IJHRMOB

International Journal of HRM and Organizational Behavior

www.ijhrmob.com

editor@ijhrmob.com

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

AN AUTHORIZED PUBLIC AUDITING SCHEME FOR DYNAMIC BIG DATA STORAGE IN PLATFORM AS A SERVICE

Rajeswaran Ayyadurai

IL Beauty and Health Natural Oils Inc. 2644 Hegan lane , Chico CA, rajeswaranayyadurai@arbpo.com

ABSTRACT

Ensuring data integrity and security has become essential with the rise in big data and the increasing reliance on cloud computing. The permitted public auditing scheme designed specifically for dynamic big data storage in Platform as a Service (PaaS) environments is presented in this paper. The plan protects data confidentiality while enabling external auditors to confirm the quality and integrity of data stored in distributed systems using cryptographic methods. To ensure compliance, scalability, and security, the methodology makes use of digital signatures, hash functions, and Proof of Retrievability (PoR) methodologies. This scheme tackles the issues of dynamic data operations and regulatory compliance by utilizing secure communication protocols and integrating with many PaaS frameworks. It offers a full solution for contemporary cloud storage requirements.

Keywords: Public Auditing, Big Data Storage, Cloud Computing, Platform as a Service, Data Integrity, Cryptographic Protocols.

1 INTRODUCTION

Cloud computing settings are the target market for a cryptographic protocol called approved public auditing scheme. The ability to check the accuracy and integrity of data stored in distributed storage systems or the cloud is granted to external auditors who possess the necessary authority. Without jeopardizing data protection, this guarantees accountability and openness. Digital signatures and hash functions are two examples of cryptographic techniques used in the approach. Alongside the data, data owners safely keep integrity proofs or tags that they create. Auditors independently check these proofs to guarantee data integrity, having been granted authorization through audit credentials provided by data owners. In order to ensure auditability and security standards, this process also handles data updates and revisions.

Platform as a Service (PaaS) dynamic big data storage describes cloud platforms' capacity to manage and store massive, ever-expanding datasets in an efficient manner. PaaS provides scalable storage solutions that can grow or shrink in response to demand, saving businesses from having to maintain their own hardware and software infrastructure. For enterprises to handle changing data quantities and processing requirements without compromising performance, this flexibility is essential. PaaS suppliers transfer data over several servers using distributed storage systems, guaranteeing availability and dependability even during times of high demand.

Another feature of dynamic big data storage in PaaS is flexibility. Different storage choices, each suited to particular use cases and access patterns, are offered by providers. For unstructured data, these possibilities include object storage, and for structured data, relational databases. These storage options can be dynamically changed to balance performance and cost depending on the needs of the application. In PaaS environments, security is critical. To protect data from breaches and adhere to industry requirements, providers employ encryption, access controls, and monitoring.

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

PaaS platforms integrate with frameworks like Apache Hadoop and Spark to provide real-time data processing and analytics. This makes it possible for companies to quickly analyze complex data and extract insightful information that improves operational efficiency and decision-making. Distributed file systems, metadata management for effective data retrieval, and complete data management services like backup and recovery are examples of technical features.

Ensuring the integrity and security of data stored in cloud environments is the goal of an authorized public auditing method for Platform as a Service (PaaS) dynamic big data storage. With the protection of privacy, it enables independent external auditors who are approved by data owners or regulatory agencies to confirm the accuracy of data. By utilizing cryptographic methods and access controls to preserve data integrity throughout its lifecycle, this approach tackles the difficulties brought about by the scalability and dynamic nature of large data in cloud systems.

Practically speaking, this auditing program helps PaaS users to confirm that their data is reliable and consistent throughout time. To produce evidence of data integrity, it incorporates cryptographic procedures such as hash functions and digital signatures. In order to give stakeholders and data owners peace of mind that their data has not been altered or distorted, auditors can validate these evidence. Additionally, the program facilitates adherence to legal mandates pertaining to security and data protection in cloud computing settings.

The development of cryptography and cloud computing has made permitted public auditing schemes possible. These strategies were first created to guarantee data integrity in conventional storage systems, but they have since changed to satisfy the needs of cloud-based infrastructures. Access control and secure data storage were the main priorities of the early implementations. The growing ubiquity of cloud platforms, especially in relation to PaaS offerings, made scalable and secure auditing solutions imperative.

In PaaS systems, permitted public auditing schemes must be implemented using a range of software tools and frameworks. Secure communication protocols, auditing APIs, and cryptographic libraries are all integrated into cloud providers' systems. AWS SDKs for auditing AWS services, Azure Security Center for Microsoft Azure compliance monitoring, and OpenSSL for encryption are a few examples.

