Communication Papers of the 20th Conference on Computer Science and Intelligence Systems (FedCSIS) pp. 19–24
DOI: 10.15439/2025F3484
ISSN 2300-5963 ACSIS, Vol. 45

# Enhancing Research Data Integrity Through Blockchain: Design and Implementation of a Web Based Management System

Sikandar Ali*
*School of Advanced Studies, Center of Neuroscience
University of Camerino
Email:sikandar.ali@unicam.it

Roberto Ciccocioppo†, Massimo Ubaldi †,
Andrea Morichetta‡, Matteo Piersantelli§
† School of Pharmacy,Center for Neuroscience, Pharmacology Unit
‡School of Science and Technology, Computer Science Division
†‡University of Camerino, §AM Microsystems Srl.
Email: {roberto.ciccocioppo@unicam.it, massimo.ubaldi@unicam.it,
andrea.morichetta@unicam.it, info@am-microsystems.com}

***Abstract*—In this digital age, data driven research has become indispensable. Ensuring secure and transparent experimental data management remains a key challenge. Blockchain technology with its decentralized architecture, immutability and resistance to tampering, presents a viable solution to these problems. This paper presents a blockchain based web management system designed to streamline the handling and integrity of experimental research data. Leveraging the capabilities of blockchain technology enables the system to ensure data integrity. A critical aspect of research is data, by securely storing file hashes on decentralized network. This blockchain based web-system allows users to login with its credentials and upload experimental data in form a csv file and associate it with respective universities and supervisors of the user. Later the system allows the supervisor to login with its credentials to access the file for further analysis. Upon file upload, the system will calculate the hash of the file and stored on blockchain network. This approach guarantees the immutability and authenticity of the uploaded research data. The system prevents tampering and ensures transparency of the experimental data, which is paramount in academic research. The proposed system addresses the growing need for secure and efficient data management in research, providing a reliable solution for maintaining data integrity throughout the research cycle.**

## I. Introduction

BLOCKCHAIN is a digital distributed ledger. The functionality of blockchain is continually increasing because of decentralized networks, lack of reliance on trust, unchangeable storage and ability to share information anonymously. In experimental research, particularly in behavioral neuroscience, maintaining the integrity and authenticity of data is very important. This paper presents a web-based system designed to store and manage experimental data in csv file, which can range in GBs. These files capture critical data which are translated into results, such as the drinking pattern of rats, observed through a micro controller-based system. This experimental data includes parameters like device ID, timestamp and liquid consumption, which are crucial as every recorded value impacts the final analysis. These datasets, often stored as CSV file, must remain unaltered to ensure unbiased, reliable results. After all, this data forms the basis for published finding, peer review, future studies. Even minor alteration could mislead entire research communities wasting time and resources. To address these challenges, we have developed a blockchain based web management system that not only sure data integrity but also make sure the traceability of data. Blockchain locks records in place, making unauthorized changes impossible. Every adjustment if allowed gets permanently logged, so anyone can trace the data's history. This transparency builds trust, journals and collaborators can verify that the numbers/data haven't been tweaked post experiment. More importantly, it enforces reproducibility, a cornerstone of good science. If other labs can't replicate results because the original data was altered, the entire study lost credibility. With research ethics under increasing scrutiny, blockchain offers a simple fix, which is immutable proof that data stays fair from collection to publication. The data stored in blockchain is immutable and transparent for the whole network [1]. Blockchain technology is changing and enables alternative approaches like tamper proof credentialing and decentralized learning system [2]. Currently many institutions still rely on collecting data either on paper or centralized data management systems. However, this form of medical system is highly prone to privacy breach [3]. Therefore, the transformation of centralized data management system to decentralized data management system is an irresistible trend [4]. However, most of the system stores and maintain their experimental data either on their server or on papers it also wastes a lot of resources [5]. Therefore, in this paper a blockchain based system has been proposed, which maintains experimental data integrity and the key feature of the system is blockchain technology for data authentication. When file uploaded on server it will calculate the hash of the file and stored on blockchain network. The data (hash of the file) will be stored via smart contracts. The smart contract is a digital set of rules that are automatically executed when predetermined terms and conditions are met. The smart contract was written in solidity language and deployed on

