e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

DATA PRIVACY AND DATA PROTECTION BASED ON COMPUTING AND BLOCKCHAIN

Ekta. R. Pandey[*1]

[*1]Department Of Information Technology, BK Birla College Kalyan, Maharashtra, India.

ABSTRACT

As medical field advances there is severe need for healthcare providers and protection of confidential data entire globe. to protect this data and maintain the integrity of the system we tried creating a data protection and privacy using blockchain technology. Since it is powerful tool that allows multiple parties to securely access and share data. Given the numerable challenges that healthcare industry faces in digitizing and sharing health records, it is expected that many are attempting to improve healthcare process and data protection by using blockchain technology.

Keywords: Healthcare, Data Protection, Blockchain, Computing.

I. INTRODUCTION

Both the technology helps in securing the data storage accessing to the medical records. blockchain provides decentralized and temper proof system on the other cloud computing focuses on scalability and accessibility. Blockchain ensures data security through its decentralized and tamper-proof nature. Each transaction or data entry is recorded in a block, which is linked to the previous block, forming a chain. This makes it extremely difficult for anyone to alter or manipulate the data without detection. It adds an extra layer of trust and transparency to the system. Blockchain works on the networks of nodes. Each node has a copy of entire blockchain, making it impossible to manipulate for unauthorized person. Aditionally data is encrypted and linked together in a chain, to maintain security a transparency. Encryption work as system code which cannot be manipulated or accessed without a decryption key. In a simple word both the processes are like putting entire data in locked box that only authorized parties can operate.

II. METHODOLOGY

Aim of this article is to maintain data protection and privacy based on the techniques of cloud computing and blockchain.

Authorization and access control using Reencryption method in cloud computing..

When a cloud hospital needs to share the data authorization with another hospital, it needs to get the other's public key. Thus, it needs to generate a corresponding switch key for every user and then sends it to the cloud. When a user requests access to these data resources, the cloud will return the encrypted text of data and the corresponding key ciphertext according to the user's public key after verifying the identity authentication and authorization authentication, and the user decrypts these two ciphertext files to get the original plaintext resources of the corresponding data [27]. The cloud needs to generate a reencrypted ciphertext for every authorized user, and those unauthorized users have no right to obtain the reencrypted ciphertext of other users [28]. Even if unauthorized users do get the reencrypted ciphertext, they cannot decrypt the corresponding plaintext data. When applying ABE in proxy reencryption, it can authorize more than one user with the same group of attribute at a time.

Medical Data Privacy Protection Scheme Based on Blockchain and Cloud Computing.

In a medical data privacy protection scheme using blockchain, patient records are stored in a decentralized and tamper-proof manner. Each transaction or update to the records is recorded in a block, forming a chain. Access to the data is controlled using encryption and cryptographic keys, ensuring that only authorized individuals can view or modify the information. This helps maintain the privacy and security of medical data. It's like having a digital vault for sensitive healthcare information. Decentralized storage in blockchain means that instead of storing data on a single central server, the data is distributed across multiple nodes in the network. Each node has a copy of the entire blockchain, including the stored data. This redundancy makes it difficult for any single point of failure or unauthorized access. It's like having multiple copies of a book in different libraries to ensure its availability and security. RSA algorithm to prevent shared medical data from leaking. If an encrypted function only satisfies the addition homomorphism, it can only be added and subtracted; if an encrypted function only satisfies multiplicative homomorphism, it can only perform multiplication and division. The Paillier algorithm is homomorphic to addition, and the RSA algorithm is homomorphic to multiplication. In an untrusted cloud storage, when the confidentiality of data cannot be guaranteed, the proxy reencryption part is used for reencryption, and the part is used for authorization. In the untrusted open environment of the third party, it can ensure the confidentiality of sensitive data in cloud storage. In homomorphic encryption, the private key encrypts medical data and only the client has the public key. In the keys generated by using proxy reencryption, even if a malicious attacker gets one of them, the attacker still needs another different key for decryption. If the attacker gets all these encrypted data, he cannot decrypt and get the original plaintext data between the client and the server. This also makes sure that even the processor cannot access the information of the data. The algorithms begin with initialization and outputs from the central authentication center the pair of public and key keys, the master key of the center, the public key of the system, and the common parameters.

III. MODELING AND ANALYSIS

What are the difficulties faced by healthcare industry in data protection?

When conducting a simulation experiment, we use the data of the patient’s routine medical checks. The data is a 25-dimensional vector, and the numerical value of every dimension can be seen in Table 1. In order to complete every encryption task τ, the processor of the encryption task ρT will firstly receive a 25-dimensional medical data vector. Then, it encrypts every element in the vector and sends the encrypted result to the cloud node ENT where it is located. As this scheme uses the frameworks of Hadoop and Spark in the side of cloud computing, it has higher storage and computing abilities. It can respond in a timely manner to the requests of users and complete the uploading, computing, and downloading operations of users, so it can achieve the purpose of dynamic sharing and patient privacy protection.

