International Journal of Engineering & Scientific Research

Vol.12 Issue 02, February 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

APPLYING DIFFERENTIAL PRIVACY TECHNIQUES TO PROTECT INDIVIDUAL PRIVACY IN GENOMIC DATA SHARING

Meghasai Bodimani

Abstract- *This study examines the evolving landscape of privacy mechanisms in Genomic data sharing, with a preliminary priority on applying differential privacy techniques. Existing strategies for sharing Genomic data usually need to include more than assuring individuals' privacy, making investigating differential privacy necessary. Genomic data has tremendous prospects for Medical Studies. However, sharing this data while safeguarding individual privacy is a notable challenge. Differential privacy proposes a profitable avenue to offset the imperative of data sharing with the necessity to protect individual privacy in the Genomics domain. Hence, this study aims to evaluate the effectiveness of implementing differential privacy techniques in safeguarding individual privacy when sharing Genomic data.*

Keywords- Differential Privacy, Genomic Data Sharing, Privacy Mechanisms, Data Utility, Privacy Budget

I. INTRODUCTION

The rapid growth of Genomics has revolutionised Medical Studies and personified healthcare, presenting remarkable perspicuity in individuals' genetic makeup. However, sharing Genomic data for analysis purposes produces notable privacy concerns, as these data and information can expose sensitive details about the health and identity of an individual. Safeguarding the privacy of individuals while enabling data sharing is a critical challenge. Therefore, this paper presents the concept of involving differential privacy approaches to manage this challenge. Differential privacy offers a profitable avenue to offset the imperative of data sharing with the requirement to protect individual privacy in the Genomics domain, making it a subject of crucial significance in modern Biotechnology and Healthcare studies.

II. BACKGROUND

Genomics has seen exceptional advancements, with the capability to sequence and examine an individual's complete genetic code quickly and cost-effectively. This worth of Genomic data has unlocked doors to a broad collection of medical breakthroughs, from comprehending genetic inclinations to modifying treatments to the unique genetic makeup of a person [1]. However, this remarkable worth of gene information comes with a profound caution, which is the threat to individual privacy. Genomic data intrinsically carries highly personal and sensitive data and information, containing not only one's health status but also family and rooted connections. The possibility of misuse or accidental exposure of this data is a growing worry, highlighting the demand for solid privacy protection mechanisms in Genomics.

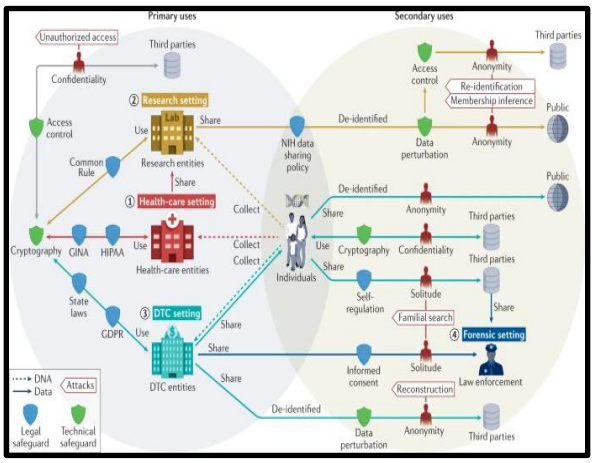

Figure 1: A Comprehensive Overview of Privacy-protective Measures in Genomic Data Flows
(Source: 2)

Historically, sharing Genomic data for study analysis has usually been a fragile balance between promoting scientific advancement and ensuring privacy [2]. Conventional de-identification methods, such as removing direct identifiers, have been used.

However, they could be more effective. Studies have shown that it is feasible to re-identify individuals by utilising genetic and publicly available data, indicating the susceptibilities of traditional privacy safeguards. As an outcome, there is a critical necessity for more rigid and quantifiable privacy-preserving methods in Genomics.

Vol.12 Issue 02, February 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Differential privacy has arisen as a profitable solution to this complicated issue. Differential privacy is a Mathematical framework that presents a formal, verifiable proof of privacy protection while still allowing the sharing of valuable data for analysis [3]. This approach can transform the way Genomic data is shared, analysed, and utilised, assuring the highest norms of individual privacy while persisting to drive innovation in Medical Study. The investigation and application of differential privacy techniques in Genomics are paramount to this study, seeking to present an understanding of the feasibility and efficacy of this approach in diminishing privacy concerns and fostering responsible data sharing in the Genomics domain [4].

III. RESEARCH AIM

The primary aim of this study is to evaluate the effectiveness of implementing differential privacy techniques in protecting individual privacy when sharing genomic data.

IV. RESEARCH OBJECTIVES

- To assess the privacy issues and concerns in Genomic data sharing;
- To evaluate the implementation of differential privacy techniques in Genomic data;
- To explore the influence of privacy mechanisms on data utility in Genomics;
- To critically analyse the real-world Genomic privacy applications;
- To investigate trade-offs in privacy and utility in Genomics data research;
- To recommend ethical Genomic data sharing and privacy protection.

V. LITERATURE REVIEW

Privacy Issues and Concerns in Genomic Data Sharing

Privacy issues and concerns in Genomic data sharing are crucial and developing aspects of modern healthcare and studies. Genomic data contains a wealth of information about a person's genetic makeup, inclinations to diseases, and familial connections [5]. It is intrinsically susceptible, and its sharing offers different challenges. One of the most significant concerns is the threat of re-identification, where hostile actors or unauthorised commodities can merge de-identified Genomic data with precise individuals. It could contribute to effective privacy violations, medical bias, and personal harm.