Numerous establishments and academic centers have put in place auditing plans specifically designed for dynamic big data storage on PaaS. Enhancing data integrity, transparency, and regulatory standard compliance are the main goals of these solutions. To ensure that audit logs are verifiable and unchangeable, they frequently use blockchain technology, timestamp-based protocols, and proof of retrievability (PoR) techniques.

An authorized public auditing method in PaaS aims to accomplish the following main goals:

- Providing accurate and untainted data storage in the cloud is known as data integrity assurance.
- Accountability and Transparency: Enabling auditors to independently confirm data accuracy.
- Compliance: Adhering to privacy and data security regulations.
- Scalability: The ability to efficiently manage high data volumes and varying workloads.
- Using strong cryptography and access control techniques will increase security.

In the realm of approved public auditing schemes, research gaps persist despite advancements: Effectively handling modifications to access control and data updates is known as dynamic data management. Privacy-Preserving Techniques: Guarding the confidentiality of data when conducting audits. Standardization is the process of creating industry norms for inspecting PaaS services. Cost-Efficiency: Reducing resource consumption through process optimization for audits. Emerging Threats: Preventing changing cybersecurity risks in cloud computing settings.

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

PaaS dynamic large data storage auditing systems are continuously improved by technological advancements: Better algorithms for safe data verification are examples of cryptographic innovations. Distributed Ledger Technology: Blockchain provides immutable audit trails. AI and ML Integration: Using machine learning to identify anomalies in audit data. Microservices and containerization for scalability auditing are examples of cloud-native solutions. Interoperable frameworks for auditing across PaaS providers are known as cross-platform compatibility.

Effective auditing systems for dynamic big data storage in PaaS continue to present challenges. Scalability: modifying auditing procedures to accommodate increasing amounts of data. Privacy Concerns: Maintaining the privacy of data when conducting audits. Regulatory Compliance: Handling intricate laws pertaining to data security. Resource Restrictions: Cutting expenses by streamlining auditing procedures. Cybersecurity Threats: Reducing the possibility of assaults and data breaches.

2 LITERATURE SURVEY

Li (2021) In order to improve security and privacy, this article presents a blockchain-based public auditing system for cloud data that makes use of self-certified public keys. The protocol allows third-party auditors to validate data integrity without seeing the actual data, while also ensuring transparent and immutable audit records through the integration of blockchain technology. Using self-certified public keys improves security and streamlines key management. This protocol is appropriate for real-time applications since it allows for dynamic data operations like insertion, deletion, and modification. It conforms with data privacy laws like the CCPA and GDPR and offers strong defense against a range of security risks. The protocol's effectiveness and efficiency, together with its low computational and storage overhead, are demonstrated by performance assessments, which make it a viable solution for real-world cloud systems.

Shu (2021) provide a decentralized public auditing protocol for cloud storage that is based on blockchain and allows third-party auditors to confirm data integrity without jeopardizing privacy. Blockchain technology guarantees audit records that are transparent and unchangeable, and the protocol allows for dynamic data operations such as addition, deletion, and modification. Because it is decentralized, it is more efficient and secure, which makes it perfect for practical uses. The protocol protects user privacy, conforms with laws like the CCPA and GDPR, and provides robust defense against tampering and unwanted access. Moreover, it has minimal computational and storage overhead, which improves the efficiency of the auditing process. Performance assessments validate its usefulness and viability in cloud storage settings.

Using AI and IoT technologies, Al-Turjman (2021) develop a proxy-authorized public auditing strategy for cyber-medical systems. This ensures security and privacy by enabling authorized proxies to confirm the accuracy of medical data stored in cloud settings. The plan guards against security lapses and unwanted access by enabling dynamic audits and real-time data processing. It maintains little computing overhead, conforms with healthcare privacy rules, and manages real-time data updates. According to evaluations, it is efficient and effective for usage in cyber-medical systems in the actual world.

An identity-based designated verifier public auditing approach for cloud storage is presented by Shao (2023) with incentives. By providing incentives, this system encourages people to take part in the auditing process and makes sure that only verified individuals who have been granted permission and are uniquely recognized are able to audit the data. This raises user engagement while improving data security and integrity. The plan has been demonstrated to work well in actual cloud systems and is efficient with little overhead in terms of computation and storage. It works with minimal computational and storage cost, improves data integrity, and keeps security throughout user revocations.

ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

This approach, which has shown to be successful in real-world cloud environments, provides a workable way to handle secure user management in group settings and conduct public audits.

