Shodhshauryam, International Scientific Refereed Research Journal
Available online at : www.shisrrj.com
OPEN ACCESS
© 2024 SHISRRJ | Volume 7 | Issue 2
ISSN : 2581-6306
doi : https://doi.org/10.32628/SHISRRJ

A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage

K. Padmanaban[1], E. Divya[2]

[1]Assistant Professor, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

[2]Post Graduate, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

Article Info

Article History
Received : 25 March 2024
Published : 09 April 2024

Publication Issue :
March-April-2024
Volume 7, Issue 2

Page Number : 412-419

ABSTRACT

A hastily growing technology, cloud computing offers very reasonably-priced information storage and lightning-speedy computing talents. Cloud carrier vendors or the cloud's custodian cope with all facts stored on the cloud. As records proprietors, they're worried approximately the legitimacy and dependability of the statistics kept on cloud servers. Any unauthorized user or character can misappropriate or control information. The reason of this work is to suggest a at ease public auditing scheme that makes use of unbiased auditors to affirm the confidentiality, dependability, and integrity of information saved on cloud servers. This recommended auditing plan consists of the usage of public key encryption (RSA-15360), integrity checking (SHA-512), and encryption the usage of the AES-256 method. And perform facts dynamics operations, which generally cope with addition, elimination, and change.

Keywords : TPA, CSS, Data owner, Upload file, Accept Request, Generate Key, Download File

I. INTRODUCTION

Cloud computing is a sophisticated era all and sundry is used internal or outer in there days world. the development and hastily increasing generation of cloud computing are used computation and garage. The very minimum cost is used storage and computation as a service in it. carrier model furnished 3 crucial offerings in it: infrastructure as a service (IaaS), platform as a provider (PaaS) and software as a service(SaaS). The NIST definition, “Cloud computing is a model permissive ubiquitous, convenient, on-demand network technique to a shared pool of configurable computing belongings(e.g. networks, servers, storage, applications, and offerings) that may be immediately provisioned and launched with fundamental control attempt or provider provider interplay. Cloud storage is a crucial service of cloud computing. They involve records

privacy, statistics protection, data availability, records region, and, relaxed transmission which is a important launch in cloud protection. The worried in cloud.

Undertaking safety are threats, information loss, degradation, outdoor malicious attack and multi-tenancy . The saved data of integrity is conserved for facts integrity within the cloud system. The unauthorized customers must now not be accessed misappropriate or range of facts. records integrity and reliability of information are devoted to keep by means of the cloud computing company. information confidentiality is also a crucial way from a person's factor of angle therefore they store their non-public or confidential data inside the cloud. statistics confidentiality is taken to guarantee get right of entry to manipulate guidelines and authentication. The religion of cloud computing could be ahead by using growing cloud authenticate and statistics confidentiality. So the preserve information at the cloud ought to be protection, integrity, privateness, and confidentiality of vital demands from the consumer attitude. A secure records storage of cloud computing is supplied of a records auditing scheme. Auditing is a refinement of checking the consumer data which may be performed through the information owner or with the aid of a TPA. The integrity of saved facts at the cloud serves to preserve it. The TPA control is split into : one is personal audibility, which lets in the records proprietor can analyze the integrity of the information. no person has the authority to inquire approximately the server considering the information. though it attains to will increase verification overhead of the person. second is public audibility, the confidentiality of the records can check with the aid of best TPA. The behalf of the client can act TPA so TPA is an entity. The verification of integrity has dealt with to appropriate work that every one critical information, capabilities, knowledge and expert ability and the location of the consumer is also decreased by it[8]. It must be crucial that TPA have to effectively or regularly audit the cloud records garage with out requesting for the neighborhood replica of facts[9] The halt of a research paper is arranged to conform section1 is discuss the introduction and phase 2 is speak associated paintings. The proposed approach is mentioned in section three and section4 is discussed in safety evaluation while the realization and future paintings in segment 5.

II. RELATED WORK

There are various important stages involved in the project-related activity for creating a Secure Data Dynamic and Public Auditing Schema for Cloud Storage. In order to comprehend current research, methodology, and issues related to secure cloud storage, dynamic data management, and public auditing, a thorough examination of the literature is first done. Subsequently, a thorough requirements analysis is conducted in order to distinguish between functional and non-functional requirements. These include elements like data integrity, scalability, compliance, and confidentiality. After that, a system architecture is created, which lists all of the parts, pieces, and interactions required to provide the intended functionality. Aspects including data encryption, access control, audit log generation, and cloud storage system integration are taken into account in this architecture. While methods for handling dynamic data operations are investigated, including real-time integrity verification mechanisms such as Merkle trees, cryptographic algorithms are assessed to guarantee strong data security and privacy.

Creating the public auditing method, including cryptographic protocols, and creating audit log management systems are all part of the implementation phase, which entails securely recording data access and change events. Thorough testing and assessment are carried out at every stage of the procedure to judge the security, functionality, and adherence to requirements of the solution. Lastly, thorough reporting and documentation are created, including the design justification, implementation specifics, assessment results, and suggestions for interested parties and the larger research community. By taking a methodical approach, it is possible to guarantee the creation of a strong and efficient auditing schema that improves the security, accountability, and transparency of cloud storage systems.

III. BACKGROUND WORK

A. Cloud storage security

Cloud garage systems have gained big adoption because of their scalability, fee-effectiveness, and ubiquitous access. however, the inherent dangers associated with storing touchy information in 1/3-birthday celebration cloud environments have precipitated enormous research into cloud storage security. traditional safety mechanisms, consisting of get entry to manage lists (ACLs) and encryption, provide foundational security measures. however, they frequently fall short in addressing the dynamic nature of information and the want for accountability in cloud storage systems.

B. Information Dynamics in Cloud storage

Dynamic data operations, inclusive of records insertion, deletion, and change, are commonplace in cloud garage environments. these operations pose giant demanding situations for ensuring data integrity, confidentiality, and availability. conventional cryptographic techniques, inclusive of symmetric and asymmetric encryption, might not properly help dynamic records control while retaining protection ensures. consequently, there's a want for specialized answers which can accommodate records dynamics in cloud storage securely.

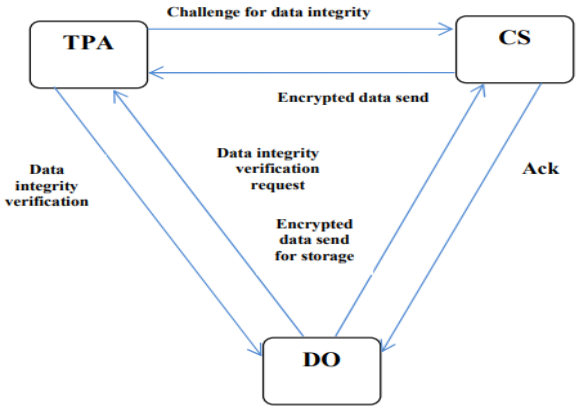
C. Public Auditing in Cloud storage

Public auditing schemes allow third-birthday party auditors to verify the integrity and correctness of data saved within the cloud without gaining access to the real statistics. these schemes provide transparency and responsibility, permitting cloud users to make sure that their facts remain unaltered and meets regulatory compliance necessities. numerous public auditing protocols, consisting of Provable statistics possession (PDP) and evidence of Retrievability (POR), had been proposed to deal with this need. however, existing schemes might also lack efficiency, scalability, or aid for dynamic facts operations.

IV. SYSTEM ARCHITECTURE

The system architecture for the Secure Data Dynamic and Public Auditing Schema for Cloud Storage encompasses the overall structure and design of the proposed solution. It outlines how various components and modules interact to achieve the project's objectives of ensuring data security, integrity, and auditability in cloud storage environments. The architecture comprises several key elements, including data encryption, access control, dynamic data management, audit log generation, public auditing mechanisms, integration with cloud storage providers, and compliance features. Each component is carefully designed to fulfill specific functions, such as encrypting data before storage, regulating user access based on

predefined roles, tracking changes in the data structure, generating comprehensive audit logs, enabling third-party auditors to verify data integrity, integrating with existing cloud platforms, and ensuring compliance with regulatory standards. By delineating the relationships and interactions between these components, the system architecture provides a blueprint for developing a robust and scalable solution that addresses the complex challenges of secure and transparent cloud storage.



1. DATA OWNER:

Register:

Data owner can Register and login with valid credentials

Upload File:

Data provider can upload the file.

View File:

Data Owner can view uploaded file once means whether the file is correctly uploaded or not.

Search a File:

Data user can search a file based on the keyword, if file is available then user can view file and send request to cloud to download the file.

View File Status: The person who is sending request he /she can view the status of that file.

Request Status: After accepting the request from the cloud and TPA.

2. Cloud Provider

Login

Cloud provider can login with his/her credentials.

View Files:

Cloud can view all uploaded files.

View Data owner:

Cloud can view all the data owner details to give permission for login the website.

Approve for public Auditing:

Cloud gets a key from Owner and send to the TPA.

3. Third party Authority:

Login:

Third party Authority login and view give authorization to owners.

Generate key to users:

Authority generate key to particular file to a particular owner.

V. ALGORITHMS

1. AES (Advanced Encryption Standards)

AES (Advanced Encryption Standards) serves as a cornerstone of the information security approach, in general applied for encrypting facts earlier than it is stored in the cloud garage system. This encryption procedure guarantees the confidentiality of the statistics, making it unreadable to unauthorized events despite the fact that intercepted during transmission or saved on cloud servers. The symmetric nature of AES encryption, where the equal secrets used for each encryption and decryption, permits efficient and comfortable information managing within the gadget. Leveraging AES encryption aligns with various compliance requirements and enterprise standards, demonstrating the task's commitment to information security and privacy policies which include GDPR, HIPAA, and PCI-DSS.

furthermore, AES encryption enhances the general security posture of the cloud storage gadget by using

offering strong protection towards cryptographic assaults. Its tremendous adoption as a well-known encryption algorithm attests to its reliability and effectiveness in safeguarding touchy data. by imposing AES encryption, the challenge ensures that information stored inside the cloud remains relaxed and inaccessible to unauthorized entities, thereby mitigating the chance of statistics breaches and unauthorized get admission to. standard, AES encryption plays a vital role in upholding the confidentiality and integrity of data inside the mission's protection structure, contributing to its overarching goal of creating a at ease and straightforward cloud garage solution.

2. RSA (Rivest Shamir Adleman)

RSA (Rivest-Shamir-Adleman) performs a crucial function in our project's security framework for cloud storage. one of its number one programs is in records encryption, where RSA serves as a sturdy cryptographic algorithm. earlier than storing statistics inside the cloud, we encrypt it the use of RSA to make certain that touchy data stays covered from unauthorized access or tampering. This encryption manner provides a further layer of safety, mitigating dangers related to data breaches or malicious sports.

Additionally, RSA is hired for generating virtual signatures, which might be vital for information integrity verification. each facts block or record undergoes signing with RSA, creating a completely unique signature. at some stage in public auditing, authorized events can confirm these signatures to confirm that the facts has now not been altered or corrupted. This mechanism helps keep facts integrity and authenticity, that are critical factors of secure cloud storage systems.

moreover, RSA plays a large function in key control inside our assignment. We utilize RSA-based totally public-private key pairs for person authentication and get entry to manipulate. This guarantees that best legal customers can carry out dynamic statistics operations within the cloud storage system, including a layer of protection against unauthorized access and records manipulation.

3. SHA (Secure Hash Algorithm)

SHA (Secure Hash Algorithm) is an essential element of our challenge's safety structure for cloud garage. considered one of its primary roles is in statistics integrity verification, in which SHA algorithms like SHA-256 or SHA-three are utilized to compute hash values for records blocks or files. these hash values act as particular virtual signatures, representing the statistics' integrity kingdom. at some point of public auditing techniques, those hash values are as compared to make sure that the information has not been tampered with or altered, therefore verifying its integrity and authenticity.

Moreover, SHA algorithms are employed in producing Message Authentication Codes (MACs) while mixed with cryptographic keys. those MACs are vital for verifying message authenticity and integrity at some point of verbal exchange between clients and the cloud garage machine. by using SHA-based totally MACs, we establish secure conversation channels that prevent unauthorized statistics adjustments or tampering at some stage in records transmission, enhancing universal information safety. furthermore, SHA hashes play a vital role in information deduplication and indexing mechanisms in the cloud garage system. by computing SHA hashes of information blocks, we are able to perceive reproduction statistics and optimize garage space with the aid of storing most effective particular facts blocks. This technique now not best improves garage efficiency however additionally reduces redundancy, leading to better usage of cloud assets. moreover, SHA hashes serve

as precise identifiers for documents stored inside the cloud. while customers request precise documents, their corresponding SHA hashes are used to fast locate and retrieve the asked facts, enhancing data retrieval efficiency and reaction times.

VI. IMPLEMENTATION AND EVALUATION

The implementation and assessment tiers are vital components of our mission on at ease statistics dynamics and public auditing schema for cloud garage. inside the implementation segment, we meticulously element the technology, tools, and architectural layout hired. This consists of discussions at the programming languages utilized, cryptographic libraries integrated, and the unique cloud structures applied for website hosting the machine. We delve into the gadget's structure, highlighting key components such as information encryption mechanisms, get entry to manage protocols, auditing strategies, and comfortable communication channels.

In the realm of statistics encryption implementation, we complex at the strategies applied, with a focus on algorithms like RSA for ensuring statistics confidentiality. This encompasses the generation of cryptographic keys, encryption techniques for records at relaxation and in transit, in addition to the corresponding decryption techniques crucial to getting access to encrypted facts securely.

The auditing protocol implementation is a pivotal aspect, encompassing procedures for verifying data integrity and correctness. We elucidate how audit trails are generated, stored securely, and subsequently verified during auditing processes to ensure the reliability and trustworthiness of data in the cloud storage system.

The evaluation phase of our project focusing on a secure data dynamics and public auditing schema for cloud storage is crucial for assessing the effectiveness, efficiency, and security of the implemented system. This phase involves a comprehensive analysis of various performance metrics, comparative assessments, security evaluations, and implications for real-world deployment.

Firstly, we define and measure key performance metrics to evaluate the system's operational efficiency. Metrics such as throughput, latency, encryption/decryption speeds, audit time, and resource utilization are quantified to gauge the system's responsiveness and resource management capabilities. Through extensive testing under diverse scenarios and workloads, we gather empirical data to assess the system's performance under different conditions.

Furthermore, we conduct a comparative analysis to benchmark the performance of our proposed schema against existing solutions or baseline methods. By comparing metrics such as data access times, auditing overheads, and system response rates, we identify the strengths and potential areas for improvement in our schema. This comparative assessment provides valuable insights into the competitive advantages and limitations of our solution within the cloud storage landscape.

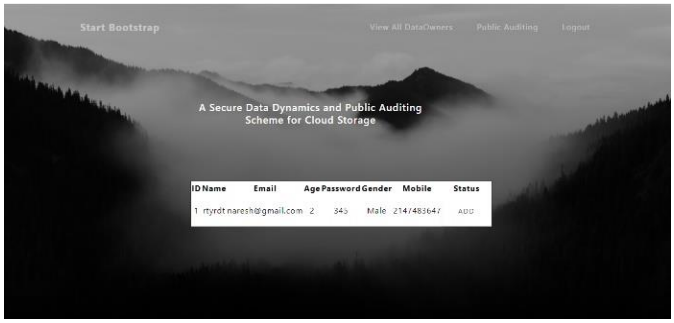
Security evaluation is another critical aspect of the evaluation phase, focusing on assessing the system's resilience against various security threats and attacks. We analyze the system's compliance with security standards, its resistance to data breaches, unauthorized access attempts, and data tampering. By conducting penetration testing, vulnerability assessments, and security audits, we validate the robustness of our security mechanisms and identify any vulnerabilities or areas requiring reinforcement.

Moreover, the evaluation phase includes considerations for scalability, reliability, and compliance with regulatory requirements. We assess the system's ability to scale seamlessly with increasing data volumes and user demands while maintaining consistent performance levels. Reliability testing involves assessing system uptime, data availability, and failover mechanisms to ensure uninterrupted service delivery.

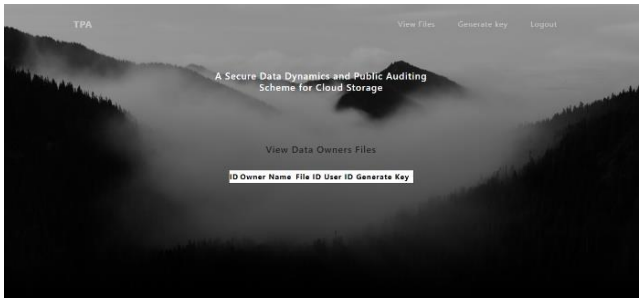
VII. RESULTS

The results validate the effectiveness, efficiency, security, and practical applicability of our secure data dynamics and public auditing schema for cloud storage, affirming its readiness for deployment and use in production environments.

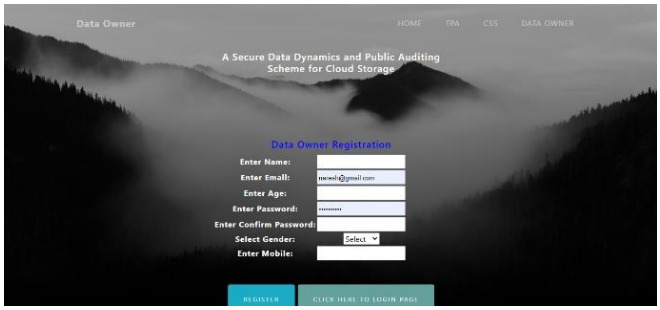
View all data owners: Cloud can view all the data owner details to give permission for login the website.



Public auditing: Cloud gets a key from Owner and send to the TPA.



Data owner registration page: Data owner can registration and login with valid credentials



All the screens show the module results and the registration of the secure data dynamics and public auditing ng for cloud storage.

VIII. CONCLUSION

The fast development of cloud computing generation has revolutionized statistics storage and computational abilities, providing price-powerful solutions for groups and individuals. but, with the benefit of cloud offerings comes concerns approximately records protection and integrity. records proprietors, which incorporates groups and individuals, are more and more worried approximately the legitimacy and reliability of their statistics stored on cloud servers. Unauthorized access, records manipulation, and safety breaches are big dangers that need to be addressed effectively.

To address those challenges, this painting proposes a cozy public auditing scheme particularly designed for cloud computing environments. The primary intention of this scheme is to verify the confidentiality, dependability, and integrity of data stored on cloud servers. with the aid of using a combination of advanced cryptographic techniques and at ease protocols, the scheme targets to offer a strong framework for making sure records safety and reliability in the cloud.

One of the key components of the proposed scheme is the use of public key encryption, especially RSA-15360, which ensures cozy statistics transmission and get proper of entry to manipulate. moreover, integrity checking the use of SHA-512 performs a important function in detecting any unauthorized changes or tampering with the statistics. AES-256 encryption in addition complements information safety by encrypting facts at rest, making it unreadable to unauthorized clients.

Furthermore, the scheme includes facts dynamics operations such as addition, elimination, and change, that are important for maintaining records accuracy and consistency. at ease protocols for those operations assist prevent unauthorized changes and ensure facts reliability over the years. moreover, the involvement of unbiased auditors offers a in addition layer of verification and bear in mind, making sure that records on cloud servers is valid and has not been compromised.

IX. REFERENCES

[1]. Zissis, Dimitrios, and DimitriosLekkas. Addressing cloud computing security issues. Future Generation computer systems 28.3(2012):583-592.

[2]. Cong Wong, Sherman S M Chow, Qian Wang, Kui Ren, and Wen Jing Lou. “Privacy Preserving Public Auditing for Secure Cloud Storage”. IEEE Transactions on Computers, Volume 62, ISSUE 2, February 2013.

[3]. Mell, Peter, and Tim Grance.The NIST definition of cloud computing(2011).

[4]. W.Stalling, ”Cryptography and network security,”LPE Sixth Edition,ISBN-978-013-335-4690. [16] Kerry Maletsky,”RSA vs ECC comparison for embedded system”Atmel8951.