Moreover, individuals may worry about stigmatisation or discrimination based on their genetic data and information, hindering them from partaking in studies or sharing their data [6]. Therefore, securing Genomic data privacy is essential to boost trust and motivate study data sharing.

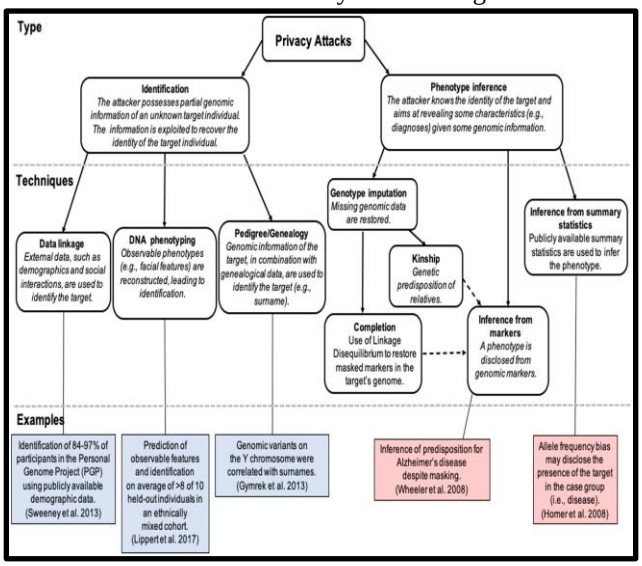

Figure 2: Taxonomy of Privacy Attacks in Genomic Data Sharing
(Source: 6)

Genomic data privacy concerns are composed of the exponential development of data gathering and sharing in Biomedicine. The accumulation of large-scale biobanks, accuracy medicine endeavours, and cooperative study projects has raised the shared volume and assortment of data [7]. Additionally, data accumulation across different sources poses a higher risk of privacy breaches.

Furthermore, Genomic data's sophisticated nature raises ethical and legal complications. Consent models may only sometimes sufficiently address the degree to which data can be shared, manipulated, or re-purposed. Offsetting the societal advantages of study analysis with individual privacy privileges is a nuanced challenge [8]. In addition, data breaches, both intentional and accidental, can have strict legal implications.

Implementation of Differential Privacy Techniques in Genomic Data

Implementing differential privacy techniques in Genomic data illustrates a profitable strategy to mitigate privacy concerns while promoting responsible data sharing. Differential privacy is a Mathematical framework that presents restrained noise or perturbation into query outcomes,

Vol.12 Issue 02, February 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

thereby protecting people's privacy within the dataset [9]. To use this method for Genomics, the first step concerns specifying a privacy budget, which quantifies the acceptable information leakage. By accomplishing this, investigators can balance the demand for precise outcomes with the imperative of safeguarding individual privacy. Differential privacy techniques in Genomics present a layer of noise or randomness, making it more challenging to re-identify distinctive individuals while permitting meaningful study outcomes [10].

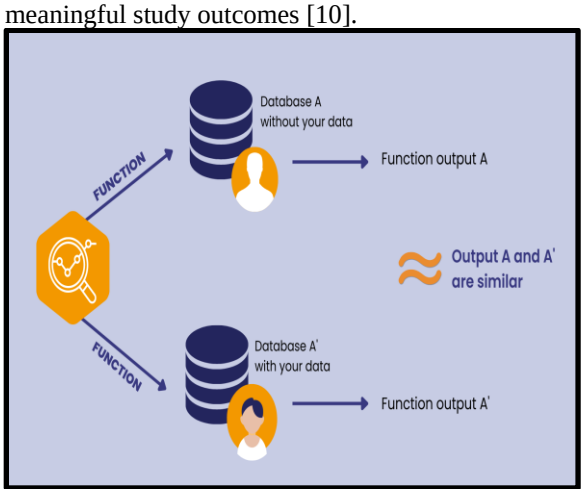

Figure 3: Differential Privacy Mechanism
(Source: 10)

The practical implementation of differential privacy in Genomic data affects different challenges. For illustration, selecting an applicable privacy parameter necessitates careful review. Too little noise may not sufficiently protect privacy, while too much noise could compromise the utility of the data for study [11]. Moreover, the sophistication of Genomic data, which contains different data types such as DNA sequences and clinical data, needs modified differential privacy mechanisms for diverse aspects of the data. Research and Development (R&D) in this field are paramount to ensure that the application of differential privacy strategies aligns with the distinctive features of Genomic data.

Influence of Privacy Mechanisms on Data Utility in Genomics

Incorporating privacy mechanisms in Genomics studies has a profound impact on data utility, as it implicates a fragile balance between protecting individual privacy and keeping the integrity and benefit of the data. One significant influence is the introduction of noise or perturbation to query responses, an essential element of differential privacy [12]. While this noise improves privacy protection, it simultaneously decreases data utility. The challenge lies in choosing the optimal noise level (controlled by the privacy parameter Epsilon-ε) to keep a desirable trade-off between privacy and utility. Less ε values deliver more substantial privacy promises. However, they result in noisier data, possibly making it more challenging to extract meaningful perspicuity. Investigators must carefully calibrate ε based on the sharpness of the data and the explicit study purposes [13]. Offsetting these elements assures that the data stays beneficial while adhering to strict privacy norms.