A blockchain-based, proxy-oriented public auditing solution for low-performance terminal devices is presented by Xie (2022). By using proxy auditors to safely check data integrity on the blockchain, our approach reduces the computing burden on these devices. The system offers strong defense against data manipulation and illegal access while guaranteeing safe, transparent, and unchangeable audit records. Even on devices with limited resources, it maintains effective performance by assigning duties to proxy auditors. With a track record of success in real-world applications, it provides a workable auditing option for settings with subpar hardware.

For cloud-assisted medical Wireless Sensor Networks (WSNs), Xu (2021) offer a certificateless public auditing approach that protects user privacy and allows for dynamic operations. By doing away with the requirement for certificates, this scheme streamlines the auditing process and offers strong data integrity and privacy protection for medical data kept on cloud servers. It supports adding and removing users and is intended for group use. The approach is economical and effective for real-world medical WSN settings since it provides better security with minimal overhead in terms of computation and storage.

Ullah (2022) present a public auditing program for cloud storage that makes use of parity authenticators to guarantee effective and safe data integrity verification. By restricting access to and auditing of data to authorized users only, the approach also safeguards the privacy of revoked users. Strong data integrity checks are provided, illegal access is stopped, and there is little computational or storage overhead. In practical and efficient cloud storage environments, this method is used.

Jalil (2022) present an automatic blocker protocol and BLS signatures-based safe and effective public auditing system for cloud storage. This technology ensures privacy by enabling independent auditors to confirm data integrity without gaining access to the real data. The automated blocker protocol stops unwanted access, while BLS signatures offer quick and safe verification. Strong protection against data breaches and unauthorized access is provided by this system, which has been demonstrated to work well in real-world cloud storage scenarios. It is also designed to be efficient with minimum computational and storage overhead.

Using blockchain technology, Chen (2022) suggest a decentralized public auditing system for safe cloud storage. Without jeopardizing user privacy, this system enables impartial auditors to safely and openly confirm the accuracy of data stored on cloud servers. Blockchain guarantees audit records that are unchangeable and impenetrable, enhancing cloud storage security and dependability. The decentralized method preserves user privacy while guarding against illegal access and data manipulation. The plan has shown to be successful in actual cloud storage environments and is efficient with little computational and storage overhead.

Hsu (2022) examines the fundamental elements and techniques of big data analysis and optimization, emphasizing effective data handling, archiving, and analysis. The article covers the use of distributed systems and parallel computing for data processing, as well as scalable storage options like Hadoop and NoSQL databases. It also emphasizes methods for process optimization for improved performance, including data mining and machine learning. Data input, storage, processing, and visualization tools are essential platform components that guarantee scalability to meet increasing data and user demands. The article also offers actual case studies of how big data optimization and analysis influence perceptions and choices across a range of sectors.

Sharma (2021)

ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

Sharma (2021) presents a Big Data as a Service (BDaaS) platform that enhances access control and privacy protection by utilizing blockchain technology. This framework uses the decentralized and immutable properties of blockchain technology to secure and manage massive databases. Robust access control systems guarantee that only authorized users may access data, and safe management of user permissions and access records preserves privacy. Blockchain's decentralized structure improves security by preventing single points of failure, and transparency is ensured by immutable audit records. This platform, which improves data security and privacy, is useful for real-world applications and is made to scale with demand.

Big data and cloud computing integration is examined in Sandhu (2021) article, which also outlines the advantages and difficulties. In addition to addressing concerns like data security, privacy, scalability, and resource management, it describes how cloud computing enhances big data processing and storage. Within cloud-based systems, the article emphasizes the significance of adhering to data protection requirements, the necessity of effective management to maximize both performance and cost, and techniques for improving application performance.

Colarusso (2022) present PROMENADE, a big data platform that uses dynamic graphs to manage intricate metropolitan networks. The platform effectively manages and displays dynamic urban data, effectively tackling the difficulties associated with extensive metropolitan networks. In order to facilitate prompt decision-making, PROMENADE provides solutions for effective data management, real-time analysis, and visualization. It has sophisticated visualization capabilities for deciphering intricate metropolitan networks, and it scales with increasing data volumes. The platform offers real-world examples of how to optimize urban services and infrastructure.

In order to enhance data storage and transaction efficiency, Hasan (2021) provide a hybrid blockchain architecture for Cloud Manufacturing-as-a-Service (CMaaS) platforms. By combining public and private blockchains, this method provides effective, scalable, and safe data management. It includes robust security mechanisms to safeguard data and transactions, improves the scalability of data storage, and optimizes transaction processing for speed and security. This architecture has been shown to increase the effectiveness and security of CMaaS systems, and it was created to satisfy the increasing demands for data and transactions.

