Manuscript Title Blockchain based General Data Protection Regulation compliant data breach detection system.

Dear Editor,

I am writing to submit my rebuttal for the comments provided by the esteemed reviewers regarding my manuscript titled “Blockchain based General Data Protection Regulation compliant data breach detection system”. Thank you for allowing a resubmission of our manuscript, with an opportunity to address the reviewers’ comments. I would like to express my sincere gratitude to the reviewers for their valuable time and constructive feedback. Their insights have undoubtedly strengthened the quality of my work. In response to their comments, I have carefully revised the manuscript to address each concern raised during the review process. I believe that the revisions made have significantly improved the overall clarity, methodology, and contribution of the manuscript.

Below, I have summarized the major points raised by the reviewers and outlined how I have addressed each concern. We are uploading (a) our point-by-point response to the comments (below) (response letter), (b) a revised manuscript with revised paper with track change (*revised paper with track changes*), and (c) a clean updated manuscript without highlights (*Main Manuscript).*

Best regards,
Kainat et al.

Response to Reviewer Comments

Respected reviewers, thank you very much for your time and effort in deeply reviewing the paper. Your comments really guided us to improve the quality of the paper to the best level. We appreciate these comments and constructive feedback. Substantial changes have been made to address the issues raised. We have now proofread the revised paper in detail and addressed those mistakes. After incorporating the suggested changes, we feel that the quality of the revised paper has improved significantly as a result and are grateful to the reviewers for pointing out the shortcomings.

Please note the following:

- The font of the reviewers' comments is highlighted in "Dark blue", and the corresponding response is in "black".
- In the excerpts from the revised manuscript, the references follow the order as the manuscript.

We finally thank the Editor and the referee for their time and look forward to hearing from you soon.

Point-by-point response to the reviewer's comments:

Reviewer 1

Basic reporting

1. The idea of this research is better, and the authors presented a better work. However, authors may consider the following.

Response: Respected reviewer, thank you for your constructive feedback and positive evaluation of the revised manuscript. We appreciate your recognition of the improvements made to the research idea and the overall quality of our work. We have carefully considered your suggestions and incorporated them into the revised version of the manuscript. Your guidance has been invaluable, and we believe these enhancements contribute to a stronger and more refined research presentation. We are grateful for your thorough review and commitment to elevating the scholarly contributions of our work.

2. Authors may revise the abstract to elaborate more on the problem statement, findings, and contributions.

Response: Respected reviewer, thank you for your insightful comments and thorough review of our manuscript. We appreciate your guidance and have diligently incorporated your suggestions into the revised version. In response to your suggestion, we have carefully revised the abstract to provide a more detailed exposition of the problem statement, findings, and contributions. The updated abstract aims to offer a more comprehensive overview, ensuring that readers can gain a deeper understanding of the research from the outset. We believe these enhancements contribute significantly to the overall quality of the manuscript. Your insights have been instrumental in refining our work, and we are grateful for your valuable guidance.

3. The introduction is not clear. Authors may contribute more towards this.

Response: Respected reviewer, thank you for your valuable feedback on our manuscript. We have carefully reviewed and addressed your comments regarding the clarity of the introduction. In the revised version, we have made substantial improvements to enhance the overall clarity and coherence of the introduction. We have focused on providing a more concise and elucidating overview, contributing significantly to the reader's understanding of the research context and objectives. We believe these revisions address the concerns raised, and we sincerely appreciate your guidance in this regard.

4. Authors may elaborate more on the novelty/contribution of their work and how it contributes to the literature in the second last paragraph of the introduction clearly. May rephrase further the details that they provided.

Response: Respected reviewer, we appreciate your insightful feedback and have diligently incorporated your suggestions into the revised manuscript. Specifically, we have extended the discussion on the novelty and contribution of our work in the second last paragraph of the introduction. The details have been carefully rephrased to offer a more explicit and comprehensive explanation of how our research contributes to the existing literature. We believe these revisions provide a clearer and more robust connection between our work and the broader scholarly context. Your guidance has been invaluable in refining our manuscript, and we sincerely hope these enhancements align with your expectations.

5. The provided contribution, such as point vi is not the contribution.

Response: Respected reviewer, we appreciate your acknowledgment of the revisions made based on your suggestions. In response to your feedback regarding the provided contribution, specifically point vi, we have revisited and redefined this aspect in the revised manuscript. We have clarified and rephrased the details to ensure a more accurate representation of its contribution to the overall study. We believe these adjustments address your concerns, and we are grateful for the opportunity to refine our work with your valuable guidance.

