IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 June 2024, accepted 30 June 2024, date of publication 4 July 2024, date of current version 12 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3423338

RESEARCH ARTICLE

Secure Reviewing and Data Sharing in Scientific Collaboration: Leveraging Blockchain and Zero Trust Architecture

S. POOJA AND C. B. CHANDRAKALA, (Member, IEEE)
Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Udupi, Karnataka 576104, India

Corresponding author: C. B. Chandrakala (chandrakala.cb@gmail.com)

ABSTRACT The current publishing landscape grapples with opacity in the review process. In response, a proposal for a blockchain-driven system is put forth to establish transparent and auditable records for evaluations. However, despite its decentralized nature, concerns persist regarding confidentiality and secure data sharing, crucial for fostering future collaborations. To address these challenges, this study advocates for the implementation of an access control mechanism (ACM) to safeguard confidentiality. Under this mechanism, only the assigned reviewer would have access to the confidential manuscript, ensuring the integrity of the review process. In scientific collaborations, the imperative for confidential data sharing extends beyond reproducibility to encompass vital collaborative endeavors such as publications, Memorandums of Understanding (MoUs), grants, and funding. While hierarchical ACM may prove insufficient in defending confidential data, a more nuanced approach is proposed, leveraging a fine-grained access control model that considers contextual opinions, embodied in the concept of Zero Trust Architecture. Additionally, an incentivization mechanism based on author feedback is proposed to bolster reviewer engagement and credibility. In summary, this study aims to tackle trust and confidentiality concerns within the review system, facilitating secure data sharing for future collaborations while enhancing the credibility of reviewers. By advocating for a transition towards decentralized scientific collaboration and review processes, this work underscores the importance of integrating confidential review and data sharing practices, thereby fortifying the scholarly ecosystem.

INDEX TERMS Research network, scientific publishing, peer review, zero trust architecture, data sharing, reviewer incentivization.

I. INTRODUCTION

For global partnership scientific collaborations and review system should facilitate data sharing, confidential peer review process to critically evaluate the outcome, transparent and audit-able process with policies beneficial to the partnership. These key aspects are shown in Figure1. Peer review is the key to the growth of scientific knowledge which validates the credibility and legitimacy of the science [1]. Though being claimed as instrumental for raising quality of publications, it still lacks transparency [2]. With the soaring advancement in IT [3], researchers have proposed integration of scientific publishing system with blockchain [4] for its inherent feature of immutability. Patent [5], heathcare data [6], review comments [7], [8], research datasets [9] are proposed to integrate with blockchain for its immutability feature. With the improvement in the traceability of review process, the existing work does not address the implementation of a confidentiality in the review process or research data sharing [10]. Reviewers breach of confidentiality causes year long hardship of researchers down the drain [11], [12], [13]. Fake reviews, lack of verifiability, vulnerability to manipulation, privacy concerns are some of the keys issues of existing review management system [4], [14], [15]. Thus, review process mandates confidentiality in manuscript submission to reviewers [16] and to the review comments [17], [18], [19].

On the same grounds sharing of confidential research data need to be carefully handled to avoid breach of

The associate editor coordinating the review of this manuscript and approving it for publication was Cesar Vargas-Rosales.

HIPAA(Health Insurance Portability and Accountability Act)Act [20], [21] or jeopardize participants identity. For audit-ability of records blockchain can be proposed to use which ensures record retention even after the destruction of smart contracts [22]. Without the exchange of research material, the collected data gets stagnated and eventually will face lock-in effect [23]. Moreover data owners may have diverse expectations regarding their data, including preferences for affiliations from institutions with which they have signed memoranda of understanding (MoUs) [24] or collaborative plans for specific time frames. These expectations may vary based on the geographical origins of the data owners, which aligns with findings of Dutra et al. [25] where only one third of authors sent the requested data for systematic literature work. To accommodate differences in opinion, a Zero Trust Architecture [26] is inculcated in data access scenario. This architecture evaluates if the researchers are capable enough to handle the set expectations. Thus the work concentrates on evaluating data access requests and secure data sharing, essential for scientific reproducibility and verifiability. Thus effective monitoring of the access activities of data or resources under authorized legitimate conditions can be implemented by access control mechanism [27]. It is urgent to strengthen the peer review confidentiality [17], [19] and privacy of research data [28].

The work proposes to address confidentiality in the blockchain based review process, sensitive data access request and sharing for scientific collaborations. The work enforces access control mechanism using blockchain based smart contracts since it involves collaboration between un-trusted parties. Restricting unauthorized users from accessing the confidential data is ensured using AES encryption [29], symmetric key generated using HKDF algorithms [30], and incorporating Lagrange Interpolation [6] for consensus between multi-partied data ownership, thus avoiding cyber incident on data silos [23]. Summarizing the contributions of the work are as follows:

1) Addressing confidentiality in review process to ensure secure and coordinated handling of unpublished manuscript between author, editor and assigned reviewers.
2) Proposing Zero trust (ZT) architecture for processing confidential data access request ensuring accountability of context based opinions between various data owners in varying hierarchy.
3) To ensure confidential data sharing after ZT acceptance.
4) To incorporate author feedback on review comments adding value added recommendation to editor for selection of future reviewers.

Section I discusses the literature work to prove the need for confidentiality in review process, access control policies implementation in existing blockchain based architecture, need for author feedback on review comments. Section II discusses the methodology starting with the discussion on threat model which gives a brief about the vulnerabilities existing in the system, possible attackers and mitigation mechanism. Further the work address the implementation of confidentiality in review process, Zero Trust architecture for gaining data access, secure data sharing on transit and using author feedback on review comments. Section III discusses result and followed by conclusion.

A. RELATED WORK

Cyberspace has provided opportunities for both learning and research. But cyber attacks [31] are targeted at academic data, research data, personal data especially proprietary designs. Blockchain [32] is proposed to use to avoid collision attack. Yang et al. has proposed VeDB [33] and LedgerDB [34] wherein applications using blockchain only for its immutability and non repudiation nature can be migrated to these platform for better scalability, throughput. But the current work proposes need to use smart contracts for enforcement of access control policy in addition to other blockchain features such as immutability and non repudiation. Yang et al. [35] has compared the use of centralized ledger for verification and audit-ability of records with Hyperledger fabric implementations. Padma and Ramaiah [36] has discussed work on incorporating access control in blockchain platforms. On the same like Padma and Ramaiah [37] has discussed work on detecting vulnerabilities in smart contracts. Thus stressing the need for automated vulnerability detection in smart contract since it carries on access control policy enforcement. The scope of the work is scientific review and collaboration system where in aspects such as review process, access control policies, data sharing are discussed. The proposed work identified the need for confidentiality of review process and data sharing in the reviewer literature stated in Table 1. Confidentiality can be ensured by protecting sensitive data using passwords [38]. Sometimes the reviewer may use the unpublished work to share among his colleagues [11]. Sometimes assigned reviewer may ask his research assistant to review the articles. But if this in not informed to the journal and if editor doesnot ensure if the assigned research assistant doesnot have any conflict of interest then it can be considered as breach of confidentiality [12]. There has been incident where rough draft of unpublished work is published in public domain by reviewers [13]. Thus it was inferred a confidentiality enforcement mechanism was much in need for the decentralized scientific review process [4]. There are many articles which specified the need of confidentiality in peer review process shown in Table 1. But methods to incorporate the same are not discussed in publishing houses such as PeerJ [40], Nature [41], Plos [42]. Brien et al. [43] proposed work on similar to PeerJ [40] which carries out review mandating need of confidentiality of identity of reviewer from authors. NIH [44] mandates confidential agreement signed with reviewers. Tenorio-Fornés et al. [39] proposed open review system using Dapp.