InFeMo, a system for managing big data using a federated cloud architecture, is introduced by Stergiou (2021). By dispersing data and processing workloads across several cloud platforms, InFeMo improves scalability. It streamlines data integration from several sources and enhances processing for increased effectiveness and speed. Additionally, the system offers adaptable solutions to meet a range of applications and guarantees strong data security. Numerous sectors have seen the usefulness of InFeMo in handling big datasets in an efficient manner.

Li (2022) offers a precision marketing strategy that analyzes data from linked devices utilizing an IoT cloud platform. Using sophisticated data mining techniques, this approach collects and analyzes massive amounts of IoT data to derive insightful information. The method increases consumer involvement, develops highly focused marketing tactics, and maximizes marketing expenditures. Through the analysis of consumer behavior patterns, marketing is successfully tailored, and campaign efficiency is improved. The system is scalable to handle large amounts of IoT data, guaranteeing reliable performance, and it allows real-time data processing for prompt decision-making.

Wang (2023) examine the progress, difficulties, and suggested architecture of a safe big-data sharing platform designed for materials genome engineering. The platform seeks to facilitate the sharing of massive datasets among academics, promoting cooperation and expediting the field of materials science. In addition to reviewing recent technological advancements, it addresses privacy and data security issues and presents a strong architecture for safe data sharing and management. The platform supports effective collaboration, scalability to manage big datasets, and is relevant across multiple materials science research situations, all while emphasizing robust security and privacy safeguards."

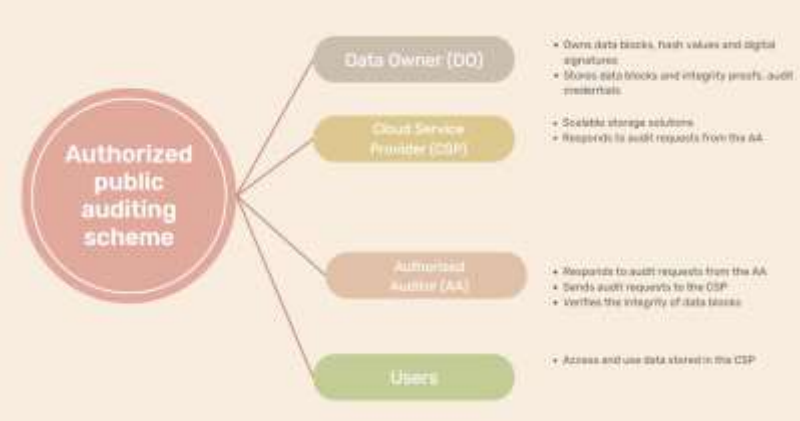
International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

In-depth research on spatiotemporal big data analytics was done by Liang (2023)it included resource management techniques, a range of processing platforms, and practical uses such as disaster relief and urban planning. They also emphasized difficulties in this industry, including problems with scalability, data diversity, expectations for real-time processing, and privacy issues. Their strategy includes robust encryption and authentication procedures to safeguard sensitive data, complex access controls based on user roles, and a scalable architecture to efficiently manage high data volumes and user loads. To guarantee strong data privacy and security procedures, they also place a strong emphasis on adhering to legal requirements.

3 Authorized Public Auditing Scheme Designed METHODOLOGY

Methodology section describes a thorough implementation process for a public auditing scheme that is permitted and created specifically for Platform as a Service (PaaS) dynamic large data storage. This method guarantees compliance, scalability, security, and integrity of data.

The Cloud Service Provider (CSP), Data Owner (DO), Authorized Auditor (AA), and users are the four main participants in our system concept. Via distributed storage systems, the CSP offers scalable storage solutions that can manage massive, constantly expanding information while guaranteeing high availability and dependability. The data is created and owned by the DO, who then contracts out the data to the CSP after tagging or integrity-proving each data block. The DO has granted permission to the AA, an independent organization, to use cryptographic methods for data integrity checks and data confidentiality maintenance. Users can access and use cloud-stored data, but they are not authorized to do audits.

