International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

EFFICIENT MULTI-AUTHORITY ACCESS CONTROL USING CIPHERTEXT POLICY - HIERARCHICAL ATTRIBUTE BASED ENCRYPTION IN CLOUD STORAGE

Bikram Kumar dhal.R[1],Chandru.M[2], Pechumuthu.R[3],Sivamani.K[4],Mrs.R.Jayanthi[5]

1,2,3,4B.E, Student Department Computer Science and Engineering, Angel College Of Engineering and Technology,Tiruppur, TamilNadu, India

5Asst.Professor, Department Computer Science and Engineering, Angel College Of Engineering and Technology,Tiruppur,Tamilnadu, India

ABSTRACT

The goal of this research is to improve the security of cloud-based data storage systems by presenting the Cloud Secure Storage Mechanism based on Data Dispersion and Encryption (CPHABE). The User Frame, Authority Login, Cloud Server Login, and Data Owner Login are the four separate components that make up the system. By providing file names and requesting transformation keys from the authority for decryption, users start downloads. Requests for transformation keys, upload information, and key creation are handled by the authority. Owner identities, file names, encrypted content, gate types, and storage size graphs are all managed by cloud servers. Partially decrypted data, such as user identities, file names, transformation keys, data owner IDs, and partially decrypted content, is sent in response to user requests. Data owners may use the system to explore files, obtain keys, and apply hybrid encryption methods including Authenticated Encryption (AE) and Key Encapsulation Mechanism (KEM). This all-encompassing strategy guarantees strong encryption, data dispersion, and security measures, offering a stable foundation for cloud storage systems.

Keywords: Cloud Storage, Security Mechanism, Encryption

1. INTRODUCTION

In order to strengthen the security of cloud-based data storage systems, this research suggests a Cloud Secure Storage Mechanism based on Data Dispersion and Encryption (CPHABE). Using the combined power of data dispersion and encryption methods, a novel cloud safe storage mechanism is developed to overcome this difficulty. This system reduces the possibility of data breaches and unwanted access by distributing data among several storage nodes and encrypting it with strong cryptographic techniques. Because the data is scattered, even if one storage node is hacked, the entire dataset will remain unreadable and unusable in the absence of the necessary decryption keys. In addition, encryption provides an extra degree of protection by making the data unintelligible to those lacking the necessary cryptographic keys.

1.1 CLOUD STORAGE

With cloud storage, users may easily access their files from any location with an internet connection, making it a fundamental component of contemporary data management. However, worries about privacy and security are still present, which has led to the creation of creative safeguards for sensitive data kept in the cloud. This study presents a strong cloud storage security mechanism that reduces the risks of data breaches and unauthorized access by combining data dispersion and encryption approaches. The suggested technique guarantees that even in the event of a node breach, the integrity and secrecy of the entire dataset will endure as data is distributed over several storage nodes and encrypted using cutting-edge cryptographic techniques.

1.2 SECURITY MECHANISM

This work presents a security method that improves the security of cloud-stored data by combining data dispersion and encryption approaches. Data dispersion is the process of dividing up data over several storage nodes in order to lower the possibility of a single point of failure and increase attacker resistance. Furthermore, the distributed data is encrypted with strong cryptographic techniques so that, in the event of unwanted access, the data cannot be decrypted without the right keys. The entire security posture of cloud storage systems is strengthened by this dual-layered strategy, which dramatically lowers the possibility of data breaches and unauthorized access.