Another impact on data utility stems from the restrictions assessed by differential privacy mechanisms. Certain questions concerning specific counting and rare genetic variants may become more difficult to accomplish accurately under the privacy-preserving framework [14]. The intrinsic randomness familiarised to protect privacy can restrict the accurate identification of explicit Genomic attributes.

Investigators must adapt their analytical techniques to account for these constraints by setting novel statistical techniques and investigating alternative approaches that strike a better harmony between privacy and utility.

Real-world Genomic Privacy Applications

Real-world Genomic privacy applications are crucial in managing the critical demand to protect individual privacy in the generation of Genomics while permitting the responsible sharing of genetic data for study and medical intentions. One notable application is in the domain of large-scale Genomics study initiatives and biobanks [15]. These institutions usually handle extensive amounts of susceptible genetic data from various sources.

To ensure privacy, they adopt vigorous privacy-preserving strategies, such as differential privacy, to de-identify data and safeguard it from re-identification attacks. These real-world privacy applications not only protect individuals' privacy but also encourage the pooling of data for worthwhile study insights.

As an illustration, ***"Genomic Data Commons"***(GDC) has assumed privacy mechanisms to facilitate data sharing while providing strict privacy protection, facilitating cooperation among investigators [16].

Vol.12 Issue 02, February 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Figure 4: Real-world Data Types
(Source: 16)

Genomic privacy also has played a critical role in customised medicine and clinical Genomics. Hence, individual genetic data is used to modify treatments and interventions. Privacy mechanisms are employed to protect patient data, assuring that sensitive genetic information stays confidential [17]. For illustration, ***"Electronic Health Records"*** (EHR) systems utilise encryption and access controls to protect Genomic data. As an outcome, patients can help from personalised treatment while having faith that their genetic information is protected.

VI. METHODOLOGY

A ***secondary qualitative*** methodology was considered to address the study's aim of evaluating the effectiveness of implementing differential privacy techniques in protecting individual privacy when sharing Genomic data. This technique is well-suited to thoroughly review and analyse the existing literature, laws and regulations, and practical implementations concerning privacy mechanisms in Genomics [18]. The process is concerned with a comprehensive review of scholarly articles, journals, reports, and case studies within the Genomics and data privacy field. This analysis technique synthesises wisdom from multiple sources, presenting a holistic familiarity with the topic.

A systematic literature review was performed to collect a complete overview of privacy mechanisms in Genomics. This review contained articles and research papers transiting privacy concerns, data protection regulations, and implementing privacy-preserving methods. It qualified for identifying trends and challenges and developing methodologies regarding Genomic data privacy [19]. In addition, the study of real-world applications delivered perspicuity into how privacy mechanisms are practically involved and their influence on data utility.

VII. RESULTS AND DISCUSSION

Critically Analyse the Evolving Landscape of Privacy Mechanisms in Genomic Data Sharing

The evolving landscape of privacy mechanisms in Genomic data sharing shows the progressively complicated interplay between genetic information's exponential development and individual privacy's imperatives. As Genomics continues to advance, there are worries about data security and privacy [20]. Differential privacy has arisen as a crucial player in managing these concerns, delivering a formal framework to offset the sharing of valuable Genomic understandings with the safeguard of individual privacy.

Vol.12 Issue 02, February 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

However, this technique has its challenges. Calibrating privacy parameters, such as ε, stays a minute assignment, as discovering the optimal balance between privacy and data utility is paramount.

Moreover, differential privacy is just one characteristic of an expanding toolkit of privacy mechanisms.

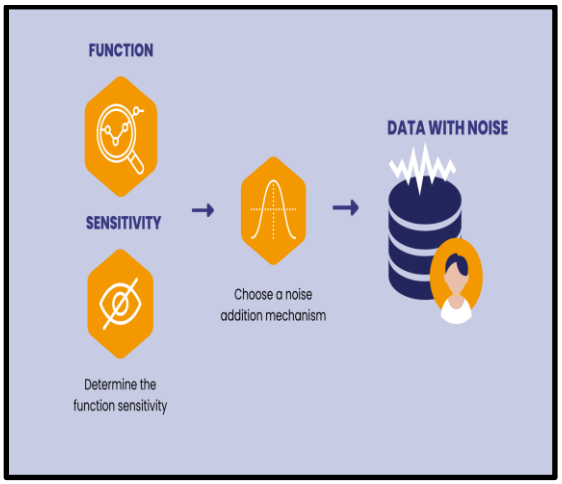

Figure 5: Adoption of Differential Privacy Mechanisms in Genomics
(Source: 20)

The landscape also scuffles with ethical and legal complications, needing a harmonisation of regulations to promote responsible data sharing while safeguarding individuals from possible harm or discrimination [21]. The future has security in the shape of standardised privacy practices, global cooperation, and continuous study to enhance the efficiency and efficacy of privacy mechanisms. The challenge lies in adjusting these mechanisms to a constantly developing Genomics landscape, where the volume and variety of data grow exponentially, and strong privacy protection is essential. This essential analysis highlights the engaged nature of privacy mechanisms in Genomics, underscoring the significance of striking the right balance between data sharing, scientific refinement, and individual privacy in this ever-evolving field [22].