This work was supported by AM Microsystems srl

network, so web system can communicate with blockchain through it. The system calculates the hash of experimental data file and stored on server as well as on blockchain networks and then for authentication, it compares both hashes of a file which is stored on server as well as on blockchain network. If the hash matches that means data is authenticated successfully and file is unaltered. Otherwise, the system will flag the file as altered while showing error message on screen. This ensures that any unauthorized modification to data is immediately detected. This system provides a robust mechanism of data integration. This system combines server-based technology for storage and access control whereas blockchain technology is used for authentication.

## II. Literature Review

Continuous and rapid development of blockchain technologies, Different features have been proposed for web-based system for maintaining the integrity[6]. A blockchain based web 3.0 system has been developed to manage the educational documents and certificates, particularly the issuance of student degree. The certificates and degrees have been issued to students without the use of centralized system. The verification process has been conducted by using Ethereum smart contracts and degree has been issued to students and as it's a decentralized system, it maintains data integrity [7]. Similarly, In another blockchain-based health contract management system has been proposed for dealing the health-related certificates by interacting with smart contracts. In this study, a blockchain based system has been proposed by the author to negotiate contracts between health insurance companies and end user. Once the contract has been finalized then it will be stored on blockchain network, because of its immutable feature [8]. In another related paper, Author has developed a time release encryption system, in which information has been stored using asymmetric key encryption without needing help from external agents. However, the study has some limitations such as changing the difficulty based on prime numbers . Additionally, the researchers discovered some new methods such as proof of semantics to develop web [9]. A decentralized blockchain based medical record system has been proposed to handle EHR. Med-Rec architecture has a modular design in which authorization, administration privileges and data sharing are among the participants [10]. Med-block was a block chain-based hybrid architecture to protect electronic health records. The architectural node of the system is divided into storing nodes, submission nodes and endorsement nodes [11]. A generic blockchain based architecture has been proposed for storing patient electronic health records [12]. EHR blockchain architecture secures the environment and stops, tempering of electronic health record by tracking all the events in blockchain networks [13]. In their study, researcher has proposed Blockchain based system called men shared. The system was able to minimize the risk of data privacy and can be used to solve the problem of data sharing among data custodians in an untrusted environment[14]. An alternative method was used by researchers, in which a private blockchain based data sharing scheme has been proposed.This system has used a consortium blockchain to save the index of security [15]. A data management and sharing platform has been proposed by combining artificial intelligence and blockchain based technologies. This plate form has used the transparency of the zone chain for data tracking, and it also ensures the data remain unaltered [16].This paper has proposed hybrid approach, ensures compatibility with existing management systems, maintains operational efficiency and provides tamper proof verification of data existence at a specific time. The blockchain timestamps server as definitive, publicly auditable evidence of data priority, effectively deterring misappropriation and protecting intellectual property claims prior to the dissemination of results.

## III. Methodology

The blockchain based web management system has been developed for collecting experimental data. The front end of the web system has been developed by using html5 and css with Bootstrap. The back end up of the system has been developed in PHP core. The smart contract has been written in solidity language and deployed on Ethereum blockchain via sepolia testnet. Smart contracts will act as a bridge between blockchain network and web-based system. The system is mainly divided into two parts, one experimental data management system and the other part is validating the experimental data through blockchain technology to maintain its integrity.

