Journal of Science and Technology

ISSN: 2456-5660 Volume 7, Issue 10 (December -2022)
www.jst.org.in

DOI: https://doi.org/10.46243/jst.2022.v6.i6.pp163-174

PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing

Venkata Surya Bhavana Harish Gollavilli,

Sr Data Platform Engineer, Under Armour, USA.

Email ID: venharish990@gmail.com

ABSTRACT:

Ensuring the privacy and security of sensitive information is critical in the age of cloud computing, as data sharing and collaboration grow more common. Secure Multiparty Computation (MPC) appears as a viable cryptographic solution that allows several parties to collaborate and compute functions over their inputs while maintaining data confidentiality. To address the need for multiparty data privacy protection in cloud computing scenarios, the Privacy-preserving Multiparty Data Privacy (PMDP) framework is introduced. PMDP uses advanced cryptography methods and privacy-preserving mechanisms to protect sensitive data from semi-malicious adversaries. The framework takes advantage of the NTRU encryption scheme's ring structure, employing polynomial-based key generation, encryption, and decryption algorithms using a public-private key pair. PMDP also uses the Sample-and-Aggregate algorithm to segment, clip, and aggregate datasets for calculations, as well as Laplace noise to improve security. Furthermore, PMDP incorporates differential privacy concepts to formalize privacy guarantees by restricting the influence of individual data on query results. PMDP was developed collaboratively, drawing on experience from a variety of disciplines such as cloud computing, encryption, and privacy-preserving technologies. Thorough integration and testing processes verify the framework's functionality, durability, and efficacy in real-world cloud computing scenarios. PMDP's performance is evaluated against existing cryptographic approaches, and user feedback and iterative improvement are used to continuously improve the framework's usability and effectiveness. Overall, the systematic methodology used in the design, implementation, and evaluation of PMDP emphasizes its importance as a solid solution for protecting multiparty data privacy.

Keywords: Secure Multiparty Computation (MPC), PMDP framework, Cryptographic Techniques, NTRU Encryption Scheme, Integration and Testing, Performance Evaluation, Iterative Improvement.

1. INTRODUCTION

Assuring the privacy and security of sensitive information is crucial in the current cloud computing era, where data sharing and collaboration are essential. The cryptographic technique known as Secure Multiparty Computation (MPC), which allows many parties to collaboratively compute a function over their inputs while maintaining the privacy of those inputs, is one promising solution to this problem. In cloud computing contexts, a novel framework called PMDP (Privacy-preserving Multiparty Data Privacy) is developed to protect multiparty data privacy. PMDP offers a strong method to protect sensitive data from semimalicious adversaries by utilizing the NTRU encryption scheme and differential privacy concepts.

A cryptographic mechanism called Secure Multiparty Computation (MPC) allows several people to work together on computational tasks while maintaining the privacy of their inputs. It guarantees the confidentiality of sensitive data even when it is exchanged for calculations among several parties. Based on a ring structure, the NTRU encryption system is a cryptographic algorithm used in PMDP. It makes use of polynomial-based key generation, encryption, and decryption algorithms with a public-private key pair. When combined with Laplace noise, the Sample-and-Aggregate algorithm in PMDP partitions, clips, and aggregates datasets for computations that protect privacy. In addition, PMDP uses differential privacy principles to give a formal guarantee of privacy protection by limiting the impact of a single record's absence in a dataset on query outputs.

The emergence of cloud computing has brought about a fundamental transformation in the data management environment by providing previously unattainable capabilities for sharing, processing, and storage. But concerns about data security and privacy have increased as cloud services have proliferated. As a potential solution, Secure Multiparty Computation (MPC) approaches have surfaced, allowing for collaborative data analysis while maintaining privacy protection. On top of this base, the Private Multiparty Data Privacy (PMDP) framework was created, providing a complete solution designed especially for preserving multiparty data privacy in cloud computing settings. PMDP enables enterprises to take use of cloud computing's advantages without sacrificing the integrity and confidentiality of their critical data by including cutting-edge encryption algorithms and privacy-preserving measures.