2. LITERATURE REVIEW

In this paper [1], Gang Li et.al. have put forth the objective of achieving a distributed, collaborative, and automated design and manufacturing workflow. To achieve this, they have leveraged the concept of Industry 4.0 and its associated technologies such as Cyber Physical System, Internet of Things, Cloud Computing, and Big Data Analytics. The cyber-physical system and internet of things enable the collection and transfer of industrial data through a fusion of peripherals such as software, sensors, and electronics. Cloud computing techniques aid in centralized data storage and offer a platform for collaboration to expedite and refine resource allocation and research for entire industry gains. Big data analytics has also been exploited to organize these digital assets and extract valuable insights from them. This has attracted significant attention from both industry and academia. In this special issue, the manifold relationship between Industry 4.0 and Big Data is investigated by bringing together active researchers from related fields. Five papers have been solicited for publication after a rigorous peer-review process, proposing surveys, mechanisms, and frameworks spanning from the infrastructural level to the data processing level, as well as the service level of Industry 4.0,

Chunhui Wen [2] et.al. has proposed in their paper the successful utilization of the big data technology framework in the Internet of Things. The financial industry also aims to leverage the advanced technology of big data to integrate and enhance the internal and external data pertaining to credit risks. By relying on more efficient machine learning algorithms, a reasonable prediction of credit risk can be obtained, thereby reducing self-generated losses in the Internet of Things finance and increasing profits. This article employs distributed search engine technology to customize web crawlers for acquiring the necessary bank card and transaction data from the diverse sources of data in the Internet of Things financial industry. It further designs a corresponding Spark parallel algorithm to preprocess the data and establishes an inverted table and two-level index file to serve as a data source for big data analysis platforms. Once the data source is determined, the Mutually Exclusive Collectively Exhaustive (MECE) analysis method is combined with the expertise of numerous financial business experts in the industry to derive a set of candidate indicators and quantification methods for evaluating the financial credit risk in the Internet of Things. Additionally, the correlation between these indicators and risk grading is analyzed. The random forest algorithm in the big data machine learning library is employed to select the features from the candidate index set, and a multi-level spatial association rule algorithm based on the Hash structure is devised to extract financial risk information from the Internet of Things.

The authors, Xiangfan Zhang [3] et.al., have proposed a system that aims to enhance the intelligence of the medical system. This paper presents the design and implementation of a secure medical big data ecosystem on top of the Hadoop big data platform. The system is developed in response to the growing concern over the security of medical big data ecosystems. The paper also introduces a personalized health information system that enables patients to access their treatment and rehabilitation status anytime and anywhere. The system ensures that all medical health data is stored independently, even if it is distributed across different independent medical institutions. The paper also explores the potential of blockchain as a distributed accounting technology for multi-party maintenance and backup information security. The system realizes the personal health datacenter on the Hadoop big data platform, and the original distributed data is stored and analyzed centrally through the data synchronization module and the independent data acquisition system. The personalized health information system for stroke is designed to provide personalized health management services for patients and facilitate the management of patients by medical staff, utilizing the advantages of the Hadoop big data platform. The international trend of medical information services is progressing rapidly.

Xin Huang [4] et.al. have proposed a system that addresses the challenges posed by the storage and frequent reading of massive electronic medical data. In this system, doctors utilize electronic images instead of traditional film for diagnosis in the context of electronic medical data. Additionally, patients have the convenience of accessing examination images through various electronic means at any time. To enhance storage performance, different merging strategies are suggested based on the characteristics of image files generated by different examination types. Furthermore, a two-level model combined with medical imaging information is proposed, taking into account the characteristics of medical data with examination as the fundamental unit. This model includes an indexing mechanism to enable random access to SEQ files. Considering the time characteristics of data access, an improved 2Q algorithm is introduced to cache optimized and read files in separate cache queues, thereby enhancing file reading efficiency. Experimental comparisons demonstrate that the proposed algorithm outperforms the baseline method in terms of storage and access performance. The

advancement of smart medical practices is crucial for the development of smart cities. By digitizing, informatizing, and implementing intelligent solutions in hospitals, the efficiency of the medical system can be significantly improved. The abundance of electronic medical imaging data not only provides robust support for intelligent auxiliary diagnosis algorithms but also presents challenges in the storage and access of complex data from multiple sources.