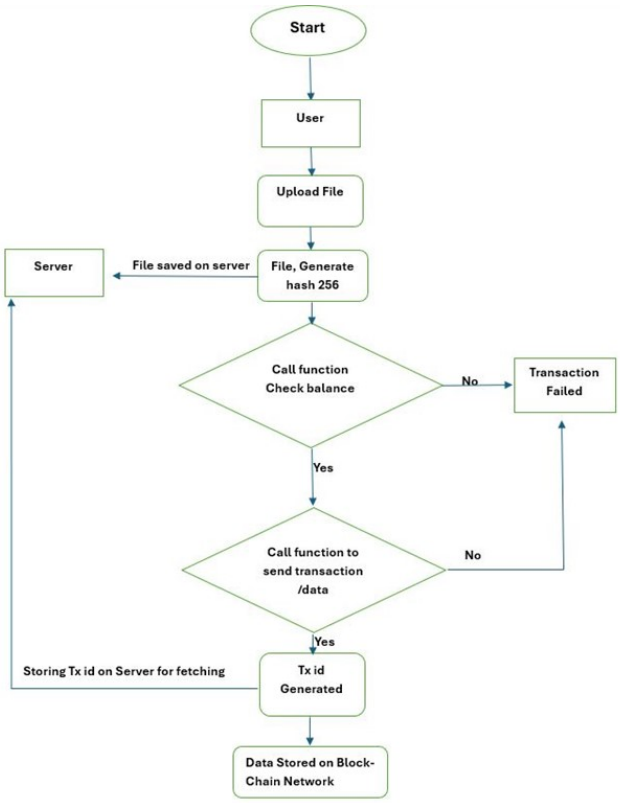


Fig. 1. Shows Flow chart for Storing Hash on Blockchain Network.

Figure 1 shows the flow chart in which the authorized user (student) can login with their credentials and upload their experimental data file on server with other details related to experiment. The file will be selected, and other experimental data will be written and uploaded. The system will calculate the hash of the file before uploading the file to the server. The file is then uploaded on the server and the database has been updated. Calculated hash will then be sent on blockchain network by calling a function. This function will communicate with smart contract, which was written in solidity language and deployed on ethereum testnet sepolia. The transaction (TX) has different parameters like nonce, gas price, gas limit, to (smart contract), value, data and chain id. The check balance function will be called which make sure the gas price would be enough for the transaction. If the gas price is not enough then it will generate errors of not enough gas price. If the price is enough then the system will generate a new transaction and signed with private key and sent onto the network. If the transaction is not successful then it will generate errors, otherwise the system will generate TX (Transaction) id through consensus mechanism, which will be stored in database.

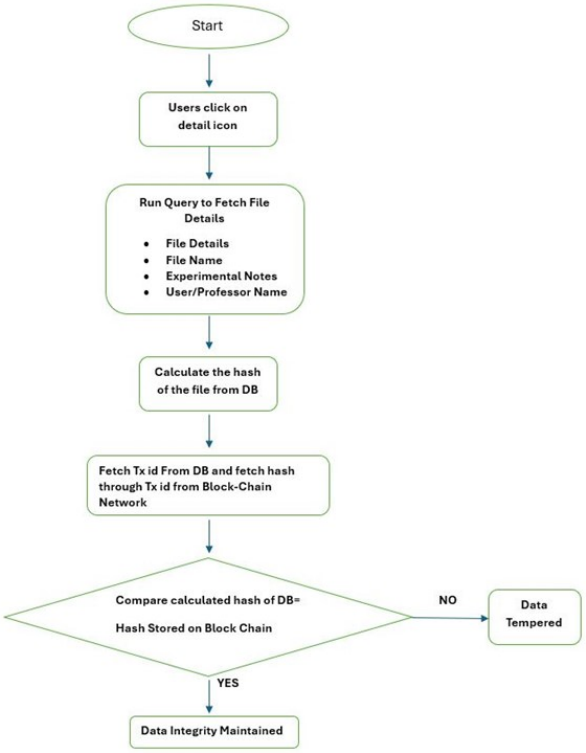


Fig. 2. Shows Flow chart of Data Integrity Process.

Figure 2 shows the flow chart for web management system for data authentication. The user (Professor->hierarchy level two) will click on details. It will run the SQL query to fetch the details related to that file such as file name, experimental notes and supervisor name. The system calculates the hash of the fetched file from server/database and also fetch its transaction id. The system will use web3 API to retrieve the hash stored on blockchain network by using tx id. The system will compare the calculated hash of the file which is retrieved from the server with the hash stored on Ethereum blockchain network. If they matches, the system will display message of data integrity, which means data is intact, otherwise it will display an error message saying data is altered.The system has been divided into three level hierarchies, which were administration (admin), student and Professor. These three different hierarchies have different permission levels.