Sourav et.al. [45] proposed cloud based electronic medical record management system. The work proposed the usage of Linear Secret Sharing Scheme, Key derivation function [30] and access policy. The access policy proposed to use Boolean formula using AND and OR operators to define policy. Shah [46] discusses about dishonest behaviour in scientific publishing system. Michael et al. [47] on the same line proposes the need for traceable and accountable review system. Dawson et al. [48] proposed a confidential data sharing and privacy of cloud data using a non deterministic cryptographic schemes. The study supported the fact that the execution time of cryptographic algorithm does not depend on data size but on the size of the security key. Zero Trust Architecture (ZTA) deployed in smart environment helps in secure communication between multiple devices with different levels of access control mechanism [49]. The work give the motivation to have different access control for data sharing based on different context levels of the data owners. ZTA is feasible in Hyperledger fabric [50]. ZTA proposed in [51] reduces oversharing of data. Lukasedar et al. [52] proposes the need for gaining trust before giving accessible to confidential resource. Adding ZTA in addition to authentication [53] results in better defense. Garcia et al. [54] proposes data provenance via blockchain and uses proxy encryption for selective disclosure. To summarise the reviewed literature are classified based on need for access control mechanism in Scientific Review and Recommendation System are shown in Table 2.

It is known that peer review process ensure quality of scientific evolution. Thus only experts in the field should evaluate the validity and quality of the research. Pooja and Chandrakala [55] proposed work on using semantic web to find domain expertise based on history of publications of a researcher. Constructive feedback can be evaluated using research quality instrument (RQI) [56] which validates peer process. Pranic et al. [57] proposes that for constructive peer review process perception by authors and editors play a vital role. However, it is noted that positive review leads to positive author feedback thus while evaluating reviewer credibility a bias may often rise [58]. Reviewer should keep in mind that harsh feedback may lead to lower academic productivity of the researcher as proposed by Jiang and Wang [59]. Cengher and LeBlanc [60] proposed that review in time is more appreciated. Publon [61], [62] gives credit to reviewer, but reviewer's eagerness and timely submissions are not accounted for. Work proposed by Cheung et al. [63], and Jha and Shah [64] motivated to consider reviewer argument quality. Table 3 reviews work which emphasize feedback on reviewer comments.

First type of cyber attack is unauthorized access to stored or data in transmission targeted at unpublished confidential dataset or patent data. Encryption which is synonymous with the term confidentiality becomes a technique for enforcing an ACP [65]. Access control ensures only qualified researches participate in the peer review, thus maintaining the integrity of the review system. ACP also protects intellectual property rights of researcher by preventing unauthorized access or distribution of work. Data shared using encryption algorithm also restricts access only to particular users [5]. Thus data security situation arises which requisite confidential and fine grained access control to unpublished data silos. Other attack type can be with intention of tampering the data, involves making the work public without proper permission. IPR and manuscript published online by reviewer [12] and associate editors [13] brings loss to authors year long efforts. Huang et al. [6] proposed Lagrange-interpolation-driven access control mechanism (LIDACM) that ensure security and confidentiality of health records. The user's private key is generated randomly through the proposed mechanism and hence no relationship exist between private keys, cracking the private key system is suggested difficult. Li and Li [5] proposed patent data fragmentation and encryption. The fragmented data are stored in various nodes of Hyperledger fabric. Hence with comparison to previous work, decryption overhead is more. The research gaps formulated are:

1) Absence of an effective access control mechanism to safeguard the confidentiality of the review process and private data sharing [4], [46], [47].
2) Mechanism to incorporate context based inputs for fine grained access control during confidential data access request.
3) Inadequate mechanisms for harnessing valuable reviewer contributions for future review recommendations [47], [57].

To address the research gaps, research objectives formulated are as follows:

1) Proposing techniques to ensure confidentiality in the review process through the utilization of blockchain transactions.
2) Exploring the implementation of Zero Trust (ZT) to enable flexible context-based access control decisions enabling scientific collaborations.
3) To leverage quality reviewer contributions for informing future recommendations.

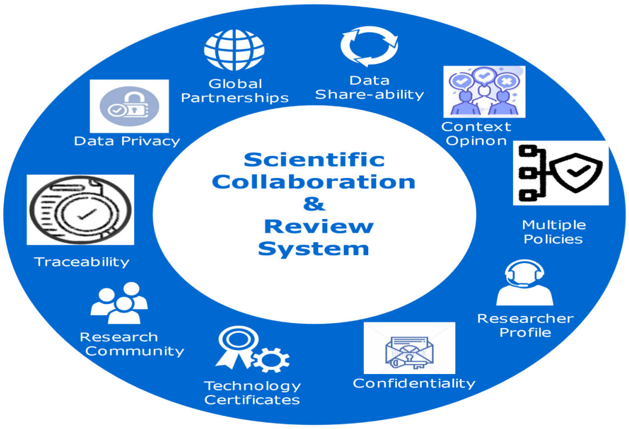

FIGURE 1. Components of a SCRS.

II. METHODOLOGY ADOPTED

The Scientific Collaboration and Review System (SCRS) is meticulously crafted to navigate a myriad of scenarios while

TABLE 1. Insights from reviewed literature on factors emphasizing the necessity of a confidential review process.

Tag	Source	CoP	CoRC_A	CoIR	CC_E	Type of Review	System Requirements
IEEE Access	[17]	✓	✓	✓	✓	single blind review	Editors should ensure that reviewer's keep manuscript, associated material strictly confidential
MDPI journal	[19]	✓	✓	✓	✓	single- or double-blind peer review	reviewers should keep the content of the manuscript, including the abstract, confidential. review reports are considered confidential
Publons	[62], [61]	✓	✓	✓	✓	NA	Display of review depends on preference of reviewer, journal as well as authors.
Wiley	[18]	✓	NR	✓	✓	single anonymous or double anonymous peer review model	confidential comment to the editor in your report
NIH	[44]	✓	✓	✓	✓	single anonymous or double anonymous peer review model	There exist signing of the Confidentiality Agreements, each peer reviewer agrees, under penalty of perjury, 18 U.S.C. §1001, to maintain confidentiality in peer review.
Brien et.al.	[43]	✓	NR	✓	✓	single blind peer review	external reviewers are aware of the author's identity, but the authors do not know the reviewers identity.
PeerJ	[40]	✓	NR	✓	✓	single blind peer review	All reviews of published articles are made public. This includes manuscript files peer review comments, author rebuttals and revised materials. Submissions before 13 February 2023, authors could opt out from publishing peer review history.
Nature	[41]	✓	NR	✓	✓	Reviewer who consent, their reviewer's get published along the article.	manuscripts submitted from February 2020 review comments and their responses are published after acceptance. Authors can opt out during the review process.
Plos	[42]	✓	✓	✓	✓	Single-anonymized peer review	Authors can decide to publish review history along with the published article .
COPE	[16]	✓	✓	✓	NA	Single or double blind , open collaborative or interactive review	Reviews are "original work of authorship" of a Reviewer. Also states that no benefit is gained out of publishing review history after final publication.

note: Confidentiality of Paper(CoP), Confidentiality of reviewer comments to authors(CoRC_A),Confidential comments to Editor(CC_E), Confidentiality of Identity of Reviewer(CoIR)

upholding fundamental principles such as impartiality, transparency, integrity, and confidentiality, as depicted in Figure 1. Confidentiality stands as a cornerstone throughout the review process, ensuring the utmost protection of sensitive information. Moreover, the system facilitates the assessment of the requestee's trustworthiness, particularly crucial in situations where multiple data owners with varying characteristics are involved. This meticulous approach ensures that data sharing is conducted securely and responsibly, maintaining the integrity of the review process and safeguarding the confidentiality of shared information. The critical review process is proposed to be considered for reviewer credibility by taking author's feedback. The architecture shown in Figure 2 shows the detailed the interaction between the modules confidential review and data sharing process and reviewer feedback.