6. Authors need to be specific about their problem statement and the scope of their research.

Response: Respected reviewer, thank you for your constructive feedback on our manuscript. Regarding your comment on the need for specificity in the problem statement and research scope, we have carefully addressed this concern in the revised manuscript. We have provided additional details to precisely define our problem statement and clearly delineated the scope of our research, ensuring a more focused and explicit presentation. We believe these enhancements contribute to the overall clarity and depth of our work.

7. Overall, the paper presentation can be improved further.

Response: Respected reviewer, thank you for your meticulous review and constructive feedback on our manuscript. We appreciate your recognition of the revisions made in response to your suggestions. Concerning the overall paper presentation, we have revisited the manuscript with a focus on improving clarity, coherence, and visual elements. We have made enhancements to ensure a smoother flow and a more engaging presentation. We believe these adjustments contribute to an improved reading experience. Your valuable insights have guided us in refining the manuscript, and we sincerely appreciate your time and effort in this review process.

8. Thorough proofreading is recommended.

Response: Respected reviewer, regarding the recommendation for thorough proofreading, we have conducted a meticulous review of the manuscript by addressing grammatical errors and improving language quality. We have endeavored to ensure clarity and correctness throughout the document. We believe these proofreading efforts contribute to an improved manuscript. Your attention to detail is invaluable, and we are grateful for your guidance in refining our work.

9. A few of the figure's resolutions are not clear and hard to read.

Response: Respected reviewer, thank you for your feedback on our manuscript, and we appreciate your recognition of the revisions made in response to your suggestions. Regarding the clarity of figures, we have carefully reviewed and enhanced the resolution of all relevant figures in the revised version to ensure improved clarity and readability. We trust that these adjustments address your concerns, and we are committed to providing a visually coherent representation of our work. Your attention to detail has been invaluable, and we sincerely appreciate your guidance in refining our manuscript.

10. A few references are missing some information; you may complete them critically.

Response: Respected reviewer, thank you for your thorough review. We appreciate your acknowledgment of the revisions made in response to your suggestions. Concerning the missing information in some references, we have diligently revisited and completed these references critically in the revised version. We believe these adjustments contribute to the overall completeness and accuracy of our citations. Your attention to detail has been instrumental in refining our work, and we sincerely value your guidance throughout this process.

11. The conclusion is not clear and needs revision and clarity and alignment with the abstract and title.

Response: Respected reviewer, thank you for your insightful feedback on our manuscript. We appreciate your acknowledgment of the revisions made in response to your suggestions. Regarding the conclusion, we have carefully revised and clarified the concluding section in alignment with the abstract and title in the revised version. We believe these adjustments contribute to a more coherent and well-aligned conclusion. Your guidance has been crucial in refining our work, and we are grateful for the opportunity to enhance the overall clarity of our manuscript.

12. Provided references are better enough. However, authors are recommended to consider more latest and related, such as,

A. P. Singh et al., "A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications," in IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5779-5789, Aug. 2021, doi: 10.1109/TII.2020.3037889.

Response: Respected reviewer, thank you for your constructive feedback and recognition of the quality of the provided references in our manuscript. We have taken your recommendation into careful consideration and, in the revised version, made efforts to incorporate more recent and related references that contribute to the current state of the field. We believe these additions strengthen the scholarly foundation of our work and provide a more comprehensive overview of the relevant literature. Your guidance has been invaluable, and we appreciate the opportunity to enhance the robustness of our manuscript.

Reviewer 2

Basic reporting

This paper proposes a blockchain based method for defending against inner attackers. The system is designed, implemented, and evaluated.

Response: Respected reviewer, thank you for your thoughtful review and valuable feedback on our manuscript. We appreciate your positive recognition of our paper's proposal for a blockchain-based method to defend against inner attackers. Your positive feedback encourages us, and we are pleased that the clarity and completeness of our work align with your expectations.

Experimental design

The experiments are sufficient.

Response: Respected reviewer, thank you for your positive feedback on the experiments conducted in our manuscript. We appreciate your recognition of the sufficiency of the experimental work. Your feedback is valuable to us, and we are pleased that the experimental design and execution meet the standards set for research.

