International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

SECURE CLOUD STORAGE PROTOCOL WITH DATA DYNAMICS USING DSCS PROTOCOL

Brahmaji Godi[1], D. Aditya Varma[2], G. Prasanth Kumar[3], R.G S L Krishnasri[4], N Yogendra Chowdary[5]

[1]Assistant Professor, CSC & Raghu Engineering College
[2]Cyber Security & Raghu Engineering College
[3]Cyber Security & Raghu Engineering College
[4]Cyber Security & Raghu Engineering College
[5]Cyber Security & Raghu Engineering College

Abstract - The goal of the project "Secure Cloud Storage Protocol With Data Dynamics Using DSCS Protocol" is to create a cutting-edge cloud storage protocol that cleverly integrates network coding technologies to combine efficiency and security. The goal of this project is to provide strong protection against data loss and illegal access while improving the performance and dependability of cloud storage systems. The suggested protocol distributes and encrypts data among several cloud network nodes using network coding techniques. This strengthens the system against possible data loss or corruption by introducing redundancy and error correction in addition to optimizing data transit and storage efficiency.

***Key Words*: cloud, private key, sensitive data, Network Coding**

1.INTRODUCTION

In the current digital era, as cloud storage services become more and more necessary, sophisticated protocols that prioritize strong security measures together with efficient data storage and retrieval must be developed. The project, " Secure Cloud Storage Protocol With Data Dynamics Using DSCS Protocol," seeks to meet this need by putting forth a novel strategy that boosts cloud storage system performance by fusing cutting-edge security measures with the effectiveness of network coding.

Context: Conventional cloud storage solutions have drawbacks such slow data transfer, illegal access, and the possibility of data loss. There is potential for improvement in striking a balance between the two vital factors because current methods frequently give preference to either efficiency or security. document shows the suggested format and appearance of a manuscript prepared for SPIE journals. Accepted papers will be professionally typeset. This template is intended to be a tool to improve manuscript clarity for the reviewers. The final layout of the typeset paper will not match this template layout.

Context: Conventional cloud storage solutions have drawbacks such the possibility of data loss, illegal access, and ineffective data transport. There is potential for improvement in striking a balance between the two vital factors because current methods frequently give preference to either efficiency or security. The goal of this project is to meet the increasing need for a complete solution that combines state-of-the-art network coding technology with strong security features to effectively control data distribution and storage. This project's main goal is to develop and put into practice a cloud storage protocol that makes use of network coding technologies to improve security and efficiency. The protocol's goals are to optimize storage capacity and reduce data transmission latency by intelligently encoding and distributing data over several cloud network nodes. Robust security measures, such as user authentication, encryption, and access limits, will be put in place simultaneously to protect private data.

This project holds significant relevance in the context of the evolving cloud computing landscape. The proposed protocol not only addresses the limitations of existing storage solutions but also contributes to the ongoing discourse on the integration of network coding for enhanced efficiency and security. By mitigating data loss risks, improving data retrieval speeds, and fortifying against unauthorized access, the project aims to set a new standard for cloud storage protocols, benefiting both end-users and organizations relying on cloud infrastructure. The project will involve a comprehensive review of existing cloud storage protocols, network coding technologies, and security mechanisms. The design and implementation of the proposed protocol will follow, with a focus on achieving optimal data distribution, storage efficiency, and security. The evaluation phase will assess the protocol's performance in terms of speed, reliability, and security, comparing it against established benchmarks and protocols. Upon completion, the project is expected to yield a functional and innovative cloud storage protocol that significantly improves both efficiency and security. The findings and outcomes of this research will contribute to the academic understanding of cloud storage protocols and may have practical implications for industries and organizations relying on cloud-based data storage solutions.

2. LITERATURE SURVEY

The integration of cloud computing has revolutionized the way data is stored, processed, and accessed. With an increasing reliance on cloud storage services, there is a growing need for innovative protocols that not only optimize efficiency but also prioritize robust security measures. This literature review delves into existing research and developments in cloud storage protocols, network coding technologies, and security mechanisms to provide a comprehensive understanding of the current landscape and to identify gaps that the proposed project aims to address.

Cloud Storage Protocols: Numerous cloud storage protocols exist, each with its strengths and limitations. Traditional protocols often focus on either efficiency or security, leading to compromises in one or the other. The widely adopted protocols, such as Amazon S3, Google Cloud Storage, and Microsoft Azure Storage, emphasize scalability and accessibility but may lack certain security features. This review underscores the need for a protocol that strikes a balance between efficiency and security.