A. THREAT MODEL

In the scientific review and collaboration landscape, maintaining the confidentiality of unpublished manuscripts, review comments, and review responses is of paramount importance. Breaches of confidentiality can lead to the wastage of years of researchers' efforts. Malicious insiders, including administrators, third-party competitors, or even reviewers, pose significant risks to confidentiality. Additionally, for scientific collaborations, the sharing of sensitive data and the criteria for deciding with whom to share this data must also remain confidential. Challenges exist in evaluating the competency of data requesters and reconciling differences in expectations of research outcomes.

If there is only a single layer of authentication, confidential data can be leaked. Therefore, assigning unpublished manuscripts only to selected reviewers, ensuring the confidentiality of data in transit, and rigorously evaluating data access requests and sharing policies are crucial checkpoints that help mitigate vulnerabilities in the system. Implementing multi-factor authentication, such as role-based access control policies, blockchain features like immutability, smart contracts, and zero-trust architecture, can help address these vulnerabilities.

Blockchain's immutability and non-repudiation attributes ensure integrity and transparent, audit-able records [22] even if smart contracts are destructed. Smart contracts automate access control policies, avoiding reliance on third-party vendors. Technologies like LedgerDB [34] and VeDB [33], [35] offer blockchain features such as scalability in transactions per second and credible audit-ability while operating within centralized systems. However, the current work requires collaboration among untrusted partners, highlighting the need for access control policy enforcement via smart contracts to ensure immutability, credibility, and controlled access levels.

Consequently, a decentralized platform like blockchain is recommended for the proposed work. The threat model discussed is shown in the Figure3.Figure reflects on the various actors involved in SCRS. The vulnerabilities stated are mitigated by the using blockchain features with access control policies embedded in smart contract. Incorporated Zero trust architecture for evaluation data request and encryption mechanism for confidential data transit marked as transactions in blockchain.

TABLE 2. Literature review work based on implementations of access control policies.

Refer	Year	Proposed	Observations / Limitations
[45]	2023	Proposed use of ACP, KDF, and Linear Secret Sharing scheme for fine grained access control in electronic medical record.	ensures un-forgeability of data, user anonymity,keyword privacy.
[48]	2023	confidential data sharing and privacy of cloud data using a non deterministic cryptographic schemes (NDCS)	NDCS method uses key creation, encryption and decryption data . -the levels of key production to provide hidden keys add security to algorithm. -comparison done based on encryption and decryption time, throughout.
[32]	2023	proposed provable data possession (PDP) scheme with group user revocation. - proposed use of blockchain technology to resist collusion attack -ring signature used to solve identity privacy	Security analysis (based on correctness , Non Repudiation, unforgeability, Privacy preservation) was performed - Performance analysis based on identity privacy protection, user revocation, collusion attack resistance, traceability were performed.
[49]	2023	blockchain based Zero trust access model for IoT	For device to device communications, device trust level scores are computed. It ensures active defense in smart grid network.
[50]	2023	ZTA implementation in Hyperledger Fabric	lacks metric used for evaluating proposed work.
[4]	2023	addresses accounatability and transparency in the review system	Confidentiality of user data and unauthorized access is not addressed
[6]	2022	Proposed Lagrange Interpolation based Access Control Policy	-Generated Polynomials for users and their access rights. Multiple indicator function employed before the final polynomial regeneration process happens.
[5]	2022	proposed re-encryption algorithm that takes 1 sec to decrypt 64KB data.	-patent data are fragmented and stored in different nodes using Hyperledger Fabric technology. -decryption overhead is more
[46]	2022	Discusses about dishonest behaviour in scientific review system.	Stress in confidentiality in handling sensitive peer review data
[54]	2022	proposes data provenance via blockchain and uses proxy encryption for selective disclosure	the work has evaluated memory allocation and execution time based on encryption, delegation key, re encryption and decryption parameters
[47]	2022	proposes the need for traceable and accountable review system	addressed the need for confidential review process to avoid colluders sending threat message for positive reviews.
[57]	2021	Proposes that for constructive peer review process perception by authors and editors play a vital role	Rejected manuscript attributed to bad author feedback and vice versa.
[39]	2021	propose open review system using Dapp. Trasparent and treaceable governance in review system is proposed. Author feeback for review comments is proposed	Lacks mechanism to ensure confidentiality of review comments
[51]	2020	proposes verification of participant and data minimisation technique to reduce oversharing the credential data	Performance measure was done based on no of threads executed, no of requests raised, number attributes used
[52]	2020	proposes ZTA in research network in German university. Implementation is evaluate in Moodle based e-learning platform	Binary decisions are considered for computation of trust scores. But explicit policies regarding the the usecase is not considered
[34]	2020	centralized ledger with blockchain features, audit-ability	high tps, lacks features of smart contracts
[35]	2022	centralized ledger with blockchain features, audit-ability and credibility features	high tps, lacks features of smart contracts
[33]	2023	centralized ledger with blockchain features, audit-ability	high tps, lacks usage of smart contracts, better than LedgerDB
[37]	2022	Discusses tools and techniques to vulnerability detection of smart contracts	smart contract because of its immutability need to be scanned for vulnerability detection before deplying. This is can the future work for the proposed work.
[36]	2024	The work proposes use of permissioned blockchain for applications associated with IoT data.	Security metrics such as confidentiality , integrity and privacy are strengthened used techniques such as OTP, encryption and hashing. -Lacks discussion on evaluating competency of data requester for sharing data.

TABLE 3. Observations from the reviewed literature underscore the importance of evaluating reviewer comments in the peer review process.

Refer	Year	Proposed	Observations
[59]	2023	suggested that harsh review feedback leads to temporary decrease in academic productivity	-timely & constructive feedback of reviewers help in journal reputation Author accept rejection letter provided there is a objective evaluation in reviewer's feedback.
[57]	2021	constructive reviews better guide the editor's decision making process. -proposed Review Quality Instrument (RQI) [56] to measure review quality	Author's rated satisfaction to constructive review & timeliness in review submission. Suggested as important for checking the validity of peer process. - Author satisfaction scores for the constructiveness of the reviews where higher for "accept or recommended" reviews
[58]	2023	proposed that reviews can be peer reviewed by authors, editors or meta -reviewers for performing evaluation of quality of reviews.	Author feedback is considered bias stemming from reviewer recommendation need to be considered. -Assuming longer review for higher quality review need to consider if such a review is generated from large-language models(LLM).
[60]	2023	proposed that editor selection for reviewer based on expertise in subject, history of conducting good reviews, writing constructive and respectful reviews.	it was observed that short review in time is better compared to great review submitted after deadline. But practically observation from Associate Editors was great review before deadline is more preferred. The work was more of a survey questionnaire shared among selected candidates

B. CONFIDENTIAL REVIEW PROCESS

Throughout the confidential review process, it is crucial to maintain exclusive access to the manuscript by the designated reviewers appointed by the editor [55]. To facilitate the confidential submission of articles to selected reviewers, the AES encryption standard [29] is proposed for use. In order to streamline key management overhead, the hash-based key derivation function (HKDF) [30] is suggested for each

