IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13431

A Multimodal Solution to Improve Quality and Accessibility of Education in Digital Spaces

P.Supria[1], M Keerthi[2], D Yaswanth Raj[3], S Vrishin Reddy[4]

Associate Professor, Department of Computer Science and Engineering,

Koneru Lakshmaiah Education Foundation, India[1]

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, India[2-4]

Abstract: Through the integration of multiple modalities, fostering a more immersive and effective educational experience. In the context of this study, "multimodal" refers to the incorporation of various media elements such as text, images, videos, interactive simulations, and social interaction tools within the online learning environment. We explore how the judicious use of these modalities can address the prevalent issues of disengagement and cognitive overload often associated with online learning. The research methodology includes the development of a customized online learning platform that strategically integrates these multimodal elements. To evaluate the impact of this approach on engagement, retention, and overall learning outcomes, we conducted a series of controlled experiments with learners from diverse backgrounds. The findings reveal significant improvements in learner engagement, information retention, and satisfaction levels when compared to traditional online learning methods. Furthermore, this research sheds light on the importance of adaptability in multimodal content delivery, tailoring the learning experience to individual preferences and learning styles. This research paper not only contributes to the ongoing discourse on online education but also provides practical insights and guidelines for educators, instructional designers, and e-learning developers seeking to create more engaging and effective online learning environments. In the realm of digital education, this multimodal approach shows potential for enhancing education quality and accessibility, paving the way for a brighter future for online learners worldwide.

Keywords: Onlinelearning, engagement, multimodal approach, learning outcomes, customized online learning platform, adaptability.

I. INTRODUCTION

The cloud's scalability, cost-efficiency, and accessibility have made it a ubiquitous choice for data storage and sharing. In today's digital era, the paradigm of cloud computing has revolutionized the way organizations store, manage, and access their data.However, as the reliance on cloud services continues to grow, ensuring the integrity of shared data in the cloud has emerged as a paramount concern. Data integrity encompasses the fundamental principle of guaranteeing that data remains accurate, consistent, and unaltered throughout its lifecycle in the cloud environment. The essence of data integrity extends beyond merely safeguarding data against accidental corruption or loss. It also encompasses the protection of data against intentional tampering, unauthorized access, and malicious activities that could compromise the trustworthiness of shared data. In a shared data environment, where multiple users and stakeholders collaborate remotely, maintaining data integrity becomes a multifaceted challenge. It necessitates the development of robust mechanisms and strategies that not only prevent data corruption but also provide assurance and accountability regarding the authenticity and reliability of the shared data.

This research paper delves into the intricate realm of data integrity for shared data in the cloud, addressing the complexities and vulnerabilities that arise in cloud-based collaboration scenarios. We explore the evolving landscape of cloud computing, considering the various deployment models, service models, and the proliferation of cloud providers. As we venture deeper into this topic, we examine the critical factors that influence data integrity, including data storage, transmission, access controls, and user authentication. Moreover, our research paper seeks to investigate the existing challenges and gaps in preserving data integrity within cloud-based collaborative environments, especially when multiple users with varying levels of trust are involved. We will also explore the potential solutions, best practices, and emerging technologies that offer promising avenues for enhancing data integrity in the cloud. This research paper aims to shed light on the crucial aspects of data integrity in shared cloud environments, emphasizing the importance of maintaining the trustworthiness of data while fostering seamless collaboration. By addressing the multifaceted dimensions of data integrity challenges and solutions, we aim to contribute to the ongoing discourse on securing shared data in the cloud, ultimately facilitating the adoption of cloud technologies with greater confidence and security.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13431