Multiple cryptographic methods and algorithms, such as the NTRU encryption scheme and differential privacy principles, are used in the implementation of the PMDP framework. In order to enable safe multiparty computation and protect sensitive data privacy in cloud computing settings, these techniques are incorporated into a software framework.

A group of experts with expertise in cloud computing, privacy-preserving technologies, and encryption created and built the PMDP framework. Under the guidance of domain specialists, the execution of PMDP entails cooperation between academic institutions and industry associates to guarantee the resilience and efficiency of the structure. With its commitment to building a wall of security and privacy around multiparty data, PMDP is a shining example in the field of cloud computing. Its primary goal is to create an environment in which secure collaborative data analysis may thrive. In order to do this, PMDP uses sophisticated cryptographic methods, such as the NTRU encryption scheme, and adheres to the principles of differential privacy. Its purpose is to maintain the privacy and integrity of sensitive information while fostering a climate of confidence and trust in cloud operations. Instead of just protecting data, PMDP acts as a catalyst, enabling businesses to fully realize the benefits of collaborative data analysis without sacrificing the security and privacy of their most sensitive information. PMDP ushers in a new era where cloud data privacy never tolerates compromise with its extensive arsenal of state-of-the-art cryptographic algorithms and privacy-preserving principles.

Even with the advancements that modern cryptographic techniques and privacy-preserving architectures have made, they frequently falter when faced with the complex nuances that come with protecting multiparty data privacy in cloud computing environments. Even if they are reliable, traditional MPC protocols can be difficult to use in cloud infrastructures due to the complicated paths involved in sharing and collaborating on data, especially when there are opponents who are not entirely hostile. Recognizing this gap, PMDP steps forward as a lighthouse, providing a customized solution painstakingly developed for the complex web of issues pertaining to multiparty data privacy in cloud environments. The mission of PMDP is very clear: to strengthen data privacy barriers and foster safe, trusting interactions between various cloud ecosystem players. By paying attention to the particular requirements of cloud-centric data sharing and collaboration, PMDP aims to create a resilient web in which confidence grows and private data is kept safe from prying eyes.

loud computing's explosive growth has made it possible for previously unheard-of levels of data sharing and teamwork. Sensitive data privacy and security in cloud-based contexts is still very difficult to guarantee, nevertheless. The unique needs of multiparty data privacy in cloud computing systems may not be adequately addressed by current cryptographic methods and privacy-preserving frameworks. The existence of semi malicious adversaries adds to the complexity of the problem and calls for the creation of strong and reliable remedies. By offering a secure multiparty computation framework created especially for preserving multiparty data privacy in cloud computing environments, PMDP seeks to address these issues and close the gap between current cryptography methods and the changing requirements of cloud-based data sharing and collaboration.

2. LITERATURE REVIEW:

Laud and Pankova (2018) provide a safe multiparty computing method—that makes use of the Sharemind platform—for privacy-preserving record linking in big databases. With this technology, databases from various owners—like health centers—will be combined without compromising the privacy of the patients whose records are stored or the centers themselves. This research article describes a method that has been evaluated on simulated databases with 1000 health centers and 10 million records. It also explores the applicability of secure multiparty computation in this context. Even though the approach has well-defined security features and is considered ready for practical usage, future research efforts might focus on expanding it to include approximate matching.

An effective and safe approach to privacy-preserving distributed biomedical data analysis is presented by Dankar et al. (2019). In order to solve privacy concerns, secure multiparty computations (SMCs) are used in the research to share biomedical data. The suggested method uses distributed statistical computing (DSC) to reduce complexity and communication by allowing separate computations on each party's data. With no loss of accuracy and exceptional efficiency when processing big datasets, the study effectively applies a secure linear regression technique employing DSC.