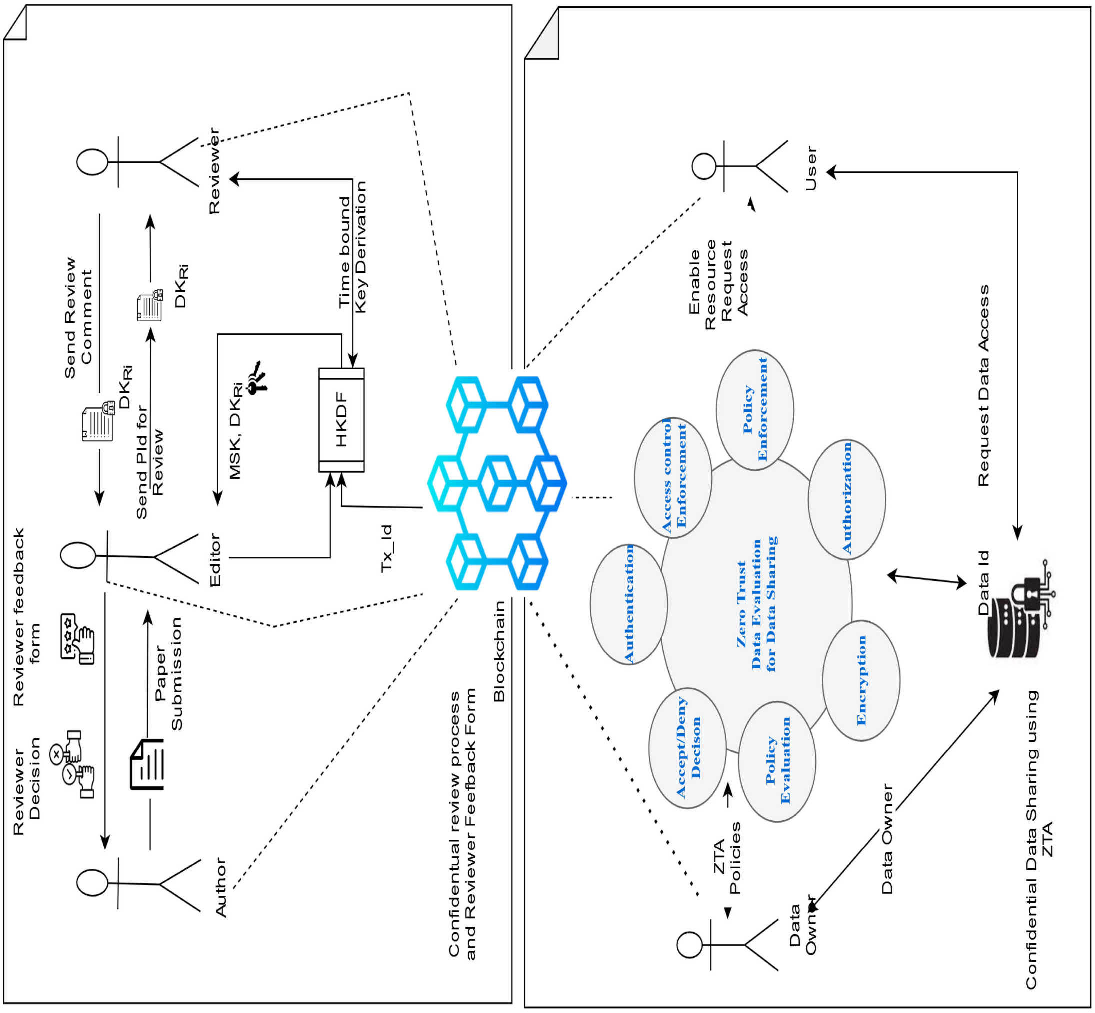

FIGURE 2. Architecture for the proposed work.

reviewer. The HKDF function necessitates the generation of a Master Secret Key (MSK), also referred to as initial key material (IKM). The MSK is produced by concatenating the Editor's address (EA) and a randomly generated ID for the paper (PId). The detailed steps are outlined in Algorithm 1. Complexity of the algorithm is based on number of reviewers, n for whom encryption and decryption keys has to be generated, which amounts to $O(nL)$, L here refers to length of derived key DK_{R_i} considered here. Additionally, access to the manuscript should be limited for an agreed-upon duration to uphold confidentiality while ensuring a timely and effective review process. This is achieved through the utilization of a time-bound key derivation function at the reviewer's profile, as depicted in Algorithm 2. The time alogithm requires extraction of current time stamp and setting start time and end time for paper submission, which amounts to complexity of $O(1)$. The derived key can subsequently be utilized to decrypt the confidential manuscript for review submission. The review comments are encrypted using derived keys generated by Algorithm 1. This guarantees confidentiality in review decision comments, allowing view-ability only to editors. Additionally facilitating constructive feedback exchange between reviewers and authors.

C. ZERO TRUST ARCHITECTURE

Zero trust does not mean that system is devoid of trust, it means that trust has to be earned [52]. User requesting a service must explicitly establish trust through combination of checks like 2 factor authentication or through their research profile [49].

Existing literature work needs satisfaction of ACP deployed via smart contract. But in smart contract once the access policy is defined it cannot be updated once deployed. Especially with changing research trends, there is often requirements for the need to change few aspects in access control policy. The current system considers the dynamic aspects of access control policy for Zero Trust Architecture(ZTA) [52]. Once the trust score is calculated, ACP deployed via smart contract is triggered for the access of service. For the scientific collaborations it is essential to

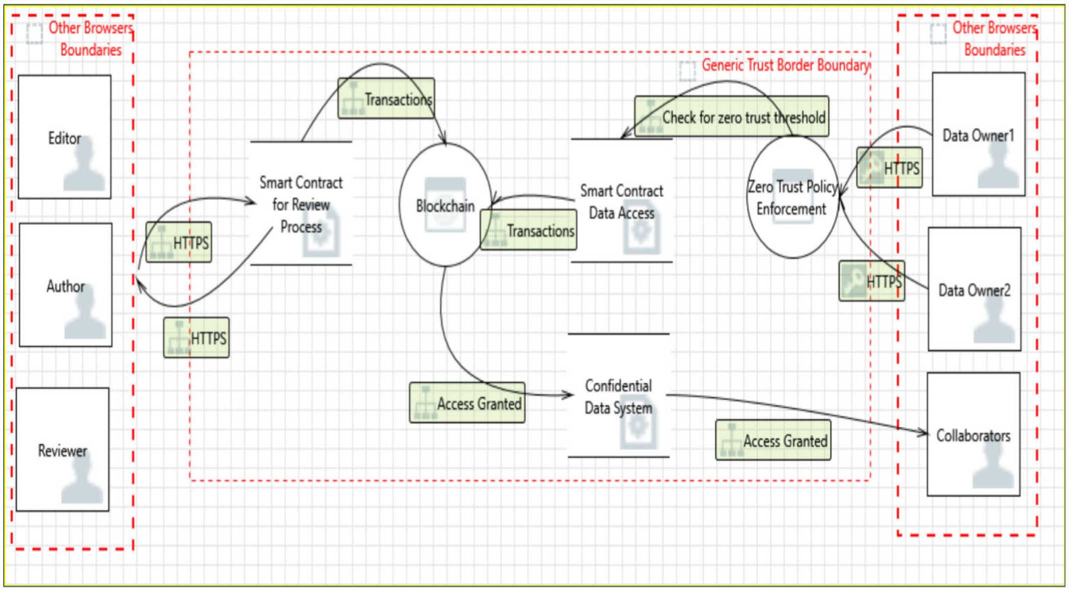
Other Browsers Boundaries
Editor
Author
Reviewer
HTTPS
HTTPS
Transactions
Smart Contract for Review Process
Blockchain
Transactions
Generic Trust Border Boundary
Check for zero trust threshold
Smart Contract Data Access
Zero Trust Policy Enforcement
HTTPS
HTTPS
Access Granted
Confidential Data System
Access Granted
Other Browsers Boundaries
Data Owner1
Data Owner2
Collaborators

FIGURE 3. Threat Model for the proposed work.