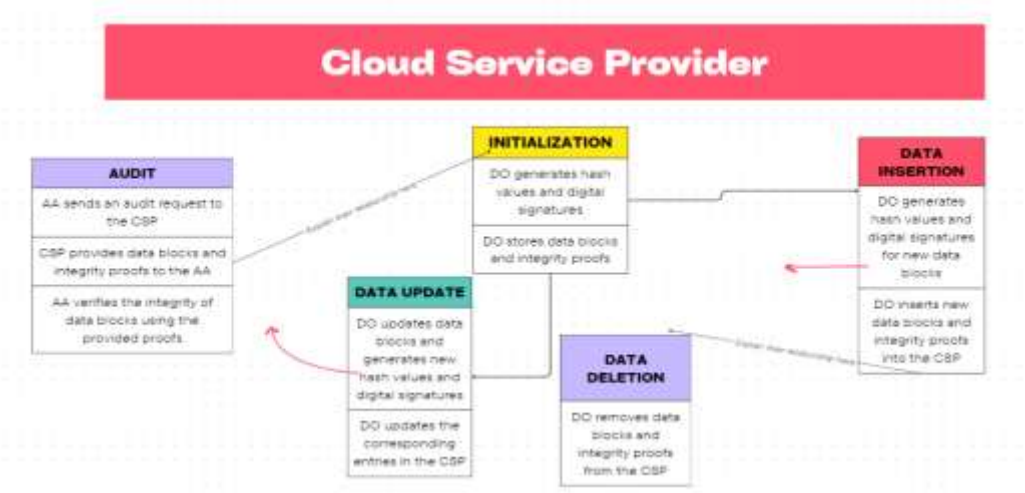


The overall architecture of the approved public auditing system for PaaS-based dynamic big data storage is depicted in this diagram. It emphasizes the communication amongst the primary players: Users, Authorized Auditor (AA), Cloud Service Provider (CSP), and Data Owner (DO). The generated, stored, and audited integrity proofs as well as the data block storage in the CSP are depicted in the diagram.

An essential component of this strategy is cryptography. As integrity proofs to ensure that data has not been altered, hash algorithms such as SHA-256 produce fixed-size hash values from data blocks. Integrity proofs like these are verified by digital signatures like ECDSA or RSA. Data integrity and authenticity can be confirmed by the AA thanks to the DO signing each hash value before passing it to the CSP. Data retrieval without corruption is guaranteed via Proof of Retrievability (PoR) techniques, such those based on Merkle Trees. The data integrity is guaranteed by the root hash, which is signed by the DO and represents a data block and its hash in a Merkle tree created by the DO.

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

The initialization phase of the public auditing protocol commences. For every data block, the DO creates integrity tags and cryptographic keys (both public and private), which are then signed and kept with the data in the CSP. In order to provide the AA permission to access integrity tags and conduct audits, the DO additionally creates audit credentials (such as tokens or certificates). In order to begin an audit, the AA challenges the CSP to provide proofs for a randomly selected portion of data blocks. The requested data blocks and associated integrity tags are returned by the CSP. Then, by examining the signatures and recalculating the hash values, the AA confirms these proofs. The data integrity is verified if the calculated hashes and the received integrity tags match.

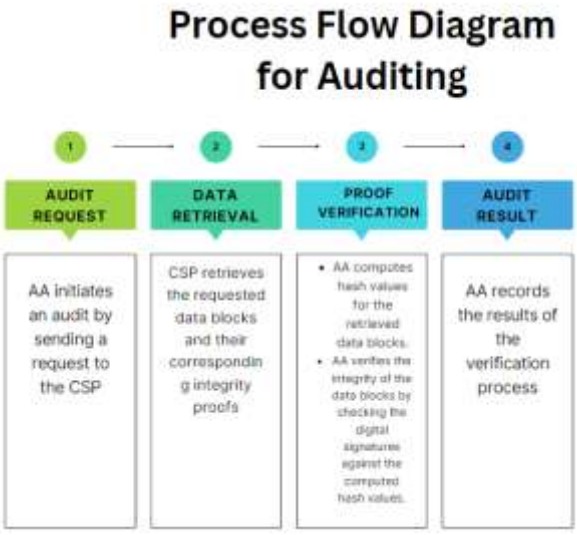


The data flow during several processes, including initialization, auditing, updating, deleting, and inserting, is depicted in this diagram.

This approach requires handling of dynamic data operations. With each data modification, the DO sends the revised integrity proofs to the CSP along with new hash values and signatures for the altered blocks. In the event that data is deleted, the DO modifies the CSP's metadata by removing the relevant integrity proofs from it. A new block's integrity proof and signature are created and sent to the CSP, which incorporates the new blocks and their proofs into the current storage architecture, in order to insert new data.

Data confidentiality and integrity must be preserved, and this requires security measures. Using strong algorithms like AES-256, data stored in the PaaS environment is encrypted. The encryption keys are either handled by the DO or the CSP using secure key management services. User permissions are governed by fine-grained access control policies, while role-based access control (RBAC) methods make sure that only authorized entities are able to undertake sensitive actions. To avoid data interception and manipulation while in transit, TLS/SSL protocols are used to secure all connections between the DO, AA, and CSP.