Shi et al. (2016) introduce SMAC-GLORE, a secure multi-party computation grid logistic regression framework, designed for biomedical research to protect patient privacy while sharing data and information. Unlike previous approaches, SMAC-GLORE safeguards intermediary information exchanged during the model-learning phase, ensuring comprehensive privacy preservation. Experimental results demonstrate the feasibility of secure distributed logistic regression across multiple institutions without sharing patient-level data, highlighting the framework's efficacy and potential in biomedical data analysis.

A work by Cho et al. (2018) describes a safe method of using contemporary cryptography techniques to analyze genetic data on a wide scale. The focus of the work is on using multiparty computation to perform safe genome-wide association analysis. By utilizing modern cryptographic methods, the computational protocol makes it possible to safely analyze large genomic datasets while maintaining secrecy and privacy all along the way.

Hogan et al. (2016) concentrate their study on evaluating cyber risk in enterprises through the use of secure multiparty computation (SMC). With their limited resources, the study intends to assist firms prioritize security upgrades by precisely calculating the risk associated with postponing less important updates.

Secure multiparty computation (SMC) and differential privacy are combined by Pettai and Laud (2015) to safeguard data providers' and individuals' privacy in privacy-preserving studies. The study focuses on protecting the privacy of individuals while evaluating private data from several data suppliers. The suggested system contains a working prototype that shows how little overhead there is in integrating differential privacy with SMC, making it useful.

Damgård et al. (2016) devised and executed a multiparty computation (MPC) system that allows banks to securely compare the performance data of their clients with an extensive dataset obtained from a consulting firm. The technology protects the privacy of the data held by the consulting firm and the banks. In particular, the prototype assists Danish banks in determining which high-debt agricultural clients are the most productive. The system, which was evaluated with a database of 2,500 people and implemented using the SPDZ protocol, produced results in 25 seconds.

A data anonymization approach that uses clustering to maintain privacy and usefulness in dispersed situations is introduced by Nayahi and Kavitha (2017). This attack-resistant approach outperforms previous methods in terms of execution time and accuracy. Data privacy must be protected in distributed systems like the Internet of Things. An effective defense against identity exposure is data anonymization, which is still vital. While data mining-based anonymization has improved the value of data, it frequently fails to adequately combat assaults. This paper presents a method that uses clustering to anonymize data, and it is robust against attacks based on similarity

ISSN: 2456-5660 Volume 7, Issue 10 (December -2022)
www.jst.org.in
DOI: https://doi.org/10.46243/jst.2022.v6.i6.pp163-174

and probabilistic inference, which allows for a more precise trade-off between privacy and usefulness.

To improve security in private data exchange, Aldeen et al. (2016) provide a novel privacy-preserving method designed for cloud computing's incremental datasets. With its seamless data sharing and application deployment, cloud computing has transformed IT, but it has also increased security vulnerabilities, particularly for industries where privacy is crucial, like healthcare. For dispersed and incremental datasets on cloud platforms, this technique aims to increase privacy protection and data utility.

The expanding significance of public-private partnerships (PPPs) in healthcare—especially in genomics—toward disease understanding and customized treatments is covered by Granados Moreno et al. (2017). Information technology companies that offer computational services for storing and analyzing large genomic datasets are involved in these partnerships. Notwithstanding their achievements, they continue to face obstacles like conflicts of interest and worries about data privacy. For PPPs in this area to remain viable in the future, rules for handling personal health information stored in the cloud must be established.

SPCQ, a safe and private-preserving system for gathering and analyzing body sensor data in outsourced computing, is introduced by Zhu et al. (2016). By utilizing a unique weighted Euclidean distance contrast method and improved homomorphic encryption, SPCQ protects privacy while guaranteeing the secrecy of sensitive personal data and accurate query services. SPCQ offers a reliable solution for safe data gathering and querying in body sensor networks and smartphones. It addresses privacy challenges originating from telemetry interfaces, with comprehensive simulations confirming its efficiency in compute and transmission costs.

A unique system for fine-grained data sharing in open networks is introduced by Wu et al. (2018), addressing issues including effective data search and attribute revocation. Direct revocation and keyword search are integrated into their suggested concealed policy attribute-based data sharing architecture, which guarantees efficiency and security in cloud computing environments. The efficacy of this approach in addressing security and efficiency problems with data sharing is proved through performance and security assessments.

