iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82258

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Privacy-Preserving Blockchain Framework for Academic Records Using Off-Chain Storage

Kusum, Dr. Preeti,
M.Tech Student, Assistant Professor, Department of Computer Science & Engineering, World College of Technology and Management Gurgaon, Haryana, India

ABSTRACT: ***The process of the fast digitalization of academic record systems has brought forth important issues addressed to the sphere of data security, privacy, and efficiency of verification.Someoftheweaknessesof traditional centralized systems are breach of data, unauthorized access and poor verification systems. A decentralized and immutable blockchain-based solution is an adequate solution to manage academic records securely, but it contradicts the privacylegislation,likeGDPR,becauseofits transparentnature.Thisstudyadvocatesa privacy-sensitive blockchain architecturethat combines off-chain storage facilities to containscalabilityandprivacyproblems.The framework provides cryptographic hash of academiccredentialsthatarestoredon-chain and other real data are stored in secure off-chainstores.Thepaperassessesthepresented model with respect to the security, scalability, and compliance and proves that transparency and privacy can be balanced well using hybrid blockchain architectures. The results indicate that blockchain may be usedwithoff-chainstorageto createaviable and scalable approach to contemporary academic systems.***

Keywords: Blockchain, AcademicRecords, Privacy, Off-Chain Storage, GDPR, Smart Contracts

I. INTRODUCTION

With the development of digital technologies, the field of academic records management changed considerably. Institutions have been compelled to use the electronic systems to digitally store, handle andcheckthestudentdetails liketranscripts, diplomas and certificates. With those developments, the existing centralized systems still have critical issues suchas data breach, unauthorized engagements, and an inefficient verification system [7]. Single databasesrunbycentralizedacademicrecord systemsare susceptible to securityrisks, and can cause a single point of failure. In addition, the verification procedure in these systems is manual, time consuming and incurs direct communication between the institutions. The result of this is delays, higher administration costs and decreased trustwithinthestakeholders.Theblockchain technology has come up as a possible solution because of its impartiality and unalterable nature. The blockchain distributesinformationamongasetofnodes, eliminating the need to rely on a central authority and data integrity. But in the academic application of blockchain transparency is a major issue since confidentialityofsensitivestudentdatais required. One of the significant weaknesses of blockchain systems is the fact that data deletion cannot be provided, which does not align with the privacy laws, including the GeneralDataProtectionRegulation(GDPR).

II. LITERATUR EREVIEW

A. CentralizedAcademicSystemsand Their Limitations

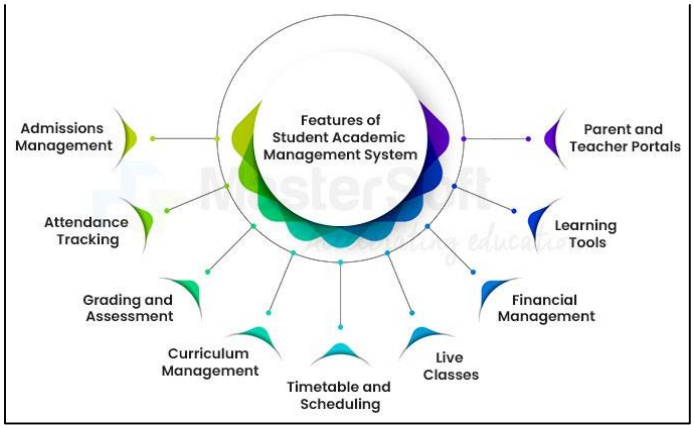


Figure1:Academicrecordmanagement systems

(Source:www.iitms.co.in)

The conventional academic record management systems mainly adhere to the centralized database structure, in which all data is maintained and managed by one authoritythat,inmostcasesisaneducational organization. Although these systems are easytomanageandaresimpletodesign,they areverylimitinginsecurity,reliabilityand effectiveness. Cyberattacks are very susceptibleincentralizedsystemssinceonce one is breached this can affect the entire database revealing sensitive student information, includingpersonalinformation, grades and certifications [2]. Also, internal threatspose arisk tothese systemswithdata being manipulated byadministrative people.