## IV. Implementation

This section explains the implementation of the tool as well as explains the different hierarchical level and how GUI base authentication process works for authenticating the experimental data.

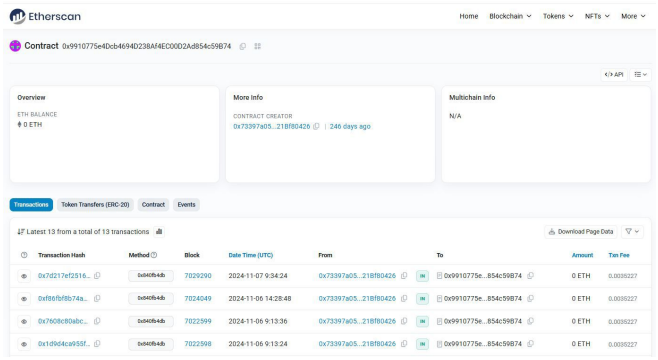


Fig. 3. Shows the successful deployment of smart contracts on blockchain networks.

Figures 3 shows the successful deployment of smart contracts in blockchain networks. To ensure smooth communication between the web-based management system and the blockchain network, the smart contract was written. The smart contract was developed to facilitate the hash storage and retrieval of hash from the blockchain network.

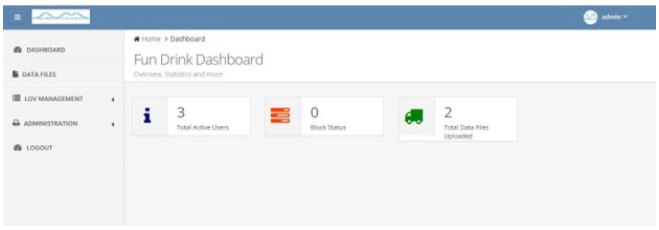


Fig. 4. shows the GUI of admin.

Figure 4 shows the admin graphical user interface. The administration has the ultimate power in this system. The admin can see all the data uploaded in the system and can see the detailed information such as total no of active users, total number of files uploaded, and has authority to block users. He can update the institution lists as well as create new users and assign them one of the hierarchies according to their position.

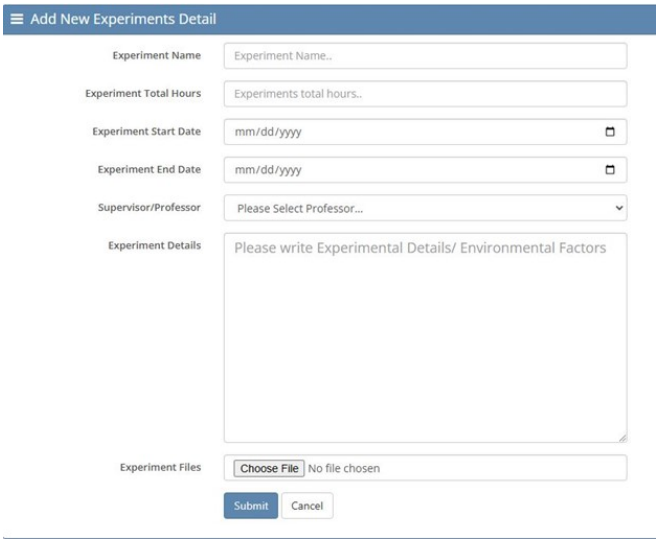


Fig. 5. Shows the GUI of student's experimental data entry Form.

Figure 5 shows the graphical user interface of the student view. The authorized student can log into their account and upload the conducted experimental file by selecting his supervisor. The user can also add more details like experiment name, total number of hours, experiment start and end dates, and can add notes in experimental detail section. Once the file has been uploaded then user will no longer has access or authority to delete file from system. Only user has access to read the files he has uploaded. He can only view them.

