SECURE REVIEWING AND DATA SHARING IN SCIENTIFIC COLLABORATION: LEVERAGING BLOCKCHAIN AND ZERO TRUST ARCHITECTURE

Saniya Taranum[1], Samreen Sultana[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, saniyatarannum02@gmail.com
[2]Asst Professor, Department of CSE, Shadan Women's College of Engineering and Technology, samreencme@gmail.com

To Cite this Article
Saniya Taranum, Samreen Sultana, "Secure Reviewing And Data Sharing In Scientific Collaboration: Leveraging Blockchain And Zero Trust Architecture", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 09, September 2025,pp: 139-150, DOI: http://doi.org/10.64771/jsetms.2025.v02.i09.pp139-150
Submitted: 08-08-2025 *Accepted: 10-09-2025* *Published: 17-09-2025*

ABSTRACT
Secure and transparent data exchange is essential to scientific collaboration, yet openness and secrecy are frequently lacking in traditional peer review and collaboration processes. In order to provide an auditable, decentralized review process and guarantee safe data exchange among users, this study suggests a blockchain-driven system coupled with Zero Trust Architecture (ZTA). Evaluations are made more trustworthy by limiting access to sensitive articles to authorized reviewers and collaborators through the use of a fine-grained access control mechanism (ACM). ZTA principles also reduce the hazards associated with hierarchical architectures by preventing unwanted access. Beyond the review process, this method strengthens the credibility of reviewers and encourages participation through author feedback, improving secure data exchange in publications, grants, and research collaborations. Finally, by guaranteeing integrity, security, and transparency in peer review and data exchange, the suggested architecture opens the door for decentralized scientific collaboration.

1. INTRODUCTION

Scientific collaborations and review systems for international partnerships should make data sharing easier, provide a private peer review mechanism for assessing the results critically, and be transparent and auditable with partnership-beneficial regulations. These crucial elements. Peer review, which confirms the legitimacy and credibility of the science, is essential to the expansion of scientific knowledge. Despite being touted as a key factor in improving the caliber of publications, it is nevertheless opaque. Because blockchain technology is inherently immutable, experts have suggested integrating it with scientific publication systems in light of the rapid advancements in IT. Due to blockchain's immutability, research datasets are suggested to be integrated with patent healthcare data review comments.

The application of secrecy in the review process and the exchange of research data are not covered by the current effort, despite the improvement in the traceability of the review process. Researchers suffer for a whole year as a result of the reviewers' breach of confidentiality. Some of the main problems with the current review management system are fake reviews, lack of verifiability, manipulation susceptibility, and privacy difficulties. Therefore, secrecy in manuscript submission to reviewers and review comments is required by the review process. Accordingly, sharing private study data must be done with caution to prevent violating the Health Insurance Portability and Accountability Act (HIPAA) or endangering the identity of participants. Blockchain technology can be used to assure record retention even when smart contracts are destroyed, making records auditable.

The gathered data becomes stagnant and eventually experiences a lock-in effect if research materials are not exchanged. Additionally, data owners may have a variety of expectations about their data, such as a desire for affiliations with organizations with which they have memorandums of understanding (MoUs) or time-limited cooperation agreements. In line with the findings of Dutra et al., who found that only one-third of writers submitted the needed data for systematic literature work, these expectations may differ depending on the geographical origins

of the data owners. A Zero Trust Architecture is ingrained in the data access scenario to account for divergent viewpoints.

Therefore, the work focuses on assessing requests for data access and secure data sharing, which are crucial for the reproducibility and verifiability of science. Therefore, access control mechanisms can be used to effectively monitor the access activities of data or resources under valid, allowed conditions. Strengthening the privacy of research data and peer review secrecy is crucial. The work suggests addressing sensitive data access requests, sharing for scientific collaborations, and secrecy in the blockchain-based review process. Because it includes cooperation between untrusted parties, the effort uses blockchain-based smart contracts to implement access control mechanisms.

In order to prevent cyber incidents on data silos, AES encryption symmetric key created using HKDF techniques and including Lagrange Interpolation for consensus between multi-partied data ownership are used to ensure that unauthorized users cannot access the secret data. The following is a summary of the work's contributions: 1) Taking care of confidentiality during the review process to guarantee that the author, editor, and designated reviewers handle unpublished manuscripts securely and cooperatively. 2) The Zero Trust (ZT) architecture is being proposed for processing requests for access to secret data, guaranteeing accountability of context-based opinions among different data owners in different hierarchies.
3) To guarantee private data exchange following ZT approval. 4) To take author comments on review comments into account when making recommendations to the editor for future reviewers.

1.2 SCOPE OF THE PROJECT

This project's scope includes creating a safe and effective blockchain-based framework to handle issues with access control and confidentiality in collaborative data sharing and the scientific review process. In order to control and enforce access permissions among untrusted parties participating in the evaluation and publication of scientific publications, smart contracts are implemented on the blockchain. The project incorporates Lagrange Interpolation to reach an agreement on multi-party data ownership, as well as the use of Advanced Encryption Standard (AES) for data protection and symmetric key generation.

