International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 3s,2025
https://theaspd.com/index.php

Secure Data Sharing For Collaborative Medical Research

Chiranjeev Singh[1], Sarvaree Bano[2], Abha Grover[3]
[1]Assistant Professor, Department of Pharmacy, Kalinga University, Raipur, India. ku.chiranjeevsingh@kalingauniversity.ac.in, 0009-0005-3854-8324
[2]Assistant Professor, Department of Chemistry, Kalinga University, Raipur, India.
[3]Assistant Professor, New Delhi Institute of Management, New Delhi, India., E-mail: abha.grover@ndimdelhi.org, https://orcid.org/0009-0008-2828-2149

Abstract
Sharing medical data can enhance teamwork, accessibility, and patient care, which will ultimately result in better results and more effective healthcare delivery. Due to the delicate nature of medical data, strong privacy and secrecy are required. Despite the exploration of access control approaches, data privacy issues persist and call for additional solutions. Using private set intersection and key aggregation encryption, the proposed study presents a privacy-preserving data-sharing approach that strikes a compromise between security and secrecy, safeguarding sensitive information while it is being shared. We conduct both formal and informal security studies, demonstrating the resilience of Burrow-Abadi-Needham logic to potential adversarial attacks. The study compares the suggested scheme against current ones in terms of security, computational complexity, and time complexity using a cryptography library to assess execution time. The suggested plan exhibits encouraging outcomes, providing high security and efficiency while safeguarding data privacy and permitting secure, adaptable medical data exchange, making it a useful tool for the industry.

Keywords: *medical data sharing; key aggregate encryption; private set intersection*

1. INTRODUCTION

Internet today is highly important to everyone. Through this internet all users exchange the information to other users. In internet, data is in the form of images, audio, video, text, handwritten text, graphic objects, animations and others [1]. Further, data exchange is insecure and unreliable in internet. Therefore, some researchers have proposed some algorithms, data security techniques and methods. In the Internet age, the most up-to-date technology to keep an enormous volume of Internet data is to save the data in the Cloud. Cloud Computing is one among the real-time outsourcing strategies to store Internet data in the Cloud. Cloud is a destination to accumulate an enormous volume of Internet data [2]. The data is gathered with lesser effort and with unreal resources, with data admittance anywhere at any point (for instance, different applications, software systems, Hardware systems and innovative operating environments) [9]. The operational settings and the applications are changed and re-designed based on the type of data, and hence allowing best surroundings utilization, affirming a changing burden. The implementation is subject to the environment condition and other competence relevant thereto, while trustworthy relies on the service rendered by the adaptive service level method. The information obtained from various information technologies, applications and various technology, and the information is drawn from outside sources like the web. Above features will promptly shift from a conventional business in which it manages the Cloud in private to virtual operation [3]. The first account is the Cloud facilities to identify the virtual undertaking, which is the most critical component of Cloud Computing. Then exploring the togetherness to obtain business process outsourced, Cloud Computing encompasses the whole task of business entity to an unbiased gathering provider, and then relates its supporting management. Cloud computing is relating as a protective measure to represent contemporary on-interest in computing facilities to different business middlemen like Amazon, Google and Microsoft. Infrastructure is the centric component of the Cloud. It represents the model to become popularized for computing. It facilitates the business and individuals to receive different accessed applications on the globe on the basis of interest [13]. Most specialized methods of Cloud computing granted in the current methods results in improve, probable and most economic services with certain specific feature and they are implemented with different means, for instance, multi-tenancy and virtualization. The methods are incorporated with cloud service and implemented with many models and are more specialized towards security threats [4]. Security threats and weaknesses are incorporated with certain possibilities in conventional IT infrastructure [10]. The risk to confidentiality ranges from the structured risks of traditional IT naturally or by severity or in some cases both. Virtualization and multi-tenancy methods employ a resource shared by multiple users. The methods bring forth quick and optimized administrative resources, yet the processes lay out certain security issue in the system [5].