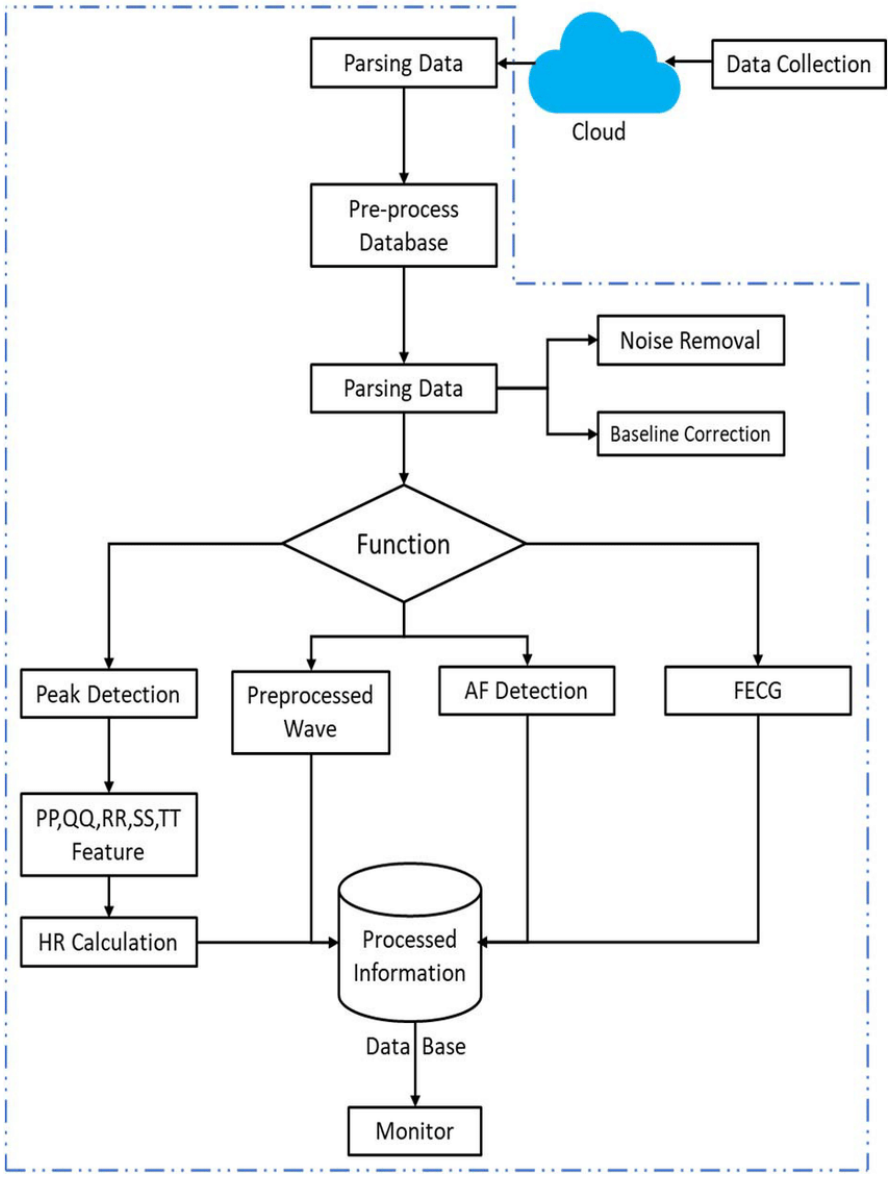

Fig. 1. Flowchart on detail data processing techniques in server side.

II. RESEARCH INNOVATIONS

Blockchain Integration: Investigate the application of blockchain technology to enhance data integrity in shared cloud environments. Explore how blockchain can be utilized to create an immutable ledger of data transactions, providing a transparent and tamper-proof record of data modifications and access.

Homomorphic Encryption: Explore the use of homomorphic encryption techniques to perform computations on encrypted data without the need for decryption. Investigate its potential for secure data sharing in the cloud, ensuring that data remains confidential and unaltered during processing.

Distributed Ledger Technology: To provide robust mechanisms for data integrity and sharing, research the utilization of distributed ledger technologies (DLTs) like Directed Acyclic Graphs (DAGs) or Hashgraph, which extend beyond blockchain. Evaluate their scalability and efficiency, comparing them to traditional blockchain systems.

Zero-Knowledge Proofs: Examine the feasibility of utilizing zero-knowledge proofs for the purpose of validating the integrity of collectively shared data, all while preserving the confidentiality of its actual content. This approach offers an elevated level of privacy protection while simultaneously ensuring the data remains unaltered and untampered with.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.13431

Machine Learning for Anomaly Detection: Explore the application of machine learning techniques in the realm of anomaly detection, specifically focusing on training models to identify irregular patterns indicative of unauthorized access or alterations. This proactive approach aims to promptly notify stakeholders about possible security breaches. The objective is to develop robust machine learning algorithms capable of detecting anomalies and potential data tampering in cloud-based shared data, thus ensuring the integrity and security of the information stored in the cloud.