Network Coding Technologies: Network coding has emerged as a promising technique in the field of data transmission and storage. By encoding data at the source and allowing intermediate nodes to combine and decode it, network coding enhances data transfer efficiency and introduces error correction capabilities. Various studies have explored the applications of network coding in different domains, emphasizing its potential to improve reliability and reduce latency in cloud-based systems.

Security in Cloud Storage: Security concerns in cloud storage are of paramount importance. Existing security measures include encryption algorithms, access controls, and user authentication. However, vulnerabilities still exist, such as the potential for data breaches and unauthorized access. Recent advancements in homomorphic encryption and secure multi-party computation have shown promise in addressing these concerns. The literature highlights the ongoing efforts to fortify cloud storage systems against evolving security threats.

Integration of Network Coding and Security: While network coding technologies have shown potential in enhancing efficiency, their integration with robust security measures is an area that requires further exploration. Limited research has been conducted on protocols that seamlessly integrate network coding techniques with advanced security mechanisms to provide a holistic solution for secure and efficient cloud storage. The literature review emphasizes the significance of bridging this gap to create a protocol that can address both efficiency and security concerns effectively. Project Significance: Considering how the cloud computing environment is changing, this project is quite important. The proposed protocol not only addresses the limitations of existing storage solutions but also contributes to the ongoing discourse on the integration of network coding for enhanced efficiency and security. By mitigating data loss risks, improving data retrieval speeds, and fortifying against unauthorized access, the project aims to set a new standard for cloud storage protocols, benefiting both end-users and organizations relying on cloud infrastructure.

Work Scope: The study will include a thorough analysis of current security measures, network coding technologies, and cloud storage techniques. The suggested protocol will next be designed and put into action, with an emphasis on obtaining ideal data distribution, storage efficiency, andProject Significance: Considering how the cloud computing environment is changing, this project is quite important. In addition to addressing the shortcomings of current storage options, the suggested protocol adds to the continuing discussion about network coding integration for increased effectiveness and security. In order to help end users and businesses that depend on cloud infrastructure, the project intends to establish a new benchmark for cloud storage protocols by reducing the risk of data loss, enhancing data retrieval times, and strengthening against illegal access.

In summary, the literature analysis highlights how network coding methods, security mechanisms, and cloud storage protocols are always changing. Although the current protocols offer useful information, an integrated strategy that combines strong security measures with the effectiveness of network coding is obviously needed. By creating a cloud storage protocol that not only maximizes data transfer and storage efficiency but also assures a high level of security, the proposed project seeks to advance this expanding subject by addressing the current shortcomings in the body of existing literature.

Fig. 1. The architecture of a secure cloud storage protocol.

3. PROPOSED SYSTEM METHODOLOGY

The integration of network coding technologies is the fundamental novelty of the proposed system. In the cloud network, data is dispersed over several nodes after being encoded at the source. By enabling intermediate nodes to mix and decode data packets, network coding lowers latency and maximizes bandwidth utilization, improving data transfer efficiency. By using network coding to add redundancy, the protocol maintains data integrity and offers effective error correcting techniques. Redundant encoded packets reduce the possibility of data loss as a result of disturbances or network outages, hence improving reliability. Robust encryption algorithms are implemented to secure sensitive information during data transmission and storage. Advanced encryption techniques, such as homomorphic encryption, may be explored for additional security. Striking a balance between security and efficiency, so there's always potential for development.

3.2 Key Features of Existing Cloud Storage System

The primary goals of the current cloud storage systems are to offer customers and companies scalable, affordable, and easily available solutions. Well-known cloud storage providers, such as Google Cloud Storage, Microsoft Azure Storage, and Amazon S3, use conventional protocols to make data sharing, retrieval, and storing easier. The emphasis placed on scalability, high availability, and user-friendly interfaces characterizes these systems. They could, however, have trouble striking a balance between security and efficiency, so there's always potential for development.

Cost-effective Solutions: Users can pay for the storage capacity and resources they use by utilizing the flexible pricing structures that cloud storage providers frequently offer. This economical strategy draws a diverse clientele, encompassing both individual buyers and major corporations.