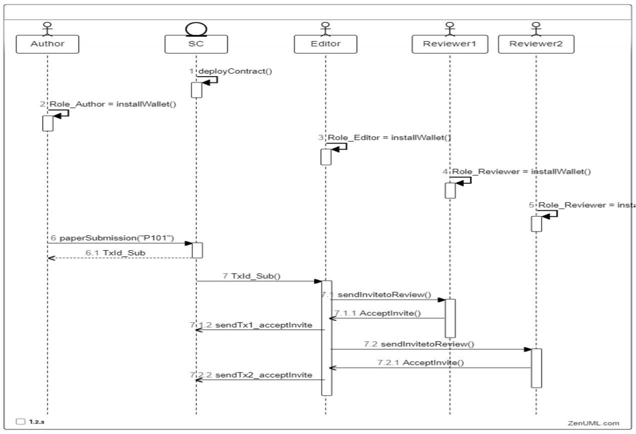

FIGURE 4. Sequence diagram exhibiting review invite and acceptance.

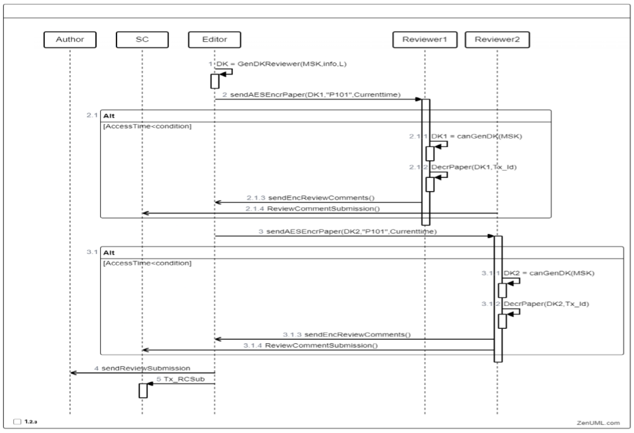
Author
SC
Editor
Reviewer1
Reviewer2
1 DK = GenDKReviewer(MSK,info,L)
2 sendAESEncrPaper(DK1,"P101",Currenttime)
2.1 Alt
[AccessTime<condition]
2.1.1 DK1 = canGenDK(MSK)
2.1.2 DecrPaper(DK1,Tx_Id)
2.1.3 sendEncReviewComments()
2.1.4 ReviewCommentSubmission()
3 sendAESEncrPaper(DK2,"P101",Currenttime)
3.1 Alt
[AccessTime<condition]
3.1.1 DK2 = canGenDK(MSK)
3.1.2 DecrPaper(DK2,Tx_Id)
3.1.3 sendEncReviewComments()
3.1.4 ReviewCommentSubmission()
4 sendReviewSubmission
5 Tx_RCSub
1.2.3
ZenUML.com

FIGURE 5. Sequence diagram exhibiting confidential review process.

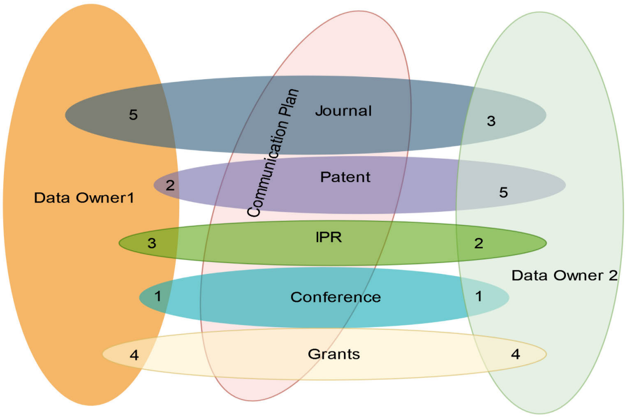

FIGURE 6. Communication Plan with context based opinion from data owners.

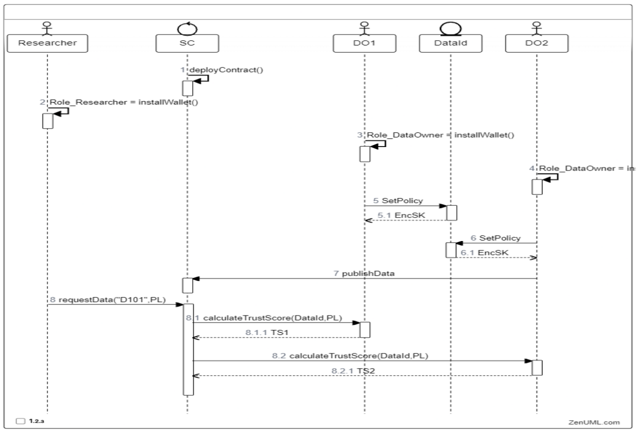

FIGURE 7. Initial set up for shared data access.

share research data for better discoverability. But research data is often confidential which involves some mandate to be filled before giving the access. Often only one third of researchers respond to data access [25]. This can be

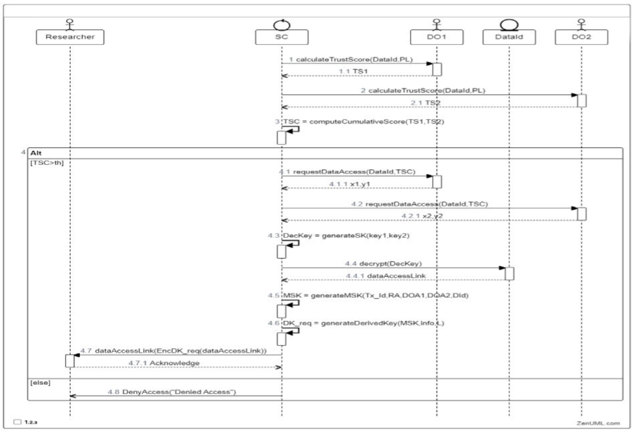
Researcher
SC
DO1
DataId
DO2
1 calculateTrustScore(DataId,PL)
1.1 TS1
2 calculateTrustScore(DataId,PL)
2.1 TS2
3 TSC = computeCumulativeScore(TS1,TS2)
4 Alt
[TSC>th]
4.1 requestDataAccess(DataId,TSC)
4.1.1 x1,y1
4.2 requestDataAccess(DataId,TSC)
4.2.1 x2,y2
4.3 DecKey = generateSK(key1,key2)
4.4 decrypt(DecKey)
4.4.1 dataAccessLink
4.5 MSK = generateMSK(Tx_Id,RA,DOA1,DOA2,DId)
4.6 DK_req = generateDerivedKey(MSK,info,L)
4.7 dataAccessLink(EncDK_req(dataAccessLink))
4.7.1 Acknowledge
[else]
4.8 DenyAccess("Denied Access")
1.2.a
ZenUML.com

FIGURE 8. Detailed process of shared data access.

attributed to the factor that data owner is unable to measure of the potential of researcher and his intentions. Through this framework, the work proposes input policies for trust score calculation. The policy engine composes of list of attribute input, PL_i and assigned weight-age, w_i decided among owners of data. Sample policies for a data access request is shown in Table 4. Weights w_i assigned for policiesPL_i is dependent upon the context relevance for acceptance of data request access. E.g. a researcher profile and affiliation will have more weight-age compared to time-line duration. Policy PL_j may have range of values refer equation 2. Data owner may have uncertainties for a multi-valued policy PL_j, thus to incorporate a diversifying opinion δ is used to represent index of scaling factor, SC in equation 1. Thus a flexible context based opinions from data owner entity can be computed using equation 3. Total trust score,Ts_{do_i} computed using equation5. The trust score computation uses cumulative fusion formula to reduce individual uncertainties using equation 6 to compute the trust score.

