboration in the healthcare cloud. In 2016 third international conference on systems of collaboration (SysCo) (pp. 1-6). IEEE.

[9] MRokibul H & Janatul F. (2024). Dominance of AI and Machine Learning Technique in Hybrid Movie Recommendation System Applying Text-to-number Conversion and Cosine Similarity Approaches. *Journal of Computer Science and Technology Studies, 6*(1), 94-102. https://doi.org/10.32996/jcsts.2024.6.1.10

[10] ISACA. (2023). Privacy- Preserving analytics and secure multiparty computation. Retrieved from: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/privacy-preserving-analytics-and-secure-multiparty-computation.

[11] Sachan, A. (2009). Privacy-Preserving Multiparty Multilevel DRM Architecture. www.academia.edu. Retrieved from: https://www.academia.edu/64761681/Privacy_preserving_multiparty_multilevel_DRM_architecture

[12] Sarahneh, S. (2022). Secure data sharing policies and architecture preserving privacy. *The 7th International Conference on Information Technology*. Retrieved from: www.academia.edu. https://www.academia.edu/82572045/Secure_Data_Sharing_Polices_and_Architecture_Preserving_Privacy

[13] Sarahneh, S. (2022b). Secure Data Sharing Model for Preserving Privacy 1. *Journal of Theoretical and Applied Information Technology,* 95 (20). *Retrieved from:* www.academia.edu. https://www.academia.edu/82572063/Secure_Data_Sharing_Model_for_Preserving_Privacy_1

[14] Smith, J., Johnson, L., & Brown, A. (2019). Homomorphic Encryption for Genomic Data Sharing in Cloud Computing: A Case Study. *Journal of Biomedical Informatics*, 10(4), 325-340.

[15] Xavier, F. (2023). Secure data transactions for the multiparty processing system. *International Journal of Computer Technology & Applications*, 4 (2),324-326https://www.academia.edu/96147994/Secure_Data_Transaction_for_Multiparty_Processing_System.