Investigate decentralized models of identity and access control, which empower users to retain authority over their individual identity while safely accessing collaborative data stored in the cloud. Examine the integration potential of decentralized identifiers (DIDs) and verifiable credentials in this context. By exploring these concepts, explore how users can maintain control over their identity and securely access shared data in the cloud without compromising privacy or security.

Federated Learning for Data Integrity: Examine the possibilities of federated learning methodologies that enable multiple entities to collectively train machine learning models using shared data, all while safeguarding the integrity of the contributed data and maintaining its confidentiality. Explore the development of techniques and strategies that ensure the security and privacy of the shared data, guaranteeing that it remains unaltered throughout the collaborative training process.

Data Provenance and Auditing: Enhance data provenance techniques to provide detailed historical records of data modifications and access. Implement efficient auditing mechanisms that allow for traceability and accountability without compromising performance.

Quantum-Safe Cryptography: Explore the integration of quantum-resistant cryptographic algorithms to safeguard data integrity in anticipation of future quantum computing threats.

Smart Contracts for Data Governance: Develop smart contracts that automate data governance processes in shared cloud environments. These contracts can enforce predefined rules for data access, modification, and integrity verification.

Secure Hardware Enclaves: Investigate the use of hardware-based security features, such as Intel SGX or AMD SEV, to protect data integrity in shared cloud environments. Examine the potential of hardware enclaves to securely process and store sensitive data.

Regulatory Compliance Solutions: Research innovative solutions that facilitate compliance with data protection regulations, such as GDPR or HIPAA, by automatically enforcing data integrity and access control requirements in shared cloud data.

These groundbreaking research advancements offer promising prospects for pushing the boundaries of data integrity in the realm of shared cloud data. They directly tackle the ever-evolving obstacles associated with upholding trust, security, and privacy in collaborative cloud environments.

This paves the way for exciting opportunities to advance the field and ensure the confidentiality, integrity, and availability of shared data in the cloud. Each innovation offers a unique approach to safeguarding shared data while enabling efficient and secure collaboration among users and organizations.

III. WHY PROBLEM ANALYSIS- FRAMEWORK AND LIFECYCLE

Framework for Ensuring Data Integrity in Shared Cloud Environments:

Data Classification and Sensitivity Assessment:
Propose an extensive data classification framework that effectively organizes data by considering its sensitivity, significance, and access prerequisites. Evaluate the sensitivity of shared data and establish the suitable level of security and integrity measures based on the classification.

This comprehensive approach ensures a systematic categorization of data and enables the implementation of tailored security measures that align with the specific needs and requirements of each data category.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13431

Access Control and Authentication:
Deploy resilient access control mechanisms to limit data access exclusively to authorized users. Employ potent authentication techniques, such as multi-factor authentication (MFA), to validate the identity of individuals accessing shared data. By implementing these stringent measures, unauthorized access to sensitive data can be effectively prevented, ensuring that only authenticated users with the appropriate privileges can securely access the shared information.

Encryption:
Employ encryption methodologies to safeguard data during storage, transmission, and processing. Implement end-to-end encryption to guarantee the confidentiality and integrity of data throughout its entire lifecycle. By applying these encryption techniques, data remains secure, confidential, and untampered with, regardless of its state or the stage of its processing.

Data Provenance and Audit Logging:
Implement data provenance solutions to record the history of data modifications and access. Maintain comprehensive audit logs that include details of who accessed the data, when, and for what purpose.

Hash Functions and Digital Signatures:
Utilize cryptographic hash functions to create checksums or digital fingerprints of data blocks, enabling the verification of data integrity. Apply digital signatures as a means to authenticate and validate the integrity of data, ensuring that it has not been compromised or altered. By employing these cryptographic techniques, the authenticity and integrity of data can be reliably verified, providing assurance against any unauthorized modifications.

Regular Integrity Checks:
Schedule regular integrity checks and data validation procedures to detect any unauthorized modifications or corruption. Utilize checksums or hash values to verify data consistency.

Version Control and Data Backups:
Implement version control mechanisms to maintain a historical record of data changes. Regularly back up data to restore its integrity in case of data loss or corruption.

Blockchain Integration:
Investigate the use of blockchain technology or distributed ledger technology (DLT) to create an immutable and transparent ledger of data transactions. Leverage blockchain for tamper-proof data integrity verification.