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25



A thorough overview of the auditing process is given by this graphic, which illustrates the actions taken from the AA's initial audit request to the integrity proofs' verification.

Adherence to regulatory requirements is essential. The auditing program complies with industry norms and laws, including CCPA, GDPR, and HIPAA. To safeguard sensitive data, compliance entails stringent access controls, data encryption, and routine audits. All data access and modification operations are tracked by thorough audit logs, which guarantee tamper-evident records that can be examined to verify compliance and identify irregularities. The auditing scheme's independent third-party accreditation upholds best practices in data security and integrity management and fosters confidence.

The two most important factors are scalability and performance. The auditing scheme uses methods like sampling and probabilistic verification to lessen the computing burden of audits, making it capable of handling massive volumes of data with efficiency. Audits can be completed more quickly and effectively by using performance optimization techniques including parallel processing and caching frequently used integrity proofs. Load balancing in distributed storage systems makes ensuring that audit requests are dispersed equally among servers, avoiding bottlenecks and preserving high availability.

Cloud platforms like AWS SDKs, Azure Security Center APIs, and Google Cloud APIs provide APIs and SDKs that make integration with PaaS environments easier. Real-time data analytics and processing are made possible through integration with data processing frameworks like Apache Hadoop and Apache Spark, which increases the usefulness of the PaaS environment. All-inclusive monitoring tools keep tabs on the functionality and condition of the storage infrastructure, and alarms and notifications are set up to recognize and address irregularities.

In the subject of authorized public auditing systems, research gaps continue to exist despite progress. Subsequent investigations ought to concentrate on enhancing methods for handling dynamic data activities, guaranteeing smooth modifications, removals, and additions without jeopardizing data integrity. It is still vital to conduct research on creating sophisticated privacy-preserving methods, like homomorphic encryption, that allow audits to be conducted without disclosing sensitive information. A larger adoption of these methods will be facilitated and interoperability

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

will be improved by efforts to create industry standards for public auditing schemes in PaaS settings. For practical implementation, it is imperative to optimize the resource consumption of auditing processes in order to minimize expenses, especially in large-scale installations. Maintaining strong data protection mechanisms requires constant adaptation to new cybersecurity threats, particularly the hazards associated with quantum computing.

Ultimately, the deployment of an approved public auditing program for dynamic big data storage in PaaS systems necessitates a multifaceted strategy that integrates strong access control, secure protocols, and cryptography. In order to handle the particular difficulties presented by dynamic and massive amounts of data in cloud computing, this methodology guarantees data integrity, security, scalability, and compliance with standards. These schemes' efficacy and flexibility in a constantly changing digital context will be further improved by ongoing research and technology developments.

To implement an authorized public auditing scheme for dynamic big data storage in PaaS, we can break down the process into several key components and provide mathematical formulations for each.

1. Cryptographic Hash Function

A cryptographic hash function H takes an input x and produces a fixed-size string of bytes. The output is typically a hash value or digest.

$$h = H(x) \tag{1}$$

2. Digital Signature

A digital signature involves two main functions: signing and verification. Using a private key sk and public key pk :

- Signing:

$$\sigma = Sign\ (sk, h) \tag{2}$$

- Verification:
  $Verify\ (pk, h, \sigma) \rightarrow \{\ \text{true, false}\ \}$

3. Proof of Retrievability (PoR)

Using Merkle Trees, a PoR scheme ensures that data can be retrieved fully. The tree is constructed with leaves l_i representing data blocks.

- Merkle Root Calculation:

$$root\ = H\big(H(l_1||l_2)\ ||\ H(l_3||l_4)\big) \tag{3}$$

4. Integrity Check

For each data block $d_{i,}$, a tag t_i is generated using a hash function and signed by the DO:

$$t_i = Sign\ \big(sk, H(d_i)\big) \tag{4}$$

During the audit, the AA verifies the integrity of the data block by checking the signature:

$$Verify\ (pk, H(d_i), t_i) \tag{5}$$

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

Algorithm: Public Auditing Scheme for Dynamic Big Data Storage in PaaS

Inputs:

- "data_blocks': Dictionary containing initial data blocks with their IDs as keys
- "private_key": Private key for signing data
- "pub1ic key" : Public key for verifying signatures
- "audit request" : List of data block IDs to be audited
- "nes data" = Dictionary containing updated data blocks with their IDs as keys

Outputs:

- "audit resalts": Dictionary containing the audit results for each data black ID
- "integrity_tags": Dictionary containing updated integrity tags for each data block ID

Initialization:

- Initialize ' data_blocks' to the input dictionary of data blocks
- Initialize 'integrity_tags' to an empty dictionary

Using the private key to sign each data block and computing its hash value, the data owner initializes the scheme. By doing this, the data blocks are guaranteed to have corresponding integrity tags that may be subsequently confirmed.