Exploration of Different Elements of Differential Privacy Technique

Privacy Budget

The privacy budget, denoted as epsilon (ε), is a fundamental notion in differential privacy, a privacy-preserving framework broadly concerned with data analysis, including Genomic data sharing. It quantifies the most significant amount of adequate privacy loss within a given analysis or dataset [22]. A less ε value indicates more robust privacy protection, which may lead to noisier or less authentic outcomes. In contrast, a larger ε allows more accurate results while presenting weaker privacy guarantees. In the context of Genomic data sharing, ε permits investigators to balance protecting individual privacy and acquiring meaningful perspicuity from Genetic information, assuring that privacy protection is effectively addressed while facilitating worthwhile study and analysis.

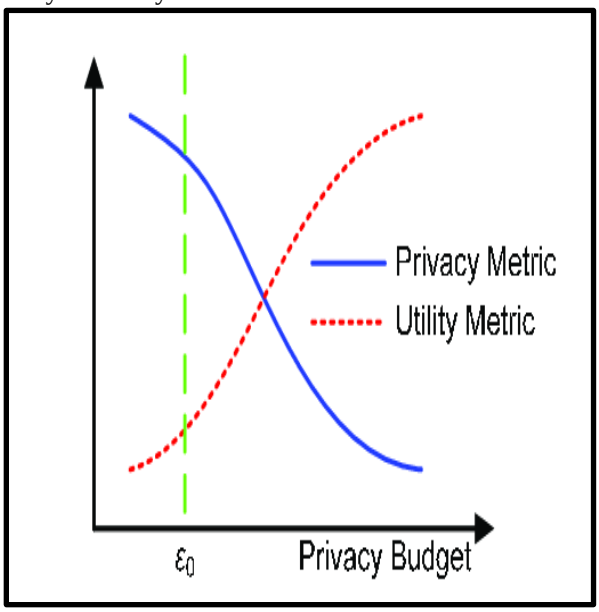

Figure 6: Trade-off of Differential Privacy
(Source: 22)

Data Perturbations

The "data perturbation" concern familiarising managed alterations to data to sweeten privacy while keeping its analytical utility. In Genomic data sharing, "data perturbations" safeguard individual genetic information [23]. This technique typically involves adding calibrated noise as well as making slight modifications to the data. It becomes complicated to specify distinct individuals within the dataset by accomplishing so.

These perturbations facilitate investigators to draw accurate conclusions and extract noteworthy perspicuity from the Genomic data while protecting the privacy and obscurity of the individuals whose data is being shared. "Data perturbations" are crucial for executing differential privacy approaches in the Genomics domain [24].