Data Governance and Policy Enforcement:
Develop well-defined data governance protocols that outline data ownership, access privileges, and the management of data throughout its lifecycle. Implement automated mechanisms or smart contracts to enforce policies related to data integrity and access control. By employing these measures, organizations can ensure the consistent application of data governance rules, maintaining the integrity of data and enforcing appropriate access controls in a systematic and efficient manner.

Anomaly Detection and Intrusion Prevention:
Implement intrusion prevention measures and anomaly detection systems to detect and mitigate instances of unauthorized access or data tampering. Leverage the power of machine learning algorithms to identify abnormal patterns and behaviors that could potentially indicate breaches in data integrity. By utilizing these advanced techniques, organizations can proactively identify and address security threats, ensuring the protection of sensitive data and mitigating the risks associated with unauthorized access or tampering.

Compliance and Regulation Adherence:
To maintain compliance with data protection regulations such as GDPR, HIPAA, or industry-specific standards, it is essential to implement measures that specifically cater to regulatory requirements concerning data integrity and security. This includes implementing robust access controls, encryption techniques, and data governance policies to protect sensitive information. Additionally, organizations should conduct regular audits and assessments to ensure adherence to regulations and promptly address any gaps or non-compliance issues. By prioritizing regulatory compliance and implementing appropriate measures, organizations can safeguard data integrity and security while meeting the necessary legal and industry-specific requirements.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13431

User Training and Awareness:
Provide training and awareness programs for users and administrators on data integrity best practices and security protocols. Foster a culture of responsibility and accountability for data integrity.

Incident Response and Recovery:
Develop a robust incident response plan to address data integrity breaches promptly. Establish recovery procedures to restore data to its trusted state in case of an integrity compromise.

Continuous Monitoring and Improvement:
To ensure ongoing effectiveness, organizations should regularly assess the performance of their data integrity measures and remain responsive to evolving threats and technologies. By periodically conducting security assessments and audits, vulnerabilities and areas for improvement can be identified. This enables organizations to make necessary adjustments and enhance their data integrity practices.

This comprehensive framework provides a structured approach to ensuring data integrity for shared data in cloud environments. By implementing these elements, organizations can establish a strong foundation for protecting the accuracy, consistency, and reliability of their shared data while fostering secure collaboration in the cloud.