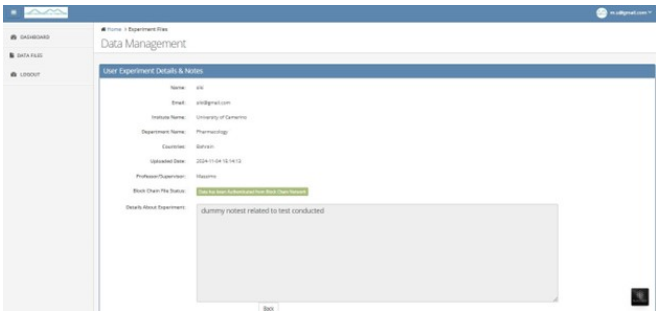


Fig. 6. Shows the GUI of Professor View Portal.

Figure 6 shows the graphical user interface of the professor's view, in which he can look into details of uploaded file with blockchain authentication. This detailed view shows the details of the experiments like the name of the student who has conducted this test, his email, his institution, uploaded date and the professor's name with additional experimental notes and it shows the statement that this file has been authenticated through a blockchain network, which shows the data integrity. The professor can analysis the file after downloading it or on the web by clicking analysis web icons for short files up to 10,000 data points.

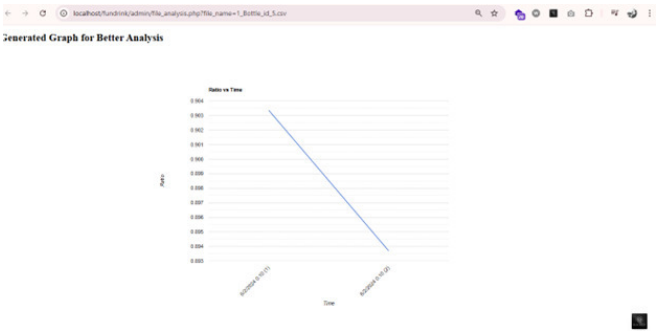


Fig. 7. Shows the data analysis of file on website.

Figure 7 shows the GUI of web-based tool analysis. This web-based system can be used to analysis the experimental data. The system can plot the graphs up to ten thousand points but after that it will run out of cache memory, therefore it halts. Detailed analysis of the file could be done through MATLAB or by using python-based script for analysis by using Matplotlib libraries.

## V. Validation of Tool

This section shows the validation of the implemented web management system that shows the error free implementation of blockchain technology, which ensures the integrity of experimental data stored by the user. This section presents the different key stages of processes like generation of Transaction id (TX ID), hash comparison and data integrity verification process.

### A. Transaction ID Generation

The system will calculate the hash upon uploading the experimental data and store the file hash on blockchain network. A transaction id TX will be generated as proof that data (hash) has been recorded on blockchain network. Figure 8 shows the generated transaction id on blockchain network, and this transaction id has been stored in database for further reference.

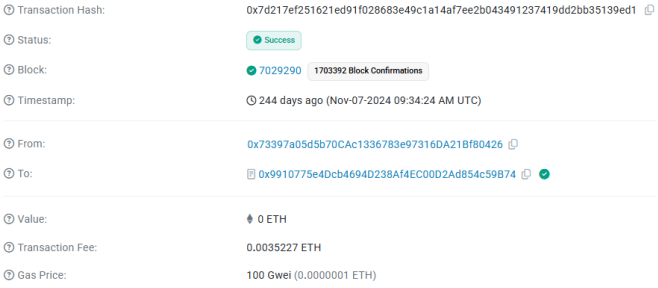


Fig. 8. Shows transaction records on block chain network.

### B. Verification on the Block Chain Network

To verify the integrity of the stored experimental data. The system will retrieve the hash stored on the blockchain networks

and compare it with the hash of the file stored on the server. Figure 9 shows a message stating that the hash has been successfully matched, indicating that the experimental data have not been altered.


Fig. 9. Shows the message conforming hash match and experimental data integrity.

If the hash doesn't match in that case the system will detect the potential tampering in experimental data and alert the user by message on screen. Figure 10 shows message, which states that the blockchain hash doesn't match with hash of the file stored on server.

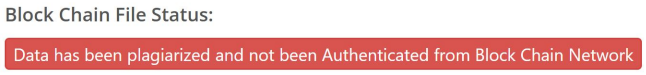


Fig. 10. Shows the message indicating data tempering.