1. *Initialization*

- For each data block d_i :
- Compute hash value $h_i = H(d_i)$
- Generate signature $\sigma_i = Sign$ (private_key, h_i)
- Store d_i and σ_i in 'datalblocks' and 'integrity_tags' respectivelh

2. *Generate Audit Credentials*

- Generate audit credentials using the private key

Using the private key, the data owner creates audit credentials. The approved auditor receives certain credentials in order to conduct audits.

3. *Perform Audit*

- For each block ID in "audit_request":
- Retrieve data block d_i and integrity $tag\ \ \sigma_1$
- Compute hash value $h_i = H(d_i)$
- Verify signature Verify(public_key, h_i, σ_i)

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

- Store the result in ' audit results

The authorized auditor recalculates hash values and compares the signatures with the public key in order to confirm the integrity of the requested data blocks. The 'audit_results' file contains the outcomes of these verifications.

4. *Update Data*

- For each updated data block d_i in "sew_data':
- Compute new hash value $h_i = H(d_i)$
- Generate new signature $\sigma_i = Sign$ (private_key, h_i)
- Update d_i and σ_i in 'data_blocks' and' integrity_tags' respectively

The integrity tags are changed in accordance with the computation of new hash values and signatures when updating data blacks.

5. *Delete Data*

- For each block ID to be deleted:
- Remove the data block and integrity tag from 'data_blocks' and 'integrity_tags"

When data blocks and the integrity tags that go with them are no longer required, the data owner can restore them.

6. *Insert Data*

- For each new data black d_i :
- Compute hash value $h_i = H(d_i)$
- Generate signature $\sigma_i =$ Sign(private_key, h_i)
- Add d_i and σ_i to "data_blocks' and 'integelity_tags" respectively

The process of adding new data blocks involves calculating their hash values and creating signatures, which are subsequently stored in the system.

Output:

- Return 'audit_results' and 'integrity_tags.

Table 1: Data Blocks and Integrity Proofs

Block ID	Data Block	Hash Value	Digital Signature
block1	Data Block 1	H(Data Block 1)	Sign(sk, H(Data Block 1))
block2	Data Block 2	H(Data Block 2)	Sign(sk, H(Data Block 2))
block3	Data Block 3	H(Data Block 3)	Sign(sk, H(Data Block 3))

The data blocks and the related integrity proofs (digital signatures and hash values) are shown in this table. Every data block has a distinct Block ID, and the CSP stores the integrity proof for each data block with it.

Table 2: Audit Request and Results

Audit Request ID	Requested Block ID	Hash Value	Digital Signature	Verification Result

International Journal of
HRM and Organizational Behavior
ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

audit1	block1	H(Data Block 1)	Sign(sk, H(Data Block 1))	True
audit2	block2	H(Data Block 2)	Sign(sk, H(Data Block 2))	True
audit3	block3	H(Data Block 3)	Sign(sk, H(Data Block 3))	False

The outcomes of an audit request are displayed in this table. It contains the desired block ID, the associated hash value, the digital signature, and the verification process' outcome.

Table 3: Dynamic Data Operations

Operation ID	Operation Type	Block ID	Old Data Block	New Data Block	Old Integrity Proof	New Integrity Proof
update1	Update	block1	Data Block 1	Updated Block 1	Sign(sk, H(Data Block 1))	Sign(sk, H(Updated Block 1))
delete1	Delete	block2	Data Block 2	-	Sign(sk, H(Data Block 2))	-
insert1	Insert	block4	-	New Block 4	-	Sign(sk, H(New Block 4))

All of the changes, removals, and insertions made to data blocks are listed in this table. Before and after the operation, it displays the old and new data blocks together with the relevant integrity proofs.

4 CONCLUSION

A major advancement in guaranteeing data integrity, security, and compliance is the approved public auditing scheme for dynamic large data storage in PaaS systems. Through the use of cryptographic techniques like digital signatures and hash functions in conjunction with Proof of Retrievability (PoR), this scheme makes it possible to independently verify the accuracy of data while protecting confidential information. This method not only solves the scalability issues caused by massive datasets in cloud environments, but it also improves accountability and transparency. The scheme's practical usability and robustness are highlighted by its integration with current PaaS platforms and adherence to regulatory norms such as GDPR and HIPAA. Encryption and role-based access control are two more thorough security solutions that help to guarantee that data is shielded from breaches and unwanted access.