B. BlockchainforAcademicRecords

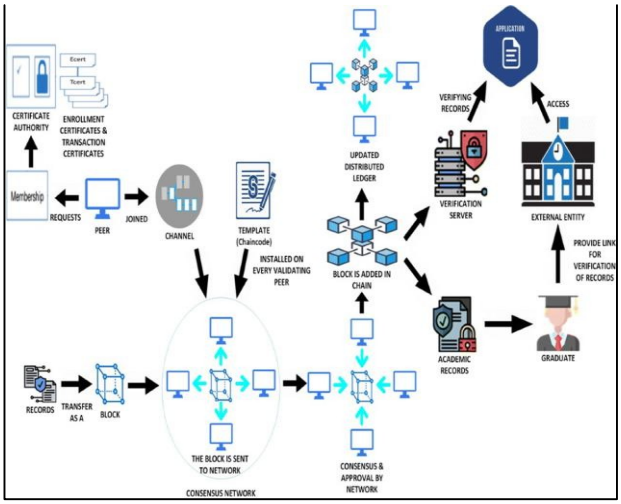


Figure2:BlockchainforAcademic Records

(Source:link.springer.com)

The blockchain technology has become a revolutionary approach to solve the shortcomingsofcentralizedacademicrecord systems. It functions on a decentralized network with information shared among severalnodes,thus,removingthecentral authority. The immutability is one of the major characteristics of blockchain as it guarantees the inability of the original data that is present on the ledger to be either altered or erased without the network participantsconsent[15].Theaboveproperty renders blockchain very capable of applications,whereintegrityofdataandtrust is important, e.g. verification of academic credentials. Blockchain could be applied in the field of academic records to store and verify credentials of students, such as degrees, transcripts, and certificates. Every record has a cryptographic hash attached to the record and which serves as a unique identifier and guarantees that any manipulation of the data is easily identified. The decentralized system of blockchain also allows emphasizing directly on credentials verification by employers or institutions, without mediators, which saves time of verification and administration costs.

C. PrivacyChallengesinBlockchain

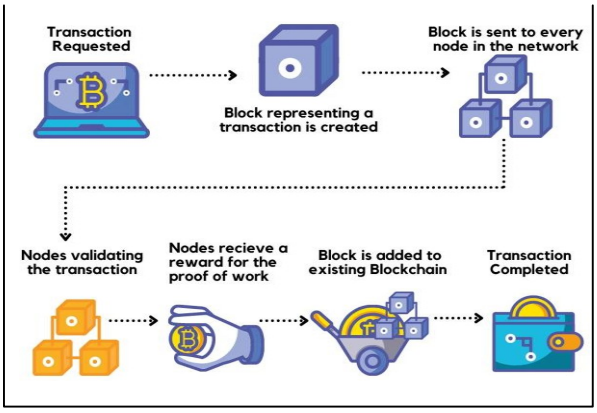


Figure3:PrivacyChallengesin Blockchain

(Source:www.getastra.com)

Although blockchain technology has good security and transparency, it is also associatedwithseriousissuesofprivacy,and particularlywhere it is used in internalareas of competency like academic records. The transparency of a blockchain is one of its natural features wherein all the transactions that go through the chain are transparent to other participants in the network[9]. As much as this feature makes business more trustworthy and accountable, it poses their ownmajorconcernsinhandlingpersonaland confidentialinformation.Studentrecordsin academicsystemsholdsensitiveinformation like identification information, academic performance and institutions. Direct storage of such data in the blockchain is likely to causeunauthorizeddisclosure,sinceeventhe encrypted data can be susceptible to some techniques of future disclosure[1]. Moreover, blockchain unfriendliness to privacyruleslikeGeneralDataProtection Regulation (GDPR) which provides individuals with the ability to alter or even erase their personal data is not compatible withtheconceptofblockchain. The fact that blockchain records cannot be destroyed or erased once stored poses a legal and ethical problem.