1.3 OBJECTIVE

This project aims to improve the selection of future reviewers and streamline the review process by integrating author data and guaranteeing the safe exchange of private information after Zero Trust validation. The project's overall goal is to use cutting-edge cryptography and blockchain technology to increase the efficiency, security, and confidentiality of scientific partnerships and review procedures.

1.4 PROBLEM STATEMENT

The integrity of assessments and the privacy of sensitive material are threatened by the present publishing environment's lack of accountability and openness in the review process. Blockchain technology provides a decentralized way to create visible and auditable records, but it falls short in addressing the crucial problems of safe data exchange and secrecy that are necessary to promote productive scientific partnerships. This paper suggests a Zero Trust Architecture-informed fine-grained access control model that improves data security and takes contextual viewpoints into account in order to get over these drawbacks. In order to increase reviewer involvement and legitimacy, the study also presents an incentive system based on author comments.

2. EXISTING SYSTEM

- The current publication environment frequently suffers from ineffective review procedures and opacity.
- In real-world situations, blockchain systems' conventional consensus methods may not always work as well. For instance, Proof of Work is infamous for its high energy consumption and lengthy transaction times, making it unsuitable for real-time review processes even though it is secure.
- Despite being more energy-efficient, Proof of Stake may still have problems with the concentration of power among larger stakeholders, which could jeopardize equity.

EXISTING SYSTEM DISADVANTAGES

- Sensitive data may not be adequately protected by conventional access control methods like Mandatory Access Control (MAC) or Role-Based Access Control (RBAC).
- Current models of access control may be inflexible and inflexible.

3. RELATED WORK

Research and educational opportunities have been made possible via cyberspace. However, academic, research, and personal data—particularly proprietary designs—are the targets of cyberattacks. It is suggested that blockchain be used to prevent collision attacks. VeDB and LedgerDB, which Yang et al. proposed, allow applications that use blockchain solely for its immutability and non-repudiation characteristics to be moved to these platforms for improved throughput and scalability. However, the existing workarounds require the usage of smart contracts in addition to other blockchain properties like immutability and non-repudiation in order to enforce the access control policy. Yang et al. have contrasted Hyperledger fabric implementations with the use of centralized ledgers for record auditability and verification.

Therefore, as smart contracts continue to enforce access control policies, it is imperative that automated vulnerability detection be implemented. The work's focus is on scientific review and cooperation systems, where topics including data sharing, access control policies, and review procedures are covered. According to reviewer literature, the proposed work determined the necessity of data sharing and review process confidentially. By utilizing passwords to secure sensitive data, confidentiality can be guaranteed. The reviewer may occasionally share the unpublished work with his peers.

The designated reviewer may occasionally ask his research assistant to evaluate the articles. However, it may be deemed a breach of confidentially if the journal is not notified of this and the editor fails to verify that the designated research assistant is free from conflicts of interest. There have been instances where reviewers have released an unpublished work's rough draft into the public domain. Therefore, it was concluded that the decentralized scientific review process greatly needed a means to maintain confidentiality. Numerous papers have underlined the necessity of confidentiality in the peer review procedure. However, publishing houses like PeerJ, Nature Plos, Brien et al. do not address how to incorporate the same. suggested work that is comparable to PeerJ, which conducts reviews and requires writers to keep the name of the reviewer anonymous. The NIH requires reviewers to sign a confidential agreement. Tenorio-Fornés et al. used Dapp to propose an open review system.

4. PROPOSED SYSTEM

- The work suggests addressing sensitive data access requests, sharing for scientific collaborations, and secrecy in the blockchain-based review process.
- Because it includes cooperation between untrusted parties, the effort uses blockchain-based smart contracts to implement access control mechanisms.
- The implementation of confidentiality in the review process, Zero Trust architecture for gaining data access, and secure data sharing on transit are proposals for processing confidential data access requests that ensure accountability of context-based opinions between various data owners in varying hierarchy.

PROPOSED SYSTEM ADVANTAGES

- The proposed ACM uses contextual considerations to make real-time access decisions, increasing flexibility and security.
- Enhanced confidentiality, and the deployment of a fine-grained access control mechanism, guided by the Zero Trust Architecture.

5. MODULES EXPLANATION AND DIAGRAM

User Interface Design

Users must enter their username and password in order to connect to the server; only then may they do so. If the user has already left, they can log in directly; if not, they must register their information on the server, including their username, password, email address, city, and country. To maintain the upload and download rate, the database will generate an account for every user. The user ID will be assigned to the name. Usually, logging in allows you to access a certain page. The query will be searched and displayed.

Editor

Ensuring the integrity, quality, and clarity of material across several platforms is the goal of an editor. Editors fix mistakes and improve readability by checking drafts for accuracy, coherence, and adherence to rules. They oversee the submission and review process, promote ethical standards, and help authors and publishers communicate.

Admin

Our project's third module is called Admin. Here, the administrator will log in using the ID and password that the BC operator created. You will be taken directly to the admin home page after logging in. An administrator's job is to supervise and control the functioning and operations of a system, project, or organization. Administrators are in charge of organizing work, enforcing rules, and making sure that procedures function properly.