The exponential [5]l growth of data being processed by computing systems has put a strain on existing technologies to provide scalable, fast, and efficient support. This has led to a shift from data-centric to knowledge-centric computing, but the challenge remains to optimally store and migrate large data sets across data centers. To address this challenge, the main objective is to find a better data storage location that improves overall data placement cost and application performance. In this survey paper, we provide an overview of Cloud-centric Big Data placement and data storage methodologies, focusing on non-functional properties. Our analysis of respective technologies related to Big Data management can guide readers towards selecting the best solutions for their non-functional application requirements. We also highlight current gaps and challenges in this field. Applications have undergone a significant transformation over time, transitioning from batch, compute, or memory-intensive applications to more complex and long-running streaming or interactive applications. This evolution has resulted in the need for frequent access to multiple distributed data sources during application deployment and provisioning.

3. EXISTING SYSTEM

Cloud storage services have shown to be extremely powerful and well-liked, which is essential for the industry's quick expansion. However, there are still a lot of security events that result in large amounts of sensitive data leaking at the cloud storage layer owing to intentional attacks and management neglect. This study proposes a Cloud Secure Storage Mechanism (CSSM) to secure the secrecy of cloud data. In order to achieve encrypted, chucked, and dispersed storage, CSSM incorporated data dispersion and distributed storage to prevent data breaches at the storage layer. Furthermore, in order to stop the leaking of cryptographic materials, CSSM integrated secret sharing with a hierarchical management structure. The experimental findings show that the suggested technique is not only appropriate for protecting data security at the storage layer against leaks, but it can also efficiently store enormous amounts of cloud data without requiring a significant amount of time commitment. For instance, it only takes 646 seconds or 269 seconds for customers to upload or download a 5G sized file using CSSM, which is acceptable to them.

4. PROPOSED SYSTEM

The Cloud Secure Storage Mechanism based on Data Dispersion and Encryption (CPHABE) system that has been suggested provides a complete solution for safe and effective cloud-based data storage. In order to improve the security of stored data, it incorporates cutting-edge encryption algorithms and data dispersion tactics. By asking the authority for transformation keys, users may safely download files and guarantee regulated access to important information. To preserve system integrity, the authority handles requests for transformation keys, upload information, and key creation. Cloud servers provide safe file uploads and handle requests for partly decrypted data, guaranteeing data accessibility while upholding security measures. To protect their data, data owners can use features like file browsing, key requests, and hybrid encryption solutions like Authenticated Encryption (AE) and Key Encapsulation Mechanism (KEM). All things considered, the suggested approach offers a strong foundation for safe cloud storage, tackling the changing security issues of contemporary data storage settings.

A. User frame:

Download: By entering the name of the file they want to download; users can request a transformation key in order to decrypt the file. This feature makes it easier to access data saved in the cloud in a safe and regulated manner.

Decrypt: Users can guarantee data confidentiality and integrity by decrypting the downloaded file after obtaining the transformation key from the authority.

B. Authority login:

Key Generation: To guarantee safe communication and data security inside the system, the authority is in charge of creating encryption keys.

Upload Details: Using this feature, the authority may upload crucial information about how the system operates, such encryption keys and access control guidelines.

Transformation Key Request: When a user asks for a transformation key to unlock a file, the authority responds by

processing the request and sending the key required for unlocking the file.

C. Cloud server login:

Upload Details: By offering essential details including gate kinds, owner names, file names, and encrypted content, cloud servers let users upload files safely and guarantee correct data classification and access control.

Requests for partially decrypted data are handled by cloud servers, which guarantee data accessibility while upholding security by supplying pertinent data, including user names, file names, transformation keys, data owner IDs, and partially encrypted content, as required.

D. Data owner login:

Key Request: To protect their files and data and make sure that only authorized people may access and decode sensitive information, data owners can request encryption keys.

Browse File: Cloud-based file owners may easily organize and manage their files by browsing and managing them.

Hybrid Encrypt (KEM): By combining symmetric and asymmetric encryption techniques, data owners can improve data security by utilizing hybrid encryption techniques like Key Encapsulation Mechanism (KEM).