D. Off-ChainStorageSolutions

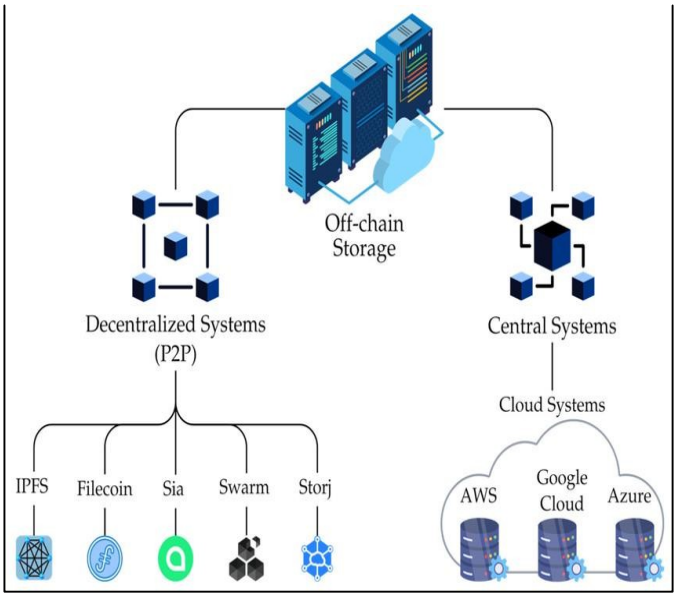


Figure4:Off-ChainStorageSolutions

(Source:www.researchgate.net)

The limitation on blockchain as far as scalabilityandprivacyareconcernedhas led to the suggestion of off-chain storage solutionsastheviablewayto dealwiththese limitations. Off-chain storage enables the datatobestoredexternallyinsteadofstoring large amounts of data directly in the blockchainbyhavingareferencetotheactual data added to the blockchain[12]. This reference is normally a cryptographic hash whichisauniquerepresentationofthestored data and guarantee actions its integrity. Off-chain management of data is typically done through technologies like the InterPlanetary File System (IPFS), cloud storage systems, and decentralized networks of storage[18]. Such systems offer scalable and flexible storagesystemsallowinginstitutionstowork with huge datasets without the high cost of storingtheminblockchains.Thetechniqueof saving the hashes on-chain and retaining the true data off-chain guarantees that any change on the off-chain data would be revealedontheverificationasthevalueofthe hashwillbedifferent.Privacywise,off-chain storage presents huge benefits in that the highly sensitive information is stored off-blockchain, thus reducing the chances of revealing it to unauthorized people.

E. Research Gap

Although the field of research investigating blockchain technologyand off-chain storage solutionshasexpanded,thereisstillacritical gap in the creation of integrated frameworks that can effectively integrate the two solutions into each other in the domain of academic record management. There are numerous sources available on using blockchain to provide data integrityor using off-chaintoincreasescalability,butnotmany consider the issue of ensuring privacy complianceandperformanceoptimisation,at thesametime[4].

Existingimplementations of blockchain often do not take into account the challenges of dealing with sensitive academic data in accordance with legal regulations, like GDPR. Although off-chain storage has been identified as one possible solution, littlehasbeendoneto studyhowto interlink it with blockchain smoothly to ensure the security, transparency, and convenience of verifying it. Moreover, the access control issues, institutional interoperability and real world problems of implementation are not sufficiently covered in the existing literature[10]. This paper seeks to fill this gap by proposing an integrated hybrid system which would capitalizeontheadvantagesofboth blockchain and off-chain storage. The suggested model aims at delivering the privacy preservation, efficiency in verification, and scalability, and deals with both administrative and real-life issues. In that way, it helps form a more powerful and practical solution to the recent academic record management systems.

III. PROBLEM STATEMENT

Thecurrent solutions, regardlessofthegreat achievements that have been made in digital academic systems, still have various fundamental problems that restrict their performanceandapplicabilityinreality. The absence of data privacy within blockchain-based infrastructure is among the key issues as the transparent aspect of blockchain may make sensitive academic data unavailable to unauthorizedparties[6].Also,directstorage in large amounts on-chain is expensive in storage and low on efficiency, which means that these systems are economically impractical to implement at scale. The final significant concern is that blockchain systems are not compatible with privacy laws,includingGDPR,thatacknowledgethe rightto modifyorerasepersonaldata,which does not align with the irreversible nature of blockchain.Moreover,existingsystemstend touseinefficientverificationmethodsbased on either manual procedures or institutional relatedness, causing delay and excessive burden on administration. These constraints underscore the imperative of an effective solution that ensures confidentiality, safety, and privacy-safe management of academic records and efficiency and credibility.