Owner

The Owner module is the fourth one in our project. Here, the owner will enter their hospital email address and password to log in. Following login, the author can upload his data immediately from the home page. Users should ask the author personally if they would like access to their data. A smart contract will be generated once the author accepts the user's request.

User

Our project's fifth module is called "User." Here, the user will enter their password and email address to log in. The user can search his data on the main page after logging in, and related data will be displayed. He or she should ask the author for access to the data,

Smart Contract

A self-executing contract with its terms directly written into computer code is called a smart contract. When specific conditions are met, it operates on a blockchain network and independently enforces and implements the terms of the contract. Smart contracts reduce the need for middlemen and the chance of fraud or errors because they are decentralized, transparent, and immutable.

TECHNIQUE USED OR ALGORITHM USED

Access control mechanism (ACM)

The key structure for controlling and managing access to resources in a system is called an Access Control Mechanism (ACM), which makes sure that only systems or people with permission can use or interact with those resources. Authentication, which confirms the identity of users or systems seeking access, and authorization, which establishes what actions authenticated users or systems are allowed to carry out in accordance with predetermined rules or policies, are usually two of the mechanism's essential elements. To enforce these rights, ACMs employ a variety of access control mechanisms. Whereas Attribute-Based Access Control (ABAC) grants access based on attributes like department or clearance level, Role-Based Access Control (RBAC) bases permissions on user roles inside an organization.

BlockChain

Blockchain technology is a distributed, decentralized ledger system that makes it possible to retain transaction records in a safe, transparent, and impenetrable manner. It functions by keeping information in "blocks," which are connected in a chain. Each block includes a list of transactions as well as a cryptographic hash of the block before it. This makes data extremely safe against fraud and tampering by guaranteeing that once it is captured, it cannot be changed or removed without changing the entire chain. Blockchain technology, which was first created as the foundation for cryptocurrencies like Bitcoin, has since spread to a number of sectors, including voting systems, supply chain management, healthcare, and finance, thanks to its capacity to enable trustless transactions devoid of middlemen.

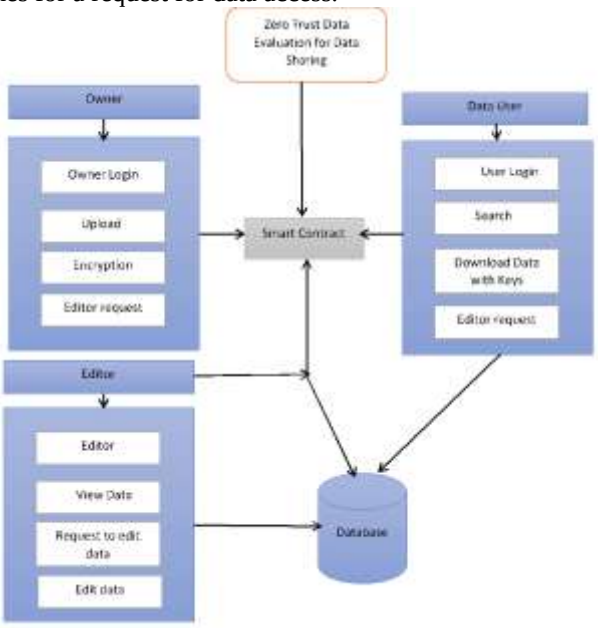
A. Smart Contract

A distributed, decentralized ledger system called blockchain technology enables the safe, transparent, and impenetrable retention of transaction records. It works by storing data in "blocks," which are linked together to form a chain. A cryptographic hash of the previous block and a list of transactions are included in every block. This ensures that once data is collected, it cannot be altered or deleted without altering the entire chain, making it incredibly safe against fraud and tampering. Due to its ability to facilitate trustless transactions without the need for middlemen, blockchain technology—which was initially developed as the basis for cryptocurrencies like Bitcoin—has subsequently expanded to a variety of industries, including voting systems, supply chain management, healthcare, and banking.

SYSTEM ARCHITECTURE

Zero trust indicates that trust must be gained, not that the system is without it. When a user requests a service, they must specifically demonstrate their trustworthiness through their research profile or a combination of

checks like two-factor authentication. The existing body of research requires that ACP be deployed using smart contracts. However, a smart contract's access policy cannot be changed once it has been implemented. A few components of the access control policy may need to be changed, particularly in light of shifting research tendencies. The current system takes into account the Zero Trust Architecture's (ZTA) dynamic access control policy. ACP deployed via smart contract is activated for the access of service after the trust score has been determined. The inability of the data owner to gauge the capability of the researcher and his intentions is a crucial aspect for scientific collaborations. The work suggests input policies for calculating trust scores using this paradigm. The list of attribute inputs, PLi, and assigned weight-age, which is determined by the data owners, make up the policy engine. Sample guidelines for a request for data access.



PoliciesPLi weights are determined by the context relevance for granting access to data requests. The research institute, the head of charge, and researchers all play different responsibilities in multi-party data ownership.