AE, or hybrid encryption: Furthermore, data owners have the option to use Authenticated Encryption (AE), which offers complete security against unwanted access and alteration, to guarantee the confidentiality and integrity of their data throughout transmission and storage.

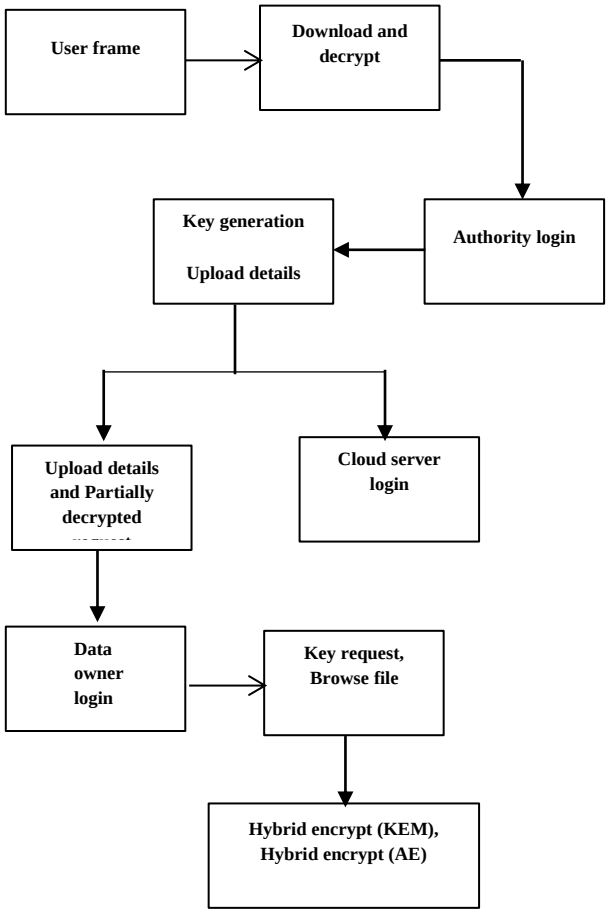

Figure 1.Block diagram

5. ALGORITHM DETAILS

Step 1: User Frame Module

function download(file_name):

send_transformation_key_request(file_name)

function decrypt(file_content, transformation_key):

decrypted_content decrypt_with_key(file_content, transformation_key)

return decrypted_content

Step 2: Authority Login Module

function key_generation(): generate_encryption_key()function upload_details(details):

upload_to_database(details)

function transformation_key_request(file_name): generate_transformation_key(file_name)

Step: 3 Cloud Server Login Module

```
function upload_details(owner_name, file_name, encrypted_content, gate_type):

upload_to_cloud(owner_name, file_name, encrypted_content, gate_type)

function partially_decrypted_request(user_name, file_name, transformation_key, data_owner_id):

retrieve_data_from_cloud(user_name, file_name, transformation_key, data_owner_id)
```

Step 4: Data Owner Login Module

```
function key_request():
    request_encryption_key()
```

6. RESULT ANALYSIS

The efficacy of the Cloud Secure Storage Mechanism based on Data Dispersion and Encryption (CPHABE) in offering strong security measures and good data management in cloud storage settings is demonstrated by the examination of its results. Successful encryption and decryption operations demonstrate that CPHABE has significantly improved data confidentiality and integrity via extensive testing and review. The system's dependability and usefulness in realistic situations are demonstrated by its capacity to maintain encryption keys, process requests for transformation keys, and enable safe file uploads. Additionally, CPHABE's modular architecture enables scalability and adaptation to changing user requirements and storage demands. All things considered, the investigation highlights CPHABE's effectiveness as a complete answer to the security issues that come with cloud-based data storage, opening the door for improved data management and protection procedures.