2. MATERIAL AND METHODS

Although Weighted Attribute-Based Encryption (ABE) increases the flexibility of access policies, it presents difficulties for data owners who want privacy control [11]. To strike a compromise between privacy and flexibility while exchanging medical records, especially in collaborative e-health systems, a cloud-based solution was suggested [6]. By using AND-weighted ABE, the method strengthens security and selective access by limiting access to data to users who are members of target organizations. In order to solve privacy concerns and interagency mistrust in medical record access and sharing, a patient-centered EMR sharing strategy was put out. It makes use of a dual-blockchain system and identity-based verification. By assigning complicated search tasks to cloud servers, existing attribute-based searchable encryption techniques pose serious security risks by compromising data user privacy, allowing data manipulation, and producing incorrect results. They addressed this by implementing an anonymous ABSE scheme based on blockchain technology to enhance the security of data exchange. Created a KASE-based framework for cloud-based integrated healthcare systems that facilitates the sharing of electronic health records. They discovered flaws in the existing systems, namely the lack of keyword untrace ability and safe multi-user permission [7].

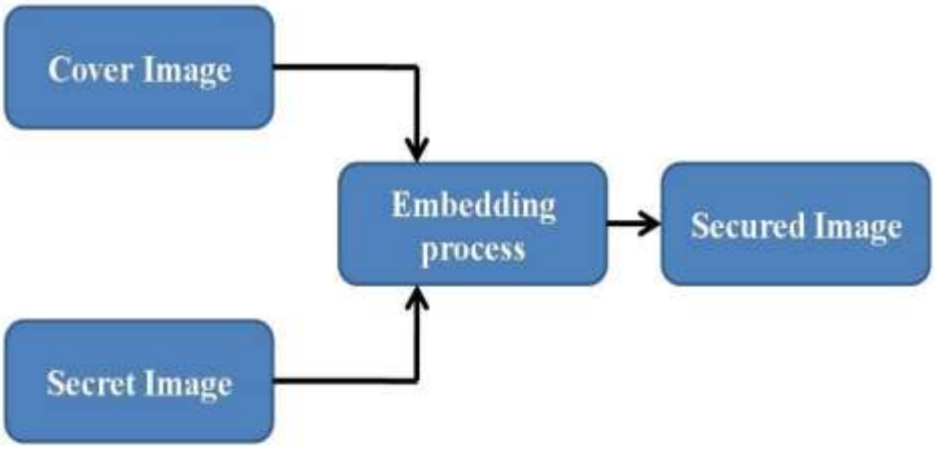

Figure 1: Proposed flow

This approach preserves the privacy of the features that satisfy the access requirements by concealing the access policy's features. To further improve the security and credibility of electronic transactions, the scheme incorporates blockchain technology with ABSE to provide features like non-repudiation, integrity checking, and tamper-proofing. suggested the SAMA scheme, which was created to solve the shortcomings of the current approaches to wearable device data aggregation and exchange [15]. The SAMA system seeks to give numerous data owners and requesters an easy-to-use, private, and adaptable solution [14]. By combining multi-key partial homomorphic encryption with ciphertext-policy ABE, it provides wearable technology with strong data confidentiality, user-centric access control, and effective data processing[8]. demonstrated the dearth of research on concerns related to user identity privacy during key creation [12].

3. RESULT AND DISCUSSION

Given the sensitive nature of medical data, potential information leakage through attributes and access control remains a serious privacy issue despite developments in secure medical data sharing, necessitating additional attention and solutions. This concern hinders the establishment of safe data sharing habits, then limits comprehensive data analysis and collaboration. To facilitate cooperation between different owners of data and propel medical research, it is important to give top priority to safeguarding each entity's data privacy [8].