Vol.12 Issue 02, February 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

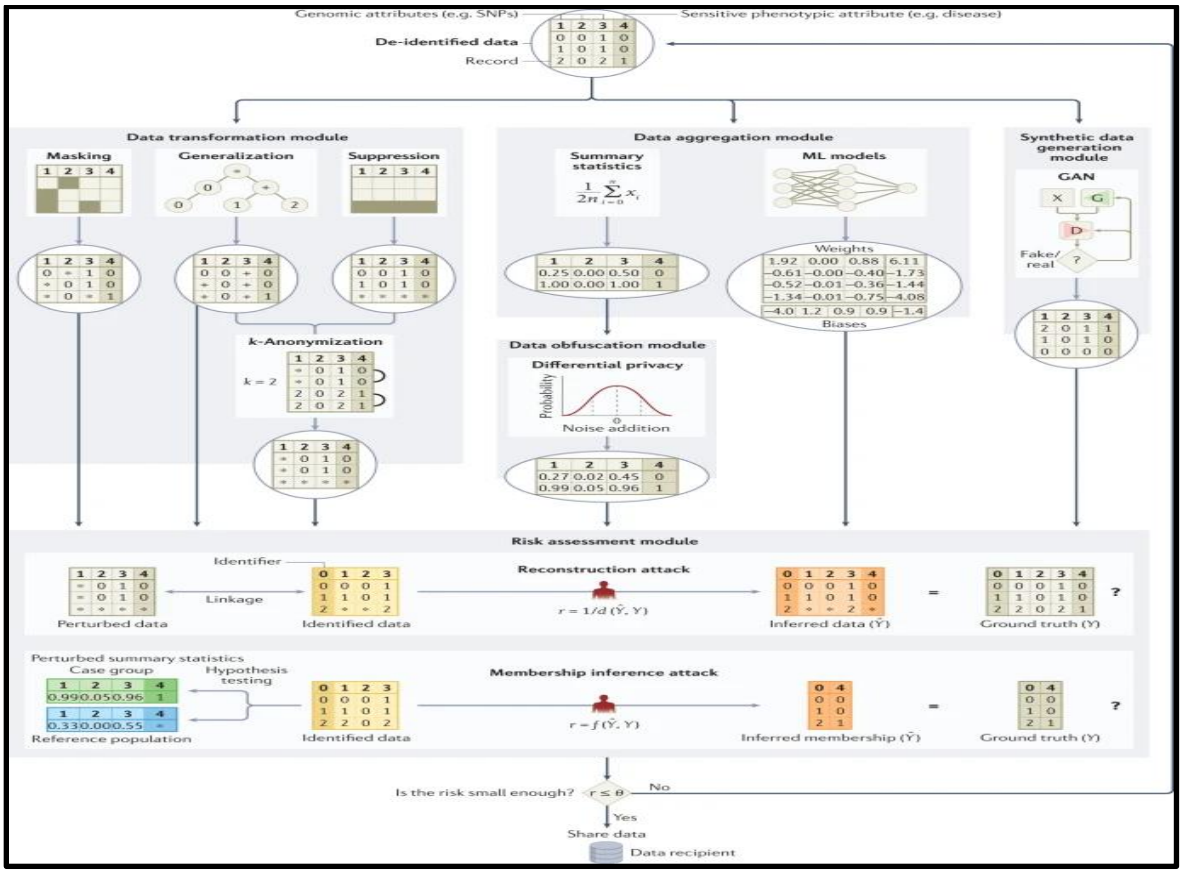

Figure 7: Data Perturbation for Privacy Safety in Genomic Data Sharing
(Source: 23)

Evaluation of Differential Privacy Mechanisms for Protection of Individual Privacy in Genomic Data Sharing

Differential privacy mechanisms are employed to add controlled noise to data or adjust data questions to safeguard individuals' privacy while still allowing significant data analysis. These mechanisms are critical for accomplishing differential privacy.

Laplace Mechanism

The "Laplace Mechanism" is an essential part of differential privacy, a privacy-preserving framework for data analysis. It adds Laplace-distributed noise to the output of questions on sensitive datasets. The quantity of noise counted is calibrated based on the query's sharpness, which measures how much the query outcome can alter when a single data point is changed [25]. By presenting this controlled noise, the "Laplace Mechanism" assures that individual contributions stay private, preventing the disclosure of explicit data while still permitting significant statistical analyses.

It strikes a harmony between privacy and data utility, safeguarding sensitive information while allowing invaluable insights from the data.

Vol.12 Issue 02, February 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

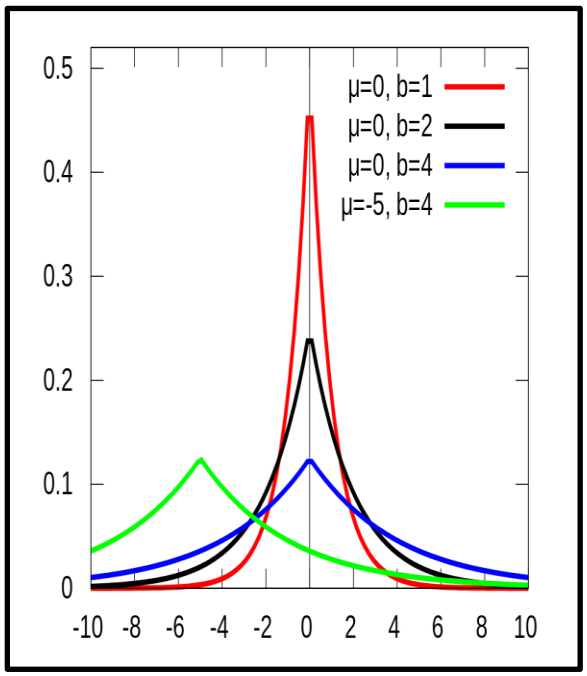

Figure 8: Laplace Distribution
(Source: 25)

In the context of a "Laplace Mechanism" with a mean (μ) of 0, it indicates that the added noise has the potential to be close to 0, with only a slight possibility of being significantly positive or negative.

The parameter' b' in the "Laplace Mechanism" is estimated as sensitivity divided by epsilon, where epsilon symbolises the privacy budget in differential privacy.

Gaussian Mechanism

The "Gaussian Mechanism" is a crucial instrument in differential privacy, a framework for protecting individual privacy in data analysis. It presents Gaussian (normal) noise to the outcomes of questions on sensitive data, equivalent to the "Laplace Mechanism" [26]. The importance of noise added is chosen based on the query's sensitivity and a user-specified privacy parameter (ε). Gaussian noise is helpful when a smoother, ongoing distribution is selected, making it convenient for preserving privacy in different data analysis scenarios. By utilising this mechanism, Genomic Labs can safeguard individuals' data privacy while conducting beneficial statistical analyses, effectively poising privacy and data utility.

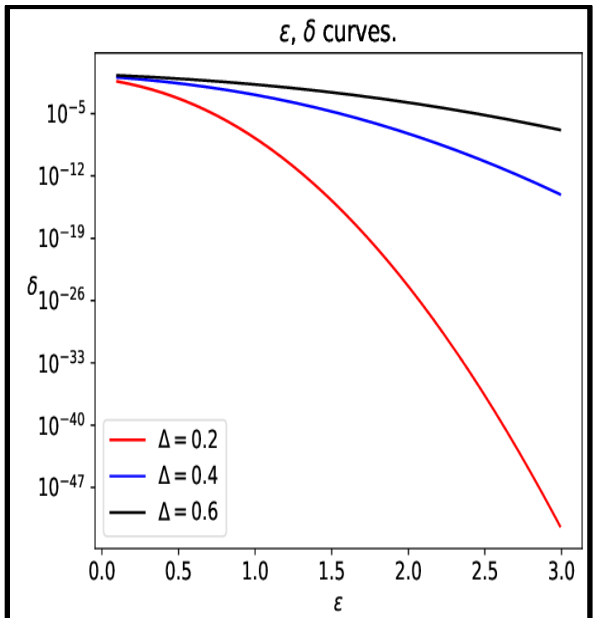

Figure 9: Gaussian Mechanism
(Source: 26)

The "Gaussian Mechanism" with a value of Δ = 0.2 delivers differential privacy for all pairs established on or above the red curve in the plot. It suggests that it presents privacy guarantees for all points on or above this distinctive curve when assuming various values of Δ.