The investigation will focus in a number of fascinating areas in the future. To further safeguard data confidentiality, audits can be carried out with no data being revealed thanks to advancements in privacy-preserving techniques like homomorphic encryption. Improved interoperability and wider acceptance throughout cloud platforms can be achieved by creating standardised protocols for public audits in PaaS environments. For large-scale installations, cost reductions through resource optimization during the auditing process can also increase its viability. Develop quantum-resistant cryptographic methods immediately in order to protect data integrity from potential quantum assaults, given the potential concerns associated with quantum computing. The final way to improve the security and dependability of cloud storage systems is to use AI and machine learning breakthroughs to identify irregularities in audit data.

REFERENCE

1. Li, H., Guo, F., Wang, L., Wang, J., Wang, B., & Wu, C. (2021). A Blockchain-Based Public Auditing Protocol with Self-Certified Public Keys for Cloud Data. Security and Communication Networks, 2021(1), 6623639.

ISSN 2454 - 5015
https://doi.org/10.62650/ijhrmob.2023.v11.i3.pp13-25

2. Shu, J., Zou, X., Jia, X., Zhang, W., & Xie, R. (2021). Blockchain-based decentralized public auditing for cloud storage. IEEE Transactions on Cloud Computing, 10(4), 2366-2380.
3. Al-Turjman, F., & Deebak, B. D. (2021). A proxy-authorized public auditing scheme for cyber-medical systems using AI-IoT. IEEE Transactions on Industrial Informatics, 18(8), 5371-5382.
4. Shao, B., Zhang, L., & Bian, G. (2023). Incentive Public Auditing Scheme with Identity-Based Designated Verifier in Cloud. Electronics, 12(6), 1308.
5. Xie, M., Zhao, Q., Hong, H., Chen, C., & Yu, J. (2022). A novel blockchain-based and proxy-oriented public audit scheme for low performance terminal devices. Journal of Parallel and Distributed Computing, 169, 58-71.
6. Xu, Z., He, D., Vijayakumar, P., Gupta, B. B., & Shen, J. (2021). Certificateless public auditing scheme with data privacy and dynamics in group user model of cloud-assisted medical WSNs. IEEE Journal of Biomedical and Health Informatics, 27(5), 2334-2344.
7. Ullah, F., & Pun, C. M. (2022). Enabling parity authenticator-based public auditing with protection of a valid user revocation in cloud. IEEE Transactions on Computational Social Systems.
8. Jalil, B. A., Hasan, T. M., Mahmood, G. S., & Abed, H. N. (2022). A secure and efficient public auditing system of cloud storage based on BLS signature and automatic blocker protocol. Journal of King Saud University-Computer and Information Sciences, 34(7), 4008-4021.
9. Chen, J., Wang, Y., Huang, Z., Ruan, C., & Hu, C. (2022). A decentralized public auditing scheme for secure cloud storage based on blockchain. Wireless Communications and Mobile Computing, 2022(1), 3688164.
10. Hsu, K. (2022). Big data analysis and optimization and platform components. Journal of King Saud University-Science, 34(4), 101945.
11. Sharma, S. K. (2021). A framework of big data as service platform for access control & privacy protection using blockchain network. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 476-485.
12. Sandhu, A. K. (2021). Big data with cloud computing: Discussions and challenges. Big Data Mining and Analytics, 5(1), 32-40.
13. Colarusso, C., De Iasio, A., Furno, A., Goglia, L., Merzoug, M. A., & Zimeo, E. (2022). PROMENADE: A big data platform for handling city complex networks with dynamic graphs. Future Generation Computer Systems, 137, 129-145.
14. Hasan, M., Ogan, K., & Starly, B. (2021). Hybrid blockchain architecture for cloud manufacturing-as-a-service (cmaas) platforms with improved data storage and transaction efficiency. Procedia Manufacturing, 53, 594-605.
15. Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2021). InFeMo: flexible big data management through a federated cloud system. ACM Transactions on Internet Technology (TOIT), 22(2), 1-22.
16. Li, W. (2022). Big Data precision marketing approach under IoT cloud platform information mining. Computational intelligence and neuroscience, 2022(1), 4828108.
17. Wang, R., Xu, C., Dong, R., Luo, Z., Zheng, R., & Zhang, X. (2023). A secured big-data sharing platform for materials genome engineering: State-of-the-art, challenges and architecture. Future Generation Computer Systems, 142, 59-74.
18. Liang, H., Zhang, Z., Hu, C., Gong, Y., & Cheng, D. (2023). A Survey on Spatio-temporal Big Data Analytics Ecosystem: Resource Management, Processing Platform, and Applications. IEEE Transactions on Big Data.