7. RESULTS AND DISCUSSION

Fig 7.1: Home Page

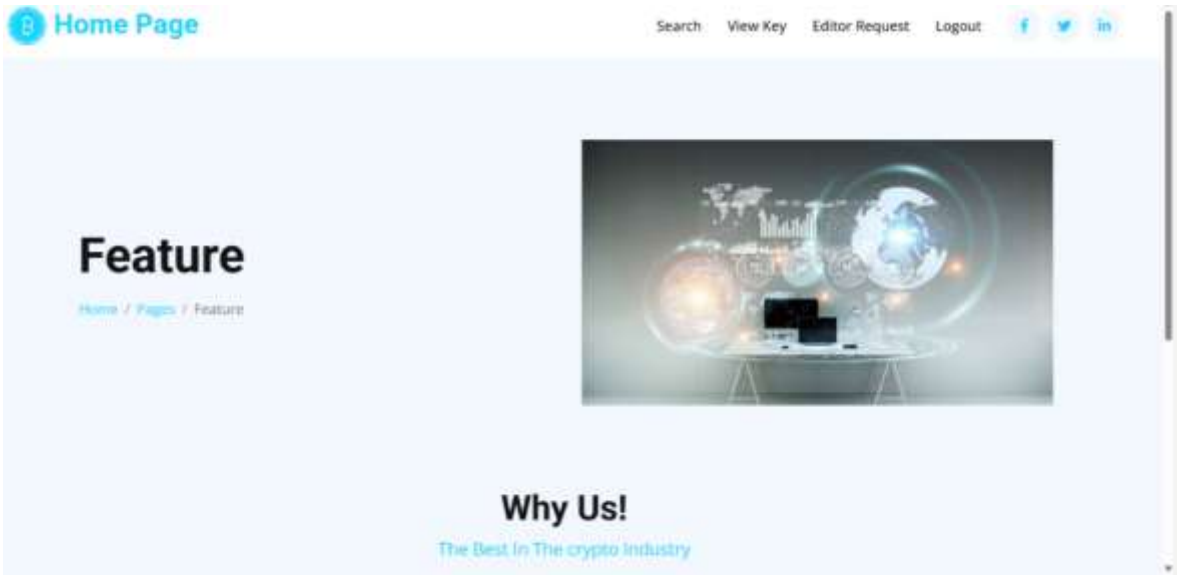


Fig 7.2: Feature Page

Fig 7.3: File searching

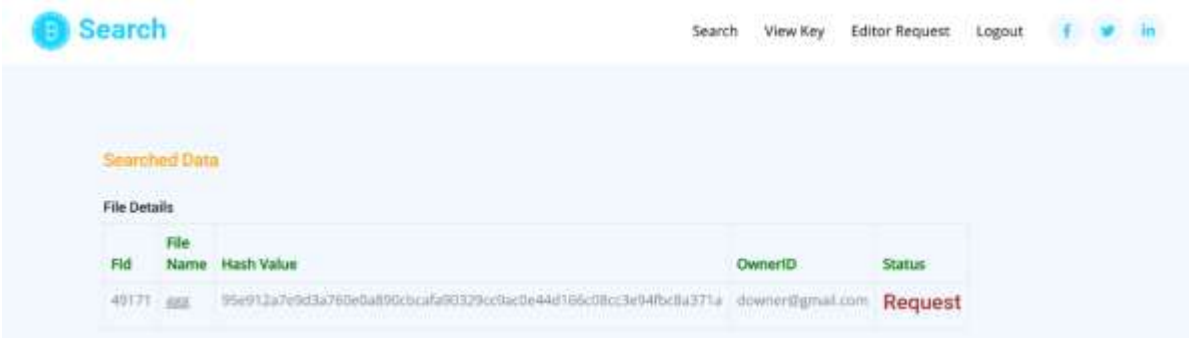


Fig 7.4: Search Data

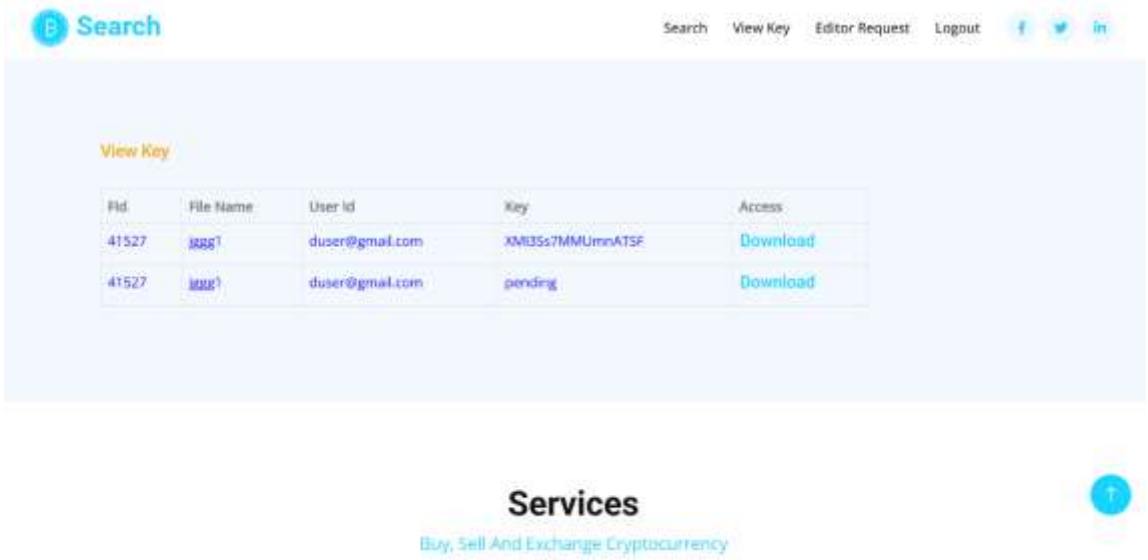


Fig 7.5: View Key

Fig 7.6: Key Verification.

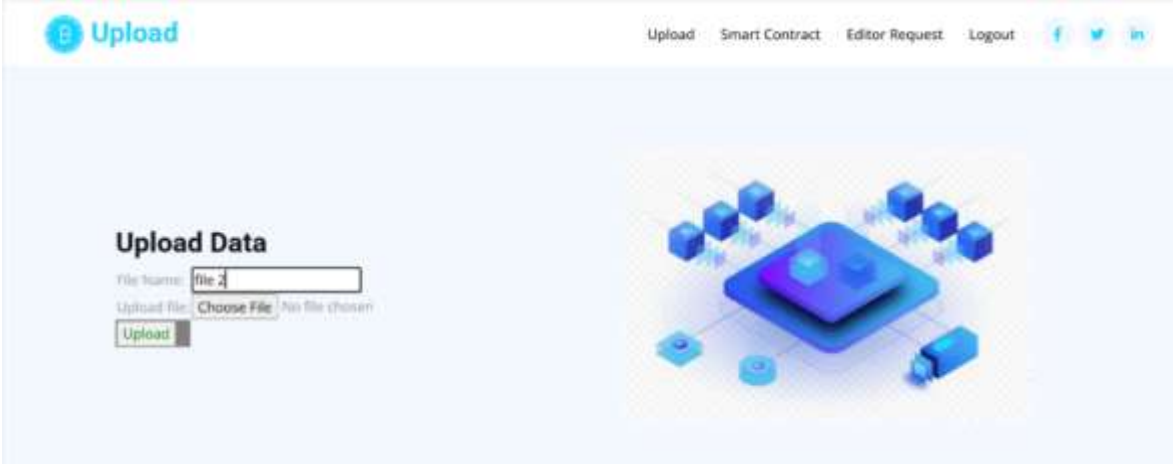


Fig 7.7: Upload Data.

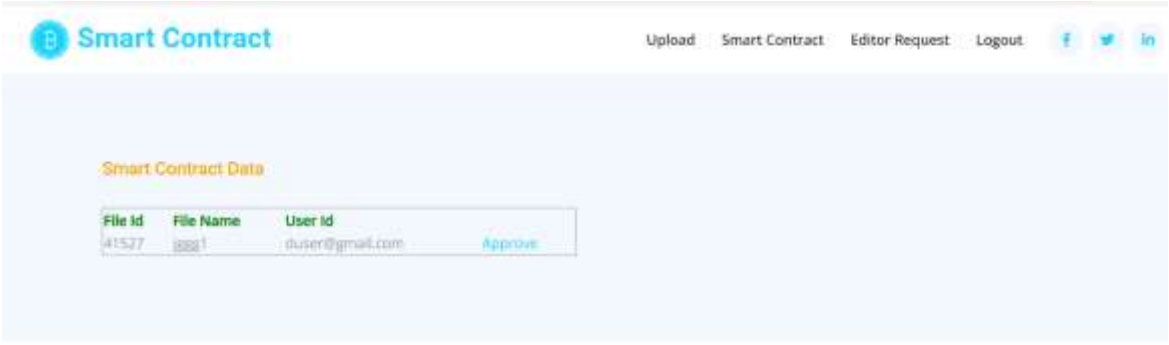


Fig 7.8: Smart Contract.

Fig 7.9: Editor Request.

Fig 7.10: View Data

8. FUTURE ENHANCEMENT

In order to further strengthen secrecy, efficiency, and flexibility, future improvements to scientific collaboration and review systems (SCRS) may concentrate on incorporating cutting-edge technologies and approaches. The use of machine learning (ML) and artificial intelligence (AI) to improve access control and smart contract functionality is one possible development. AI could be used to provide a more responsive and adaptable security framework by dynamically modifying access rules in response to real-time data and behavioral patterns.

.