Validity of the findings

The results are sound.

Response: Respected reviewer, thank you for your positive feedback on the results presented in our manuscript. We appreciate your assessment of the soundness of our findings. Your acknowledgment is valuable, and we are pleased that our results meet the expected standards.

Additional comments

(1) The relation between GDPR and inner attackers should be addressed.

Response: Respected reviewer, thank you for your insightful feedback on our manuscript. We appreciate your suggestion to address the relation between GDPR and inner attackers. In the revised version, we have carefully examined and incorporated a dedicated section to elucidate the connection between GDPR regulations and the challenges posed by inner attackers. This addition aims to provide a more comprehensive understanding of the regulatory implications associated with our proposed blockchain-based defense method. We hope these enhancements contribute positively to the overall coherence and relevance of our work. Your valuable input has been instrumental, and we are grateful for the opportunity to strengthen our manuscript.

(2) The log data is encrypted and stored in the block? The storage of block should be low.

Response: Respected reviewer, thank you for your insightful comment on our manuscript. We appreciate your attention to the storage aspect of our proposed system. In response to your concern, we have added following text:

Yes, the log data is encrypted before being stored in each block of the blockchain. This encryption adds an extra layer of security, ensuring that the information within the block is not accessible to unauthorized entities. Additionally, the storage requirements for each block are optimized to be efficient and low. This not only contributes to the overall scalability of the system but also aligns with the principle of resource optimization, a crucial aspect in designing an effective and sustainable blockchain-based data breach detection system.

(3) The consensus of blockchain is what? The article is not clear enough about this.

Response: Respected reviewer, thank you for your valuable feedback. In response to your comment, we have added the following text:

The consensus mechanism employed in our blockchain-based data breach detection system is a crucial aspect that ensures the reliability and integrity of the information stored in the blockchain. We employ a consensus mechanism known as Proof of Authority (PoA), where the nodes validating transactions and adding blocks to the blockchain are trusted and authorized entities. This mechanism enhances security and efficiency, as it requires validators to have a specific level of authority, reducing the risk of malicious actors influencing the system. We understand the importance of clarity on this aspect and will ensure that the article provides a more detailed and explicit explanation of the consensus mechanism for a better understanding.

(4) The hospital case is illustrated as a use case may not be proper, as in this case more concerns should be addressed, such as privacy.

Response: Respected reviewer, thank you for your thoughtful consideration of our use case illustration involving the hospital scenario. We acknowledge your concern about potential privacy issues, and in response, we have re-evaluated the use case in the revised manuscript as shown below:

Hospital Use Case Scenario: GDPR Compliant Blockchain-Based Data Breach Detection System with Privacy Considerations

In current hospitals, the need for a robust data breach detection system compliant with the General Data Protection Regulation (GDPR) is needed. This scenario revolves around the hospital's commitment to safeguarding sensitive patient information while ensuring transparency and accountability in accordance with GDPR guidelines.

In this hospital setting, a multitude of patient records, containing highly sensitive health information, are stored electronically. Privacy concerns arise due to the necessity of providing healthcare professionals with seamless access to patient data for effective treatment while concurrently safeguarding this information against unauthorized access or potential breaches.

The GDPR emphasizes the importance of explicit patient consent for the processing of their personal data. The hospital use case involves a careful consideration of how the blockchain-based system manages and records patient consent, ensuring that only authorized individuals access specific information and that patient preferences are respected at all times.

To mitigate privacy risks, the hospital employs advanced data anonymization techniques within the blockchain system. This ensures that patient identities remain confidential while still allowing healthcare practitioners access to relevant clinical data for diagnostic and treatment purposes.

The GDPR mandates a transparent audit trail of data access and processing activities. The blockchain system, being inherently transparent and immutable, creates an auditable record of every interaction with patient data. This includes details such as who accessed the data, when it was accessed, and the nature of the interaction, providing a clear and GDPR-compliant audit trail.

Data Breach Detection:

The hospital's GDPR-compliant blockchain-based data breach detection system operates on a permissioned blockchain using a Proof of Authority (PoA) consensus mechanism. Authorized healthcare personnel, including doctors, nurses, and administrative staff, are granted specific roles within the blockchain network, ensuring that only trusted individuals have the authority to validate transactions and access patient data.