Exponential Mechanism

The "Exponential Mechanism" is an essential instrument in differential privacy. It is operated to choose an item or create a decision from a group of options while maintaining individual privacy. The mechanism gives a score to each option based on its applicability to a shared query. Noise, generally "Laplace noise", is added to these scores, and the option with the most boisterous score is specified [27]. The probability of choice is determined by the query's sensitivity and the user-defined privacy parameter, ε.

The "Exponential Mechanism" provides that alternatives with higher relevancy are more likely to be selected while still supplying strong privacy assurances in the decision-making procedure.

Vol.12 Issue 02, February 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

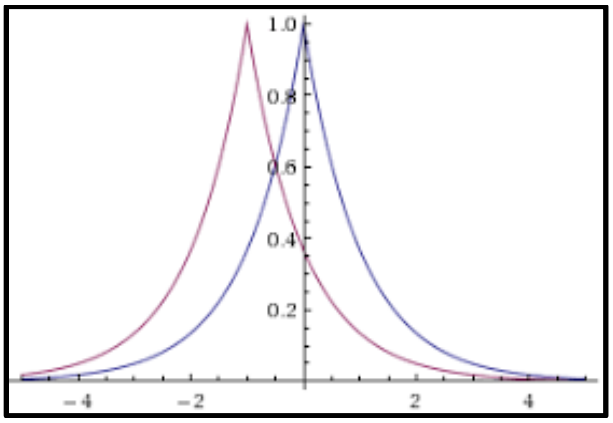

Figure 10: Exponential Mechanism
(Source: 27)

The above Figure shows the exponential mechanism of differential privacy.

Identification of Other Mechanisms for Protection of Individual Privacy in Genomic Data Sharing

Randomised Response

"Randomised Response" is a privacy-preserving survey method employed in situations where respondents may feel uncomfortable answering sensitive or potentially incriminating questions honestly. It was designed to facilitate open answers while still protecting individual privacy.

Respondents are shown a randomised element, which specifies how they answer the question [28]. This method permits investigators to gather worthwhile Genomic data for analysis while conserving the anonymity and privacy of the individuals concerned.

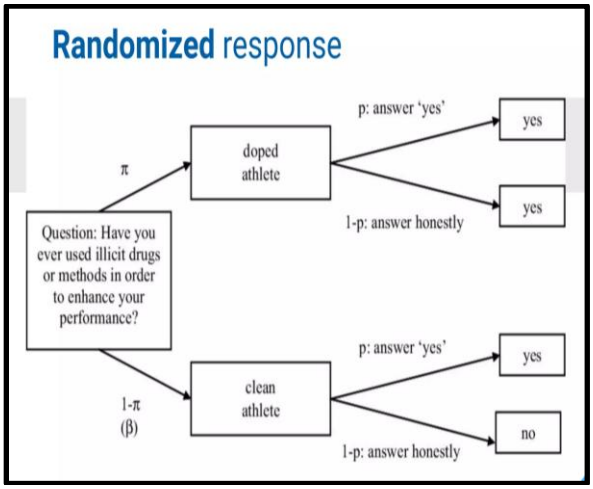

Figure 11: Randomised Response
(Source: 28)

Noise Calibration

Noise calibration is a crucial stage in implementing privacy-preserving methods, specifically in the context of Genomic data sharing [29]. It concerns explicitly adjusting the noise level to be counted to data or query outcomes. The calibration approach strives to strike a fragile balance between maintaining individual privacy and keeping the precision and utility of the data.

In Genomic data sharing, noise calibration assures that genetic information remains secret and secure. It allows investigators to conduct beneficial analyses and draw significant perspicuity from the data. Accurate calibration is necessary to specify the correct quantity of noise, permitting the privacy budget to be manipulated effectively [30].

VIII. CONCLUSION

In conclusion, the application of differential privacy mechanisms portrays a critical phase forward in assuring the safeguarding of individual privacy in the sharing and analysing of Genomic data. These mechanisms strike a fragile balance, permitting invaluable genetic perspicuity to be harnessed while protecting personal information.

As the Genomics landscape develops, adapting and optimising these privacy standards is crucial to fulfil the growing demand for data sharing. Standardised practices and continuous investigation will play a critical role in promoting the reliable and secure improvement of Genomics while admiring the essential rights of individual privacy.

IX. REFERENCE LIST

[1] Almadhoun, N., Ayday, E., & Ulusoy, Ö. (2020). Differential privacy under dependent tuples—the case of genomic privacy. *Bioinformatics*, *36*(6), 1696-1703. Retrieved on 20th October 2023, from: http://repository.bilkent.edu.tr/bitstream/handle/11693/75604/Differential_privacy_under_dependent_tuples%E2%80%94the_case_of_genomic_privacy.pdf?sequence=1

[2] Carpov, S., Gama, N., Georgieva, M., &Jetchev, D. (2022, July). GenoPPML–a framework for genomic privacy-preserving machine learning. In *2022 IEEE 15th International Conference on Cloud Computing (CLOUD)* (pp. 532-542). IEEE.

