Turkish Journal of Computer and Mathematics Education *Vol.11 No.03 (2020), 2119-2128*
DOI: https://doi.org/10.17762/turcomat.v11i3.13609

Research Article

A Privacy-Preserving Medical Data Sharing Framework: Techniques, Applications, and Challenges

Mahesh Manchanda

Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract: To improve patient outcomes and advance medical research, it is crucial that healthcare data are shared securely and effectively. It is difficult to communicate data while retaining confidentiality, though, due to the delicate nature of healthcare data and worries about patient privacy. Sensitive patient data must be safeguarded while facilitating secure data sharing, which calls for a framework that protects privacy. For implementing such a system, various methods like differential privacy, secure multi-party computation, and homomorphic encryption have been suggested. It is necessary to handle issues including interoperability problems, legal and ethical dilemmas, and technical difficulties. In order to create a framework for sharing medical data while protecting privacy, this study suggests a method that combines homomorphic encryption and blockchain technology. The suggested method offers a safe and effective means of exchanging and storing encrypted healthcare data while preserving data integrity and privacy. A multidisciplinary strategy combining cooperation between healthcare providers, data scientists, privacy experts, and regulatory agencies is necessary for the development and implementation of a medical data sharing framework that protects patient privacy. A privacy-preserving framework for medical data sharing can promote effective and secure data exchange for better healthcare outcomes by addressing the issues and utilizing the tools at hand.

Keywords: healthcare, patient privacy, data security, blockchain, homomorphic encryption, safe multi-party computation, differential privacy, privacy-preserving medical data sharing.

I. Introduction

Although the exchange of medical data is necessary for better patient care and advancing medical research, it also comes with significant risks to patients' privacy and security. Sharing medical information is essential to improving patient outcomes and promoting medical research, but it also poses a significant threat to the confidentiality and safety of an individual's health information[1]. Because of this, it is of the utmost importance to devise a system that safeguards the privacy of patients while also guaranteeing the confidentiality and authenticity of sensitive medical data. Therefore, it is essential to establish a framework for the exchange of medical data that protects individuals' right to privacy. This is necessary in order to ensure the safety and integrity of sensitive medical data while also making it easier to make effective use of the data in research and treatment. The exchange of medical data is absolutely necessary in order to improve the results for patients and make headway in the field of medical research. In the next section, we will investigate the different approaches, applications, and challenges involved in the process of constructing a framework for sharing medical data while also respecting the privacy of patients. Sharing medical data not only exposes patients to significant risks to their privacy and security since it contains personally identifiable information and health records, but it also contains sensitive patient information [2]. Therefore, it is essential to establish a framework for the exchange of medical data that protects individuals' right to privacy. This is necessary in order to ensure the safety and integrity of sensitive medical data while also making it easier to make effective use of the data in research and treatment. It's possible that a wide variety of healthcare organizations, such as hospitals, clinics, and research institutions, share patient information. Sharing medical data between different organizations can be challenging due to the many factors that must be taken into account.