9. CONCLUSION

The system of scientific collaboration and review includes data sharing among collaborators as well as a critical evaluation procedure. Since both procedures handle sensitive data, secrecy is necessary. For a decentralized review system, BC guarantees traceability, integrity, and auditable data; nevertheless, the implementation of an access control mechanism via smart contract is essential to guarantee secrecy. The key management procedure and encryption standards are discussed for the same's implementation. The zero trust architecture encourages the data owner to establish the requirements for data access. ZTA enables customizable and fine-grained access control to protect data and prevent unauthorized users from accessing it. Encryption standards were also used to ensure confidentiality when transferring data in transit.

REFERENCE

[1] D. Strang and K. Siler, ‘‘Revising as reframing: Original submissions versus published papers in administrative science quarterly, 2005 to 2009,’’ Sociol. Theory, vol. 33, no. 1, pp. 71–96, Mar. 2015.

[2] F. Bianchi and F. Squazzoni, ‘‘Can transparency undermine peer review? A simulation model of scientist behavior under open peer review,’’ Sci. Public Policy, vol. 49, no. 5, pp. 791–800, Oct. 2022.

[3] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi, ‘‘The revolution of blockchain: State-of-the-art and research challenges,’’ Arch. Comput. Methods Eng., vol. 28, no. 3, pp. 1497–1515, May 2021.

[4] M. Mwamba Merlec, N. Kabulo Sinai, and H. Peter In, ‘‘A blockchainbased trustworthy and secure review system for decentralized e-Portfolio platforms,’’ in Proc. 14th Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Oct. 2023, pp. 675–680.

[5] H. Li and M. Li, ‘‘Patent data access control and protection using blockchain technology,’’ Sci. Rep., vol. 12, no. 1, p. 2772, Feb. 2022.

[6] Y.-T. Huang, D.-L. Chiang, T.-S. Chen, S.-D. Wang, F.-P. Lai, and Y.-D. Lin, ‘‘Lagrange interpolation-driven access control mechanism: Towards secure and privacy-preserving fusion of personal health records,’’ Knowledge-Based Syst., vol. 236, Jan. 2022, Art. no. 107679.

[7] S. Tanwar, D. Ribadiya, P. Bhattacharya, A. R. Nair, N. Kumar, and M. Jo, ‘‘Fusion of blockchain and IoT in scientific publishing: Taxonomy, tools, and future directions,’’ Future Gener. Comput. Syst., vol. 142, pp. 248–275, May 2023.

