Secure Storage Mechanism Cloud-Based Using Data DiSspersion and Data Encryption.

Ali Azam Pathan
Department of Computer Science and Engineering
SET, Jain University
Bengaluru, India
19btrcs053@jainuniversity.ac.in

Mastani Shaik
Department of Computer Science and Engineering
SET, Jain University
Bengaluru, India
19btrcs072@jainuniversity.ac.in

Deepak K Sinha
Department of Computer Science and Engineering
SET, Jain University
Bengaluru, India
Sk.deepak@jainuniversity.ac.in

Imran Khan Abdul
Department of Computer Science and Engineering
SET, Jain University
Bengaluru, India
19btrcs001@jainuniversity.ac.in

Heena Shaik
Department of Computer Science and Engineering
SET, Jain University
Bengaluru, India
19btrcs071@jainuniversity.ac.in

***Abstract*--Cloud secure storage mechanism of data encryption and dispersion is a technique used to ensure the confidentiality, integrity, and availability of data stored in the cloud. In this mechanism, data is encrypted using a strong encryption algorithm before it is stored in the cloud. The encryption key is then dispersed into several parts using a secret sharing scheme and these parts are distributed to different servers in the cloud. As a result, even if one of the servers is compromised, an attacker cannot access the encryption key or the original data. To retrieve the data, the dispersed parts of the encryption key are reassembled using the secret sharing scheme, and then the encrypted data is decrypted. This mechanism provides a high level of security for data stored in the cloud, even in the event of a security breach.**

1)Cloud secure storage mechanism refers to a method of storing data in a cloud-based system that ensures the security and privacy of the data.

2)The mechanism involves two key components - encryption and dispersion - which work together to protect data from unauthorized access.

3)Encryption is the process of converting plain text data into a coded form, which can only be read by authorized parties with the decryption key.

4)Dispersion involves splitting the encrypted data into multiple fragments and storing them in different locations to prevent a single point of failure.

5)The dispersion process can be done through various methods such as secret sharing, erasure coding, or geographic dispersal.

Keywords — Cloud storage, Secure storage mechanisms ,Data dispersion, Encryption, Cybersecurity, Hacking ,Data breaches, Homomorphic encryption ,Secret sharing. Redundancy, Availability, Durability, Decryption key Standardized security protocols, Security audits, Cloud storage services, Monitoring, Management.

I. INTRODUCTION

Cloud secure storage mechanism of data encryption and dispersion is a technique used to ensure the confidentiality, integrity, and availability of data stored in the cloud. In this mechanism, data is encrypted using a strong encryption algorithm before it is stored in the cloud. The encryption key is then dispersed into several parts using a secret sharing scheme and these parts are distributed to different servers in the cloud. As a result, even if one of the servers is compromised, an attacker cannot access the encryption key or the original data. To retrieve the data, the dispersed parts of the encryption key are reassembled using the secret sharing scheme, and then the encrypted data is decrypted. This mechanism provides a high level of security for data stored in the cloud, even in the event of a security breach. There are several techniques for combining data dispersion and encryption in a secure cloud storage mechanism. One approach is to use a technique called secret sharing, where the data is split into fragments using a mathematical algorithm and each fragment is encrypted using a separate encryption key. These encrypted fragments are then distributed across multiple cloud servers or locations, making it difficult for an attacker to reconstruct the original data without access to all of the encryption keys.

Another approach is to use a technique called homomorphic encryption, where data is encrypted in a way that allows computations to be performed on the encrypted data without requiring access to the decryption key. This allows sensitive data to be processed in the cloud without ever being decrypted, providing an additional layer of security.

In summary, cloud secure storage mechanisms rely on a combination of data dispersion and encryption techniques to protect sensitive data stored in the cloud. These techniques help to ensure that data remains secure even in the event of a

breach or other security incident.

A. Background information:

Cloud secure storage mechanisms have become increasingly important in recent years due to the growing use of cloud storage services and the need to protect sensitive data from unauthorized access, theft, or other security threats.

Cloud storage allows users to store and access data over the internet, eliminating the need for on-premises storage infrastructure and reducing costs. However, storing sensitive data in the cloud also introduces new security risks, as the data may be vulnerable to hacking, data breaches, and other types of cyber-attacks.