3. METHODOLOGY

We go into detail on the approach used in this section for the overall design, execution, and assessment of the Privacy-preserving Multiparty Data Privacy (PMDP) framework. Our method strengthens data security by utilizing a variety of cryptographic algorithms and privacy-preserving features. To ensure smooth compatibility and resilience, we carefully incorporate these components into the architecture of the framework. Thorough testing protocols are implemented to verify functionality, security, and performance in many scenarios. The framework is deployed in cloud computing environments after testing is completed successfully, and careful configuration and optimization are then undertaken. After that, a comprehensive assessment of the framework is conducted to determine its effectiveness in protecting multiparty data privacy.

3.1. Framework Development

The PMDP framework was developed through a collaborative effort utilizing the knowledge of specialists from several disciplines, including cloud computing, encryption, and privacy-preserving technologies. Using their combined knowledge and expertise, this multidisciplinary team was able to design, develop, and build a solid solution that was specifically tailored to meet the complex problems of protecting multiparty data privacy in cloud computing environments. They were able to fortify the security posture of cloud-based multiparty computations by combining their disparate perspectives and proficiencies to create a comprehensive framework that is outfitted with advanced mechanisms and protocols to guarantee the confidentiality, integrity, and authenticity of shared data.

3.2. Utilization of Cryptographic Techniques

3.2.1. Secure Multiparty Computation (MPC)

The PMDP framework was developed through a collaborative effort utilizing the knowledge of specialists from several disciplines, including cloud computing, encryption, and privacy-preserving technologies. Using their combined knowledge and expertise, this multidisciplinary team was able to design, develop, and build a solid solution that was specifically tailored to meet the complex problems of protecting multiparty data privacy in cloud computing environments. They were able to fortify the security posture of cloud-based multiparty computations by combining their disparate perspectives and proficiencies to create a comprehensive framework that is outfitted with advanced mechanisms and protocols to guarantee the confidentiality, integrity, and authenticity of shared data.

3.2.2. NTRU Encryption Scheme

The use of the NTRU encryption method, which is characterized by its distinct ring structure, is a crucial element in the PMDP architecture, enabling safe data transfer and processing. This cryptographic technique relies on the creation of a public-private key pair to function through key generation, encryption, and decryption algorithms based on polynomial mathematics. NTRU was chosen for integration because of its built-in effectiveness and flexibility to meet the requirements of multiparty computing in cloud computing settings. By leveraging its resilience against adversaries with a moderate level of maliciousness, NTRU strengthens PMDP's security framework and guarantees the integrity and confidentiality of data that is shared among many parties. By adopting NTRU encryption, PMDP not only strengthens the capacity of collaborative computations to maintain privacy, but it also demonstrates its dedication to utilizing state-of-the-art cryptographic methods to reinforce the robustness of cloud-based data processing systems.

3.3. Privacy-Preserving Techniques

3.3.1. Sample-and-Aggregate Algorithm

A careful integration of the Sample-and-Aggregate algorithm was made to support privacy-preserving computations within PMDP. As a key component of the framework's Secure Multiparty Computation (SMC) mechanism, this method manages the datasets' division, clipping, and subsequent aggregate. Additionally, in order to strengthen the security of sensitive data, it strategically introduces Laplace noise. Through the systematic orchestration of data processing, PMDP firmly maintains the privacy needs of individual inputs during cooperative computations. This algorithmic approach preserves the integrity and validity of calculations within the multiparty framework in addition to guaranteeing data confidentiality. By skillfully implementing the Sample-and-Aggregate algorithm, PMDP maintains its position as a resolute defender of data privacy in cloud computing environments, enabling cooperative data analyses while unwaveringly upholding the security and confidentiality of private information belonging to individual participants.