/ireless Communications and Mobile Computing

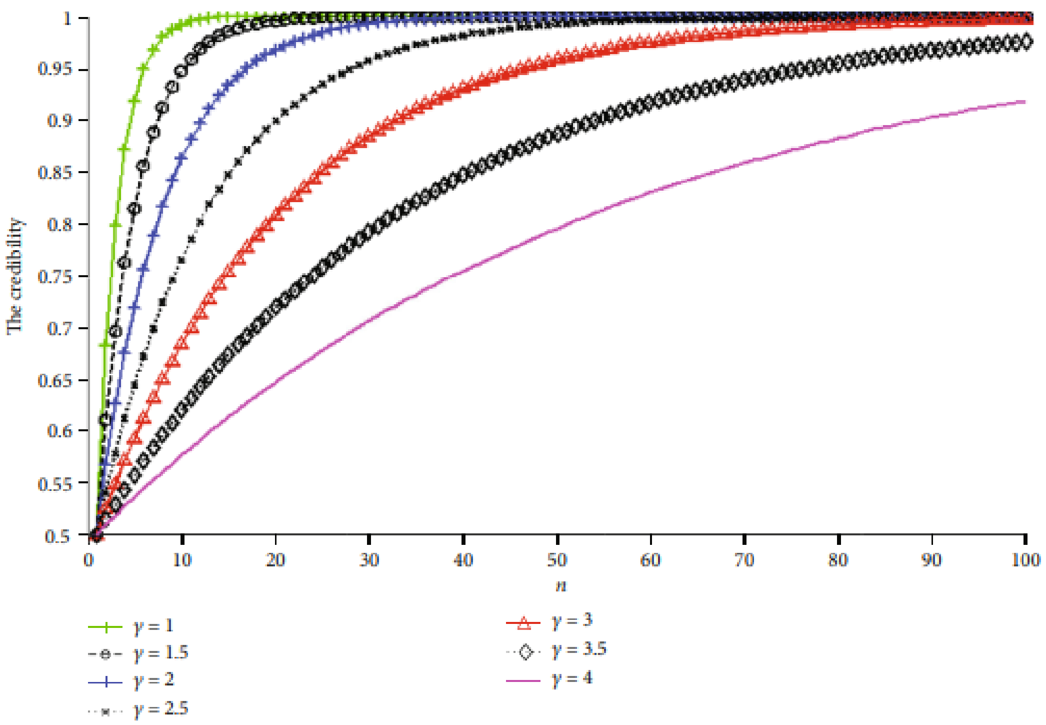

Figure 1: Impact of η on credibility.

IV. RESULTS AND DISCUSSION

When it comes to the result and discussion of medical data privacy using cloud computing and blockchain, several benefits arise. Cloud computing provides scalability and accessibility to medical data, allowing healthcare providers to efficiently store and access patient information. Blockchain, on the other hand, ensures the security and integrity of the data through decentralization and encryption. By combining these technologies, medical data can be securely stored, accessed, and shared while maintaining patient privacy. It's like having the best of both worlds for data privacy and accessibility in healthcare. Some common data security threats in cloud computing include unauthorized access to data, data breaches, insecure APIs, data loss or leakage, and insider threats. It's important to implement strong authentication mechanisms, encryption, regular security audits, and access controls to mitigate these risks. Additionally, choosing reputable cloud service providers with robust security measures can help ensure the safety of your data in the cloud. Stay vigilant and proactive in protecting your data. In addition to providing flexible and scalable resources, cloud computing offers many advantages, such as scalability and flexibility in terms of processing capacity and storage. These benefits have added cloud computing's growth in popularity across a range of business industries. In recent years, this approach has appeared to have been accepted in the health care industry. In the popular literature, at a minimum, there is an increasing number of articles and publications by healthcare IT companies, while cloud computing for therapeutic diagnostics is also gaining momentum in scientific study.

