USING A CLOUD COMPUTING ENVIRONMENT, RELOCATION AND REMOVEMENT OF PROTECTED INFORMATION USING SPECIFIED DEVELOPING FILTERS.

THIRUPATHI BHAVANA[1]

[1]PG Scholar, Department of CSE, Sri Indu College of Engineering and Technology,(Autonomous),Hyderabad

Prof.CH.G.V.N.PRASAD[2]

[2]Professor & HOD, Department of CSE, Sri Indu College of Engineering and Technology, (Autonomous),Hyderabad.

ABSTRACT

A growing number of data owners are choosing to outsource their data to cloud servers since cloud storage continues to progress quickly, which dramatically lowers the overhead associated with local storage. Owing to variances in the caliber of data storage services provided by various cloud service providers, which include aspects like security, dependability, speed of access, and cost, data owners now absolutely require the capacity to move data between clouds. As a result, data owners' top concerns are now safely transferring data across clouds and guaranteeing that transferred data is permanently erased from the original cloud. In this study, we address this difficulty by presenting a novel technique based on counting Bloom filters.The suggested plan makes permanent data deletion easier in addition to achieving secure data transport. Furthermore, it guarantees public verifiability without requiring any assistance from a reliable third party. In conclusion, a simulation has been executed to exhibit the feasibility and effectiveness of our suggestion.

Key words — Cloud storage, Data deletion, Data transfer, Counting Bloom filter, Public verifiability

I.INTRODUCTION

The burgeoning and extremely promising paradigm of cloud computing seamlessly unifies network bandwidths, processing power, and large-scale dispersed storage resources [1]. Tenants can use a wide range of excellent cloud services under this paradigm. Cloud storage services are especially popular among resource-constrained data owners who want to reduce their overhead associated with local storage. A study by Cisco predicts that almost 55% of the 3.6 billion internet users in 2019 will make use of cloud storage services.

Many businesses, like Microsoft, Amazon, and Alibaba, offer cloud storage services with different features, like cost, security, and access speed, because of the promising market opportunities. Data owners may choose to move cloud storage service providers in order to take advantage of better cloud storage services [2]. As a result, it might be necessary for them to move their outsourced data [3] from one cloud to another and then remove the transferred data from the first cloud. According to Cisco, by the end of 2021, cloud traffic will account for 95% of all traffic, with over 14% of that traffic being transferred between various cloud data centers. From the standpoint of the data owners, outsourcing data transfer is likely to become essential.

In In an effort to provide secure data migration, a number of solutions have been developed, like the outsourced data transfer software Cloudsfer, which uses cryptographic methods to protect data from invasions of privacy during the transfer process. Nonetheless, security issues continue to arise when executing cloud data deletion and migration. Due to cloud server bandwidth-saving methods, only a fraction of the data may be migrated, or even irrelevant data may be delivered in an attempt to mislead the data owner. During the transfer phase, network instability may cause data blocks to be lost, and attackers may damage sent data blocks. [4] Furthermore,Unexpectedly for data owners, the original cloud server might maliciously keep the transferred data for its own purposes. In conclusion, even though they are financially appealing, cloud storage services have serious security issues, especially with regard to secure data transfer, integrity verification, and verifiable deletion. If these issues are not properly resolved, this could impede the public's acceptance and use of cloud storage services [5].In this paper, we explore the difficulties of safe data deletion and transfer in cloud storage, emphasizing public verifiability in particular. We present a counting Bloom filter-based system that allows data deletion that can be verified by the public while also facilitating proven data transit between multiple clouds. The verifier, which consists of the data owner and the target cloud server, can identify malicious acts by examining the returned transfer and deletion evidence in the event that the originating cloud server fails to move or delete data in an honest manner. Unlike other methods, ours does away with the requirement for any kind of Trusted Third Party (TTP) [6]. We provide security analysis to demonstrate that our proposal meets the specified design goals. Simulation experiments corroborate the efficiency and practicality of our new proposal.

II. PRELIMINARIES

1) PRACTICAL TECHNIQUES FOR SEARCHES ON ENCRYPTED DATA

To lower security and privacy threats, encrypted data should be stored on data storage servers like mail servers and file servers [7]. However, this typically means that security must come at the expense of functionality. For instance, it was previously unknown how to allow the data storage server to do the search and respond to the query without jeopardizing the confidentiality of the data if a client wanted to obtain just documents that contained specific phrases. In this work, we present our cryptographic algorithms for the encrypted data search issue and give security guarantees for the resulting crypto systems. Our methods offer several important benefits. They offer provable secrecy for encryption, making them provably secure [8].

