Response to Reviewer 2 Comments

This study focusing his work uses the Access Control Enabled Blockchain (ACE-BC) framework to enhance overall data security in Cybersecurity information sharing. Overall, the paper is good, however, there are few minor issues that must be addressed before the publication.

1. The CIS model needs more details explanations.

   Ans: Thank you for your constructive comment. The challenging tasks of internet networks are efficient data sharing and approved access control. Thus, the blockchain model is integrated with access control and cybersecurity information-sharing mechanisms to remove the problems in conventional policies. As a result, blockchain solves many more effective problems in providing data integrity, fairness, authenticity, security, and distribution. Smart contracts are utilized to handle access control and data sharing. Additionally, user behavior is monitored. Further, some permission stages are defined for the subject to access the object's service.

2. Figures qualities are low. Improve all figures, some are blurry.

   Ans: Thank you for your constructive comment. All figures quality have been improved

3. Author can look into some latest research on blockchains such as “Blockchain Technology: Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends ” (Electronics, 2023).

   Ans: Thank you for your constructive comment. Zhang Wenhua et al. [29] stated the evolution of medical care is moving into a new era with the creation of Health 5.0. Blockchain, as a technology solution, has decentralization, safe sharing, high privacy and non-tampering, which presents a breakthrough for the current bottleneck of EHR privacy and security development fresh viewpoint. Safeguarding patient medical information against cyberattacks and protecting privacy with verified access is one of the healthcare industry's most essential problems. While blockchain security is the cornerstone of healthcare growth, the future development of blockchain security can largely rest in technological applications, application extending, and monitoring models.

4. Simulation parameters need to discuss.

   Ans: Thank you for your constructive comment. The simulation parameters are related to the depiction of security specifications, which are defined in Table 1.

Table 1: Simulation Parameters

Parameter	Description
Block size	1MB
Transmission Range	300 meters
Message Size	1.5 GB
Total Number of Nodes	Random (10,000-30,000)
Number of Blocks	Random (100-250)
Security Protocols	AP, CKP
Traffic Type	Constant Bit Rate
Timestamp	128 bit

5. References formatting should follow the same text style as body. Check the overall formatting of MDPI journal.

Ans: Thank you for your comment Reference formatting has been modified

6. There are many instances where the language interferes with comprehensibility. The author should proofread and edit their manuscript for clarity.

Ans: Thank you for your constructive comment. Proofreading is done

I would like to thank Reviewer 2 for his time and suggestions. Hope the changes made in the revised manuscript can get his approval.