### C. System Performance

The system has successfully maintained the data integrity of experimental data by using blockchain based web system. The use of transaction id for fetching the data and hash comparison method ensures that any unauthorized modification to the experimental data can be detectable. The results confirm the system has achieved its primary goal of data integrity.

## VI. Conclusion

The development of blockchain based web management system has been successfully implemented for storing and managing experimental data. This system addresses the critical challenges of maintaining data integrity by using blockchain technology. The use of cryptographic hashing provides the robust mechanism for detecting unauthorized modification in data. The system ensures the integrity of data by verifying it. The validity of the system has been conducted through series of tests like calculation of hash while uploading file secondly generation of transaction id then storing the cryptographic hash on blockchain network and verification of data integrity through hash comparison. The validation process shows that the system successfully identifies the tampered data, while conforming to the integrity of experimental data files, which were unaltered. This system has a strong need in academic and research fields where the reliability of experimental data is paramount. In future work. This system should focus on the scalability of the system so that the system can handle large datasets. In addition, exploring the implementation of other decentralized technologies that could improve the security and efficiency of the system. Overall, this project shows the potential of blockchain technology in ensuring data security / integrity and providing a particular solution for managing experimental data in research environment.

## VII. Acknowledgment

We thank AM Microsystems for the collaboration to this study. The author Sikandar Ali was supported by fellowship from the Eureka program of the Region Marche, Italy. The work was supported by PRIN-PNRR2022 -P202274WPN (to RC), PRIN-2022 20227HRFPJ (to RC), MNESYS (PE0000006)- Project AMSUD 2024, PRIN 2022X9X5MS (to MU).

## References

[1] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, Q. Li, and Y.-C. Hu, "Make web3. 0 connected," *IEEE transactions on dependable and secure computing*, vol. 19, no. 5, pp. 2965–2981, 2021.

[2] J. Bhattacharya, "What is web 3.0? the future of the internet," Single Grain, 2022, accessed: Dec. 2022. [Online]. Available: https://www.singlegrain.com/Web3.0/web-3-0/

[3] X. Zhang and Y. Wang, "Retracted article: Research on intelligent medical big data system based on hadoop and blockchain," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, p. 7, 2021.

[4] H. Li, D. Han, and M. Tang, "A privacy-preserving storage scheme for logistics data with assistance of blockchain," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4704–4720, 2021.

[5] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[6] S. K. Shawon, H. Ahammad, S. Z. Shetu, M. Rahman, and S. A. Hossain, "Diucerts dapp: a blockchain-based solution for verification of educational certificates," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 2021, pp. 1–10.

[7] Z. Sun, D. Han, D. Li, X. Wang, C.-C. Chang, and Z. Wu, "A blockchain-based secure storage scheme for medical information," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 40, 2022.

[8] E. Chondrogiannis, V. Andronikou, E. Karanastasis, A. Litke, and T. Varvarigou, "Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100049, 2022.

[9] F. Yang and X. Yuan, "Toward timed-release encryption in web3 an efficient dual-purpose proof-of-work consensus," *arXiv preprint arXiv:2205.09020*, 2022.

[10] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd international conference on open and big data (OBD)*. IEEE, 2016, pp. 25–30.

[11] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *Journal of medical systems*, vol. 42, pp. 1–11, 2018.

[12] A. F. da Conceição, F. S. C. da Silva, V. Rocha, A. Locoro, and J. M. Barguil, "Eletronic health records using blockchain technology," *arXiv preprint arXiv:1804.10078*, 2018.

[13] G. Yang and C. Li, "A design of blockchain-based architecture for the security of electronic health record (ehr) systems," in *2018 IEEE International conference on cloud computing technology and science (CloudCom)*. IEEE, 2018, pp. 261–265.

[14] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[15] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of medical systems*, vol. 42, no. 8, p. 140, 2018.

[16] S. Zhang, A. Kim, D. Liu, S. C. Nuckchady, L. Huang, A. Masurkar, J. Zhang, L. Tseng, P. Karnati, L. Martinez *et al.*, "Genie: a secure, transparent sharing and services platform for genetic and health data," *arXiv preprint arXiv:1811.01431*, 2018.