. In this work, we present our cryptographic algorithms for the encrypted data search issue and give security guarantees for the resulting crypto systems. Our methods offer several important benefits. They are provably secure in the following ways: they offer query isolation for searches, which prevents the untrusted server [9] from learning more about the plaintext than the search result; they provide controlled searching, which prevents the untrusted server from searching for any word without the user's permission [10]; they provide provable secrecy for encryption [8], which means that the untrusted server cannot learn anything about the plaintext when only given the ciphertext;

they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms we present are simple, fast (for a document of length , the encryption and search algorithms only need stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.The suggested approach successfully accomplishes keyword-based semantic search and is safe under the suggested model, according to security and performance analyses [11]. The pay-as-you-use cloud computing model is becoming more and more common since it offers consumers a number of convenient services, relieves storage burdens, allows for flexible data access, and lowers hardware and software costs. Numerous businesses have established up and are offering a range of cloud computing services. A growing amount of sensitive consumer data, including emails, photo albums, financial transactions, personal health records, and more, is being consolidated into the cloud due to its cost-effectiveness and flexible management.. Researchers are proposing numerous technical schemes connected to cloud computing services in the meantime. A flexible communication bus paradigm was presented by Noh et al. for cloud-based multimedia services. A practical IEEE 802.11e EDCA model [12] for QoS-aware differentiated multimedia mobile cloud services was put forth by Shahnaza et al. In a cloud environment, Cabarcos et al. suggested a middleware architecture that enables sessions started on one device to be smoothly transferred to another.

Cloud computing is a new model of enterprise IT infrastructure that provides on-demand high quality applications and services from a shared pool of configuration computing resources [13]. However, there may be existed unauthorized operation on the outsourced data on account of curiosity or profit. To protect the privacy of sensitive information and combat unauthorized accesses, sensitive data should be encrypted by the data owner before outsourcing [13]. However, encrypted data make the traditional data utilization service based on plaintext keyword search useless. The simple and awkward method of downloading all the data and decrypting locally is obviously impractical, because the data owner and other authorized cloud customers must hope to search their interested data rather than all the data. What's more, taking the potentially huge number of outsourced data and great deal of cloud customers into consideration, it is also difficult to meet both the requirements of performance and system usability [30]. Hence, it is an especially important thing to explore privacy-preserving and effective search service over encrypted outsourced data.

2) EFFICIENT SEMANTIC SEARCH OVER ENCRYPTED DATA IN CLOUD COMPUTING

The increasing popularity of cloud storage can be attributed to its several advantages over conventional storage systems. Cloud storage has numerous advantages, but it has also developed a number of security issues that keep businesses from moving their data to the cloud. Consequently, the proprietors encrypt their confidential information prior to keeping it on cloud storage. Although encryption makes data more secure, it also makes data less searchable, which lowers search efficiency. Research has recently been conducted on a number of systems that allow cloud computing users to search for keywords on encrypted data.

Nevertheless, many designs have flaws that render them unworkable in realistic situations. In this study, we created three distinct schemes—"Synonym-Based Keyword Search (SBKS)," "Wikipedia-Based Keyword Search (WBKS)," and "Wikipedia-Based Synonym Keyword Search (WBSKS)"—to facilitate semantic search on encrypted data in cloud computing. Our findings showed that compared to the previously suggested schemes, our schemes are more effective in terms of performance and storage needs.Therefore, our developed schemes are more practical than the former proposed schemes.

Cloud storage has become a preferred method of storage as it provides many benefits over traditional storage solutions. With cloud storage, corporations can purchase only the needed amount of storage from the cloud storage provider (CSP) to fulfill their storage needs instead of maintaining their own data storage infrastructures. They can rely on CSP to handle all data maintenance tasks such as backup and recovery. It also allows all data to be accessed remotely in order to streamline their operations among different locations. With all these benefits, companies can significantly reduce their operation costs by simply outsourcing their business data to cloud storage.Customers can take advantage of high-quality on-demand applications and services from a centralized pool of reconfigurable computing resources thanks to cloud computing. This new computing paradigm can reduce the strain of managing storage, enable global data access from separate geographic areas, and save money on capital expenses for things like software, hardware, and staff maintenance. As cloud computing develops, a growing amount of sensitive data—such as government documents, private health records, and data from secret enterprises—is thought to be consolidated into cloud servers. Encrypting sensitive data prior to outsourcing is a simple way to safeguard data privacy.

Unfortunately, data encryption, if not done appropriately, may reduce the effectiveness of data utilization. Typically, a user retrieves files of interest to him/her via keyword search instead of retrieving back all the files. Such keyword-based search technique has been widely used in our daily life, e.g. Google plaintext keyword search. However, the technologies are invalid after the keywords are encrypted.

In this research, we present a similar search method that supports similarity ranking and is based on semantic query expansion from a novel angle. The system usability is strengthened by semantic expansion-based comparable search, which yields precisely matched files as well as files containing terms semantically connected to the query keyword. Each file in the suggested approach has a corresponding file metadata created for it. Next, the file collection and encrypted metadata set are uploaded to the cloud server. The cloud server creates the semantic relationship library (SRL) and inverted index for the keywords set using the metadata set.