Retrieved on 20th October 2023, from: https://eprint.iacr.org/2021/733.pdf

[3] Chen, J., Wang, W. H., & Shi, X. (2020). Differential privacy protection against membership inference attack on machine learning for genomic data. In *BIOCOMPUTING 2021: Proceedings of the Pacific Symposium* (pp. 26-37). Retrieved on 20th October 2023, from: https://www.worldscientific.com/doi/pdf/10.1142/9789811232701_0003

[4] Choudhury, O., Gkoulalas-Divanis, A., Salonidis, T., Sylla, I., Park, Y., Hsu, G., & Das, A. (2019). Differential privacy-enabled federated learning for sensitive health data. *arXiv preprint arXiv:1910.02578*. Retrieved on 20th October 2023, from: https://arxiv.org/pdf/1910.02578

[5] Gürsoy, G., Li, T., Liu, S., Ni, E., Brannon, C. M., & Gerstein, M. B. (2022). Functional genomics data: privacy risk assessment and technological mitigation. *Nature Reviews Genetics*, *23*(4), 245-258. Retrieved on 20th October 2023, from: https://web.stanford.edu/~cbrannon/publication/pub6/pub6.pdf

[6] Gursoy, M. E., Tamersoy, A., Truex, S., Wei, W., & Liu, L. (2019). Secure and utility-aware data collection with condensed local differential privacy. *IEEE Transactions on Dependable and Secure Computing*, *18*(5), 2365-2378. Retrieved on 20th October 2023, from: https://arxiv.org/pdf/1905.06361

[7] Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential privacy techniques for cyber physical systems: a survey. *IEEE Communications Surveys & Tutorials*, *22*(1), 746-789. Retrieved on 20th October 2023, from: https://arxiv.org/pdf/1812.02282

[8] Husnoo, M. A., Anwar, A., Chakrabortty, R. K., Doss, R., & Ryan, M. J. (2021). Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. *IEEE Access*, *9*, 153276-153304. Retrieved on 20th October 2023, from: https://ieeexplore.ieee.org/iel7/6287639/6514899/09594795.pdf

[9] Isie, D., & Reza, H. (2023). Application of Blockchain Technology & Integration of Differential Privacy: Issues in E-Health Domains. Retrieved on 20th October 2023, from: https://www.preprints.org/manuscript/202310.0553/download/final_file

[10] Islam, T. U., Ghasemi, R., & Mohammed, N. (2022, January). Privacy-preserving federated learning model for healthcare data. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0281-0287). IEEE. Retrieved on 20th October 2023, from: https://mspace.lib.umanitoba.ca/bitstream/handle/1993/37192/Islam_Tanzir.pdf?sequence=2

[11] Jacobs, D., McDaniel, T., Varsani, A., Halden, R. U., Forrest, S., & Lee, H. (2021). Wastewater monitoring raises privacy and ethical considerations. *IEEE Transactions on Technology and Society*, *2*(3), 116-121. Retrieved on 20th October 2023, from: https://par.nsf.gov/servlets/purl/10277368

[12] Jafarbeiki, S., Gaire, R., Sakzad, A., Kermanshahi, S. K., & Steinfeld, R. (2021, December). Collaborative analysis of genomic data: vision and challenges. In *2021 IEEE 7th International Conference on Collaboration and Internet Computing (CIC)* (pp. 77-86). IEEE. Retrieved on 20th October 2023, from: https://arxiv.org/pdf/2202.04841

[13] Javed, L., Anjum, A., Yakubu, B. M., Iqbal, M., Moqurrab, S. A., & Srivastava, G. (2023). ShareChain: Blockchain- enabled model for sharing patient data using federated learning and differential privacy. *Expert Systems*, *40*(5), e13131. Retrieved on 20th October 2023, from: https://www.researchgate.net/profile/Bello-Yakubu-2/publication/362907574_ShareChain_Blockchain-enabled_model_for_sharing_patient_data_using_federated_learning_and_differential_privacy/links/6306d977acd814437fd4da7c/ShareChain-Blockchain-enabled-model-for-sharing-patient-data-using-federated-learning-and-differential-privacy.pdf

[14] Jiang, B., Li, J., Yue, G., & Song, H. (2021). Differential privacy for industrial internet of

things: Opportunities, applications, and challenges. *IEEE Internet of Things Journal*, *8*(13), 10430-10451. Retrieved on 20th October 2023, from: https://www.academia.edu/download/96834000/2101.10569v3.pdf

[15] Khanna, A., Schaffer, V., Gürsoy, G., & Gerstein, M. (2022, July). Privacy-preserving model training for disease prediction using federated learning with differential privacy. In *2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)* (pp. 1358-1361). IEEE. Retrieved on 20th October 2023, from: https://ieeexplore.ieee.org/iel7/9870821/9870822/09871742.pdf

[16] Kim, W., & Seok, J. (2022, February). Privacy-preserving collaborative machine learning in biomedical applications. In *2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (pp. 179-183). IEEE. Retrieved on 20th October 2023, from: https://www.researchgate.net/profile/Wonsuk-Kim/publication/358955456_Privacy-preserving_collaborative_machine_learning_in_biomedical_applications/links/6307946c61e4553b9539cfef/Privacy-preserving-collaborative-machine-learning-in-biomedical-applications.pdf