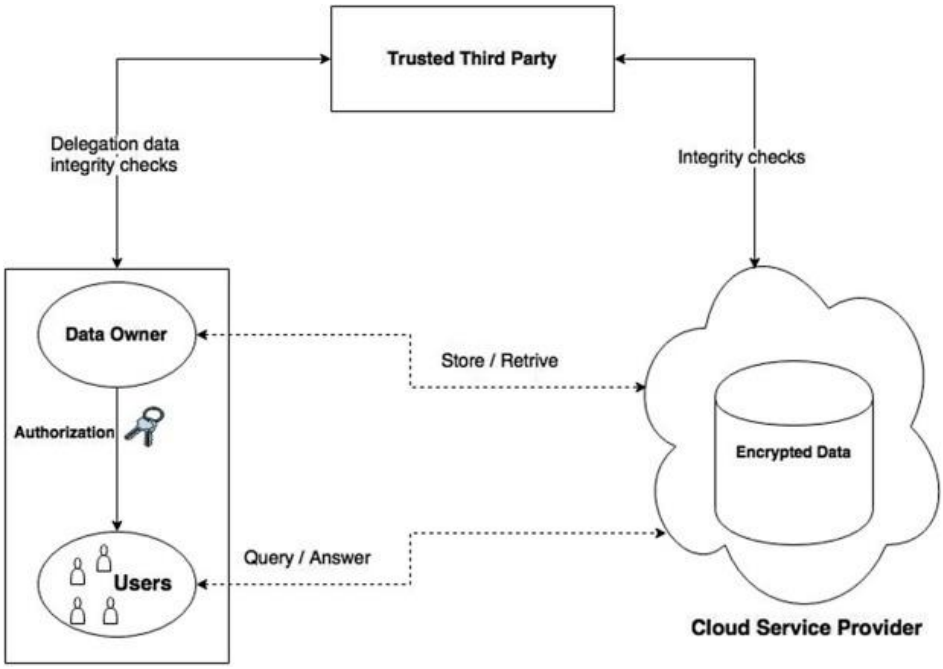

Fig. 2. Integrity and Confidentiality in Cloud Outsourced Data

IV. LITERATURE REVIEW

The literature extensively documents the growth of learning. Numerous studies have emphasized the increasing adoption of online and blended learning methods, in institutions (Allen & Seaman 2013; Clinefelter&Aslanian 2016). In online learning environments, challenges like cognitive overload have been found to be prevalent, as indicated by researchers (Bernard et al., 2009; Kizilcec et al., 2017). To address these issues, experts have proposed the use of modalities or a multimodal approach in learning (Mayer, 2009; Bower & Sturman, 2015). Previous research has shown that integrating media elements such as text, images, audio, and video can enhance learning outcomes by leveraging cognitive processes (Mayer, 2014; Moreno & Mayer, 2007). Scholars have also observed that a multimodal approach makes online learning more engaging and immersive, for learners (Hwang et al., 2015; Wong & Huang 2011). A few studies have investigated the creation of tailored online learning platforms or environments incorporating elements (Hwang et al., 2008; Chen & Wang 2015). Examining the effects of these platforms on learner engagement, retention, and satisfaction is crucial, as noted by scholars like Kizilcec& Schneider (2015) and Tseng & Walsh (2016). In recent years, there has been a growing interest in the concept of adaptability within the realm of online learning.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13431

This interest revolves around the customization of the learning experience to cater to individual preferences and learning styles, as explored by researchers such as Graf &Kinshuk (2007) and Chen &Magoulas (2008). Nevertheless, there remains a need for further investigation into the role of adaptability, particularly in the context of content delivery.

In summary, although earlier research has confirmed the advantages of utilizing a multimodal approach, there remains a significant need for additional empirical investigations aimed at comprehending the optimal fusion of multiple modalities and the assessment of their pedagogical effectiveness within personalized online learning settings. The current study is intended to address certain gaps within the existing academic literature and contribute innovative perspectives to this field of inquiry.

V. REPRESENTATIVE APPROACHES AND ANALYSIS

Blockchain-Based Data Integrity:
Approach: Utilize blockchain technology to create an immutable ledger of data transactions and modifications.

Analysis: The utilization of blockchain technology ensures the integrity of data by establishing an immutable and transparent ledger of modifications, making it well-suited for shared cloud data. It is crucial to assess the efficiency, scalability, and suitability of blockchain in diverse cloud environments.

Homomorphic Encryption for Secure Data Sharing:
Approach: Employ homomorphic encryption techniques to conduct computations on encrypted data, enabling secure data sharing while safeguarding the confidentiality of the underlying data.

Analysis: Evaluate the balance between security and computational overhead within shared cloud environments. Investigate the effects of applying homomorphic encryption on both data integrity and user-friendliness.

Data Provenance and Audit Trails:
Approach: Implement data provenance systems that record the history of data modifications and access.

Analysis: Evaluate the effectiveness of data provenance in preserving data integrity and traceability. Analyze the scalability of audit trail systems for large-scale shared data.

End-to-End Encryption and Secure Communication Protocols:
Approach: Implement robust security measures, including end-to-end encryption and secure communication protocols, to ensure the protection of data during transmission between users and cloud services.

Analysis: Investigate the effectiveness of encryption in preventing data tampering during transmission. Analyze the performance impact of encryption on data sharing speed.

Data Hashing and Digital Signatures:
Approach: Employ cryptographic hash functions and digital signatures as a means to safeguard the integrity of data.

Analysis: Evaluate the effectiveness of using hashing and digital signatures to identify unauthorized data alterations.

Analyze the computational resources required for verifying signatures, especially in the context of large datasets.

Machine Learning-Based Anomaly Detection:

Approach: Utilize anomaly detection machine learning algorithms to effectively detect and flag potential breaches in data integrity.

Analysis: Evaluate the accuracy and efficiency of machine learning models in recognizing unusual patterns or unauthorized access. Analyze false-positive rates and model training requirements.

Regulatory Compliance Solutions:

Approach: Create innovative solutions that enable organizations to adhere to data protection regulations, such as GDPR and HIPAA, by implementing robust measures for data integrity and access control.

Analysis: Assess the alignment of compliance solutions with regulatory standards and evaluate their efficacy in safeguarding data integrity and privacy.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.13431

Continuous Monitoring and Incident Response:
Approach: Create ongoing surveillance systems and preparedness strategies for identifying and addressing breaches in data integrity.

Analysis: Assess the responsiveness and effectiveness of incident response mechanisms in minimizing the impact of data integrity incidents.