$$SC \in \big[u, u+1, u+2, \ldots v\big] \tag{1}$$

$$PL_j \in \big[a_1, a_2, \ldots, a_m\big] \tag{2}$$

$$b_x = \sum_{k=1}^{m} (a_k * SC[\delta]) \tag{3}$$

$$n = count(PL_i),\; a_x \in SC[\delta] \tag{4}$$

$$TS_{do_i} = w_1 * a_i + ..w_i * (b_x) + .. + w_n * a_n \tag{5}$$

$$TSC = \frac{1}{2} * (TS_{do_1} + TS_{do_2} + \ldots + TS_{do_p}) \tag{6}$$

D. DATA SHARING AFTER ZT ACCEPTANCE

For multi partied ownership of data, parties involve research institute, in-charge head and researchers, with various roles. For ease of sharing of data in multiparty collaboration if SC is generated which states n out of k parties are needed for consent, the access control uses Shamir's secret sharing key. Request for confidential data is raised from requestee to multiparty owner, which triggers a transaction $Tx_{req}Id$. Algorithm 3 presents the scenario considered for data sharing once ZT threshold is above the acceptance level. The Algorithm has complexity of $O(k)$ for generating polynomial of degree $k-1$ involving k coefficients. For generating (x_i, y_i) coordinates for n data owner the complexity amounts to $O(n)$. To form secret key using polynomial coefficients it amounts to $O(k)$, thus the complexity for protection of data at rest amounts to $O(n+k)$. For getting consensus from k parties the complexity is attributed to $O(k)$. Combining the complexity of derived key generation based on key length, L, total complexity for protection of data at transit would be $O(k+L)$. Assuming AES is working on a fixed block size, approximately the complexity can be attributed to $O(1)$.

Algorithm 1 Confidential Review Process

```
Require: Editor has txID with reviewer's accepted to review,$Tx_A Id_{R_i}$.
Ensure: Editor has generated PaperID($PId_i$) using random no generator.
RSS ∈ {"Submission","Under Review","Review Submitted"}
Generates $(MSK) = concat(EA||PId) \oplus RSS$.
For each accepted reviewer, generate $DK_{R_i}$
for each $R_i$ do
    $salt = Tx_{Sub}Id_{PId_i}$
    $info = concat(Tx_A\_Id_{R_i}||RA_i)$
    $L = 256 bits$
    $DK_{R_i} = KDF(MSK, salt, info, L)$
end for
For Encryption
while each $R_i$ is sent $PId_i$ do
    Encrypt using $DK_{R_i}$ to obtain Cipher Text, $CT$, $E_{DK_{R_i}}(full\ details\ PId_i, URL) = CT$
end while
For Decryption
for each $R_i$ do
    if $calculate\_time\_factor(CTS) = 0$ then

        return $interpolate\_key = MSK$
    else
        $interpolate\_key = null\ key$
    end if
    $DK_{R_i} = KDF(interpolate\_key, salt, info, L)$
    while $interpolate\_key! = null\ key$ do
        Decrypt $CT$ using $DK_{R_i}$, $D_{DK_{R_i}}(CT)$
    end while
end for
```

1) MULTIPARTY OWNER PROCESS

For multi-partied ownership first tier need to be defined which defines ownership of data. Example Tier 1 may be the first author, second author. Tier 2 may be the corresponding author or research lab incharges. Tier 3 may be department research institute, Tier 4 may be Institute research head. Thus if a request is raised to corresponding author's Id, access control policy defined with the participating entities need to consent as shown in equation (7) to decrypt the data at

TABLE 4. Description of policies considered for data request access.

Sl.No	Policy Description	Weights assigned
PL1.	Researcher ORCID ID	w_1
PL2.	Affiliation	w_2
PL3.	Communication Plan	w_3
PL4.	Funding Agency	w_4
PL5.	Software Tools used for analysis	w_5
PL6.	Commercial Purpose	w_6
PL7.	Time-line duration	w_7
PL8.	Ethics Committee Approval	w_8
PL9.	Type of Access	w_9
PL10.	GPS Location of access requests	w_{10}
PL11.	Time stamp difference in successive request	w_{11}
PL12.	Number of Active data request	w_{12}
PL13.	Type of Meta data	w_{13}
PL14.	Mentor research Profile	w_{14}
PL15.	Mentor Affiliation	w_{15}

Algorithm 2 Algorithm for Time Based KDF

```
Require: Extract Current Time Stamp, $CTS$.
Ensure: Editor has generated Start_Time, $ST$ and
    End_Time, $ET$ for the PaperID($PId_i$).
Compute Time_range_allowed, $TRA = ET - ST$
Compute Time_after_ST, $TST = CTS - ST$
Compute $key\_type = MAX(0, MIN(1, TST/TRA))$
if $key\_type == 0$ then
    return $MSK$
else
    return $null\ key$
end if
```

rest. The data at rest is encrypted using Shamir's Secret Key. Polynomial generated is of degree $k - 1$, where minimum k-threshold key set is required to obtain the polynomial using Lagrange Interpolation [6]. The coefficient of polynomial forms the secret key (SK) with which data is encrypted. SK is the symmetric key, obtained from coefficient of the polynomial. DK_{Req} is the symmetric key, used to encrypt the file containing manuscript details, $PId_{details}$, dataset url, $dataset_{url}$, Copyright form, CP.

2) ENCRYPTION AND DECRYPTION OF DATA AT REST

1) Generate coordinate set assuming the stakeholders are researcher, incharges, research institute. (x_o, y_o), (x_{AOP}, y_{AoP}), (x_{R_1}, y_{R_1}), (x_{R_2}, y_{R_2}).
2) y coordinate can be generated by evaluating polynomial shown in equation (8), where x_i, y_i are the coordinates of each participant.
3) With the consent of k out of n parties satisfying the defined ACP for PaperID(PID),ACP_{PId}, SK can be derived using equation (9) and data silo can be decrypted.
4) SK is used to encrypt the file containing manuscript details, $PId_{details}$, dataset url ($dataset_{url}$), Copyright form (CP) as shown in equation (10). **Data Transmission**
5) The data need to be transmitted, using derived key, DK_{Req}.
6) Master Secret Key, MSK_{do} is generated by data owner using TxId of the recorded data request recieved($Tx_{data}Id$), paperId(PId) and address of data owner(DOA) and is shown using equation11. $Tx_{data}Id$ can be used to verify data owners authenticity [53].
7) Derived key for requestee,DK_{Req} is generated using KDF with arguments as shown in equation (12).
8) DK_{req} is symmetric key used for encryption and decryption as shown in equation(14).

E. AUTHOR FEEDBACK ON REVIEW COMMENTS

Publon [61] works with reviewer and publisher to give credit for the reviewing service to the reviewer which can be used in promotion. It gives 1 merit for completing review, 2 merits if editor verifies the review, 2 merits if reviewer publishes full review(if allowed).But few shortcoming such as reviewer eagerness to review is never accounted for giving credits in Publon. Also reviewer may write unnecessary recommendation or write unnecessarily cruel or personal comment, which editor is not able to identify inconsistencies [61]. Thus a mechanism to evaluate the reviewer comments helps in review credibility.