[17] Li, J., Ye, H., Li, T., Wang, W., Lou, W., Hou, Y. T., ... & Lu, R. (2020). Efficient and secure outsourcing of differentially private data publishing with multiple evaluators. *IEEE Transactions on Dependable and Secure Computing*, *19*(1), 67-76. Retrieved on 20th October 2023, from: https://www.cs.unb.ca/~rlu1/paper/LiYLWLHLL21.pdf

[18] Lou, J., & Cheung, Y. M. (2020). An uplink communication-efficient approach to featurewise distributed sparse optimization with differential privacy. *IEEE Transactions on Neural Networks and Learning Systems*, *32*(10), 4529-4543. Retrieved on 20th October 2023, from: https://www.comp.hkbu.edu.hk/~ymc/papers/journal/10.1109TNNLS.2020.3020955.pdf

[19] Marks, J., Montano, B., Chong, J., Raavi, M., Islam, R., Cerny, T., & Shin, D. (2021, March). Differential privacy applied to smart meters: a mapping study. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing* (pp. 761-770). Retrieved on 20th October 2023, from: https://dl.acm.org/doi/pdf/10.1145/3412841.3442360

[20] Öksüz, A. Ç., Ayday, E., &Güdükbay, U. (2021). Privacy-preserving and robust watermarking on sequential genome data using belief propagation and local differential privacy. *Bioinformatics*, *37*(17), 2668-2674. Retrieved on 20th October 2023, from: https://academic.oup.com/bioinformatics/article-pdf/37/17/2668/50339159/btab128.pdf

[21] Qu, Y., Ma, L., Ye, W., Zhai, X., Yu, S., Li, Y., & Smith, D. (2023). Towards Blockchain-Assisted Privacy-Aware Data Sharing For Edge Intelligence: A Smart Healthcare Perspective. *arXiv preprint arXiv:2306.16630*. Retrieved on 20th October 2023, from: https://arxiv.org/pdf/2306.16630

[22] Subramanian, R. (2022, September). Differential Privacy Techniques for Healthcare Data. In *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)* (pp. 95-100). IEEE. Retrieved on 20th October 2023, from: https://intelligenttech.org/IDSTA2022/IDSTApackingList/14_IDSTA2022_RC_7407.pdf

[23] Venkatesaramani, R., Wan, Z., Malin, B. A., &Vorobeychik, Y. (2023). Enabling trade-offs in privacy and utility in genomic data beacons and summary statistics. *Genome Research*, gr-277674. Retrieved on 20th October 2023, from: https://genome.cshlp.org/content/early/2023/05/19/gr.277674.123.full.pdf

[24] Wang, Q., Li, Z., Zou, Q., Zhao, L., & Wang, S. (2020). Deep domain adaptation with differential privacy. *IEEE Transactions on Information Forensics and Security*, *15*,

3093-3106. Retrieved on 20th October 2023, from: https://www.cse.sc.edu/~songwang/document/tifs20.pdf

[25] Xiang, Z., Ding, B., He, X., & Zhou, J. (2020, June). Linear and range counting under metric-based local differential privacy. In *2020 IEEE International Symposium on Information Theory (ISIT)* (pp. 908-913). IEEE. Retrieved on 20th October 2023, from: https://arxiv.org/pdf/1909.11778

[26] Yan, J., Han, Z., Zhou, Y., & Lu, L. (2022). A Differential Privacy Approach to Preserve GWAS Data Sharing based on A Game Theoretic Perspective. *KSII Transactions on Internet & Information Systems*, *16*(3). Retrieved on 20th October 2023, from: https://koreascience.kr/article/JAKO202211563852034.pdf

[27] Yoon, J., Drumright, L. N., & Van Der Schaar, M. (2020). Anonymization through data synthesis using generative adversarial networks (ads-gan). *IEEE journal of biomedical and health informatics*, *24*(8), 2378-2388. Retrieved on 20th October 2023, from: https://ieeexplore.ieee.org/ielaam/6221020/9159696/9034117-aam.pdf

[28] Yousif, H. M., & Hameed, S. M. (2023). Review of Challenges and Solutions for Genomic Data Privacy-Preserving. *Iraqi Journal of Science*, 4729-4746. Retrieved on 20th October 2023, from: https://ijs.uobaghdad.edu.iq/index.php/eijs/article/download/7057/4099

[29] Zhang, Y., Bai, G., Li, X., Nepal, S., Grobler, M., Chen, C., & Ko, R. K. (2022). Preserving Privacy for Distributed Genome-Wide Analysis Against Identity Tracing Attacks. *IEEE Transactions on Dependable and Secure Computing*. Retrieved on 20th October 2023, from: https://research-repository.griffith.edu.au/bitstream/handle/10072/422336/Bai5479330-Accepted.pdf?sequence=2

[30] Zhu, T., Ye, D., Wang, W., Zhou, W., & Philip, S. Y. (2020). More than privacy: Applying differential privacy in key areas of artificial intelligence. *IEEE Transactions on Knowledge and Data Engineering*, *34*(6), 2824-2843. Retrieved on 20th October 2023, from: https://ieeexplore.ieee.org/iel7/69/4358933/09158374.pdf