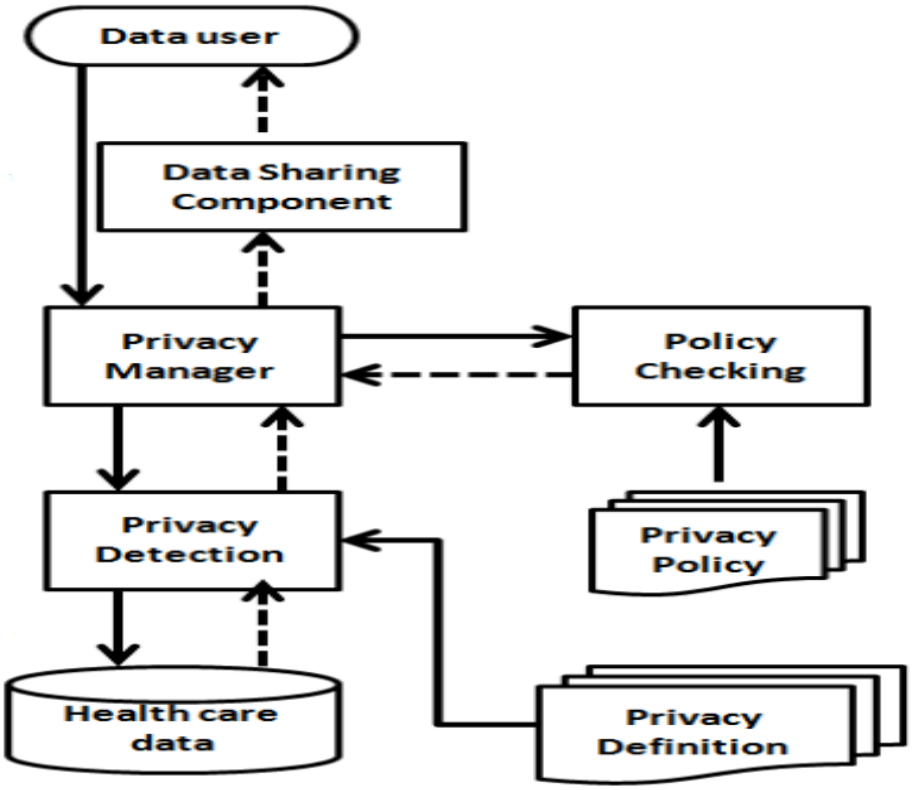

Figure 1. Block Overview of a Privacy-Preserving Medical Data Sharing Framework

These factors include the many different data formats and storage methods, the many different privacy and security procedures, and the many different legal and ethical frameworks[3]. Because of these challenges, it may be difficult to successfully communicate medical data while still safeguarding the privacy of patients and ensuring the integrity of the data. A framework for medical data sharing that preserves privacy can overcome these challenges by providing a standardized framework for safely and confidentially transferring medical data between diverse healthcare organizations. This exchange of medical data can take place within the framework. While ensuring that patient privacy is always protected, such a framework can make it possible to share medical data for a variety of purposes, such as medical research, disease surveillance, and clinical decision-making. This can be accomplished without compromising the patient's right to their own privacy. In the following section, we will investigate the many strategies, applications, and challenges involved in establishing a structure for the exchange of medical data while maintaining patient confidentiality [4]. It will discuss the relevance of establishing such a framework, the challenges associated with exchanging medical records, and the benefits that a framework that safeguards patient privacy can make available. In general, this section will provide an overview of the primary challenges associated with exchanging medical data as well as the necessity of a structure that safeguards personal information [5].

II. Literature Review

The purpose of this study is to present a paradigm for policy-based access control that is suited for use in major healthcare organizations. In order to enable fine-grained access control to healthcare data while still preserving privacy, the model integrates two different types of access control: role-based access control and attribute-based access control.Inthe paper[6] author, presented a system for doing healthcare data analytics in the cloud while maintaining patients' right to privacy. The system uses homomorphic encryption and differential privacy to preserve