IV. RESEARCH OBJECTIVES

- To analyze privacy challenges in blockchain-basedacademicsystems
- Todesignahybridframeworkusing off-chain storage
- Toevaluatesecurity,scalability,and compliance of the proposed model
- Toproviderecommendationsfor real-world implementation

V. PROPOSED FRAMEWORK

A. *System Architecture*

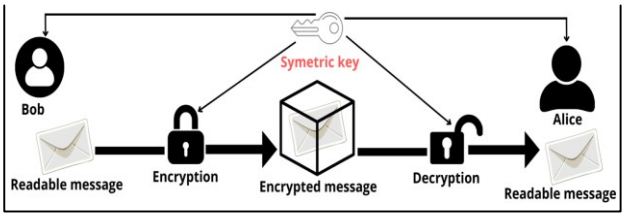


Figure5:Blockchaintechnologywithoff-chain storage system

(Source:www.mdpi.com)

The proposed framework is developed as a hybrid solution which combines blockchain technology with off-chain storage system to provide security as well as privacy in the management of academic records. The system consists of three layers that are closely associated with each other and each deals with respective set of functionalities that collectively guard data integrity, confidentiality and effective validation [14]. The initial element is the blockchain layer that is a building block of the system. This layeristaskedwithstoringthecryptographic hashes of academic records instead of the information. In this way, it makes sure once a record is put on record it can never be changed without being noticed. Decentralization of blockchain also leads to transparency and trust, all the participating nodeshavea matchedcopyofthe ledger[3]. Thisendstheneedtohaveacentralauthority and the possibilityof having single points of failure. The second element is the off-chain storagelayerwhereactualacademicrecords, which have been stored, are stored like the transcripts, certificates and degree records. As it isnot efficient and costlyto store large amounts of data directly on the blockchain, the layer is an efficient and scalable alternative. To preserve these records, such technologiescouldbeusedasthe InterPlanetary File System (IPFS), or secure cloud storage systems.

B. *Working Mechanism*

The operating principle of the suggested framework is ordered and organized sequence of actions that guarantees safe storing of academic materials and effective validation of academic records. Once an institutioncreatesastudentrecord,therecord will be uploaded to the off-chain storage system. This guarantees that the real data doesnotputunnecessarystressanddemands on the blockchain with extensive storage needs.Whentherecordisrecordedoff-chain, cryptographic hash of the document is computed with the help of the hashing algorithm e.g. SHA-256. This hash is a special form of the digital fingerprint of the record in such a way that any minor modification of the document will yield a totally different value of the hash [17]. The resultinghashwillbeaddedtotheblockchain creating a reference that is forever and irreversible. Upon an employer or another institution, having initiated a verification request, all the smart contract does is trigger verification of the authenticity of the record. The system accesses the stored document in off-chain database and re-generates its hash. Thisnewly-createdhashiscomparedtothe stored one on the blockchain. When the two hashes are the same, record is recognized, falsifying which will result in the record being tagged as tampered or invalid. This mechanism would guarantee quick and efficientverificationwithouttheneedtohave direct institution-to-institution communication.

C. *PrivacyMechanism*

The privacy policy of the suggested framework will focus on reducing exposure to sensitive data and ensuring integrity and verifiability of records. The system does not store actual academic information on the blockchain, but rather, only encrypted cryptographic references in the form of hashes. This would make sure that none of the personal identifiable information is availableintheblockchainnetworkpublicly. All confidential information is safely stored intheoffchainstoragetierwhereitissecured byusing an authentication and authorization process. Smart contracts are crucial in applying these access controls by defining whoisallowedtoaccessand/orverifycertain records [8]. Moreover, off-chain data can be encrypted in order to make it even more confidential. This has been defined as a hybrid solution, which complies with data securitystandards(likeGDPR)becauseit enables data to be changed or erased out of off-chain storage when necessary, a verifiable presence is logged on the blockchain. Subsequently, the system successfully balances transparency and privacy, which is why it would work well in the real-life academic scenario.

VI. METHODOLOGY

A. *ResearchType*

The research period is conceptual and analytical research as it does not involve empirical experimentation but design and assessment of a proposed system. The study is based on comprehensive research of the current literature on the blockchain technology, record management related to academic activities, and systemsdesigned to preserve privacy. Integrating the findings of previous research, the study will provide a systematic platform that will remove the inexistence of limitations.

B. *DataCollection*

The information that is employed in this researchisobtainedusingsecondarysources likepeer-reviewedjournals,conferencesand online databases that are considered to be credible. Theexistingstudiesconcerningthe implementation of blockchain, off-chain storagesolutions,anddataprivacyregulation areexaminedinordertodeterminethemajor challenges and possible solutions [11]. This method will make sure that the framework proposedisfoundedontestedknowledgeand up to date trends in technology.

