**CHATPER- 1**

**INTRODUCTION**

**1.INTRODUCTION**

In the cloud maintenance requirements, allowing users to easily access their data on cloud servers. However, cloud servers have full control over outsourced data, which raises security corners about data integrity. Public auditing address issue by utilizing a third-party auditor to verify the correctness of the data in the cloud on behalf of users. Public auditing works by dividing a file into many blocks, with each block associated with auditing metadata. It is especially useful in terms of integrity checks because testing only a few blocks is sufficient to verify file integrity. The owner splits the code into a fixed number of lines and group them with each set associated with a tag as auditing metadata. As more cloud backed services adopt dynamic file updates

Public auditing is required to support data dynamics such a block wise modification, insertion and deletion. It is also desirable for a TPA to rapidly complete the verification and notify the user of the results. However, according to our measurements. Typically, a TPA is assigned numerous files, it would be highly advantageous if the TPA-side computation cost with respect to verification can be reduced. The auditing challenge response protocols reduces the computation cost of the TPA significally.

The proposed schemes facilitate pre computation capabilities such that after sending an auditing request to the cloud, the TPA can pre-compute all exponentiation operations need for the subsequent phase. The proposed scheme is compatible with any symmetric key encryption algorithm such that the blocks are encrypted any encryption algorithm of the data owner’s choice. Data confidentially is preserved against the cloud due to the CPA-secure property of the underlying encryption algorithm. Public auditing with data dynamics which selectively preserves privacy against the TPA

and the cloud to deviate from the protocol. This allows the users to ensure the correctness of a search result by using protocols.

Hosting data in the cloud minimizes maintenance requirements, allowing Users to easily access their data on cloud services. Moreover, the project should be indulged to enhance the development for providing security to the data through the protection to the given data in the cloud server.

**1.1 PURPOSE**

The purpose of this project is to enhance the security of cloud storage systems while accommodating data dynamics efficiently. Traditional cloud storage systems face challenges related to data security and dynamic data updates, which can compromise the integrity and confidentiality of stored data. By leveraging secure network coding techniques, this project aims to prvide robust protection against various security threats such as eavesdropping, data tampering, and unauthorized access, while ensuring seamless data management and access control in dynamic environments.7

Network coding techniques have been used to construct distributed storage systems where the client’s data are disseminated across multiple servers. The primarily aim to reduce the repair bandwidth when some of the servers fail, we explore whether we can exploit the algorithms involved in an SNC protocol to construct an efficient and secure cloud storage protocol for dynamic data (for a single storage server.)

**1.2 SCOPE**

During an audit, the client sends a random challenge to the server which produces proofs of storage computed on the stored data corresponding to that challenge. Secure cloud storage protocols are publicly verifiable if an audit can be performed by an third party auditor using public parameters; or privately verifiable if an auditor needs some secret information of the client.

The scope of this project encompasses the development and implementation of a secure cloud storage system that integrates secure network coding techniques to safeguard data confidentiality, integrity, and availability. Key aspects of the system include:

Implementation of secure network coding algorithms to encode and decode data packets for secure transmission and storage.

Integration of access control mechanisms to regulate data access based on user privileges and authentication. Support for dynamic data operations such as insertion, deletion, and modification while maintaining data consistency and security.

Implementation of cryptographic protocols for secure communication between clients and cloud servers. Evaluation of system performance, security, and scalability through simulations and real-world experiments.

**1.3 NEED FOR SYSTEM**

**1. Enhanced Data Security:**

Traditional cloud storage systems are susceptible to security breaches such as unauthorized access, data interception, and tampering. With the increasing volume of sensitive data stored in the cloud, there is a critical need for advanced security measures to protect confidential information from potential threats.

**2. Dynamic Data Management:**

Modern applications require dynamic data management capabilities, including frequent updates, additions, and deletions. Conventional cloud storage systems often struggle to efficiently handle dynamic data operations while ensuring data integrity and security. There is a need for innovative solutions that can accommodate data dynamics without compromising security or performance.

**3. Confidentiality and Privacy:**

Data privacy is a significant concern for organizations and individuals entrusting their data to cloud storage providers. Secure network coding techniques offer enhanced confidentiality by encrypting data at the packet level, ensuring that sensitive information remains protected even if intercepted during transmission or storage.

**4. Regulatory Compliance:**

Many industries are subject to strict regulations regarding data security and privacy, such as GDPR, HIPAA, and PCI DSS. Implementing robust security measures, including secure network coding, can help organizations comply with regulatory requirements and avoid potential legal and financial consequences associated with data breaches.

**5. Data Integrity and Availability:**

Ensuring the integrity and availability of data stored in the cloud is essential for maintaining trust and reliability. Secure network coding techniques provide mechanisms for error detection and correction, ensuring data integrity even in the presence of network failures or malicious attacks.

In summary, the proposed secure cloud storage system addresses the growing need for enhanced data security, dynamic data management, confidentiality, privacy, regulatory compliance, and data integrity and availability, making it an indispensable solution for organizations seeking to leverage cloud storage while mitigating security risks.

**Existing system:**

Existing System Old systems designed to support unshared multi-owner setting, and cannot be directly applied in the shared multi-owner setting. As existing system does not provide server data for which multi-keyword and multi owner search. It is difficult to identify malicious users who leak the secret keys when more than one data user has the same subset of attributes.

Data privacy is a significant concern for organizations and individuals entrusting their data to cloud storage providers. Secure network coding techniques offer enhanced confidentiality by encrypting data at the packet level, ensuring that sensitive information remains protected even if intercepted during transmission or storage.

**Disadvantages:**

* Single Owner Sharing
* It takes high time.
* Comple.
* Uncontrollable.

**Proposed System:**

This paper focuses on direct switching attacks on the electric power distribution system. The proposed algorithm consists of a decentralized system implemented by a multi-agent system (MAS), and a centralized system that performs network reconfiguration. The contributions of this paper are as

**Advantages:**

* More Effective
* Data Cleaning and Visualization
* Scalability
* Less Time