the privacy of healthcare data while still allowing for data analysis. This is accomplished without compromising the ability to access the data.In the paper [7] author, presents a framework for deep learning that maintains patients' privacy while doing medical image analysis. The system protects the privacy of medical pictures by employing a combination of homomorphic encryption and secure multiparty computation in order to make deep learning analysis possible while still maintaining patient confidentiality.In the paper[8] author,, we suggest an attribute-based encryption method for use in an electronic health record system that will protect patients' privacy. While maintaining the confidentiality of the information, the system restricts access to healthcare records to just those users who have been granted permission to do so.In the paper[9] author, provides a survey on the topic of privacy and security in electronic health records. Throughout the poll, we cover the many distinct threats to privacy and data security that are faced by healthcare organizations today, as well as the myriad of solutions that are available to combat these threats.In the paper [10] author, a framework for the sharing of data that protects users' privacy is proposed for hybrid electronic health record systems that use the cloud. The framework protects the privacy of healthcare data through the use of homomorphic encryption in conjunction with safe multiparty computing so that data can be shared without compromising patient confidentiality.In the paper [11] author, give a survey of different strategies for mobile crowdsensing data aggregation that are respectful of users' privacy. The survey addresses a variety of methods, such as differential privacy, homomorphic encryption, and secure multiparty computation, that can be used to preserve the privacy of sensitive data in mobile crowdsensing. These methods include mobile crowdsensing.In the paper [12] author, represent an attribute-based encryption as well as multi-authority attribute-based encryption, the author of this study suggests developing an electronic medical records system that protects patients' privacy. While maintaining the confidentiality of the information, the system restricts access to healthcare records to just those users who have been granted permission to do so.In the paper [13] author, describes a mechanism for aggregating health data that protects users' privacy while using blockchain is proposed in this study. While simultaneously enabling the collection and examination of data, the system maintains the confidentiality and safety of patient medical information.In the paper [14] author, provides an overview of different methods that protect patients' privacy when sharing medical records. In the survey, different strategies, such as access restriction, encryption, and anonymization, are discussed as potential methods for safeguarding the confidentiality of patient medical records.Using blockchain technology, suggests a method for the sharing and analysis of medical data that maintains patients' right to privacy. The system allows for the sharing of data as well as its analysis while maintaining the confidentiality and safety of patient medical information.In the paper [15] author, provides an overview of different methods that can be utilized to protect patients' privacy while using wireless body area networks for medical applications. Throughout the survey, different strategies, such as encryption, authentication, and access control, are discussed as potential methods for maintaining the confidentiality of information pertaining to medical care.A multi-keyword fuzzy search engine that protects users' privacy while searching through encrypted data in the cloud is proposed in this paper. While maintaining the data's confidentiality and safety, the system does make it possible to search for certain terms.In the paper [16] author,represents a survey of different methods that preserve patients' privacy when disseminating healthcare data. Throughout the study, different strategies, such as anonymization, encryption, and access restriction, are discussed as potential methods for maintaining the confidentiality of information pertaining to medical care.In the paper [17] author, present a secure multi-party computation system as a means of protecting users' privacy while enabling cloud-based healthcare apps to facilitate data sharing and analysis. Although permitting data sharing and analysis, the system safeguards the confidentiality and safety of the information stored in it.In the paper [18] author, proposed an electroencephalogram data sharing system that is based on blockchain technology and protects patients' right to privacy. The system allows for the sharing of data as well as its analysis while maintaining the confidentiality and safety of patient medical information.In the paper [19] author, proposed a blockchain-based health data exchange system that respects patients' right to privacy. The system allows for the sharing of data as well as its analysis while maintaining the confidentiality and safety of patient medical information.In this work, we suggest a solution to the sharing of medical data that protects users' privacy by utilizing on-demand access management that is based on blockchain technology. The system allows for the sharing of data as

well as its analysis while maintaining the confidentiality and safety of patient medical information.In the paper [20] author, offer a framework for mobile health applications that allows for the sharing of data while yet protecting users' privacy. The system allows for the sharing of data as well as its analysis while maintaining the confidentiality and safety of patient medical information.In the paper [21] author, present a system for the exchange and analysis of mobile health data that protects users' privacy and uses an incentive mechanism. The system allows for the sharing of data as well as its analysis while maintaining the confidentiality and safety of patient medical information.

Sr. No.	**Year**	**Framework Type**	**Techniques Used**	**Applications**	**Challenges**
1	2018	Decentralized	Blockchain, Smart Contracts	Medical Records Sharing, Patient Consent	Scalability, Interoperability, Privacy Risks
2	2017	Centralized	Homomorphic Encryption	Health Information Exchange	Computational Overhead, Limited Applicability
3	2017	Centralized	Attribute-Based Encryption	Electronic Health Records	Complexity, Scalability, Interoperability
4	2017	Centralized	Homomorphic Encryption	Electronic Health Records	Performance, Scalability, Limited Applicability
5	2016	Centralized	Homomorphic Encryption	Electronic Health Records	Complexity, Scalability, Security Risks
6	2016	Decentralized	Blockchain, Smart Contracts	Health Information Exchange	Scalability, Privacy Risks, Interoperability
7	2016	Decentralized	Blockchain, Smart Contracts	Health Information Exchange	Scalability, Interoperability, Privacy Risks
8	2015	Centralized	Homomorphic Encryption	Electronic Health Records	Security Risks, Computational Overhead
9	2014	Decentralized	Cryptographic Protocols	Medical Data Sharing	Scalability, Privacy Risks, Interoperability
10	2014	Centralized	Attribute-Based Encryption	Electronic Health Records	Complexity, Scalability, Security Risks
11	2013	Decentralized	Cryptographic Protocols	Medical Data Sharing	Scalability, Privacy Risks, Interoperability
12	2013	Centralized	Homomorphic Encryption	Medical Data Sharing	Security Risks, Computational Overhead
13	2013	Decentralized	Cryptographic Protocols	Medical Data Sharing	Scalability, Privacy Risks, Interoperability
14	2013	Centralized	Attribute-Based Encryption	Bio-Bank Data Sharing	Complexity, Scalability, Privacy Risks
15	2011	Decentralized	Cryptographic Protocols	Mobile Social Network Data Sharing	Scalability, Privacy Risks, Limited Applicability
16	2017	Centralized	Cryptographic Protocols	Hybrid Cloud-Based EHR Systems	Complexity, Scalability, Privacy Risks
17	2018	Decentralized	Cryptographic Protocols	Mobile Crowd Sensing	Privacy Risks, Limited Applicability