The system continuously monitors the blockchain for any irregularities or unauthorized attempts to access patient records. In the event of a potential breach, the blockchain's decentralized nature ensures that the information is not only tamper-proof but also immediately flagged for investigation, allowing the hospital's cybersecurity team to respond promptly and mitigate the breach. The objective of this section is to discuss the use case scenario of our proposed system. We assume that the data owner Alice is the patient in this case scenario, and the data processor Bob is a surgeon that often requests patients' medical records for operation purposes. In paper Figure1 provides a high-level overview of the hospital use case, where Alice's medical data are stored on the blockchain after receiving consent from Alice. Bob can obtain their desired patient data from the patient database by sending a request to the data controller Mike. Mike uses our proposed system to perform necessary tasks such as consent validation and data verification. Our proposed system allows Mike to detect any alteration in the database record and verify the authenticity of any record 24/7 before sharing data with Bob.

(5) How blockchain can be compatible with the legacy systems, which should be addressed.

Response: Respected reviewer, thank you for your insightful comment on the compatibility of blockchain with legacy systems. We appreciate your consideration of this important aspect, and in the revised manuscript as shown below:

The compatibility of blockchain with legacy systems is a crucial consideration, and addressing this integration challenge is key to the successful implementation of blockchain technology. One approach involves creating application programming interfaces (APIs) that act as bridges between the blockchain and existing legacy systems. These APIs facilitate seamless communication and data exchange, allowing the blockchain to complement and enhance the functionalities of legacy systems without necessitating a complete overhaul. Additionally, the adoption of standardized protocols and interoperability frameworks can facilitate smoother integration, ensuring that blockchain solutions can coexist and collaborate with legacy infrastructure.

(6) Fig. 2 is not clear.

Response: Respected reviewer, thank you for bringing the concern regarding Fig. 2 to our attention. We have carefully revised the figure to improve its clarity, incorporating clearer labels and enhancing visual elements for better comprehension. We appreciate your diligence in reviewing our manuscript, and we hope that the revised figure meets the standard of clarity expected.

Reviewer 3

Basic reporting

1. This paper presents a well-thought-out and potentially impactful solution to a critical problem in data security. The focus on GDPR compliance, combined with the innovative use of blockchain and smart contracts, sets a solid foundation for a robust data breach detection system. The proposed future work indicates a forward-thinking approach, although it will be important to balance technological advances with privacy and ethical considerations.

Response: Respected reviewer, thank you for your positive feedback on our manuscript. We appreciate your recognition of the well-thought-out and potentially impactful solution presented for the critical problem of data security. Your acknowledgment of the focus on GDPR compliance and the innovative use of blockchain and smart contracts is encouraging. We understand the importance of balancing technological advances with privacy and ethical considerations, and we are committed to addressing these aspects in our future work. Your insights are invaluable, and we are grateful for your thoughtful review.

2. The literature review of this article is very terse. This part should be expanded by discussing the following studies: Enabling Integrity and Compliance Auditing in Blockchain-based GDPR-compliant Data Management; Blockchain-based recommender systems: Applications, challenges and future opportunities; A systematic literature review of the tension between the GDPR and public blockchain systems; Latest trends of security and privacy in recommender systems: a comprehensive review and future perspectives; Assessment and treatment of privacy issues in blockchain systems; An Enterprise Data Privacy Governance Model: Security-Centric Multi-Model Data Anonymization.

Response: Respected reviewer, thank you for your insightful feedback on the literature review. We appreciate your suggestion to expand this section by incorporating discussions on the studies you mentioned, namely: "Enabling Integrity and Compliance Auditing in Blockchain-based GDPR-compliant Data Management," "Blockchain-based recommender systems: Applications, challenges and future opportunities," "A systematic literature review of the tension between the GDPR and public blockchain systems," "Latest trends of security and privacy in recommender systems: a comprehensive review and future perspectives," "Assessment and treatment of privacy issues in blockchain systems," and "An Enterprise Data Privacy Governance Model: Security-Centric Multi-Model Data Anonymization."

In the revised manuscript, we have expanded the literature review to encompass these relevant studies, providing a more comprehensive context for our work. We trust that these additions enhance the overall quality and depth of our manuscript. Your guidance has been invaluable, and we appreciate the opportunity to improve our contribution.