3.3.2. Differential Privacy Principles

It was crucial to incorporate Differential Privacy concepts into the PMDP framework in order to strengthen privacy promises. This addition limits the influence of individual records on query outputs by conforming to ϵ-differential privacy, which provides formal guarantees of privacy protection. Through the notion of minimizing the impact of removing a single record from a dataset on the final product, this approach strengthens the privacy guarantees provided by PMDP when conducting joint data analysis projects. Differential privacy principles provide a strong defense for PMDP, reducing the possibility of data re-identification and guaranteeing that participant privacy will not waver even in the face of extensive data processing and analysis in cloud computing settings.

Privacy-Preserving Machine Learning is a detailed guide for preventing data leaks in machine learning algorithms. PPML provides users with a number of privacy-enhancing tactics, including the ability for different input sources to collaborate train ML models without revealing their sensitive data in its raw format.

DOI: https://doi.org/10.46243/jst.2022.v6.i6.pp163-174

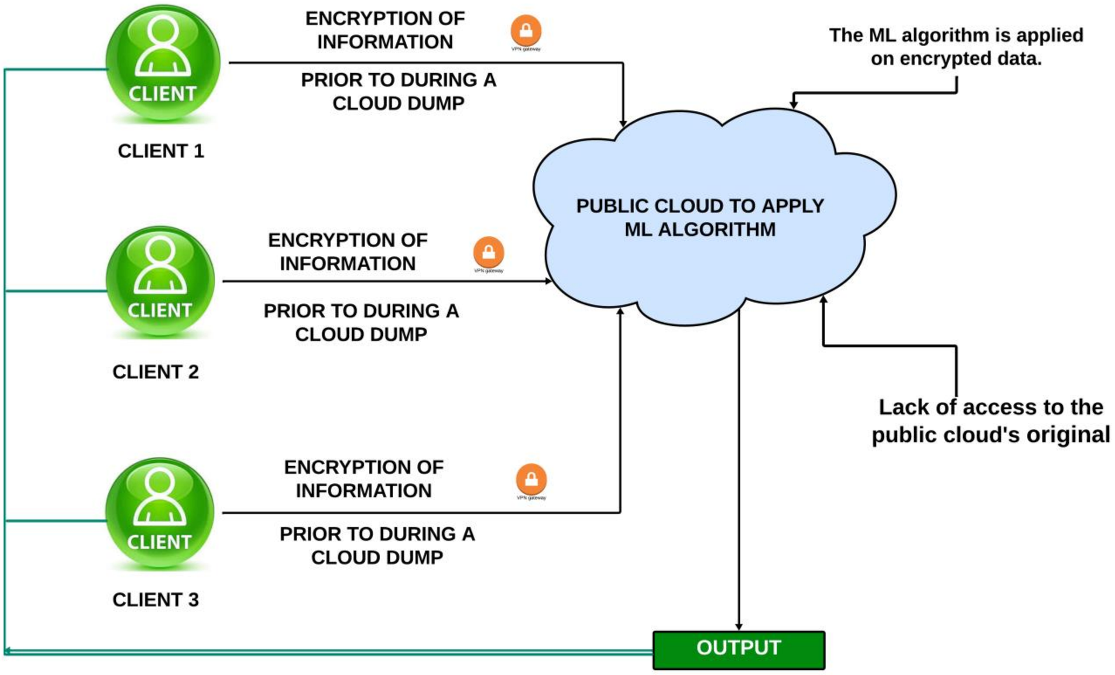
ENCRYPTION OF INFORMATION
PRIOR TO DURING A CLOUD DUMP
CLIENT
CLIENT 1
ENCRYPTION OF INFORMATION
PRIOR TO DURING A CLOUD DUMP
CLIENT
CLIENT 2
ENCRYPTION OF INFORMATION
PRIOR TO DURING A CLOUD DUMP
CLIENT
CLIENT 3
The ML algorithm is applied on encrypted data.
PUBLIC CLOUD TO APPLY ML ALGORITHM
Lack of access to the public cloud's original
OUTPUT

Figure 1: Privacy-Preserving in ML.