To address these risks, cloud storage providers and organizations have developed a range of secure storage mechanisms that rely on data dispersion and encryption techniques to protect data stored in the cloud.

Data dispersion involves splitting data into fragments and distributing them across multiple cloud servers or locations, making it difficult for attackers to access the entire data set. This approach also provides redundancy and ensures that data is available and durable even in the event of a server failure or outage.

Encryption is used to protect data both in transit and at rest. Data is encrypted before being stored in the cloud, and decryption keys are required to access the data. This helps to ensure that even if an attacker gains access to the data, they will not be able to read or use it without the decryption key.

There are several techniques for combining data dispersion and encryption in a secure cloud storage mechanism, including secret sharing and homomorphic encryption. These techniques help to ensure that data remains secure even in the event of a breach or other security incident, providing organizations with greater confidence in the security of their cloud storage solutions

B. Problem Statement

The problem addressed by cloud secure storage mechanisms using data dispersion and encryption techniques is the need to protect sensitive data stored in the cloud from unauthorized access, theft, or other security threats.

Cloud storage services provide a convenient and costeffective way to store and access data over the internet, but they also introduce new security risks. Sensitive data stored in the cloud may be vulnerable to hacking, data breaches, and other types of cyber-attacks, which can result in significant financial and reputational damage for organizations.

To address these risks, it is essential to implement secure storage mechanisms that use data dispersion and encryption techniques. These mechanisms help to ensure that even if an attacker gains access to the data, they will not be able to read or use it without the decryption key. Data dispersion also provides redundancy and ensures that data remains available and durable even in the event of a server failure or outage.

C. Hypothesis

The hypothesis of cloud secure storage mechanisms using data dispersion and encryption techniques is that by implementing effective security measures, organizations can significantly reduce the risk of unauthorized access, theft, or other security threats to sensitive data stored in the cloud.

This hypothesis is based on the assumption that data dispersion and encryption techniques provide an effective way to protect sensitive data stored in the cloud. By splitting data into fragments and distributing them across multiple cloud servers or locations, and encrypting the data using strong encryption algorithms, organizations can make it difficult for attackers to gain access to the entire data set or read the data without the decryption key. Additionally, these techniques can provide redundancy and ensure that data remains available and durable even in the event of a server failure or outage.

The hypothesis also assumes that effective security measures must be implemented consistently across all cloud storage services used by an organization to ensure a consistent and effective level of security. This may involve the use of standardized security protocols, regular security audits, and ongoing monitoring and management of cloud storage environments.

Overall, the hypothesis of cloud secure storage mechanisms is that by implementing effective data dispersion and encryption techniques and maintaining a consistent and effective level of security across all cloud storage services, organizations can significantly reduce the risk of unauthorized access, theft, or other security threats to sensitive data stored in the cloud.

II. METHODOLOGY

Identify the types of sensitive data that need to be stored in the cloud and the appropriate level of security needed to protect them. This includes identifying which data needs to be encrypted and the level of encryption required.

Evaluate cloud storage services and providers to determine which ones offer the necessary security features and capabilities. This includes reviewing their security certifications, compliance with relevant regulations, and their track record of security incidents.

Develop a cloud storage security plan that includes data dispersion and encryption techniques. This involves selecting an appropriate data dispersion and encryption method, such as secret sharing or homomorphic encryption, and developing policies and procedures for data storage, access, and retrieval.

Implement the security plan by configuring cloud storage services and applications to comply with the established policies and procedures. This includes configuring encryption settings, access controls, and monitoring and logging capabilities.

Test and validate the security plan to ensure that it is effective and meets the intended security goals. This includes testing data dispersion and encryption techniques to ensure that data remains secure even in the event of a security breach or other security incident.

Regularly review and update the cloud storage security plan to ensure that it remains effective and up-to-date with changing security threats, regulations, and best practices.

The methodology may also involve engaging with external security experts or consultants to provide additional expertise and guidance in developing and implementing secure cloud storage solutions.

A. Data collection and pre-processing

- Data collection and pre-processing for Cloud secure storage mechanism on data dispersion and encryption introduction may involve gathering information from various sources, including academic research papers, industry reports, and whitepapers from cloud storage providers.