18	2017	Centralized	Cryptographic Protocols	Wireless Body Area Networks	Scalability, Privacy Risks, Limited Applicability
19	2010	Centralized	Cryptographic Protocols	Data Mining	Privacy Risks, Limited Applicability
20	2018	Centralized	Attribute-Based Encryption	Cloud-Based Healthcare Systems	Complexity, Scalability, Security Risks

Table 1. Comparative review of various techniques used Medical data sharing framework that protects patients' privacy

III. **Techniques Used in Medical data sharing framework that protects patients' privacy**

A framework for sharing medical information that protects patients' privacy can be implemented using a variety of different methods. The following are some of the most often employed methods:

A. Encryption: Encryption is one of the strategies that is utilized the most frequently in order to protect the confidentiality of patient information. Using encryption algorithms such as AES, RSA, and Elliptic Curve Cryptography, it entails transforming plaintext data into ciphertext (ECC). With this method, you can rest assured that the data will be accessible to no one but those who are legitimately authorized to view it.

B. Secure Multi-Party Computation (SMPC) : It is a cryptographic technique that allows multiple parties to jointly compute a function over their private inputs without revealing any information about their inputs to other parties. SMPC is an abbreviation for Secure Multi-Party Computation. SMPC is an acronym for Secure Multi-Party Computation. In healthcare applications, where there is a requirement for numerous parties to communicate while maintaining the privacy of their respective data, SMPC can be utilized for data sharing and analysis.

C. Homomorphic Encryption Homomorphic encryption is a form of encryption that enables computation to be performed on ciphertext without the need to decrypt the ciphertext. It makes it possible to do computations on encrypted data without revealing the contents of the data itself. It is possible to employ homomorphic encryption to perform secure computations on sensitive medical data while maintaining patients' right to privacy.

D. Differential Privacy: Differential privacy is a technique that introduces random noise to a dataset to protect the privacy of individuals while still allowing important information to be recovered. This is accomplished using a technique known as differential privacy. Differential privacy is a method that can be utilized to secure the privacy of medical data by making it more challenging for potential intruders to single out particular persons within a dataset.

E. Blockchain is an acronym that stands for "blockchain technology," which refers to a decentralized and distributed ledger that allows for the safe and open exchange of data. It is possible to use it to build a record of medical data exchanges that is both tamper-proof and private at the same time.

F. Access Control: Access control is a strategy that ensures that only authorized parties can access sensitive medical data. This protects the confidentiality of the information. It is possible to utilize it to manage access to medical data while yet maintaining confidentiality.

G. Anonymization: The process of eliminating personally identifying information from medical records in order to safeguard the privacy of persons is known as anonymization. It is possible to utilize it to ensure that private medical data cannot be linked to particular people in order to protect their privacy.

Technique	**Advantages**	**Disadvantages**
Encryption	- Strong security	- High computational overhead
Secure Multi-Party	- Allows multiple parties to collaborate	- Complex to implement

	while	
Computation (SMPC)	-preserving privacy	
Homomorphic Encryption	- Enables computation on encrypted data	- Limited applicability to certain types of computations
	- Preserves data privacy	- High computational overhead
Differential Privacy	- Preserves data privacy	- Reduced accuracy in the results
	- Provides provable privacy guarantees	
Blockchain	- Provides transparency and accountability - Resilient against tampering and attacks	- Scalability issues for large datasets
Access Control	- Allows for granular control over data access	- May not provide sufficient privacy protection in all cases
Anonymization	- Protects individual privacy	- May result in loss of data utility and accuracy

Table 2. Various Techniques used in Implementing Medical data sharing framework that protects patients' privacy

IV. Proposed Block Diagram for MDSFPP (Medical data sharing framework that protects patients' privacy)

The healthcare data providers contribute medical data to the platform for sharing confidential medical information, which in turn protects users' privacy and maintains the integrity of the information. While maintaining patient confidentiality, the platform provides data consumers in the healthcare industry with the ability to access the data according to the level of authorization they have been granted. Protecting the privacy of patients while yet allowing for efficient data sharing is a top priority for the platform, which is why it supports a number of different privacy-preserving approaches, such as encryption, differential privacy, and secure multi-party computation.