C. *EvaluationCriteria*

The framework is suggested and tested on several criteria to determine the level of its effectiveness and feasibility. Security is examined as a capability of the system to avoidunauthorizedaccessandmanipulations ofthedata.Privacycomplianceassesseshow the system follows the data protection rules and its capacity to protect confidential data. Scalabilityismeasuredthroughtheabilityof the systemwhen dealing with large amounts of data and users to scale up to meet the needs. Cost efficiency is measured through thecostofstorage(coststostore),transaction cost, and total maintenance cost of the system.

VII. RESULTS AND DISCUSSION

A. *SecurityAnalysis*

The given model can be characterized by a high-security level based on the use of cryptographic hash and decentralized storage.

Hashing algorithm can be used to send any record, such that any alteration in therecordiseasilynoticedsincethehash value is modified. The blockchain is also decentralized, which helps to increase securityeven more asit doesnot have single pointsoffailureanditischallengingtoattack the system [5]. Also, blockchain records are immutable such that once information is added, it cannot be changed without consensus, thus offering a tamper-proof environment.

B. Privacy Analysis

The proposed framework greatly enhances privacy by implementing off-chain storage. Having sensitive information out of the blockchain makes it possible to avoid exposure of personal details by an unqualifiedmeans.Encryptedreferencingon theblockchainmeansthat exceptinanevent that the ledger is hacked, no valuable information can be gleaned. Moreover, the system helps to adhere to the regulations of data protection, as well as to control access and even possible modification of off-chain information. This contributes to the fact that theframeworkisapplicabletothecaseofthe environment where privacy is a vital issue.

C. Scalability Analysis

The scalability of the system can be significantlyincreasedwiththeintegrationof off-chain storage. As hash values only in small sizes are stored on the blockchain, the numberofdataloadedisconsiderably minimized.Thisresultsinincreasedspeedof transactions and performance of the system. Theoff-chainstoragelayercanalsobescaled veryeasilyto handlea significant amount of data, and the framework can be adapted to accommodate institutions having a huge amount of academic data.

D. CostAnalysis

The proposed system has a hybrid architecturethatenhancesthecostefficiency ofthesystembyreducingthequantityofdata to be stored at the blockchain. This lowers transactioncostsanddatastoragecostswhich are incurred in blockchain activities. Cloud-based storage systems and other off-chain data confirmation solutions provide seaweeds with a flexible and affordable alternative to operate and handle big data. Consequently, the total cost of system operation by this approach is less than with fully on-chain solutions.

VIII. ADVANTAGES OF PROPOSED SYSTEM

The suggested system has a number of key benefits in comparison to traditional and solely blockchain-based solutions. It improves the privacy of data, as it is not revealed onthe blockchain as sensitive. Off-chain storage can help to decrease storage expenses and enhance scalability, enabling thesystemtoprocesslargeamountsofdata [13].Smartcontractshavemadeitpossibleto verify academic records ina faster and more dependable manner due to the automated verification process. Also, it can be easily used in real-life applications since it aids in adhering to data protection rules. On the whole, the framework offers a moderate solution that is based on the security, efficiency, and privacy.

IX. LIMITATIONS

Although the proposed system has some benefits, it also has some limitations which should be listed. The effectiveness of the securityoftheframeworkalsopartiallyrelies on the reliability of the off-chain storage system which could pose vulnerabilities in case ofpoor management. Using blockchain with available institutional systems could be involving and might demand a lot of technical skills. Moreover, lack of a unified design of protocols to support an academic blockchain system can reduce interoperability between organizations.

X. FUTURE SCOPE

The advanced technologies and methodologies can be incorporated in the proposed framework as well. The use of intelligentverificationandanomalydetection can be achieved through incorporating artificial intelligence, which will ensure a better system performance. Zero-knowledge proofs can ensure much higher privacy guarantees, as they require data verification, but not informationdisclosureinactualform [16]. Also, the academic records blockchain networks across the world can be tested to enable a flawless interoperability of academic institutions, and a single and standardized system.