- Some specific data collection and pre-processing steps include:
- Collecting data on cloud storage security threats and vulnerabilities, such as data breaches, hacking incidents, and insider threats.
- Identifying cloud storage providers that offer data dispersion and encryption techniques, and collecting data on their security features, certifications, and compliance with relevant regulations.
- Gathering data on the different types of data dispersion and encryption techniques, including secret sharing and homomorphic encryption, and their respective strengths and weaknesses.
- Collecting data on industry best practices for secure cloud storage, including security protocols, access controls, and monitoring and logging capabilities.
- Pre-processing the collected data to remove duplicates, inconsistencies, and irrelevant information.
- Categorizing the pre-processed data into relevant topics and subtopics, such as data dispersion techniques, encryption algorithms, and cloud storage security protocols.
- Analyzing the pre-processed data to identify trends and patterns, and to draw insights and conclusions about the effectiveness of different data dispersion and encryption techniques in protecting sensitive data stored in the cloud.
- The pre-processing of data may also involve the use of data visualization tools, such as charts and graphs, to help convey key insights and findings. Overall, the data collection and pre-processing steps aim to provide a solid foundation of knowledge and information for developing and implementing secure cloud storage solutions using data dispersion and encryption techniques.

B. Architecture

The architecture of cloud secure storage mechanisms using data dispersion and encryption techniques typically involves several key components, including:

Cloud Storage Service Providers: These are third-party service providers that offer cloud storage solutions, including data dispersion and encryption techniques, to organizations and individuals.

Data Dispersion Techniques: These techniques involve splitting data into fragments and distributing them across multiple cloud servers or locations, to make it difficult for attackers to gain access to the entire data set or read the data without the decryption key. Some examples of data dispersion techniques include secret sharing, erasure coding, and RAID (redundant array of independent disks).

Encryption Techniques: These techniques involve converting data into a coded format that can only be read with a decryption key. This helps to protect the data from unauthorized access or theft. Some examples of encryption techniques include Advanced Encryption Standard (AES), RSA, and homomorphic encryption.

Access Control: This component involves controlling who has access to the data stored in the cloud, and what actions they can perform on the data. This includes implementing role-based access controls (RBAC), multifactor authentication, and audit trails.

Key Management: This component involves managing the encryption keys that are used to encrypt and decrypt the data stored in the cloud. This includes key generation, distribution, and revocation.

Monitoring and Logging: This component involves monitoring and logging all access and usage of data stored in the cloud, to detect any unauthorized access or suspicious activity.

Compliance and Governance: This component involves ensuring that the cloud storage solutions and data dispersion and encryption techniques comply with relevant regulations and governance policies, such as GDPR, HIPAA, and ISO 27001.

Overall, the architecture of cloud secure storage mechanisms using data dispersion and encryption techniques involves a combination of different components and techniques, working together to provide effective protection against unauthorized access and theft of sensitive data stored in the cloud.

C. Algorithm

The Advanced Encryption Standard (AES) is a widely used encryption algorithm in cloud secure storage mechanisms using data dispersion and encryption techniques. AES is a symmetric-key encryption algorithm, which means that the same key is used for both encryption and decryption.

The AES algorithm works by dividing the plaintext (original data) into blocks of fixed size, typically 128 bits. The encryption process involves multiple rounds of substitution and permutation operations, using a secret key. The key length can be 128, 192, or 256 bits, depending on the desired level of security.

During the encryption process, each plaintext block is transformed into a corresponding ciphertext block using a series of mathematical operations, such as substitution and permutation. The resulting ciphertext block is then passed onto the next round of encryption, using the same secret key.

The decryption process is essentially the reverse of the encryption process, where each ciphertext block is transformed back into its corresponding plaintext block using the same secret key.

One of the key advantages of AES is its strong encryption and decryption capabilities, which make it difficult for attackers to decipher the encrypted data without the secret key. AES is also widely used and has been extensively tested and validated for security by industry and government organizations.

However, one of the potential limitations of AES is its symmetric-key encryption approach, which means that the same key is used for both encryption and decryption. This can create challenges in key management and distribution, especially in large-scale cloud storage environments.

Overall, the AES algorithm is an important component of cloud secure storage mechanisms using data dispersion and encryption techniques, providing a strong and reliable means of encrypting sensitive data stored in the cloud.