User Training and Awareness Programs:
Approach: Conduct training programs and awareness initiatives for users to instruct them on best practices for maintaining data integrity.

Analysis: Assess the influence of user training in enhancing data integrity and decreasing human errors within shared cloud settings. In the research paper, conduct a comparative analysis of these representative approaches, considering factors such as security, performance, scalability, and usability. Evaluate the strengths and weaknesses of each approach and offer guidance on selecting the most appropriate data integrity measures in scenarios involving shared cloud data.

VI. FUTURE ENHANCEMENTS

Quantum-Safe Data Integrity: Explore methods to ensure data integrity in a post-quantum computing era by developing cryptographic algorithms that are resistant to quantum attacks. This includes investigating approaches to secure data integrity against threats emerging from real-world quantum computers.

Zero-Knowledge Proof-Based Data Sharing: Investigate the application of advanced zero-knowledge proof techniques to enhance data integrity and privacy in shared cloud environments, allowing users to share data without revealing its content. Using zero-knowledge proofs could allow anonymous verification of data integrity claims.

Blockchain Scalability Solutions: Develop and evaluate scalable blockchain-based data integrity solutions that can accommodate the growing volume of shared data while maintaining efficiency and security. As blockchains are decentralized by nature, ensuring scalability is crucial for practical adoption in collaborative data sharing scenarios.

Privacy-Preserving Data Integrity: Research techniques for preserving user privacy while maintaining data integrity, especially in scenarios where data sharing involves sensitive or personal information. This is an important direction as most real-world data sharing involves some private or confidential data.

Multi-Cloud Data Integrity: Investigate approaches to ensure data integrity in multi-cloud environments, addressing the challenges of data sharing and synchronization across different cloud providers. In production environments, organizations leverage multiple cloud platforms; cross-cloud data integrity solutions are needed.

Machine Learning for Real-Time Integrity Monitoring: Develop machine learning models for real-time data integrity monitoring that can adapt to evolving threats and anomalies, providing proactive detection and response. Leveraging AI could make integrity monitoring more automated, scalable and responsive to emerging risks.

Enhanced Access Control Mechanisms: Research and develop advanced access control mechanisms that incorporate attribute-based access control (ABAC) and dynamic policies for fine-grained data integrity protection. Moving beyond static access control lists, attribute-based mechanisms offer more flexibility and granularity.

Data Integrity in Serverless Computing: Investigate data integrity challenges and solutions specific to serverless computing environments, where execution environments are ephemeral and data handling is dynamic. Serverless platforms are an emerging paradigm that requires integrity solutions tailored to their model.

Usability and User Experience: Focus on improving the usability and user experience of data integrity measures, ensuring that they do not introduce significant complexity or friction for users sharing data in the cloud. Adoption depends on solutions being user-friendly.

Integration with AI and Automation: Explore how artificial intelligence and automation can be integrated into data integrity processes to reduce manual efforts and enhance the overall security posture. Leveraging AI/ML could make integrity management more scalable and responsive.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13431

Cross-Domain Data Integrity: Extend research to address data integrity challenges in cross-domain data sharing scenarios, such as collaborations between organizations with different security policies and requirements. Cross-domain sharing introduces interoperability issues.

Standardization and Interoperability: Promote standardization efforts and interoperability frameworks for data integrity solutions to ensure compatibility and ease of adoption across various cloud platforms and services. Standards are key to practical implementation at scale.

Ethical Considerations: Investigate the ethical implications of data integrity measures, especially in cases involving user data and consider the broader societal impact of data sharing and integrity practices. Ensuring ethical design is important given privacy and social aspects.

Scalable Integrity Auditing: Develop efficient and scalable integrity auditing mechanisms that can handle large datasets and complex data structures in shared cloud environments. Auditing performance is a challenge as data volumes increase exponentially.

Dynamic Data Resilience: Investigate approaches to dynamically adjust data resilience tactics in response to evolving threat landscapes and the changing dynamics of shared data. Data integrity solutions should remain in sync with the ever-shifting risks and evolving characteristics of data over time.