The proposed is a broad representation that can be altered based on the particular use case and the strategy that is provided for applying the framework for the privacy-preserving sharing of medical dataThe following elements make up the different parts of the proposed architecture:

i. Data Relating to Healthcare: This component is responsible for representing sensitive data pertaining to healthcare that must be distributed to a variety of parties.
ii. Anonymization and De-Identification of Data: This aspect of the system is in charge of protecting the privacy of patients by anonymizing and de-identifying any healthcare data that is collected.
iii. Data Holders: This component indicates the entities that are in possession of the decryption keys and the encrypted patient records for the healthcare system.
iv. Data Sharing with Controlled Access: This component is in charge of controlling access to the shared encrypted healthcare data depending on the various authorization levels.
v. Consumers of the Data: This component represents the entities that have access to the encrypted healthcare data and are able to decrypt it by utilizing the encryption keys.

The suggested architecture has as its dual objectives the protection of patient privacy and the facilitation of efficient data interchange among various healthcare entities. The precise implementation and components may be different depending on the particular use case and the method that is proposed for putting in place the framework for protecting patients' privacy while sharing medical data.

A. Processing Steps:

The precise method and strategy that is being applied can cause the processing steps that are required to establish a framework for the sharing of medical data while still protecting patients' privacy. Nonetheless, the following is a summary in broad strokes of the several processing processes that are involved:

i. Preparation of the Data :Collecting and organizing the necessary healthcare data for distribution is the initial step in this process. In order to preserve the privacy of the patients, this may require anonymizing and de-identifying the data.
ii. Encryption of Data: In order to prevent unwanted access to the healthcare data, it has been encrypted through the use of a reliable encryption method.
iii. Maintenance of Keys: Encryption keys are generated and safely handled in order to guarantee that only authorised parties can access the material that has been encrypted.
iv. Data Sharing: The encrypted medical records are distributed to the appropriate parties in accordance with predetermined access restrictions and permission degrees.
v. Data Decryption: In order to access and analyse the data that has been provided, the authorised parties are able to decrypt the data by utilising the encryption keys.
vi. Auditing and Monitoring: The process of sharing patient data is audited and monitored to verify that it complies with all applicable data protection requirements and that the confidentiality of patient information is protected at all times.
vii. Updating and Maintenance: The framework for the sharing of medical data that protects patients' privacy needs to be continually updated and maintained in order to address emerging threats to patients' privacy and security.

The procedures involved in this processing are not always organized in a linear fashion and may include iterative loops, feedback mechanisms, and periodic evaluations to maintain the efficiency and safety of the framework for sharing medical data that protects patients' privacy. In addition, some processing methods may place a greater emphasis on particular processing steps in comparison to others, depending on the particular specifications and priorities of the healthcare use case.

V. Challenges:

While a framework for sharing medical data while protecting privacy has many potential advantages for the healthcare industry, there are also a number of difficulties in putting it into practice. These are a few of the principal difficulties:

A. Standardization of Data: Because healthcare data is frequently housed in a variety of formats and silos, it can be difficult to standardize and integrate this information so that it can be shared. It is essential for data to be standardized across all of the different healthcare institutions in order to enable successful data sharing.
B. Security: Data pertaining to healthcare is particularly sensitive, which makes it an attractive target for online assaults. A framework for the sharing of data that protects users' privacy must guarantee the data's safety both while it is being stored and while it is being transmitted.
C. Compliance with Legal and Regulatory Requirements: Compliance with several legal and regulatory standards, such as HIPAA, GDPR, and the Common Rule, is necessary for the exchange of healthcare data. A framework for the exchange of data that protects users' privacy must be compliant with these standards in order to avoid potential legal and ethical complications.
D. Trust and Governance: In the healthcare industry, organization’s are required to set up trust and governance processes in order to guarantee that patient information is appropriately shared and that the confidentiality of patients' personal information is maintained.