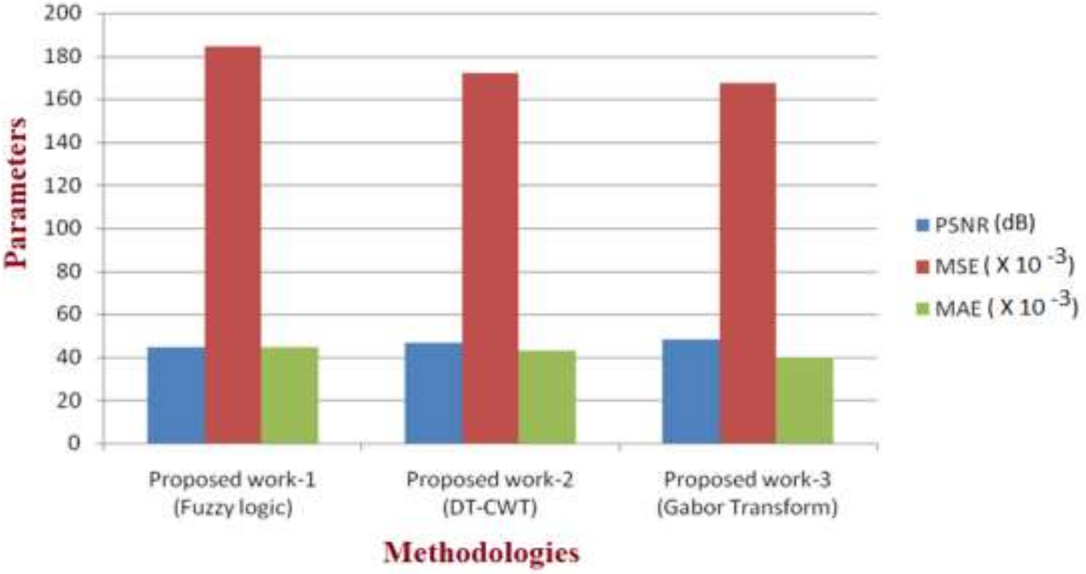

Figure 2: Graphical illustrations of performance comparison

We use private set intersection and key aggregation encryption to assure data security and stop the leaking of sensitive information, and we restrict data sharing to only the information that is absolutely essential.

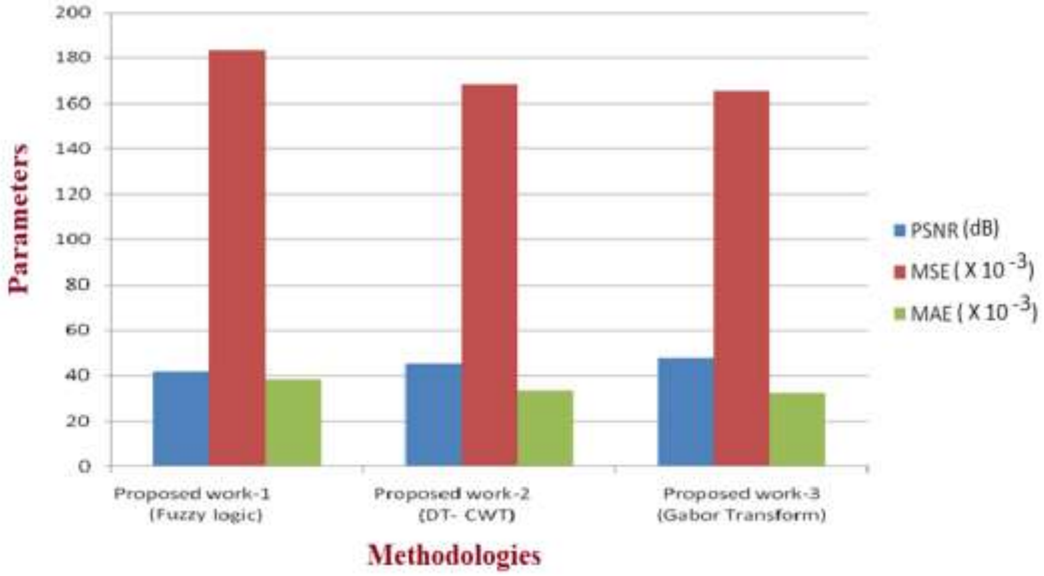

Figure 3: Graphical illustrations of performance comparison

In response, they developed a decentralized ciphertext-policy ABE approach specifically designed to improve the secure sharing of confidential medical data in blockchain-enabled healthcare systems. By distributing the master key throughout the entire set of attribute nodes on the blockchain, their strategy improved upon Shamir's threshold secret sharing, increasing system resilience and thwarting hostile attacks.