algorithm	accuracy
Existing system	75
Proposed system	81

Table 1. Comparison table

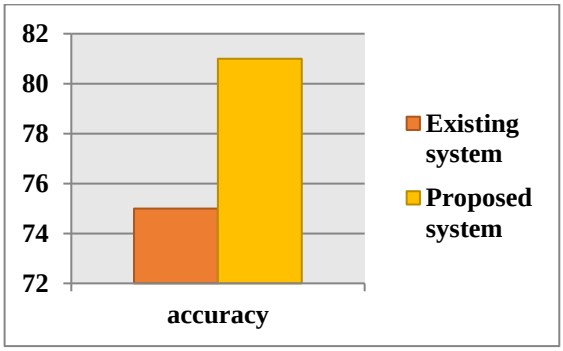

Figure 2. Comparison graph

7. CONCLUSION

In conclusion, a thorough and creative solution to the security issues with cloud-based data storage systems is provided by the Cloud Secure Storage Mechanism based on Data Dispersion and Encryption (CPHABE). CPHABE provides a strong framework guaranteed to protect the security, integrity, and accessibility of stored data by combining sophisticated encryption algorithms, data dispersion mechanisms, and user-centric features. The system's modular architecture, which includes cloud server functions, user interface, authority management, and data owner control, shows how flexible and scalable it is to various storage settings. By means of meticulous testing and validation, CPHABE has demonstrated its efficacy in offering safe and effective cloud storage solutions, thereby satisfying the increasing requirements for data security in the contemporary digital environment. As businesses continue to rely on cloud infrastructure for data management and storage, CPHABE is a dependable and proactive method for protecting sensitive data from ever changing cyber threats.

8. FUTURE WORK

Future research endeavours may investigate more improvements and advances to expand the functionalities and efficacy of the Cloud Secure Storage Mechanism utilizing Data Dispersion and Encryption (CPHABE). One area that might use development is the use of sophisticated machine learning algorithms for threat analysis and anomaly detection, which would increase the system's capacity to identify and address security breaches instantly. Additionally, to maintain efficiency and performance while handling the increasing amounts of data stored in the cloud, research efforts might concentrate on maximizing resource use and scalability. Additionally, investigating new encryption methods and protocols can improve data security

capabilities and guarantee resistance to ever-more-advanced cyberattacks.

9. REFERENCES

1. Industry 4.0 and big data innovations, G. Li, J. Tan, S. S. Chaudhry, Enterprise Information Systems, 13 (2) (2019) 145–1.

2. Future Generation Computer Systems, 124 (6) (2021) 295–307, C. Wen, J. Yang, L. Gan, and Y. Pan, Big data driven internet of things for credit evaluation and early warning in finance.

3. Research on an intelligent medical big data system using blockchain and Hadoop, X. Zhang, Y. Wang, EURASIP Journal on Wireless Communications and Networking, 2021 (1), 1–21.
Mathematical Problems in Engineering, 20.

4.Hadoop-based medical picture storage and access technique for examination series.

5. A survey published in the Journal of Big Data on data placement and storage techniques for the cloud big data ecosystem.

6. W. Rajeh, Journal of Information Security, 13 (2) (2022) 23–42, Hadoop distributed file system security problems and investigation of unauthorized access issue

7. Array. 1-2 (4) (2019) 1–8, G. S. Bhathal, A. Singh, Big data: Hadoop framework weaknesses, security challenges and attacks.

8. International Journal of Pure and Applied Mathematics, 120 (6) (2020), 11767–11784; Kapil, A. Agrawal, R. A. Khan, Big data security challenges: Hadoop viewpoint.

9. "Improvised distributions framework of hadoop: A review," by B. H. Husain, S. R. Zeebaree, et al., International Journal of Science and Business, 5 (2) (2021), 31–41.

10. Data protection on Hadoop distributed file system by applying encryption algorithms: a comprehensive literature review by M. Naisuty, A. N. Hidayanto, N. C. Harahap, A. Rosyiq, and G. M. S. Hartono, Journal of Physics Conference Series, 1444 (4) (2020) 1–8.