Review credibility are identified as source credibility, review consistency, review sidedness [63], and argument quality [64]. The mechanism to evaluate reviewer's review history can be used for future recommendations to the editor. Once the review is received by the editor and review decision is passed to author. A set of questions can be sent to an author to evaluate the quality of review comments. Reviewer Feedback form may contain the following qns:

1) Can the majority of review comments be addressed.
2) Do you think the review comment will improvise your work technically.
3) Rate if the reviewer suggested to cite recent relevant references are related to your work.
4) Has reviewer cited references are helpful to author to address the review comments.
5) Has reviewer used any rude comments which was hurtful to author.

$$ACP_{PId} = (T_2 \cap T_1 i) \cup (T_1 i \cap T_1 j) \cup ((T_2 \cup T_1 i) \cap (T_3 \cap T_4)) \tag{7}$$

$$y_i = PC_i * x_i + PC_0 \tag{8}$$

$$SK = PC_k||..||PC_i||..PC_0 \tag{9}$$

$$ED@R = E_{SK}(PId_{details}, dataset_{url}, CP). \tag{10}$$

$$MSK_{do} = concat(Tx_{req}Id||PId||DOA) \tag{11}$$

$$DK_{req} = KDF(MSK_{do}, info, L) \tag{12}$$

$$info \in \{Tx_{req}Id, ReqA, PID\} \tag{13}$$

$$ED@T = E_{DK_{req}}(PId_{details}, dataset_{url}, CP) \tag{14}$$

For each of the question weight-age can be given, which can be used to compute the review credibility of Reviewer,

Algorithm 3 Algorithm for Data Sharing With Multi-Partied Ownership

```
Require: Confidential data which has multiparty ownership.
Ensure: Access policy, $ACP_{PId}$ is defined in Smart Contract
    which states k-threshold parties required to decrypt the
    data repo. **Protection of Data at rest**
  Polynomial of power (k-1) is generated.
  Generate $(x_i, y_i)$ coordinates for each data owner(8).
  Polynomial coefficients, $PC_k||, .||PC_i||PC_0$ form the
    symmetric secret key for data confidentiality. **Protection
    of data at Transmit**
  Requestor initiates the request to the data owner.
  Requestee consensus with k-parties defined in $ACP_{PId}$.
  Decrypt the data with k parties after agreement.
  Data Owner/Requestee generates $MSK \in \{Tx_{req}Id, DOA, PID\}$ refer equation (11)
  Requestee generated derived key $DK_{req}$ refer
    equation (12).
  $DK_{req}$ is the symmetric secret key used for encryption &
    decryption.
```

ER_{R_i}. ER_{p_i} is computed based on weight-age to each scale w_i and ratings submitted by author on a range of 1 to 5, denoted by η_i. Activity rate, AR_{R_i} can be composed of Review request processing rate(RR) and skill value obtained from score of history of reviewer publications, DS_{domain_i}, [55]. RR is computed based on rate of positive responses to review invite, count of timely response to accepted review request instances(μ_{p_i}) w.r.t. total accepted review invites (ε_A) and efficiency rate. ψ denotes editor option to mask or include the review rating obtained from author. Rate of positive response is computed using κ_{p_i}, denoting response duration to review invite, max_{p_i}, w.r.t. total review invites received(ε_T). Since it is observed that satisfaction of author is more associated with acceptance of manuscript, hence the RR rating can be kept as an option by the editor to include in Activity rate and is shown in equation 16.

$$ER_{p_i} = \frac{\eta_i * w_i}{\sum_i^n w_i} \tag{15}$$

$$RR = \delta_1 \sum \frac{max_{P_i}}{\kappa_{P_i} * \varepsilon_T} + \sum \frac{(\delta_2 * \mu_{p_i}) + (\delta_3 * ER_{p_i}^{\psi})}{\varepsilon_A} \tag{16}$$

$$AR_{R_i} = \lambda_i DS_{domain_i} + \lambda_j RR \tag{17}$$

III. RESULTS

The work uses localhost implementation of Ethereum blockchain in Hardhat framework using Web3.js library, Metamask wallet and React framework. The metrics considered for the proposed implementation is processing time for ensuring confidentiality in review process and evaluating data access request using Zero trust architecture and is shown in fig:resultVisualization. Moreover a cost analysis is proposed for each of the modules suggested in the work.

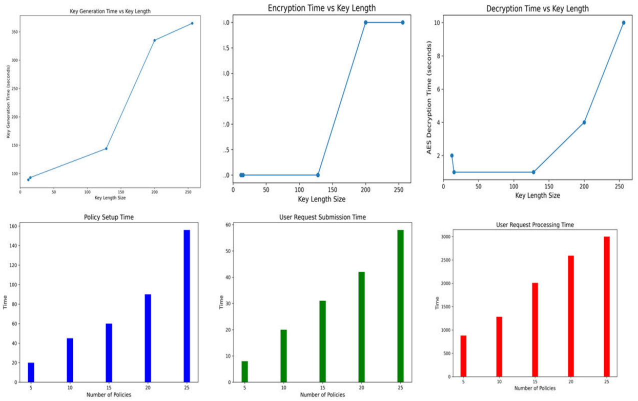

FIGURE 9. Processing time for review process and zero trust data sharing.

TABLE 5. Cost analysis.

Function	Gas	cost(ETH)	cost($)
Send manuscript for Review	27379	0.000054	0.18
Send Review Comments	27367	0.00005738	0.20
Data Access Request	26431	0.00004689	0.18
Data Sharing	27379	0.00004636	0.17

note: Hardhat framework, Ether.js, Metamask Wallet.

TABLE 6. Qualitative evaluation of proposed work with existing literature work.

Paper	AA [1]	AZN[2]	RM [3] & AUD[3']	CRP[4]	DA[5]	SDS[6]	Iy[7]	RI [8]	I/P [9]
[4]	✓	✓	✓	✓	×	×	✓	✓	I
[7]	✓	✓	✓	✓	×	×	✓	✓	I
[39]	✓	×	✓	×	×	×	✓	✓	I
PW[10]	✓	✓	✓	✓	✓	✓	✓	✓	I

note: [1] Authentication, [2] Authorization , [3] Research Misconduct, [3'] Audit-ability , [4] Confidential Review Process, [5] Data Access, [6]Secure Data Sharing, [7]Integrity, [8]Reviewer Incentive, [9]Implementation (I) or Prototype(P), [10]Proposed Work.

Qualitative analysis is also proposed based on parameters such as authentication, authorization, research misconduct, integrity, audit-ability, confidentiality in the review process, data acess and sharing, reviewer incentive with existing work [4], [7], [39]. It is shown in Table 6, also Table7 highlights the techniques used in each modules for better understandability. The key generation time for varying L bits, to ensure confidentiality is shown in Figure9. The processing time for zero trust mechanism such as policy setup, user request submission and user request processing is also shown in Figure 9. Though processing time for multiple policies increases computation time, but this overhead can be compensated with the fine grained context based access

TABLE 7. Specifications for addressing proposed objectives.

Obj_i	Application Scenario	AA[1]	Authorization		Confidentiality		Shared Data Access		Integrity
			RBAC	ABAC	KG	Enc	DA	ZTA	
Obj1	Confidential Review Process	MW	Editor & Reviewer	Tx_Ids, PId, EA, RA, RSS	KDF	AES	AES Dec	NA	Tx_Id_{sub}, Tx_Id_{RA}
Obj2	ZTA for Data Access		DO_i, T_i & DReq	SC_{do_i}	NA	AES	NA	PL_i, w_i, CFS	Tx_Id_{Req}
Obj3	Data Share			Tx_Ids, PId, DOA, ReqA	KDF	AES	SSK & LI	$TSC > th_{TSC}$	Tx_Id_{Req}

control provisioned to the data owner. The proposed work is evaluated in terms of attainment of parameters such as authorization, authentication, confidentiality, integrity, data access and is shown in Table 7. This emphasizes the technique used, thereby clarifies the methodology used to achieve the criteria. The work is also compared with existing work to emphasize the contribution of the proposed research work and is shown in Table 6. The work considers blockchain based review system to evaluate the proposed work based on factors such as authorization, authentication, confidential review process, data sharing and reviewer in-centivization and also audit-ability of records.

A. AUTHORIZATION

The proposed system provides dynamic authorization by implementing attribute and role based access control. Role based access control (RBAC) is implicit because there exist user who may have login as author or reviewer based on the submission type. Attribute based access control(ABAC) uses blockchain transaction ids, (Tx_{id}) w.r.t. to each scenario necessitates the user to be connected to the previous history transactions. Also wallet addresses by Metamask is used as attributes to generate keys for encryption. This helps in mandatory assignment of particular user for a task, thereby external user cannot masquerade attacks.