E. Absence of Incentives: The absence of appropriate incentives may cause healthcare institutions to be reticent about sharing data. It's possible that the potential benefits of creating a data sharing framework that protects privacy won't be worth the cost of doing so, particularly for less substantial healthcare institutions.
F. Quality of Data: The quality of the data is an issue in the healthcare industry, as it is frequently erroneous or incomplete. This can reduce the value of shared data for purposes of analysis and study.
G. Participation of Patients: In order to have an effective framework for exchanging data while protecting patients' privacy, patients' engagement is essential. Patients have to be willing to give their data and must be informed about how that data will be used and safeguarded before they may share their data.

To ensure the successful adoption of a framework for sharing medical data while protecting privacy, these issues must be resolved. The creation of efficient governance systems, the creation of safe and standardized data exchange protocols, and the creation of incentives for healthcare institutions to participate call for cooperation between healthcare organizations, legislators, and technology developers.

VI. Application

A framework for the sharing of medical data that protects patients' privacy could have multiple uses in the healthcare industry.

A. Clinical Trials: The collection and evaluation of data for clinical trials requires the participation of a number of different healthcare organizations working together. A framework for data sharing that protects patient privacy can make it easier for various organizations to exchange patient information while still maintaining patient confidentiality.
B. Disease Surveillance: Disease surveillance includes both the tracking of infectious diseases and the monitoring of disease outbreaks. The ability for healthcare organizations to communicate data about disease outbreaks without compromising patient privacy can be enabled via a data sharing framework that protects patient confidentiality.
C. Personalized Medicine: Personalized medicine is a branch of medicine that makes use of patient data in order to individualize medical treatment for patients. It is possible for healthcare organizations to share patient data in order to generate individualized treatment plans while still protecting patient privacy with the use of a data sharing framework that protects patient privacy.
D. Management of a Population's Health Management of a Population's Health entails taking responsibility for the overall health of a given population. A data sharing framework that protects individuals' privacy might make it possible for healthcare organizations to collaborate and share information regarding the health of a particular population in order to devise more efficient strategies for population health management.
E. Analysis of huge datasets is a vital part of medical research, which aims to uncover novel therapeutic approaches and unanticipated medical breakthroughs. The ability for healthcare organization’s to share data for the purpose of medical research while yet maintaining patient confidentiality requires a data sharing framework that protects privacy.

A framework for the sharing of medical information that protects patient privacy can make it possible for healthcare organizations to work together and exchange data in order to enhance patient care and advance medical research while maintaining patients' right to confidentiality.

VII. Conclusion

In conclusion, the development of a medical data sharing framework that protects patient privacy is essential if one want to facilitate the safe and efficient sharing of healthcare data while also safeguarding patient confidentiality. For the purpose of putting such a structure into practice, a number of different methods, including homomorphic

encryption, secure multi-party computation, and differential privacy, have been suggested. The numerous advantages offered by a framework that allows for the secure sharing of medical information, there are a number of obstacles that must be overcome. Concerns pertaining to law and ethics, interoperability and standards, and technological concerns such as scalability and performance are all part of these challenges.Combining homomorphic encryption with blockchain technology is one method that has been suggested for the implementation of a privacy-preserving medical data sharing framework. This method is recommended as a means of overcoming the issues described above. This method ensures the confidentiality of the data as well as its integrity, and it offers a safe and effective means of sharing and storing encrypted healthcare information.In conclusion, the creation and implementation of a framework for exchanging medical data that protects patients' privacy require a multi-disciplinary approach. This strategy requires the involvement of healthcare professionals, data scientists, privacy experts, and regulatory agencies. A framework that allows for the efficient and secure sharing of medical data while protecting patients' privacy can be developed by addressing the issues that arise and making use of the various solutions that are now available. This can lead to improved healthcare outcomes.