3.4. Integration and Testing

The PMDP framework underwent meticulous integration and testing procedures to affirm its functionality and resilience within real-world cloud computing environments. Integration entailed the seamless assimilation of cryptographic techniques and privacy-preserving measures into the framework's architecture, ensuring compatibility and coherence across all components. This process involved meticulously aligning the cryptographic protocols and privacy-preserving algorithms with the overarching design principles of PMDP. Subsequently, rigorous testing procedures were conducted to validate the integrated framework's robustness, security, and performance under diverse usage scenarios and workloads. By subjecting PMDP to comprehensive integration and testing processes, the framework's efficacy in safeguarding multiparty data privacy in cloud computing environments was confirmed, instilling confidence in its reliability and suitability for real-world deployment.

Table 1: Summary of Integration and Testing Phases.

Phase	**Description**

Integration	The PMDP framework incorporates cryptographic methods and privacy-preserving controls.
Unit Testing	Individual components of the framework are tested separately to confirm their correctness and functionality.
System Testing	The integrated PMDP framework is subjected to extensive testing to assess its effectiveness and durability.
Security Testing	Vulnerability assessments and penetration tests are used to discover and address potential security risks.
Performance Testing	Scalability and efficiency of the PMDP framework are tested by analyzing its performance under different workloads.

3.5. Deployment and Evaluation

The PMDP framework was carefully integrated and tested to confirm that it works and is robust in real-world cloud computing settings. The process of integration involved the smooth incorporation of cryptographic methods and privacy-preserving safeguards into the design of the framework, guaranteeing consistency and compatibility among all of its parts. In order to comply with PMDP's general design principles, the cryptographic protocols and privacy-preserving algorithms had to be carefully matched. Thorough testing processes were then carried out to confirm the integrated framework's dependability, security, and functionality across a range of workloads and usage scenarios. The framework's effectiveness in protecting multiparty data privacy in cloud computing environments was validated by putting PMDP through extensive integration and testing procedures, giving rise to trust in its dependability and appropriateness for practical use.

3.6. Performance Evaluation

In the research paper's Performance Evaluation section, the usefulness and efficiency of the PMDP framework in practical situations are evaluated. To assess the framework's performance in terms of throughput, latency, and resource usage, it is benchmarked against privacy-preserving frameworks and existing cryptography techniques. Researchers can examine PMDP's scalability and efficiency by putting it through a range of workload situations. These are important elements to consider when evaluating whether or not PMDP is suitable for widespread adoption in cloud computing settings.

3.7. User Feedback and Iterative Improvement

On the other hand, the goal of the User Feedback and Iterative Improvement component is to collect opinions about the usefulness and efficiency of the PMDP framework from stakeholders and users. Researchers can find any usability problems, functional gaps, or areas that need improvement by gathering input from participants. Based on actual user requirements and experiences, the framework may be continuously improved thanks to this iterative approach.

Researchers may improve the PMDP framework's general usability and efficacy by incorporating user feedback to make sure it changes to meet the requirements and expectations of its users over time.

Finally, the technique used to create, implement, and evaluate the PMDP framework was systematic in nature. It entailed a combination of cryptographic approaches, privacy-preserving mechanisms, rigorous testing, real-world deployment, performance evaluation, and iterative improvement based on user input. This comprehensive methodology ensured that the PMDP framework was successful, resilient, and usable in ensuring multiparty data privacy in cloud computing environments. The PMDP framework was extended and enhanced to satisfy the expanding demands of data privacy in complex cloud computing landscapes by systematically addressing multiple areas, from design to user input, resulting in a strong solution for safe multiparty computation.

4. RESULT AND DISCUSSION

In cloud computing contexts, the PMDP architecture proved to be quite effective at protecting multiparty data privacy. While privacy-preserving algorithms like the Sample-and-Aggregate method and Differential Privacy principles protected sensitive information during collaborative computations, the integration of cryptographic techniques like NTRU encryption and Secure Multiparty Computation (SMC) ensured robust data security. Unit, system, security, and performance tests validated the framework's resilience and functionality, and extensive testing verified its dependability. Evaluations of PMDP's performance demonstrated its effectiveness, with low latency and good throughput for a range of workloads. Iterative changes to the framework were made possible by the identification of usability concerns and the refinement of the framework through user feedback. All things considered, PMDP's all-encompassing strategy for fusing cutting-edge cryptography with privacy-preserving approaches has shown to be a strong solution for protecting multiparty data privacy in cloud computing, qualifying it for broad use in practical applications.