[8] Y.-M. Teng, K.-S. Wu, and Y.-C. Lee, ''Do personal values and motivation affect women's solo travel intentions in Taiwan?'' Humanities Social Sci. Commun., vol. 10, no. 1, pp. 1–12, Jan. 2023.
[9] C. Woo and J. Yoo, ''Exploring the determinants of blockchain acceptance for research data management,'' J. Comput. Inf. Syst., vol. 63, no. 1, pp. 216–227, Jan. 2023.
[10] S. Murrinl, ''Nih has acted to protect confidential information handled by peer reviewers, but it could do more,'' U.S. Dept. Health Human Services Office Inspector Genera, Washington, DC, USA, Tech. Rep. OEI-05-19-00240, 2020.
[11] COPE Case Number: 14–06. (2014). Possible Breach of Reviewer Confidentiality. Accessed: Oct. 29, 2023. [Online]. Available: https://publicationethics.org/case/possible-breach-reviewerconfidentiality .
[12] COPE Case Number: 11-29. (2011). Reviewer Asks Trainee to Review Manuscript. Accessed: Oct. 29, 2023. [Online]. Available: https://publicationethics.org/case/reviewer-asks-trainee-reviewmanuscript#
[13] Case Number: 13-15. (2013). Online Posting of Confidential Draft by Peer Reviewer. Accessed: Oct. 29, 2023.
[14] J. S. Yadav, N. S. Yadav, and A. K. Sharma, ''Security analysis of smart contract based rating and review systems: The perilous state of blockchain-based recommendation practices,'' Connection Sci., vol. 34, no. 1, pp. 1273–1298, Dec. 2022.
[15] C. Silpa, P. Prasanth, S. Sowmya, Y. Bhumika, C. H. S. Pavan, and M. Naveed, ''Detection of fake online reviews by using machine learning,'' in Proc. Int. Conf. Innov. Data Commun. Technol. Appl. (ICIDCA), Mar. 2023, pp. 71–77.
[16] C Council. (Sep. 2017). Cope Discussion Document: Who Owns Peer Reviews?. Accessed: Feb. 29, 2023.
[17] IEEE Publication Services and Products Board Operations Manual 2023. Accessed: Oct. 1, 2023. [Online]. Available: https://pspb. ieee.org/images/files/PSPB/opsmanual.pdf
[18] WA Learning and T Channel. (Apr. 12, 2010). Step by Step Guide to Reviewing a Manuscript. Accessed: May 1, 2023. [Online]. Available: https://authorservices.wiley.com/Reviewers/journal-reviewers/ how-to-perform-a-peer-review/step-by-step-guide-to-reviewing-amanuscript.html
[19] (2023). Guidelines for Reviewers. [Online]. Available: https://www. mdpi.com/reviewers10.
[20] B. K. Rai, ''PcBEHR: Patient-controlled blockchain enabled electronic health records for healthcare 4.0,'' Health Services Outcomes Res. Methodology, vol. 23, no. 1, pp. 80–102, 2023.
[21] D. D. F. Maesa, P. Mori, and L. Ricci, ''A blockchain based approach for the definition of auditable access control systems,'' Comput. Secur., vol. 84, pp. 93–119, Jul. 2019.
[22] R. Hashem, A.-R. I. Mubarak, and A. Abu-Musa, ''The impact of blockchain technology on audit process quality: An empirical study on the banking sector,'' Int. J. Auditing Accounting Stud., vol. 5, no. 1, pp. 87–118, 2023.
[23] V. Schlatt, J. Sedlmeir, J. Traue, and F. Völter, ''Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of E-prescription management,'' Distrib. Ledger Technol., Res. Pract., vol. 2, no. 1, pp. 1–31, Sep. 2023.
[24] A. Carvajal, ''A comparative study of commitment of collaboration (COC) and memorandum of understanding (MOU) as instruments in driving successful partnerships in ASEAN member countries,'' Int. J. Open-Access, Interdiscipl. New Educ. Discoveries ETCOR Educ. Res. Center (iJOINED ETCOR), vol. 20, no. 3, pp. 503–20496, 2023. [Online]. Available: https://etcor. org/storage/iJOINED
[25] N. D. dos Reis, C. M. Ferreira, M. T. Silva, and T. F. Galvão, ''Frequency of receiving requested data for a systematic review and associated factors: A cross-sectional study,'' Accountability Res., vol. 29, no. 3, pp. 165–177, Apr. 2022.
[26] Z. Liu, X. Li, and D. Mu, ''Data-driven zero trust key algorithm,'' Wireless Commun. Mobile Comput., vol. 2022, pp. 1–9, Mar. 2022.
[27] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, ''A survey on access control in the age of Internet of Things,'' IEEE Internet Things J., vol. 7, no. 6, pp. 4682–4696, Jun. 2020.
[28] R. Jiang, S. Han, Y. Yu, and W. Ding, ''An access control model for medical big data based on clustering and risk,'' Inf. Sci., vol. 621, pp. 691–707, Apr. 2023.
[29] A. M. Abdullah, ''Advanced encryption standard (AES) algorithm to encrypt and decrypt data,'' Cryptogr. Netw. Secur., vol. 16, no. 1, p. 11, 2017.
[30] H. Krawczyk and P. Eronen, HMAC-based Extract-and-expand Key Derivation Function (HKDF), document RFC-5869, 2010.
[31] A. R. Alzighaibi, ''Cybersecurity attacks on academic data and personal information and the mediating role of education and employment,'' J. Comput. Commun., vol. 9, no. 11, pp. 77–90, 2021.
[32] Y. Qi, Y. Luo, Y. Huang, and X. Li, ''Blockchain-based privacy-preserving group data auditing with secure user revocation,'' Comput. Syst. Sci. Eng., vol. 45, no. 1, pp. 183–199, 2023.