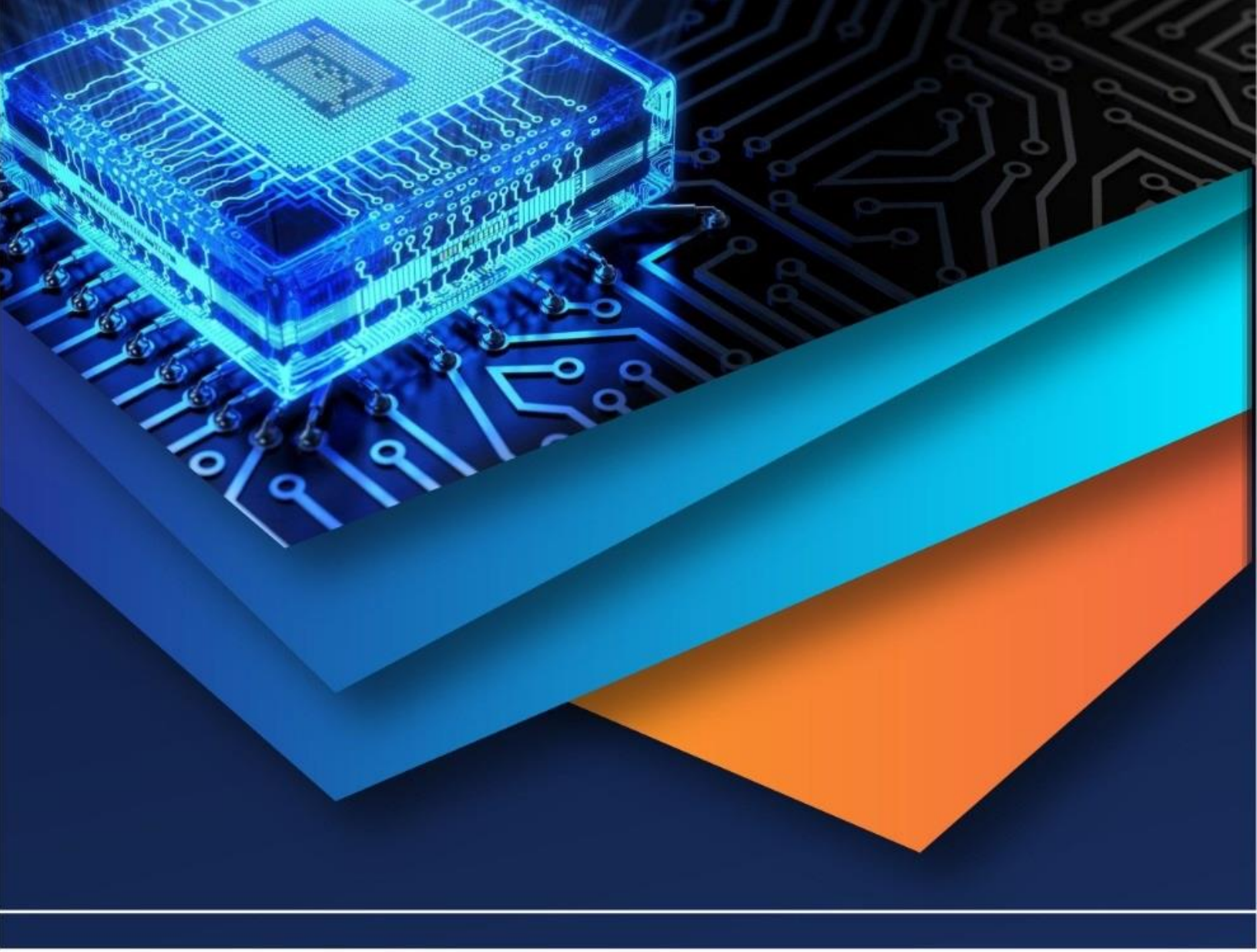
XI. CONCLUSION

The current study outlines a privacy-aware blockchain architecture within academic recordmanagement that effectivelyusesoff-chain storage as a means of potentially managing the main issues of privacy, scalability, and costs.

The suggested model balances between transparency and confidentiality by storing sensitive data out of the blockchain and guaranteeing cryptographic integrity via on-chain reference. The framework exhibits significant possibilities of real-world applicationandprovidesasafe,effectiveand scaledsolutiontohandlingacademicrecords. With digital transformation ever transforming the education sector, these hybrid architectures are bound to be an importantaspectinmakingsurethatthereis trustandreliabilitywhenit comesto academic credential systems.