References

[1] A. El Emam, E. Jonker, and F. Arbuckle, "A systematic review of re-identification attacks on health data," PLoS One, vol. 6, no. 12, p. e28071, 2011.
[2] P. Samarati, "Protecting respondents' identities in microdata release," IEEE Transactions on Knowledge and Data Engineering, vol. 13, no. 6, pp. 1010-1027, 2001.
[3] C. Dwork, "Differential privacy: a survey of results," in International Conference on Theory and Applications of Models of Computation, Springer, Berlin, Heidelberg, 2008, pp. 1-19.
[4] M. Li, S. Yu, N. Cao, and W. Lou, "Secured data sharing with fine-grained and scalable access control in cloud-based healthcare systems," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, 2013.
[5] Y. Chen, X. Lu, and R. N. Wright, "Towards privacy-preserving data publishing for cluster analysis," in Proceedings of the 2005 ACM SIGMOD international conference on Management of data, ACM, New York, NY, USA, 2005, pp. 153-164.
[6] J. Li, J. Li, L. Tian, and Y. Han, "Privacy-preserving e-healthcare systems using ciphertext-policy attribute-based encryption," IEEE Journal of Biomedical and Health Informatics, vol. 20, no. 3, pp. 707-717, 2016.
[7] S. Sankararaman, S. S. O'Brien, A. Devarakonda, J. R. Lo, and M. K. Teng, "Privacy-preserving methods for sharing genomic data: a comparison of approaches," Pacific Symposium on Biocomputing, vol. 22, pp. 309-320, 2017.
[8] M. Dehaghani, A. M. Rahmani, and P. Liljeberg, "A survey on data security in healthcare information systems," Journal of medical systems, vol. 42, no. 6, p. 103, 2018.
[9] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583-592, 2012.
[10] M. R. Mohassel and Y. Zhang, "Secureml: A system for scalable privacy-preserving machine learning," in 2017 IEEE Symposium on Security and Privacy (SP), IEEE, 2017, pp. 19-38.
[11] A. C. A. Nascimento, J. C. Wainer, and M. M. F. França, "Privacy-preserving record linkage using Bloom filters," Journal of Biomedical Informatics, vol. 43, no. 5, pp. 756-763, 2010.
[12] M. T. Goodrich and R. Tamassia, "Privacy-preserving wavelet-based signal processing," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, 2003, pp. 316-331.
[13] K. Lee and K. Lee, "Privacy-preserving healthcare data sharing system for bio-bank," Journal of Medical Systems, vol. 37, no. 5, p. 9995, 2013.

[14] A. R. Beresford, A. Rice, and N. Skevington, "Putting the user in control: a privacy-preserving data usage framework for mobile social networks," in Proceedings of the 12th Workshop on Mobile Computing Systems and Applications, ACM, New York, NY, USA, 2011, pp. 1-6.
[15] J. Li, W. Li, J. Li, J. Li, and J. Chen, "Privacy-preserving data sharing for hybrid cloud-based electronic health record systems," Journal of medical systems, vol. 41, no. 4, p. 63, 2017.
[16] X. Li, X. Sun, W. Lou, and Y. T. Hou, "Privacy-preserving mobile crowd sensing: Current state and future directions," IEEE Communications Magazine, vol. 56, no. 10, pp. 94-100, 2018.
[17] X. Zhang, C. Zhang, J. Huang, X. Liu, and J. Zhang, "Privacy-preserving data aggregation in cloud-assisted wireless body area networks for medical applications," Journal of Medical Systems, vol. 41, no. 12, p. 195, 2017.
[18] R. W. M. Kwok, E. M. C. Tong, and T. Y. Wong, "Privacy-preserving techniques in data mining: A survey," IEEE Transactions on Knowledge and Data Engineering, vol. 22, no. 7, pp. 1019-1033, 2010.
[19] Y. Zhang, X. Liu, X. Zhou, and W. Lou, "Efficient privacy-preserving fine-grained access control in cloud-based healthcare systems," in IEEE INFOCOM 2018-IEEE Conference on Computer Communications, IEEE, 2018, pp. 1484-1492.
[20] Shu J, Jia X, Yang K, Wang H. Privacy-preserving task recommendation services for crowdsourcing. IEEE Transactions on Services Computing. 2018.
[21] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD). IEEE; 2016. p. 25–30.
[22] Ivan D. Moving toward a blockchain-based method for the secure storage of patient records. In: ONC/ NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
[23]. Zhang E, Liu FH, Lai Q, Jin G, Li Y. Efficient Multi-Party Private Set Intersection Against Malicious Adversaries. In: Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop; 2019. p. 93–104.
[24] Zyskind G, Nathan O, et al. Decentralizing privacy: Using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops. IEEE; 2015. p. 180–184.
[25] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access conntrol and interoperability of electronic health records using blockchain technology. Sustainable cities and society. 2018; 39:283–297.