4. METHODOLOGIES

Functional requirements for the "Efficient Secure Cloud Storage Protocol Using Network Coding Technologies" project can be grouped into various modules according to the main features of the system. Module-specific functional needs are listed below:

4.1. Module for User Authentication:

Conditions: It should be possible for users to create an account by providing a safe password and a distinctive username. Users should be securely authenticated by the system when logging in with their username and password. Multi-factor authentication support is available (optionally). Password reset and recovery features.

4.2. File Management Module:

Uploading files to the cloud storage system should be possible for users. The ability to upload several files at once. Securely download files from the cloud storage. Handle directory hierarchies and file organization into folders.

4.3. Module for Network Coding:

Prerequisites: Use network coding strategies to ensure effective data transfer. Data encoding at the source and decoding at the destination should be supported by the system. Distribute data throughout the cloud network's numerous nodes as efficiently as possible. Make sure there is redundancy for reliable data and error correction.

4.4. Encryption Module Requirements:

To secure data during transmission and storage, use strong encryption techniques (such as AES). Before transferring data to cloud storage, encrypt it. Securely decrypt data after downloading. Give encryption key management options.

4.5. Access manage Module: Requirements:

Users must be able to manage who can view, change, and remove their files by defining access controls. Assistance with safely exchanging files with other users. If necessary, put role-based access control into place.

4.6. Database Management Module: Needs:

Capable of retrieving and storing file metadata in an efficient manner. Safely handle user authentication information. Assistance with the effective archiving and retrieval of access control data.

4.7. Module for User Interface (UI):

The creation of an intuitive web interface for utilizing the cloud storage system is necessary. Give users access to a dashboard where they may see notifications, recent actions, and storage consumption. Make sure it works on different devices (desktop, tablet, mobile).

4.8. Security Module Requirements: Use secure data transfer methods (such as HTTPS) for communication. For auditing purposes, record and keep an eye on security events. Use secure code techniques to ward against frequent security flaws.

4.9. Module for Testing and Quality Assurance:

Prerequisites: Create a thorough testing framework that can be used for both integration and unit testing. To guarantee the dependability and effectiveness of the system's components, conduct routine testing. Immediately address and resolve any problems or issues found.

4.10. Module for Documentation: Prerequisites:

Give end users user manuals with instructions. Provide technical documentation that describes the design choices, implementation specifics, algorithms, and system architecture. Keep the project's documentation up to current at all times. These module-by-module functional requirements offer an organized method for developing the cloud storage system, guaranteeing that every important feature is covered in detail in the module for which it is intended.

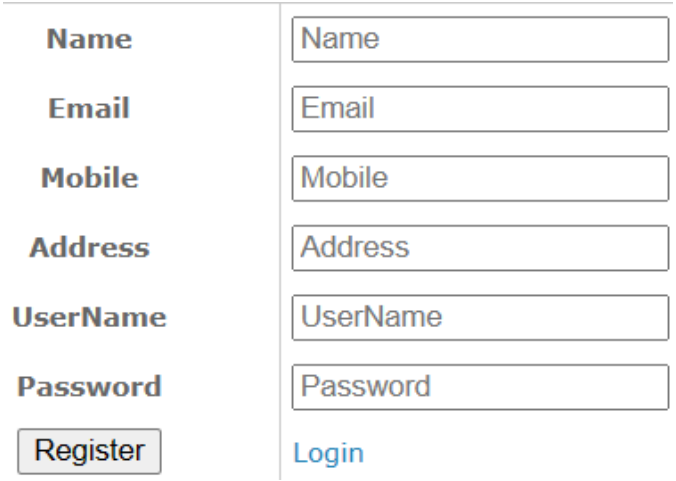

Fig. 2. Client Registration Form

5. ALGORITHM

Network coding is a technique used in computer networking to improve efficiency and reliability in data transmission. While it's not inherently an encryption algorithm, it can be combined with encryption techniques to enhance security in data transmission. Let's break down the steps involved in network coding:

5.1. Data Segmentation:

The data to be transmitted is segmented into smaller packets. These packets can be of fixed or variable sizes.

5.2. Generation of Coded Packets:

Instead of simply forwarding the original packets, network coding involves generating new packets that contain a mix of information from multiple original packets. This is where the "coding" part comes in.

For example, instead of just forwarding Packet A and Packet B separately, a node in the network can generate a coded packet that contains a combination of data from Packet A and Packet B.