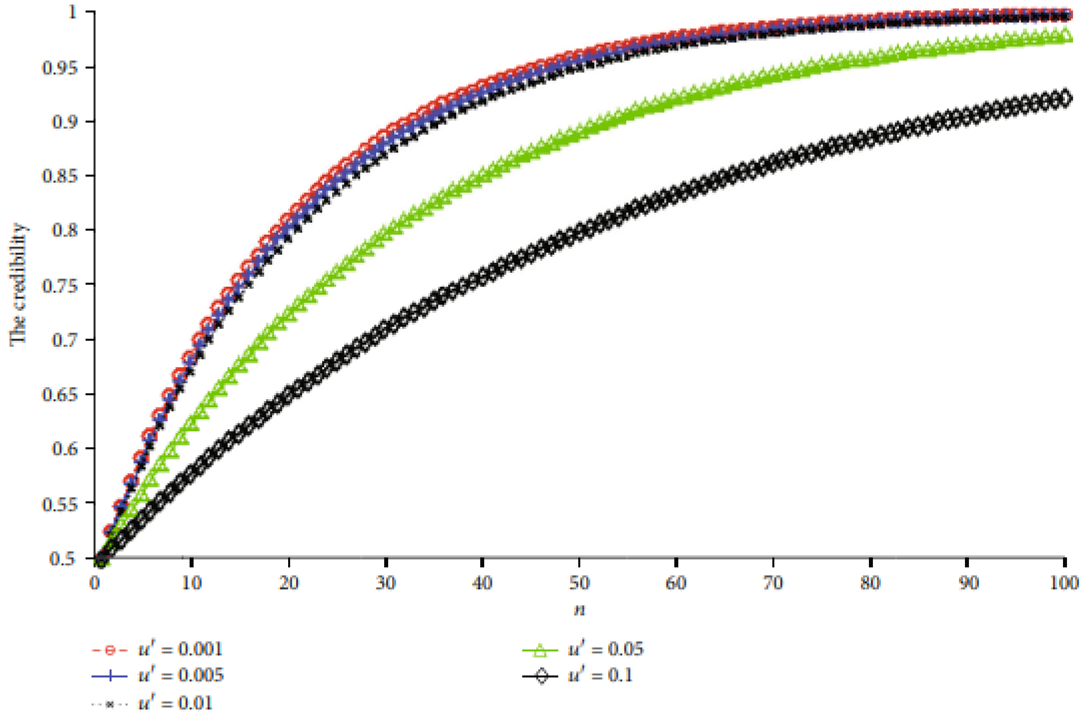

Figure 2: Impact of u′ value on credibility

V. CONCLUSION

Blockchain is a brand-new decentralized distributed database, and it is a series of data blocks by using cryptographic methods. In this paper, we combined two encryption methods: proxy reencryption and attribute-based encryption and built key technical solutions for cloud computing based on blockchain to be applied in security and privacy protection of distributed medical data. It can not only achieve integrity testing of cloud data but also achieve broader security encryption computing. Intelligent hospitals only need to give the proxy key to the cloud server, which can convert medical data into the encrypted text in the designated format. The fixed client can access these shared data resources with their private key at any time. Even if the cloud server has the proxy.

ACKNOWLEDGEMENTS

I would like to give my acknowledgment and warmest welcome the tutor of my research methodology mam. For providing entire help from beginning till publishing of our research paper without her active participation and enthusiast this could never have been completed. And also great appreciation to all my reference bodies working in the backend of this research paper.

VI. REFERENCES

[1] https://www.researchgate.net/publication/345747105_A_Medical_Data_Privacy_Protection_Scheme_Based_on_Blockchain_and_Cloud_Computing.

[2] https://www.hindawi.com/journals/wcmc/2020/8859961/

[3] https://www.sciencedirect.com/science/article/abs/pii/S221478532203098X#:~:text=Blockchain%20will%20facilitate%20effective%20data,has%20been%20their%20latest%20interest.

[4] https://www.iwriteessays.com/example/acknowledgement-sample

[5] H. Liang, J. Zou, K. Zuo, and M. J. Khan,"An improved genetic algorithm optimization fuzzy controller applied to the well head back pressure control system," Mechanical Systems and Signal Processing, vol. 142, p. 106708, 2020.

[6] H. Zheng, W. Guo, and N. Xiong, "A kernel-based compressive sensing approach for mobile data gathering in wireless sensor network systems," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 12, pp. 2315–2327, 2018.

[7] Z. Wan, N. Xiong, N. Ghani, A. V. Vasilakos, and L. Zhou, "Adaptive unequal protection for wireless video transmission over, P. Liu, X. Zhang, and F. Neri, "Cloudassisted secure eHealth systems for tamper-proofing EHR via blockchain," Information Sciences, vol. 485, no. 6, pp. 427– 440, 2019.

[8] https://www.hindawi.com/journals/wcmc/2020/8859961/#conclusion

[9] https://www.google.com/search?q=blockchain+technoogy+for+healthcare+based+on+cloud&rlz=1C1YTUH_enIN1018IN1019&oq=blockchain+technoogy+for+healthcare+based+on+cloud&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIJCAEQIRgKGKABMgkIAhAhGAoYoAEyCQgDECEYChigATIMCAQQIRgKGBYYHRgeMg4IBRAhGAoYDxgWGB0YHtIBCTMzMDQzajBqNKgCALACAA&sourceid=chrome&ie=UTF-8

[10] L. Huang, J. Zheng, and G. Tan, "Research on task scheduling convergence non-dominated sorting method in cloud computing," International Journal of Grid Distribution Computing, vol. 8, no. 1, pp. 237–246, 2015.