D. Related Work

There is a significant amount of related work on cloud secure storage mechanisms using data dispersion and encryption techniques. Some notable research and development efforts in this area include:

Secure Distributed Storage Systems: This research focuses on developing secure and efficient distributed storage systems using data dispersion and encryption techniques. Examples of secure distributed storage systems include Tahoe-LAFS, Freenet, and InterPlanetary File System (IPFS).

Homomorphic Encryption: Homomorphic encryption is an emerging area of research that involves performing computations on encrypted data, without decrypting it first. This allows for secure and private computation of sensitive data in cloud storage environments.

Privacy-Preserving Data Analysis: This research focuses on developing techniques for analyzing sensitive data stored in the cloud, without compromising privacy. Techniques used in privacy-preserving data analysis include differential privacy, secure multi-party computation, and secure function evaluation.

Blockchain-Based Storage Systems: Blockchain technology can be used to create secure and decentralized cloud storage systems, using data dispersion and encryption techniques. Examples of blockchain-based storage systems include Story and Sia.

Attribute-Based Encryption: Attribute-based encryption is a technique that allows access control to be applied to individual data items, rather than to an entire file or data set. This allows for more fine-grained access control in cloud storage environments, and can be combined with data dispersion and encryption techniques for added security.

Overall, there is a growing body of research and development efforts focused on cloud secure storage mechanisms using data dispersion and encryption techniques, driven by the need for secure and reliable cloud storage solutions in today's data driven world.

III. IMPLEMENTATION

Implementing a cloud secure storage mechanism using data dispersion and encryption techniques involves several steps.

Here are some general guidelines for implementing such a mechanism:

A. Determine the data dispersion and encryption techniques to be used: Depending on the specific requirements and use case of the cloud storage system, different data dispersion and encryption techniques can be used. For example, Reed-Solomon coding can be used for data dispersion, while the Advanced Encryption Standard (AES) can be used for encryption.

B. Choose a cloud storage platform: There are many cloud storage platforms available, such as Amazon S3, Google Cloud Storage, and Microsoft Azure. Choose a cloud storage platform that meets your requirements in terms of features, security, and cost.

C. Set up the cloud storage system: Set up the cloud storage system according to the platform's documentation, and configure the necessary access controls and permissions.

D. Implement data dispersion and encryption: Implement the chosen data dispersion and encryption techniques to secure the data stored in the cloud. This may involve coding the algorithms yourself or using pre-existing libraries.

E. Manage keys: Ensure that keys used for encryption and decryption are managed securely. This involves generating and storing keys securely, and ensuring that only authorized users have access to them.

F. Test and monitor: Test the system thoroughly to ensure that data is properly dispersed and encrypted, and monitor the system for any signs of unauthorized access or data breaches.

G. Regularly update and maintain the system: Keep the system up to date with security patches and updates, and regularly review the system's security policies and access controls to ensure that they are still appropriate.

Overall, implementing a cloud secure storage mechanism using data dispersion and encryption techniques requires careful planning and execution, as well as ongoing maintenance and monitoring to ensure that the system remains secure over time.

.

IV. RESULT

The results of implementing a cloud secure storage mechanism using data dispersion and encryption techniques can be measured in terms of the security and reliability of the cloud storage system. Specifically, the results can include:

Improved data security: Data dispersion and encryption techniques can provide an added layer of security to cloud storage systems, protecting data from unauthorized access or theft.

Reduced risk of data breaches: By dispersing data across multiple locations and encrypting it, the risk of a data breach is reduced, as attackers would need to access multiple locations and decrypt the data to gain access.

Better access control: By using attribute-based encryption or other access control techniques, access to individual data items can be controlled more granularly, improving overall data security.

Improved data availability: By dispersing data across multiple locations, the likelihood of data loss due to a single point of failure is reduced, improving overall data availability.

Increased scalability: Cloud secure storage mechanisms using data dispersion and encryption techniques can be highly scalable, allowing for the storage and retrieval of large amounts of data in a secure and efficient manner.

Overall, the result of implementing a cloud secure storage mechanism using data dispersion and encryption techniques can be a highly secure and reliable cloud storage system, capable of storing and retrieving large amounts of data while protecting it from unauthorized access or theft.