[33] X. Yang, R. Zhang, C. Yue, Y. Liu, B. C. Ooi, Q. Gao, Y. Zhang, and H. Yang, ''VeDB: A software and hardware enabled trusted relational database,'' Proc. ACM Manage. Data, vol. 1, no. 2, pp. 1–27, Jun. 2023.
[34] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, ''LedgerDB: A centralized ledger database for universal audit and verification,'' Proc. VLDB Endowment, vol. 13, no. 12, pp. 3138–3151, Aug. 2020.
[35] X. Yang, S. Wang, F. Li, Y. Zhang, W. Yan, F. Gai, B. Yu, L. Feng, Q. Gao, and Y. Li, ''Ubiquitous verification in centralized ledger database,'' in Proc. IEEE 38th Int. Conf. Data Eng. (ICDE), May 2022, pp. 1808–1821.
[36] A. Padma and M. Ramaiah, ''Blockchain based an efficient and secure privacy preserved framework for smart cities,'' IEEE Access, vol. 12, pp. 21985–22002, 2024.
[37] A. Padma and R. Mangayarkarasi, ''Detecting security breaches on smart contracts through techniques and tools a brief review: Applications and challenges,'' in Proc. Int. Conf. Inf. Manage. Eng. Singapore: Springer, 2022, pp. 361–369.
[38] Guide for Reviewers. Accessed: Jan. 23, 2024.
[39] Á. Tenorio-Fornés, E. P. Tirador, A. A. Sánchez-Ruiz, and S. Hassan, ''Decentralizing science: Towards an interoperable open peer review ecosystem using blockchain,'' Inf. Process. Manage., vol. 58, no. 6, Nov. 2021, Art. no. 102724.
[40] editorial support team @peerj. (Apr. 12, 2010). Confidentiality. Accessed: May 1, 2023. [Online]. Available: https://peerj.com/about/policies-andprocedures/#open-peer-review
[41] Nature Editorial. (Apr. 12, 2010). Editorial Criteria and Processes. Accessed: May 1, 2023. [Online]. Available: https://www.nature. com/nature/for-authors/editorial-criteria-and-processes
[42] P Editorial. (2010). Guidelines for Reviewers. Accessed: May 1, 2023. [Online]. Available: https://journals.plos.org/plosone/s/reviewerguidelines
[43] B. C. O'Brien, A. R. Artino, J. A. Costello, E. Driessen, and L. A. Maggio, ''Transparency in peer review: Exploring the content and tone of reviewers' confidential comments to editors,'' PLoS ONE, vol. 16, no. 11, 2021, Art. no. e0260558.
[44] N Editorial. (Apr. 12, 2010). Integrity and Confidentiality in Nih Peer Review. Accessed: May 1, 2023. [Online]. Available: https://grants.nih.gov/policy/research_integrity/confidentiality_peer_ review.htm
[45] S. Bera, S. Prasad, and Y. S. Rao, ''Verifiable and Boolean keyword searchable attribute-based signcryption for electronic medical record storage and retrieval in cloud computing environment,'' J. Supercomput., vol. 79, no. 18, pp. 20324–20382, Dec. 2023.
[46] N. B. Shah, ''Challenges, experiments, and computational solutions in peer review,'' Commun. ACM, vol. 65, no. 6, pp. 76–87, Jun. 2022.
[47] M. L. Littman, ''Collusion rings threaten the integrity of computer science research,'' in Proc. AAAI Conf. Artif. Intell., 2022, vol. 36, no. 5, pp. 4843–4850.
[48] J. K. Dawson, F. Twum, J. B. H. Acquah, and Y. M. Missah, ''Ensuring confidentiality and privacy of cloud data using a non-deterministic cryptographic scheme,'' PLoS ONE, vol. 18, no. 2, Feb. 2023, Art. no. e0274628.
[49] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, ''A blockchain-inspired attribute-based zero-trust access control model for IoT,'' Information, vol. 14, no. 2, p. 129, Feb. 2023.
[50] V. Awale and S. Gaikwad, ''Zero trust architecture using hyperledger fabric,'' in Proc. 14th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), Jul. 2023, pp. 1–4.
[51] R. Mukta, J. Martens, H.-y. Paik, Q. Lu, and S. S. Kanhere, ''Blockchainbased verifiable credential sharing with selective disclosure,'' in Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom), 2020, pp. 959–966.
[52] T. Lukaseder, M. Halter, and F. Kargl, ''Context-based access control and trust scores in zero trust campus networks,'' in Proc. SICHERHEIT. Göttingen, Germany: Gesellschaft für Informatik eV, 2020, pp. 53–66. [Online]. Available: https://dl.gi.de/server/api/core/bitstreams/7f5c3a3e51e7-4114-bbe6-bbb9bcb2355f/content
[53] C. F. I. Blumzon and A.-T. Pănescu, ''Data storage,'' in Good Research Practice in Non-Clinical Pharmacology and Biomedicine, A. Bespalov, M. C. Michel, and T. Steckler, Eds. Cham, Switzerland: Springer, 2020, pp. 277–297, doi: 10.1007/164_2019_288.
[54] R. D. Garcia, G. S. Ramachandran, R. Jurdak, and J. Ueyama, ''Blockchain-aided and privacy-preserving data governance in multistakeholder applications,'' IEEE Trans. Netw. Service Manage., vol. 19, no. 4, pp. 3781–3793, Dec. 2022.
[55] S. Pooja and C. B. Chandrakala, ''System and method for reckoning professional summary of a researcher,'' Indian Patent 202 341 030 448, Apr. 27, 2023. [Online]. Available: https://iprsearch. ipindia.gov.in/PublicSearch/PublicationSearch/ApplicationStatus

[56] F. P. Rivara, P. Cummings, S. Ringold, A. B. Bergman, A. Joffe, and D. A. Christakis, ‘‘A comparison of reviewers selected by editors and reviewers suggested by authors,’’ J. Pediatrics, vol. 151, no. 2, pp. 202–205, Aug. 2007.
[57] S. M. Pranić, M. Malički, S. L. Marušić, B. Mehmani, and A. Marušić, ‘‘Is the quality of reviews reflected in editors’ and authors’ satisfaction with peer review? A cross-sectional study in 12 journals across four research fields,’’ Learned Publishing, vol. 34, no. 2, pp. 187–197, Apr. 2021.
[58] A. Goldberg, I. Stelmakh, K. Cho, A. Oh, A. Agarwal, D. Belgrave, and N. B. Shah, ‘‘Peer reviews of peer reviews: A randomized controlled trial and other experiments,’’ 2023, arXiv:2311.09497.
[59] X. Jiang and D. Wang, ‘‘Enhancing journal reputation and academic socialization: Review feedback matters beyond its gatekeeping function,’’ Learned Publishing, vol. 36, no. 4, pp. 506–516, Oct. 2023.
[60] M. Cengher and L. A. LeBlanc, ‘‘Editors’ perspectives on the selection of reviewers and the quality of reviews,’’ J. Appl. Behav. Anal., vol. 57, no. 1, pp. 153–165, Jan. 2024.