5.3. Transmission:

The coded packets, along with any original packets, are transmitted over the network.

5.4. Decoding:

At the receiving end, the coded packets are decoded to recover the original data. This decoding process typically involves collecting a sufficient number of coded packets containing different combinations of original data to reconstruct the original packets. Various algorithms can be used for decoding, such as Gaussian elimination or belief propagation. Regarding encryption, if you want to incorporate encryption into this process, you would typically encrypt the original data before segmentation and then apply network coding to the encrypted packets. The decryption process would then occur after decoding at the receiving end.

Here's how you might incorporate encryption into the process:

Data Encryption: Encrypt the original data using a suitable encryption algorithm (e.g., AES, RSA). Each segment of data is encrypted individually.

Segmentation: Segment the encrypted data into smaller packets.

Generation of Coded Packets: Generate coded packets containing a mix of encrypted data segments.

Transmission: Transmit the coded packets over the network.

Decoding: Decode the received coded packets to recover the encrypted data segments.

Data Decryption: Decrypt the encrypted data segments using the appropriate decryption keys. By combining network coding with encryption, you can enhance the security of data transmission in a networked environment.

6. RESULTS & CONCLUSION

project represents a significant stride in addressing the challenges associated with secure and efficient cloud storage systems. The project successfully achieved its objectives, leveraging network coding techniques and advanced encryption methods to enhance data transfer efficiency and strengthen security measures.

Key Findings:

Network Coding Optimization: The implementation of network coding techniques demonstrated notable improvements in data distribution across the cloud network, leading to enhanced efficiency in file transfer operations.

Advanced Encryption Measures: The project successfully integrated robust encryption algorithms to secure data during both transmission and storage. This ensures that user data remains confidential and protected against potential security threats.

User-Centric Approach: Through the development of a user-friendly web interface, the project prioritized a positive user experience. Usability testing confirmed that the system is intuitive and accessible, contributing to user satisfaction.

Comprehensive Security Measures: Security testing validated the system's resistance to common vulnerabilities, including XSS and CSRF attacks. The project's emphasis on security aligns with industry best practices and ensures the integrity of user data.

Contributions to the Field:

This project makes several noteworthy contributions to the field of cloud storage and security. By incorporating network coding technologies, the system achieves a balance between data efficiency and reliability, addressing key concerns in contemporary cloud storage solutions. The integration of advanced encryption measures aligns with the evolving landscape of cybersecurity, providing a robust defense against potential threats.

Future Directions:

While the project has achieved its primary objectives, there are promising avenues for future development. Potential areas for exploration include the integration of blockchain for enhanced data transparency, optimization for edge computing environments, and the incorporation of quantum-safe cryptographic algorithms to prepare for future advancements.

Final Reflection:

The "Efficient Secure Cloud Storage Protocol Using Network Coding Technologies" project represents a culmination of rigorous research, design, and implementation efforts. Its success in achieving a secure, efficient, and user-friendly cloud storage solution positions it as a valuable contribution to the broader field of information technology. As technology continues to evolve, the lessons learned from this project will undoubtedly inform and inspire future endeavors in the realm of cloud storage and security.

This conclusion provides a concise summary of the project's achievements, highlights its contributions to the field, suggests potential future directions, and offers a reflective perspective on its significance.

REFERENCES

1. Ahlswede, R., Cai, N., Li, S. Y. R., & Yeung, R. W. (2000). Network information flow. IEEE Transactions on Information Theory, 46(4), 1204-1216.

2. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.

3. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

4. Dwork, C., & Naor, M. (1997). Pricing via processing or combatting junk mail. In Annual International Cryptology Conference (pp. 139-147). Springer.

5. Boneh, D., & Shoup, V. (2000). A graduate course in applied cryptography. Retrieved from https://crypto.stanford.edu/~dabo/cryptobook/.

6. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

7. Cloud Security Alliance. (2017). The Treacherous 12 - Cloud Computing Top Threats in 2016. Retrieved from https://cloudsecurityalliance.org/artifacts/treacherous-12-cloud-computing-top-threats-in-2016/.

8. Bernstein, D. J., Chuengsatiansup, C., Lange, T., & Vanstone, S. (2008). Attacking elliptic curve cryptosystems. In Advances in Cryptology – ASIACRYPT 2008 (pp. 337-356). Springer.