V. DISCUSSION

The implementation of a cloud secure storage mechanism using data dispersion and encryption techniques is an important step towards improving the security and reliability of cloud storage systems. By dispersing data across multiple locations and encrypting it, the likelihood of data loss due to a single point of failure is reduced, and the risk of data breaches is mitigated.

The use of Reed-Solomon coding for data dispersion and the Advanced Encryption Standard (AES) for encryption is a widely accepted approach that can provide a high level of security and reliability to the cloud storage system. However, there are other techniques available that can be used depending on the specific requirements and use case of the system.

One important aspect of implementing a cloud secure storage mechanism is the management of keys used for encryption and decryption. Keys must be generated and stored securely, and only authorized users should have access to them. Additionally, access control mechanisms such as attribute based encryption can be used to further control access to individual data items, improving overall data security.

Regular testing and monitoring of the cloud secure storage mechanism is also critical to ensure that it is working as intended and that any potential vulnerabilities are identified and addressed promptly. In addition, ongoing maintenance and updates to the system's security policies and access controls are essential to ensure that the system remains secure over time.

VI. CONCLUSION

In conclusion, the implementation of a cloud secure storage mechanism using data dispersion and encryption techniques is a critical step towards improving the security and reliability of cloud storage systems. By dispersing data across multiple locations and encrypting it using techniques such as Reed Solomon coding and the Advanced Encryption Standard (AES), organizations can significantly reduce the risk of data breaches and improve data availability.

This paper has discussed the background, problem statement, hypothesis, methodology, and implementation of a cloud secure storage mechanism using data dispersion and encryption techniques. The paper has highlighted the importance of carefully planning and executing the implementation of such a mechanism, as well as ongoing maintenance and monitoring to ensure its effectiveness.

The use of data dispersion and encryption techniques provides an added layer of security to cloud storage systems, protecting sensitive data from unauthorized access or theft. Additionally, access control mechanisms such as attribute based encryption can be used to further control access to individual data items, improving overall data security.

As organizations increasingly rely on cloud storage solutions for their data storage and management needs, implementing a cloud secure storage mechanism using data dispersion and encryption techniques can provide significant benefits in terms of data security, reliability, and scalability. Overall, the implementation of such a mechanism is a worthwhile investment for organizations that require secure and scalable cloud storage solutions.

REFERENCES

[1] Wang, X., Shen, J., & Zhang, J. (2019). Data storage security in cloud computing: A survey. Journal of Network and Computer Applications, 129, 33-48.

[2] Wang, X., Zhang, J., & Huang, X. (2020). A secure cloud storage mechanism using data dispersion and attribute-based encryption. Journal of Information Security and Applications, 50, 102433.

[3] Puthal, D., Malik, N. M., Mohanty, S. P., Kougianos, E., & Yang, C. (2019). The internet of things security using blockchain technology. IEEE Consumer Electronics Magazine, 8(1), 41-47

[4] Sharma, P., Kumar, A., & Khamparia, A. (2018). Cloud data storage security: A systematic review. Journal of Network and Computer Applications, 116, 28-45.

[5] Zeng, X., Xiao, Y., Jiang, X., & Zhou, J. (2017). Ensuring data storage security in cloud computing via disjoint coding. Journal of Network and Computer Applications, 88, 16-26

[6] Alharthi, H., & Elleithy, K. (2021). A novel cloud storage security system using enhanced AES encryption algorithm. Future Generation Computer Systems, 120, 35-46.

[7] Chavan, S., & Dhamdhere, J. (2017). A review on secure data storage mechanisms in cloud. Journal of Network and Computer Applications, 98, 50-63.

[8] Sharma, S., & Rana, N. P. (2019). A review of security and privacy issues in cloud computing. Journal of Network and Computer Applications, 135, 1-25.

[9] Wu, H., Shen, Y., Wang, X., Zhang, H., & Zhang, X. (2020). A secure cloud storage system with data dispersion and multiple layers of encryption. IEEE Transactions on Services Computing, 13(2), 338349.

[10] Jia, Y., Li, F., Zhang, S., Li, Q., Li, X., & Li, J. (2019). Cloud data security: A survey. Journal of Network and Computer Applications, 131, 64-82.