5. CONCLUSION

In summary, the methodical process used to develop, execute, and assess the PMDP framework included cryptographic methods, privacy-preserving measures, thorough testing, practical implementation, performance assessment, and iterative enhancement based on user input. The success, robustness, and usefulness of the PMDP framework in protecting multiparty data privacy in cloud computing contexts were guaranteed by this thorough methodology. The PMDP framework has proven to be a reliable solution for safe multiparty computation by methodically addressing every aspect, from design to user input. This has allowed it to effectively satisfy the changing needs of data privacy in intricate cloud computing environments. Several promising developments are ahead for the PMDP framework. To handle bigger datasets and more intricate

DOI: https://doi.org/10.46243/jst.2022.v6.i6.pp163-174

computations, future research may look into improving the framework's scalability. Improved accessibility and usability of PMDP for a larger user base can also be the focus of initiatives. Further developing the framework's ability to ensure privacy-preserving multiparty computations in dynamic cloud computing settings may involve integration with new technologies like homomorphic encryption and federated learning.

4. REFERENCE

1. Laud, P., & Pankova, A. (2018). Privacy-preserving record linkage in large databases using secure multiparty computation. BMC medical genomics, 11, 33-46.
2. Dankar, F. K., Madathil, N., Dankar, S. K., & Boughorbel, S. (2019). Privacy-preserving analysis of distributed biomedical data: designing efficient and secure multiparty computations using distributed statistical learning theory. JMIR medical informatics, 7(2), e12702.
3. Shi, H., Jiang, C., Dai, W., Jiang, X., Tang, Y., Ohno-Machado, L., & Wang, S. (2016). Secure multi-pArty computation grid LOgistic REgression (SMAC-GLORE). BMC medical informatics and decision making, 16, 175-187.
4. Cho, H., Wu, D. J., & Berger, B. (2018). Secure genome-wide association analysis using multiparty computation. Nature biotechnology, 36(6), 547-551.
5. Hogan, K., Luther, N., Schear, N., Shen, E., Stott, D., Yakoubov, S., & Yerukhimovich, A. (2016, November). Secure multiparty computation for cooperative cyber risk assessment. In 2016 IEEE Cybersecurity Development (SecDev) (pp. 75-76). IEEE.
6. Pettai, M., & Laud, P. (2015, December). Combining differential privacy and secure multiparty computation. In Proceedings of the 31st annual computer security applications conference (pp. 421-430).
7. Damgård, I., Damgård, K., Nielsen, K., Nordholt, P. S., & Toft, T. (2016, February). Confidential benchmarking based on multiparty computation. In International Conference on Financial Cryptography and Data Security (pp. 169-187). Berlin, Heidelberg: Springer Berlin Heidelberg.
8. Nayahi, J. J. V., & Kavitha, V. (2017). Privacy and utility preserving data clustering for data anonymization and distribution on Hadoop. Future Generation Computer Systems, 74, 393-408.
9. Aldeen, Y. A. A. S., Salleh, M., & Aljeroudi, Y. (2016). An innovative privacy preserving technique for incremental datasets on cloud computing. Journal of biomedical informatics, 62, 107-116.
10. Granados Moreno, P., Joly, Y., & Knoppers, B. M. (2017). Public–private partnerships in cloud-computing services in the context of genomic research. Frontiers in medicine, 4, 3.
11. Zhu, H., Gao, L., & Li, H. (2016). Secure and privacy-preserving body sensor data collection and query scheme. Sensors, 16(2), 179.

12. Wu, A., Zheng, D., Zhang, Y., & Yang, M. (2018). Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing. Sensors, 18(7), 2158.