B. AUTHENTICATION

The users in the collaborative system of for scientific review and data sharing must be associated with blockchain wallets. Local host deployment creates 20 default accounts addresses and are assigned to test users with different roles. Authentication requires the user to share ORCID Id to generate a research profile.

C. CONFIDENTIALITY

The work uses Key Derivation Function to generate separate unique keys for each user role based on functionality. This simplifies the system from managing multiple key sets existing in recent work. AES encryption, because of its symmetric nature further lightens the user from managing keys associated with each kind of submission or task alloted.

D. INTEGRITY

Integrity allows the user to check if the stated data it owns is consistent and true to nature. Immutability and non-repudiation features of blockchain incorporated in the system for key derivation satisfies integrity check. Malicious user registered to the system cannot interact with the data access unless associated with a transaction history of the request submission or the data Id linked to the blockchain.

TABLE 8. Annotations used.

Symbol	Quantity
AES Dec	AES Decryption
AES Enc	AES Encryption
ACP_{PId}	Access Control Policy for PaperId
ABAC	Attribute based Access Control
DA	Data Owner Role
DAO	Data Owner Address
DO	Data Owner Role
DReq	Data Requestee Role
DReq	Data Requested
DK_{R_i}	Derived key for each reviewer
EA	Editor's Address
$ED@R$	Encrypted dataset at Rest
$ED@T$	Encrypted Data at Transit
KDF	Key Derivation function
LI	Lagrange Interpolation
MSK_{do}	Master Secret of data owner
MW	Metamask wallets
PId	Paper's ID
PC	Polynomial Coefficient
PL_i	Policy defined for flexible access
RA	Reviewer's Address
ReqA	Address of Data Requestee
RBAC	Role based access control
RSS	Review Status String
SSK	Shamir's Secret Key
SC_{do_i} T_i	Scaling factor by data owner do_i Tier's depicted in data ownership
TSC	Trust Score Calculation
Tx_{Id}	Transaction Id's
th_{TSC}	Threshold trust score value
ZTA	Zero Trust Architecture

E. DATA ACCESS

Research cannot be reproduced unless data is shared among collaborators with similar interest. Research work has stated rules for sharing data access using Lagrange interpolation, blockchain ids. These work lack context based approach for evaluating the request for data access. The Zero Trust architecture enables context based opinion to be considered. Dynamic nature evaluates individual perspective on category(affiliation, researcher profile), expectation(communication plan, funding agency), trust (monitoring transaction history), and discards user request with behavioural anomalies. Once the context based access control is evaluated confidential data to be transmitted securely is of utmost importance. users are assigned different tiers according to the range of their respective contribution. Shamir's secret key generation using Lagrange Interpolation secures data transmission once context based validation is received.

F. AUDITABLE RECORDS

The blockchain with its immutability and non repudiation features provides auditable records ensuring transparency.For each transaction pertaining to confidential review process or data access request, the policy enforced and result from the evaluted request executes through smart contract are saved as transactions into the blockchain. Thus, if any user claims of fraudulant denial of access request can be looked up in blockchain and thus can be proved. Even revocation of contracts doesnot affects the records stored in blockchain as it will logged for the long storage time. Further adding blockchain for audit-ability saves times in classical audit tasks such as verification of paper proofs, confirmation and verification of access control policy rules [22].

IV. CONCLUSION

Scientific collaboration and review system consist of critical review process and involves data sharing between collaborators. Both the process requires confidentiality since it deals with data of sensitive nature. BC ensures traceability, integrity and auditable records [21] for a decentralized review system, but to ensure confidentiality use of access control mechanism via smart contract is indispensible. For the implementation of the same, encryption standards and key management process are discussed. This ensures that only the assigned reviewers gets access to confidential unpublished manuscript, confidential review comments and review responses from authors throughout the review process.

For an effective scientific collaborations, the data sharing is indispensable. Sensitive data requires a mechanism to enforce dynamic user constraints. Zero trust architecture promotes data owner to set the criteria required to access the data. ZTA allows fine grained and flexible access control for the data protection and restricting access to undesired user. Data sharing in transit also required confidentiality implemented via encryption standards. Lastly author's feedback is proposed in reviewer's comments. This can be referenced by the editor for future recommendations in the SRCS. Thus the study ensures confidentiality is review process and collaborative data sharing mechanism by using access control mechanism and Zero Trust architecture for flexible context based access control allowing data owners to measure the competency of the researchers. Thus the requisite of SCRS

APPENDIX A

See the Table 8.

REFERENCES

[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 blockchain-based 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-reviewer-confidentiality

[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-review-manuscript#

[13] Case Number: 13-15. (2013). *Online Posting of Confidential Draft by Peer Reviewer*. Accessed: Oct. 29, 2023. [Online]. Available: https://publicationethics.org/case/online-posting-confidential-draft-peer-reviewer

[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. [Online]. Available: https://publicationethics.org/sites/default/files/WhoownspeerRev.Discuss.document.pdf

[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-a-manuscript.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. [Online]. Available: https://academic.oup.com/jxb/pages/notes_for_peer_reviewers#data

[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-and-procedures/#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/reviewer-guidelines

[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, "Blockchain-based 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/7f5c3a3e-51e7-4114-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 multi-stakeholder 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.

[61] E Academy. *Publons Giving Credit to Peer Reviewers*. Accessed: May 1, 2023. [Online]. Available: https://www.enago.com/academy/publons-giving-credit-to-peer-reviewers/

[62] L. Reilly. (Apr. 12, 2010). *Review Privacy on Web of Science Researcher Profile*. Accessed: May 1, 2023. [Online]. Available: https://publons.freshdesk.com/support/solutions/articles/12000089393-review-privacy-on-web-of-science-researcher-profile

[63] C. Cheung, C.-L. Sia, and K. Kuan, "Is this review believable? A study of factors affecting the credibility of online consumer reviews from an ELM perspective," *J. Assoc. for Inf. Syst.*, vol. 13, no. 8, pp. 618–635, Aug. 2012.

[64] A. K. Jha and S. Shah, "Disconfirmation effect on online review credibility: An experimental analysis," *Decis. Support Syst.*, vol. 145, Jun. 2021, Art. no. 113519.

[65] The OWASP Foundation. *Owasp Access Control*. Accessed: Oct. 29, 2023. [Online]. Available: https://owasp.org/www-community/Access_Control#:~:text=Since%2C%20in%20computer%20security%2C%20confidentiality,enforcing%20an%20access%2Dcontrol%20policy

S. POOJA received the bachelor's degree in information and technology from the College of Engineering Perumon, Kollam, Kerala, India, and the master's degree in cyber security from the College of Engineering Trivandrum, Trivandrum, Kerala. She is currently pursuing the Ph.D. degree in cyber security with the Department of Information and Communication Technology, Manipal Institute of Technology (MIT), Manipal Academy of Higher Education, Manipal, Karnataka, India. She is an Assistant Professor Sr. Scale with Manipal Academy of Higher Education. Her research interests include blockchain, semantic web, machine learning, deep learning, and cryptography.

C. B. CHANDRAKALA (Member, IEEE) received the bachelor's degree in electronics and communication engineering from the Sri Jayachamarajendra College of Engineering, Mysore University, Karnataka, India, and the master's degree in technology (software engineering) from SJCE Mysore, VTU, Karnataka, and the Ph.D. degree from MAHE, Manipal. She has working experience in both industry and academia. Currently, she is an Additional Professor with the Department of Information Technology and Communication, Manipal Institute of Technology, MAHE, Manipal. Her research interests include distributed computing, speech processing and recognition, blockchain technology, and software engineering.