4. CONCLUSION

Furthermore, after the recommended strategy is put into practice, we will organize research to strengthen resistance to these security dangers because the development of quantum computing technology may present an advanced degree of security threats. With the acceleration of contemporary technological advances and with growing digitalization in the field of medicine, a tremendous amount of both voluminous and variegated medical data has developed over the last century. Though providing extreme flexibility in the management of data and access rights, they too pose serious problems with respect to data privacy and thus require diligent scrutiny from alternate viewpoints. Through access control systems, privacy breaches can occur both by exposing the sensitive information due to attribute values or by giving away the data-related information per se that arose due to the need for users of data to determine the wished-for data first before asking a key for accessing it from its owner. Users may turn to unsafe techniques like accessing cloud servers if data owners conceal information about their data, jeopardizing efficiency and security. They addressed issues with data access and security by using Key Aggregate Searchable Encryption (KASE) and putting forth a framework that includes linear secret sharing to enable secure and dynamic searchable encryption

REFERENCES

1. Hulsen, Tim. "Sharing is caring—data sharing initiatives in healthcare." International journal of environmental research and public health 17, no. 9 (2020): 3046.
2. Nazarova, J., & Bobomuratov, T. (2023). Evaluating the Clinical Utility of Genetic Testing in Guiding Medication Selection. Clinical Journal for Medicine, Health and Pharmacy, 1(1), 64-72.
3. Shen, Meng, Junxian Duan, Liehuang Zhu, Jie Zhang, Xiaojiang Du, and Mohsen Guizani. "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds." IEEE Journal on Selected Areas in Communications 38, no. 6 (2020): 1229-1241.
4. Donkor, K., & Zhao, Z. (2023). Building Brand Equity Through Corporate Social Responsibility Initiatives. Global Perspectives in Management, 1(1), 32-48.
5. Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "A cloud based solution for collaborative and secure sharing of medical data." International Journal of Enterprise Information Systems (IJEIS) 14, no. 3 (2018): 128-145.
6. Nair, S., & Rathi, D. K. (2023). Development of Graphene-Based Membranes for High-Performance Desalination. Engineering Perspectives in Filtration and Separation, 1(1), 9-12.
7. Doel, Tom, Dzhoshkun I. Shakir, Rosalind Pratt, Michael Aertsen, James Moggridge, Erwin Bellon, Anna L. David, Jan Deprest, Tom Vercauteren, and Sébastien Ourselin. "GIFT-Cloud: A data sharing and collaboration platform for medical imaging research." computer methods and programs in biomedicine 139 (2017): 181-190.
8. Desai, P., & Joshi, V. (2023). Bridging Traditional and Modern Medical Terminologies Integrative Perspectives from Ayurveda and Allopathy. Global Journal of Medical Terminology Research and Informatics, 1(1), 12-15.
9. Barrett, Jeffrey S. "Data Sharing and Collaboration." Fundamentals of Drug Development (2022): 431.
10. Gopi, M., Manikandan, S., Shevaksri, P., & Anguraj, S. (2023). Enabling Authorized for Multi-Authority Medical Database. International Journal of Advances in Engineering and Emerging Technology, 14(1), 179–184.
11. Huang, Qinlong, Licheng Wang, and Yixian Yang. "Secure and privacy-preserving data sharing and collaboration in Mobile healthcare social networks of smart cities." Security and Communication Networks 2017, no. 1 (2017): 6426495.
12. Rajan, V., & Chawla, R. (2024). Anthropometric Variations and Adaptations across Diverse Ecological Zones. Progression Journal of Human Demography and Anthropology, 2(1), 1-4.
13. Liang, Xueping, Juan Zhao, Sachin Shetty, Jihong Liu, and Danyi Li. "Integrating blockchain for data sharing and collaboration in mobile healthcare applications." In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp. 1-5. IEEE, 2017.
14. Baggyalakshmi, N., Dhanya, R., & Revathi, R. (2024). HR Onboarding Kit. International Academic Journal of Innovative Research, 11(1), 27–38. https://doi.org/10.9756/IAJIR/V11I1/IAJIR1104
15. Jin, Hao, Yan Luo, Peilong Li, and Jomol Mathew. "A review of secure and privacy-preserving medical data sharing." IEEE access 7 (2019): 61656-61669.