REFERENCES

[1] Alao,O.,Adekeye,O.E.,Adeagbo,B.T. and Oyerinde, A.T., 2025. Privacy Preserving Blockchain Architecture for Securing Cloud Based Information Systems. ScientificJournalofEngineering,and Technology, 2(2), pp.165-171.
[2] Ayare, A.A., Jadhav, V.A., Banatwala, M.K., Changlere, S.V., Mote,A.,Joshi,P.,Mr,A.A.A.,Ms, V.A.J. and Banatwala, M., 2025. A systematic review on blockchain-based framework for storing educationalrecords using interplanetary file system. Cureus J Comput Sci, 2.
[3] Cruz,M.M.P., Balogo,K.M., Cofino, C.L.andDandan,D.G.,2024,March. A proposed distributed off-chain medical health record management using blockchain technology and IPFS for HEIs. In 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 627-635). IEEE.
[4] Eren, H., Karaduman, Ö. and Gençoğlu, M.T., 2025. Security challengesandperformancetrade- offs in on-chain and off-chain blockchainstorage:Acomprehensive review. Applied Sciences, 15(6), p.3225.
[5] Fernández-Iglesias, M.J., Delgado von Eitzen, C. and Anido-Rifón, L., 2024. Efficient traceability systems with smart contracts: Balancing on-chain and off-chain data storage for enhanced scalability and privacy. Applied Sciences, 14(23), p.11078.
[6] Goint, M., Bertelle, C. and Duvallet, C., 2023. Secure access control to data in off-chain storage in blockchain-based consent systems. Mathematics, 11(7), p.1592.
[7] Hlaing, H.H. and Asaeda, H., 2023, November. PrivOff: Secure and Privacy-Preserving Data Management for Distributed Off-Chain Networks. In 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 326-333). IEEE.
[8] Jayabalan, J. and Jeyanthi, N., 2022. Scalableblockchainmodelusingoff-chainIPFSstorageforhealthcaredata security and privacy. Journal of Parallel and distributed computing, 164, pp.152-167.
[9] Kaneriya, J. and Patel, H., 2023. A secure and privacy-preserving studentcredentialverificationsystem using blockchain technology. International Journal of Information and Education Technology, 13(8), pp.1251-1260.
[10] Kaur, J., Rani, R. and Kalra,N., 2022. A blockchain-based framework for privacy preservation of electronic health records (EHRs). Transactions on Emerging Telecommunications Technologies, 33(9), p.e4507.
[11] Kumar,A.,Kumar,R.and Sodhi,S.S.,2022.Anovelprivacy preservingblockchainbasedsecure storage framework for electronic
[12] Mandinyenya,G.andMalele, V.,2025.AHybridFrameworkfor EnhancingPrivacyinBlockchain-BasedPersonalDataSharingusingOff-Chain Storage and Zero-Knowledge Proofs. Journal of Information Systems and Informatics, 7(2), pp.1977-2005.
[13] Mohanta, B.K., Awad, A.I., Dehury, M.K., Mohapatra, H. and Khan, M.K., 2025. Protecting IoT-enabled healthcare data at the edge: Integratingblockchain,AES,andoff- healthrecords.JournalofInformation and Optimization Sciences, 43(3), pp.549-570.
[14] Li,K.,Lohachab,A.,Dumontier, M. and Urovi, V., 2025. Privacy preservation in blockchain-based healthcare data sharing: A systematic review. Peer-to-Peer Networking and Applications, 18(6), pp.1-53.
[15] Liu,C.,Hou,C.,Jiang,T.,Ning, J., Qiao, H. and Wu, Y., 2024. FACOS:Enablingprivacyprotection through fine-grained access control with on-chain and off-chain system. IEEE Transactions on Information Forensics and Security, 19, pp.7060-7074. chain decentralized storage. IEEE internet of things journal, 12(11), pp.15333-15347.
[16] Momin,R.J.I.,Rumi,A.M.S.and Reaz, R., 2026. ParikkhaChain: Blockchain-Based Result Processing and Privacy-Preserving Academic Record Management for the Complete Examination Lifecycle. arXiv preprint arXiv:2604.16827.
[17] Wang,B.,Jiang,R.,Pu,X.and Zhang, H., 2025. An on-chain andoff-chaincollaborativedata sharing and access control model for electronic medical records: B. Wang etal.TheJournalofSupercomputing, 81(2), p.396.
[18] Zhao,K.,Zhang,W.,Su,L., Wang,X.andLi,C.,2025.Research on blockchain-enabled consistency enhancementtechniquesforon-chain and off-chain interactions of privacy data.J.COMBIN.MATH.COMBIN. COMPUT, 127, pp.8979-8996.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY