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

Reliability Guaranteed Solution for Data Storing and Sharing

N Bhavana[1], Bejawada Pavani[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 : 02 April 2024
Published : 13 April 2024

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

Page Number : 478-485

ABSTRACT

Certified digital data from reputable organizations carries substantial importance and is frequently exchanged or stored online. However, several obstacles need addressing: (1) Ensuring the anonymity of certificate-issuing organizations, (2) Securely storing valuable digital data within the system, and (3) Facilitating data reliability verification while preserving content confidentiality and ensuring safety, transparency in the sharing process of data. To tackle these challenges, we propose a holistic framework comprising data storing & sharing schemas. We implement a scheme in group for providing the similar services to RO. Each organization processes data from a owner to generate valuable digital data and issues a cipher text certificate of this data. Within data storage framework, the owner uploads data onto the public IPFS network. Then record address of the stored data, along with the certificate, onto the block chain ledger. In this framework, all participants can verify trustworthiness of data shared before initiating a request with the owner. Data sharing process is facilitated through a smart contract involved, required to escrow funds to incentivize. Data storing & sharing schemas ensure various securities, including privacy, secrecy, integrity, & non-repudiation thereby comprehensively addressing the aforementioned challenges.

Keywords : Block chain, data storing & sharing, DC, IPFS.

I. INTRODUCTION

The growth of data globally has elevated trusted data as valuable assets for individuals & organizations. By 2025, it is projected that the total data created & stored worldwide will reach approximately 175 zetabytes, with an estimated 5 billion global consumers interacting with data daily. This surge in data usage underscores the immense demand for efficient data storage and sharing solutions, while also presenting challenges related to data security.

Current data storage and sharing architectures primarily fall into two categories: centralized and decentralized. Centralized architectures involve storing data in organizational data center systems, which can be costly to operate and lack scalability. Cloud storage services offer a more flexible and cost-effective alternative, particularly suitable for IoT systems, having the privacy & security of data with the use of encryption algorithms.

Decentralized architectures, on the other hand, leverage blockchain (BC) technology for its properties. Despite these advantages, existing solutions do not adequate to check the reliability & accuracy of data to be shared on the network. Data which was Meaningful (MD), approved by reputable organizations (RO), requires secure storage and sharing mechanisms. In the medical field, for instance, diagnostic results published by reputable medical organizations represent MD. To address these challenges, Data sharing methods should empower requesters to verify the data.

Traditional sharing methods rely on trust between participating partners, leading to potential integrity issues. ROs must ensure the anonymity of MD generated and protect the privacy of DO. Moreover, the identities of involved parties and the content of shared data must remain anonymous while ensuring reliability verification.

Certified digital data storage and sharing necessitate solutions meeting specific requirements:

Data storing: Storing the data confidentially by Safeguarding the information of the data owners (DOs) with privacy maintaining the safety measures.
Data sharing: Enabling reliability verification of shared data by all system participants without compromising content privacy, direct data sharing between DO and requesters, and ensuring system.

Present solutions have no scope of filling these criteria. As defined reputable organizations (ROs) as data providers (DPs), organizing them into groups to provide similar services. A designated DP converts raw data from the data owner (DO) into meaningful data (MD), encrypts it by a symmetric algorithm and protected key, produces a certificate on the encrypted MD, and securely transmits the encrypted MD (EMD), certificate, and DP information to the DO.

II. METHODS AND MATERIAL

The methodology utilized for RGS & DSS adopts a systematic approach to ensure the successful implementation and deployment of the application. It would typically outline the specific techniques, methodologies, and materials employed in the development and evaluation of the proposed solution. Here's an expanded overview of what this section might entail:

Data Producing Methodology: The method of processing data into meaningful data (MD) by data providers (DPs) within the proposed solution. This may involve detailing the steps involved in data transformation, encryption, certificate generation, and secure transmission to the data owner (DO).

Data Storing Approach: Explain how the data owner securely stores the meaningful data (MD) on the IPFS within the proposed solution. Provide insights into the mechanisms used to record the access of MD on IPFS & information in a transaction related to blockchain.

Data Sharing Mechanism: Discuss the methods employed for enabling reliable data sharing between the data owner (DO) and requesters within the proposed solution. This may include outlining the process of requester verification of the data before initiating data-sharing contracts.

Blockchain Integration: Detail how blockchain technology is integrated into the solution to ensure transparency, decentralization, and auditability. Explain the role of blockchain in recording access addresses, certificates, and related information, as well as its impact on data integrity and reliability verification.

Security Measures: Describe the security measures implemented to protect the privacy of shared data within the proposed solution. This may involve encryption algorithms, access control models, anonymity preservation techniques, and mechanisms for preventing unauthorized access or modification of data.

Evaluation Methodology: This may include performance metrics, simulation studies, experimental setups, and validation techniques used to assess the effectiveness and practicality of the solution.

Materials Used: Provide details about the materials, tools, and technologies utilized in the development and evaluation of the proposed solution. This may include software frameworks, programming languages, simulation environments, and hardware platforms.

Statistical Analysis: If applicable, discuss any statistical analysis or data processing techniques used to analyze experimental results, identify trends, and draw conclusions about the performance and effectiveness of the proposed solution.

Ethical Considerations: Address any ethical considerations or implications associated with the use of data storing and sharing solutions, including privacy concerns, data ownership rights, and potential biases or discrimination.

Limitations and Future Directions: Acknowledge any limitations or constraints of the future solution and discuss potential areas for research and improvement.

III. SOFTWARE REQUIREMENT SPECIFICATION

The software program requirements Specification (SRS) for the system outline the practical and non-useful necessities important for the success development and deployment of the application.

Practical Necessities:

Functional requirements are essential features and capabilities that end users expect the system to provide. These requirements are directly observable in the final product, as they define specific inputs, operations, and expected outputs. Here are expanded examples of functional requirements:

User Authentication: The system must authenticate users whenever they log in the system. This may involve username/password authentication, biometric authentication, or multi-factor authentication methods.

Cyber-Attack Response: In the event of a cyber-attack, the system must initiate a shutdown procedure to prevent further damage and protect sensitive data. This may include automatically disconnecting from the network, backing up critical data, and notifying system administrators.

User Registration Email Verification: When a user registers for the first time on the software system, a verification email to the user's registered email address with a unique verification link that the user must click or enter to confirm their registration and activate their account.

Data Encryption: The system must encrypt sensitive data stored within the system to protect it from unauthorized access or tampering.

Search Functionality: The system must provide users with the ability to search for specific information within the system. This may include searching for records, documents, or other data based on keywords, filters, or criteria specified by the user.

Data Backup and Recovery: The system is required to routinely back up data and offer mechanisms for data recovery in the event of accidental deletion, system failure, or other instances of data loss.

Group Manger Control: The system is implemented as controls given to the manager lever allowing managers to define user roles & permissions.

Reporting & Analytics: The system provides reporting & analytics features, allowing users to generate and analyze data reports, charts, and graphs. This enables users to gain insights into system performance, trends, and patterns.

Notification System: The system must have a notification system to alert users about important events, updates, or changes within the system. Notifications may be delivered via email, SMS, in-app notifications, or other communication channels.

Integration with External Systems: The system must be capable of integrating with external systems or third-party applications to exchange data, share information, or automate processes. This ensures interoperability and seamless communication between different systems.

Non-Functional requirements:

Defines the qualities that a system to meet user expectations regarding its performance, usability, security, and other aspects. These requirements are not directly observable in the final product but are critical for ensuring the overall effectiveness, reliability, and quality of the system. In the context of "A Reliability Guaranteed Solution for Data Storing and Sharing," non-functional requirements play a important role in shaping the design & implementation. Here's an expanded overview of non-functional requirements for such a solution:

Security: The system is obligated to guarantee the data privacy and availability of stored. This encompasses implementation of encryption mechanisms, access control policies, and data backup procedures to thwart unauthorized access, prevent data breaches, and mitigate data loss incidents.

Reliability: The system must operate reliably under normal and adverse conditions, ensuring consistent performance and minimal downtime. This involves robust error handling, fault tolerance mechanisms, and redundant systems to prevent disruptions and maintain data accessibility.

Scalability: The system must be able to handle growing volumes of data and user requests without sacrificing performance or functionality. This requires scalable architectures, distributed processing capabilities, and resource allocation strategies to accommodate increasing workload demands.

Performance: The system must meet predefined performance objectives, such as response time, throughput, and latency requirements. This involves optimizing system components, minimizing bottlenecks, and leveraging caching and optimization techniques to enhance overall performance.

Usability: The system is more user-friendly navigate, & interact users, and understand its features and functionalities. This includes providing clear user interfaces, informative error messages, and comprehensive documentation to support user adoption and usability.

Interoperability: The system must be compatible with existing technologies, standards, and protocols to facilitate seamless integration with external systems and interoperability across heterogeneous environments. This requires adherence to industry standards, open APIs, and data exchange formats to enable data sharing and communication between different systems.

Compliance: The system must adhere to applicable laws, rules and regulations of industry. Which includes adherence to protection of data regulations such as GDPR, HIPAA, or PCI-DSS, as well as industry-specific standards and best practices?

Maintainability: The system must be easy to maintain, update, and modify over time to address evolving user needs, technological advancements, and changing requirements. This involves adopting modular architectures, version control systems, and documentation practices to facilitate system maintenance and evolution.

Cost-effectiveness: The system must be cost-effective to develop, deploy, and operate, ensuring optimal resource utilization and return on investment. This requires careful consideration of resource allocation, licensing costs, infrastructure expenses, and ongoing maintenance requirements to minimize total cost of ownership.

Resilience: The system must demonstrate against external threats, including cyber-attacks, natural disasters, and hardware failures. to ensure continuous operation and data availability. This involves implementing disaster recovery plans, backup strategies, and redundancy measures to mitigate risks and maintain business continuity.

IV. PROPOSED SYSTEM

In our proposed scheme for data production, storage, and sharing, we implement a group authentication protocol within the data generation framework. This protocol facilitates collaboration among a consortium of reputable companies offering the same service. Within this structure, one organization within the group transforms raw data provided by a data owner into valuable online information. Subsequently, this organization issues certificates of information digitally as a message which is encrypted.

Enhanced Security: By using encryption and group authentication protocols, the system is authorized by only authorized parties can access data and process data, significantly reducing the risk of data security.

Data Integrity: Issuing certificates of information digitally as a message which is encrypted aids in safeguarding the integrity of the data.. This means that any tampering with the data can be easily detected, preserving its accuracy and reliability.

Scalability: The system is designed to accommodate a group of organizations, making it scalable. It can easily expand to include more participants without compromising on performance or security.

Collaboration Efficiency: The scheme fosters a collaborative environment among reputable companies, enabling efficient data sharing and processing. This collaboration can lead to improved services and innovations.

Cost-Effectiveness: By sharing resources and infrastructure among a group of companies, the overall costs associated with data storage and processing can be reduced.

Data Redundancy and Reliability: The system can provide higher data redundancy and reliability. If one company faces technical issues, others in the group can ensure the continuity of service, minimizing data loss risks.

Quick Data Access: With the data being stored and managed by a group of service providers, access times can be optimized based on geographical and logistical considerations, leading to faster data retrieval.

Regulatory Compliance: The scheme can be designed to meet various regulatory requirements related to data protection and privacy, making it easier for companies to comply with laws and regulations.

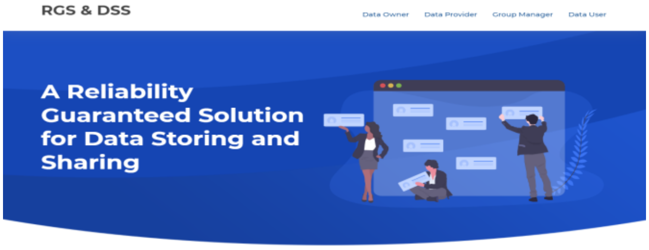
Flexibility in Data Handling: Companies within the group can specialize in different aspects of data handling, such as storage, analysis, or security, leading to a more flexible and efficient overall system.

Enhanced Trust: The group authentication protocol and collaborative approach can enhance trust among participating companies and with their clients, knowing that the data is handled securely and efficiently by reputable organizations.

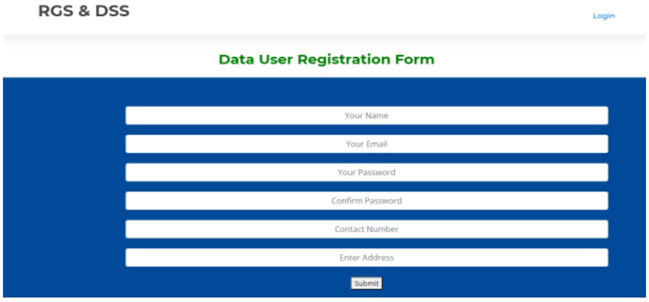
Accuracy is good: Ensuring accuracy in cloud-based test results is crucial for maintaining the reliability of applications and services.

Low Complexity: The complexity arises from the swift adoption of cloud migration and the development of new systems without prior consideration of the operational challenges it introduces..

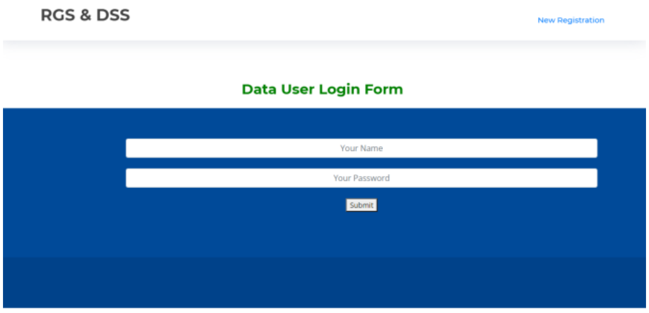
Here in the project we have different kinds of users, Data owner / user / provider, Group manager,


RGS & DSS
Data Owner
Data Provider
Group Manager
Data User
A Reliability Guaranteed Solution for Data Storing and Sharing

All the users has to register to upload the files, manage the files, access the files, check the security levels of the files

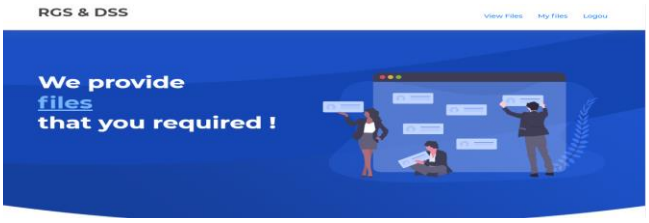


All the users have to authenticate their credentials to access the pages for the above functionality like upload, access & authenticate the security levels based on their access levels



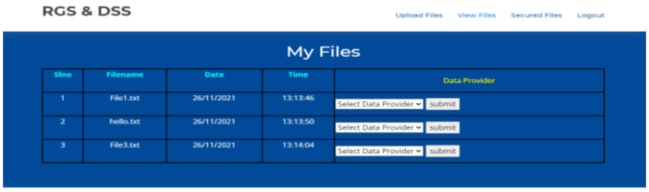
Data User Login Form

After the authentication user has the dashboard page based on the access levels.



We provide files that you required !

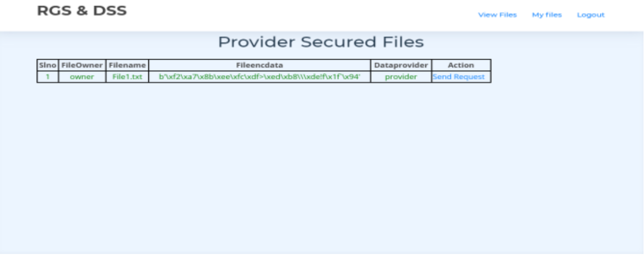
Users or Owners has to access the files in the system based on the authorisation to the panels.



My Files

Slno	Filename	Date	Time	Data Provider
1	File1.txt	26/11/2021	13:13:46	Select Data Provider ⌄ submit
2	hello.txt	26/11/2021	13:13:50	Select Data Provider ⌄ submit
3	File3.txt	26/11/2021	13:14:04	Select Data Provider ⌄ submit

Finds the security levels of the projects based on the authorization and checks the security levels of the projects where the manager has assigned.



Provider Secured Files

Slno	FileOwner	Filename	Fileencdata	Dataprovider	Action
1	owner	File1.txt	b'\xf2\xa7\x8b\xee\xfc\xdf>\xed\xb8\\\xde!f\x1f'\x94'	provider	Send Request

ACKNOWLEDGEMENT

Acknowledging the efforts and contributions of individuals and organizations involved in the development of the RGS & DSS app is crucial to recognize their support and assistance throughout the project. Here's a sample paragraph for the acknowledgment section:

"I would like to express my sincere gratitude to all those who have contributed to the successful completion of this project. First and foremost, I extend my heartfelt thanks to [Supervisor/Project Manager's Name], whose guidance, encouragement, and valuable insights were instrumental in shaping the course of this endeavour. I am deeply grateful to the entire team involved in the development process, including developers, designers, testers, and support staff, for their dedication, hard work, and collaboration. Special thanks are due to [Organization/Institution's Name] for providing the necessary resources, facilities, and support throughout the project duration. Additionally, I would like to extend my appreciation to all the stakeholders, including farmers, equipment owners, and users, whose feedback and input were invaluable in shaping the features and functionalities of the app."

VI. CONCLUSION

Finally, the three schemes: data producing storing, and sharing. In data producing, we conceptualize reputable organizations (ROs) as data providers (DPs), with a manager establishing DPs offering similar services. DPs are empowered to generate meaningful data (MD) from raw data (RD) provided by the data owner (DO) and issue certificates on the encrypted MD (EMD). Our schema not only addresses the DPs and DO privacy but also ensure the secrecy and integrity of the data with are not properly addressed. Furthermore, in our scheme all participants have ability to verify the data reliably before initiating a request with DO. It's important to note the users cannot access the data where everyone verifies the reliability of data shared and accessed a feature lacking in current solutions. Additionally, avoiding the intermediaries during the process of sharing data directly between DO and DU. Security analysis indicate that our proposed schemes uphold essential security properties.

V. REFERENCES

[1]. Curtmola, R., Garay, J., Kamara, S., & Ostrovsky, R. (2006). Searchable symmetric encryption: improved definitions and efficient constructions. Proceedings of the 13th ACM conference on Computer and communications security. CCS '06.

[2]. Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2014). Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems, 25(1), 222-233.

[3]. Kamara, S., Papamanthou, C., & Roeder, T. (2012). Dyna2mic searchable symmetric encryption. Proceedings of the 2012 ACM conference on Computer and communications security. CCS '12.

[4]. Zhang, Y., Deng, R. H., Liu, X., & Zheng, D. (2015). Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. ACM Transactions on Privacy and Security (TOPS), 18(3), 1-30.

[5]. Fu, Z., Wu, X., Guan, C., Sun, X., & Ren, K. (2016). Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Transactions on Information Forensics and Security, 11(12), 2706-2716.

[6]. Wang, B., Song, L., Li, Q., Li, H., & Xiang, Y. (2019). A blockchain-based privacy-preserving multi-keyword search scheme. Future Generation Computer Systems, 94, 541-550.