Experimental design

3. Explore alternative blockchain platforms or layer 2 solutions that offer better scalability and lower transaction costs. A hybrid blockchain model could also be considered to balance transparency and efficiency.

Response: Respected reviewer, thank you for your insightful comment regarding exploring alternative blockchain platforms or layer 2 solutions for improved scalability and lower transaction costs. We appreciate your suggestion and have duly considered it in the revised manuscript. In addition, we have discussed the potential merits of a hybrid blockchain model to strike a balance between transparency and efficiency.

4. Incorporate machine learning algorithms for advanced anomaly detection to improve the system's ability to identify complex insider threats. This could also help in reducing false positives/negatives.

Response: Respected reviewer, thank you for your valuable suggestion. We have incorporated machine learning algorithms for advanced anomaly detection in our future work to enhance the system's capability in identifying complex insider threats. We believe this addition will not only improves the system's overall performance but also contributes to the reduction of false positives/negatives. Your insights have been instrumental in refining the sophistication of our proposed solution.

Validity of the findings

5. The reliance on blockchain and smart contracts, particularly on platforms like Ethereum, raises concerns about scalability, especially given the variable gas costs. High transaction volumes in a real-world deployment could lead to inefficiencies and increased costs.

Response: Respected reviewer, we appreciate your insightful observation regarding scalability concerns, particularly in the context of platforms like Ethereum with variable gas costs. In response, we have acknowledged and discussed these scalability challenges in the revised manuscript. We have also explored potential mitigations and alternative platforms that may address these concerns, emphasizing the importance of real-world efficiency and cost-effectiveness. Your feedback has been crucial in refining our work, and we hope these revisions align with your expectations.

7. While GDPR compliance is a strength, the system's approach to handling sensitive personal data, especially with the inclusion of biometric traits, needs thorough consideration in terms of privacy and security.

Response: Respected reviewer, we appreciate your thoughtful evaluation of our manuscript. Your observation regarding the handling of sensitive personal data, particularly the inclusion of biometric traits, is indeed crucial, and we appreciate your emphasis on privacy and security. In response, our system prioritizes a privacy-by-design approach, incorporating robust encryption techniques and secure storage mechanisms to safeguard sensitive information. Additionally, stringent access controls and anonymization protocols are implemented to restrict unauthorized access and minimize the risk of data breaches. Regular privacy impact assessments are conducted to ensure ongoing compliance with GDPR regulations and other relevant data protection standards. We acknowledge the significance of continuously evaluating and enhancing our privacy and security measures, and we are committed to addressing this concern comprehensively in the system's design and implementation to guarantee the utmost protection for users' sensitive information.

Additional comments

8. Conduct extensive testing in diverse real-world scenarios to evaluate the system's effectiveness comprehensively. This should include stress testing for high transaction volumes and advanced penetration testing to simulate sophisticated insider attacks.

Response: Respected reviewer, Thank you for your insightful suggestion. In response, we have expanded our testing procedures to include extensive evaluations in diverse real-world scenarios. This encompasses stress testing for high transaction volumes and advanced penetration testing to simulate sophisticated insider attacks. These enhancements aim to provide a more comprehensive evaluation of the system's effectiveness in various challenging conditions. Your feedback has been crucial in strengthening the robustness of our proposed solution.

9. Engage with potential end-users and stakeholders (such as data protection authorities) to gather feedback and insights. This can help in fine-tuning the system to meet practical needs and regulatory expectations more effectively.

Response: Respected reviewer, we appreciate your valuable suggestion. To enhance the practicality and regulatory alignment of our system, we have initiated engagement with potential end-users and relevant stakeholders, including data protection authorities. This collaborative approach aims to gather valuable feedback and insights that will aid in fine-tuning the system to better meet practical needs and regulatory expectations. We believe this engagement will contribute significantly to the real-world applicability and acceptance of our proposed solution. Your feedback has been instrumental in guiding our efforts.

10. Investigate how the proposed system can be integrated with existing security infrastructures in organizations. Seamless integration is essential for widespread adoption and effectiveness.

Response: Respected reviewer, Thank you for your valuable input. In response to your suggestion, we have conducted a thorough investigation into the integration aspects of our proposed system with existing security infrastructures in organizations. We have emphasized the importance of seamless integration to facilitate widespread adoption and enhance overall effectiveness. We believe these enhancements align with your recommendation and contribute to the practical applicability of our proposed solution.