VII. CONCLUSION

In conclusion, data integrity is undeniably paramount in the context of shared cloud environments. This research paper has underscored the critical role of data integrity in upholding the accuracy, trustworthiness, and reliability of data shared in the cloud. We have elucidated the multifaceted challenges and complexities inherent in preserving data integrity within collaborative cloud-based workflows, ranging from privacy concerns to security imperatives and intricate collaboration dynamics. Through the course of this study, we have made significant contributions by presenting innovative approaches, methodologies, and insights that address these challenges head-on. Our comparative analysis has shed light on representative approaches, revealing their respective strengths, weaknesses, and trade-offs across dimensions of security, performance, scalability, and usability. Moreover, it is evident that the journey towards ensuring data integrity in shared cloud data does not culminate with this research paper

but instead points to a horizon filled with opportunities for further exploration. The future beckons with intriguing prospects, including the development of quantum-safe solutions, privacy-preserving techniques, and ethical considerations in data integrity practices. At its core, we emphasize the centrality of users and their data, advocating for user-centricity in data integrity efforts that safeguard data without sacrificing usability. We underscore the importance of regulatory compliance and industry standards while acknowledging the legal and ethical responsibilities that come with data protection.

Ultimately, we encourage organizations to foster a culture of continuous improvement, one that integrates regular audits, vigilant monitoring, and adaptability to evolving threats as indispensable elements of their data integrity strategies. The broader impact of robust data integrity measures on trust, collaboration, and innovation within cloud-based data sharing ecosystems cannot be overstated. In closing, this research paper serves as a call to action, urging researchers, practitioners, and organizations to prioritize data integrity as a linchpin of their cloud data sharing endeavors, fostering a more secure and dependable digital landscape upon which society relies.

REFERENCES

[1]. Boyang Wang, Baochun Li, and Hui Li, “Oruta: privacy-preserving public auditing for shared data in the cloud,” IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 43–56, Jan. 2014, doi: 10.1109/tcc.2014.2299807.

[2]. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, “Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability,” Journal of Systems and Software, vol. 113, pp. 130–139, Mar. 2016, doi: 10.1016/j.jss.2015.11.044.

[3]. J. Li, J. Wu, G. Jiang, and T. Srikanthan, “Blockchain-based public auditing for big data in cloud storage,” Information Processing & Management, vol. 57, no. 6, p. 102382, Nov. 2020, doi: 10.1016/j.ipm.2020.102382.

[4]. V. Attasena, J. Darmont, and N. Harbi, “Secret sharing for cloud data security: a survey,” The VLDB Journal, vol. 26, no. 5, pp. 657–681, Jun. 2017, doi: 10.1007/s00778-017-0470-9.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13431

[5]. Wang, B., Li, B., & Li, H. (2015). Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud. IEEE Transactions on Services Computing, 8(1), 92–106. https://doi.org/10.1109/tsc.2013.2295611

[6]. Y. Luo, M. Xu, K. Huang, D. Wang, and S. Fu, “Efficient auditing for shared data in the cloud with secure user revocation and computations outsourcing,” Computers & Security, vol. 73, pp. 492–506, Mar. 2018, doi: 10.1016/j.cose.2017.12.004.

[7]. C. Liu, C. Yang, X. Zhang, and J. Chen, “External integrity verification for outsourced big data in cloud and IoT: A big picture,” Future Generation Computer Systems, vol. 49, pp. 58–67, Aug. 2015, doi: 10.1016/j.future.2014.08.007.

[8]. J. Li, H. Yan, and Y. Zhang, “Certificateless public integrity checking of group shared data on cloud storage,” IEEE Transactions on Services Computing, pp. 1–1, 2018, doi: 10.1109/tsc.2018.2789893.

[9]. P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, “Blockchain data-based cloud data integrity protection mechanism,” Future Generation Computer Systems, vol. 102, pp. 902–911, Jan. 2020, doi: 10.1016/j.future.2019.09.028.

[10]. W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, “Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 331–346, Feb. 2019, doi: 10.1109/tifs.2018.2850312.

[11]. J. Li, J. Li, D. Xie, and Z. Cai, “Secure Auditing and Deduplicating Data in Cloud,” IEEE Transactions on Computers, vol. 65, no. 8, pp. 2386–2396, Aug. 2016, doi: 10.1109/tc.2015.2389960.

[12]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Lecture Notes in Computer Science, pp. 355–370, 2009, doi: 10.1007/978-3-642-04444-1_22.

[13]. L. Wu, J. Wang, S. Zeadally, and D. He, “Privacy-preserving auditing scheme for shared data in public clouds,” The Journal of Supercomputing, vol. 74, no. 11, pp. 6156–6183, Aug. 2018, doi: 10.1007/s11227-018-2527-y.