The co-occurrence of terms is used to evaluate the semantic relationship between terms in SRL. Upon receiving a query request, the cloud server automatically finds out the terms which are semantically related to the query keyword according to the value of semantic relationship between terms in SRL. Then both the keyword and the semantically expanded words are used to retrieve files. Finally, the matched files are returned in order according to the total relevance score. In the process, to ensure security and final result ranking, we properly modify a crypto primitive order-preserving encryption to protect the relevance score. Detailed security analysis shows that the solution correctly realizing the goal of semantic search, while preserving the privacy. Extensive experimental evaluation demonstrates the efficiency and effectives of the scheme.

III. SYSTEM MODEL

A) EXISTING SYSTEM :

In this study, we tackle problems concerning the security of data deletion and transfer in cloud storage, with an emphasis on guaranteeing generic authentication. This input permits both publicly verifiable data deletion and demonstrable data transfer between two unique clouds of two different clouds because the Bloom filter is not included as an input. The primary cloud server in our current setup is unable to move or remove data. By looking through the returned data and deleting the credentials, credentials created by the target cloud server and the data owner can detect these illicit activities. It also makes use of trustworthy third-party eradication programs.

B) **PROPOSED SYSTEM :**

Our objective is to establish a mechanism for verifiable data transfer between two distinct clouds and reliable data deletion in cloud storage. Therefore, our new construction involves three key entities.

In our example, a resource-constrained data owner might choose to outsource their large amount of data to cloud server A in order to drastically cut down on local storage overhead. The data owner can also ask cloud A to move particular data to cloud B or to remove specific data from storage. The data owner can access cloud storage services from both cloud A and cloud B. We assume that cloud A is the original cloud, and that its job is to remove the transferred data from cloud B and migrate its data to cloud B. But given that they are separate businesses, cloud A might not carry out these tasks with sincerity because of financial concerns. As a result,

both clouds will independently adhere to the protocol. Moreover, we assume that the target cloud B will not engage in malicious practices to discredit the original cloud A.

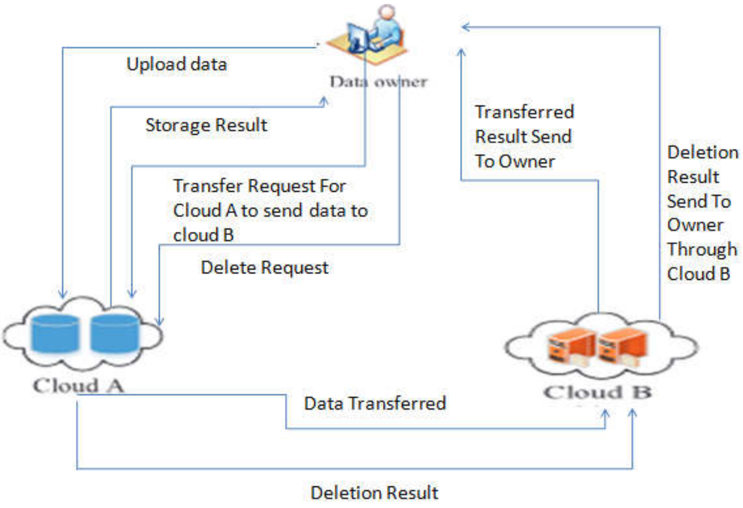
Advantages

1) Data confidentiality. The outsourced file may contain some private information that should be kept secret. Hence, to protect the data confidentiality, the data owner needs to use secure algorithms to encrypt the file before uploading it to the cloud server.

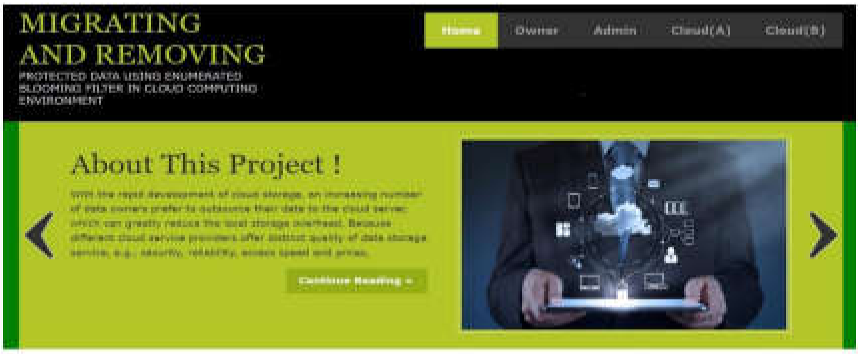
2) Data integrity. The cloud A might only migrate part of the data, or deliver some unrelated data to the cloud B. Besides, the data might be polluted during the transfer process. Hence, the data owner and the cloud B should be able to verify the transferred data integrity to guarantee that the transferred data is intact.

3) Public verifiability. The cloud A may not move the data to the cloud B or delete the data faithfully. So, the verifiability of the transfer and deletion results should be satisfied from the data owner's point of view.

C) SYSTEM ARCHITECTURE :


Upload data
Data owner
Storage Result
Transfer Request For Cloud A to send data to cloud B
Delete Request
Transferred Result Send To Owner
Deletion Result Send To Owner Through Cloud B
Cloud A
Cloud B
Data Transferred
Deletion Result

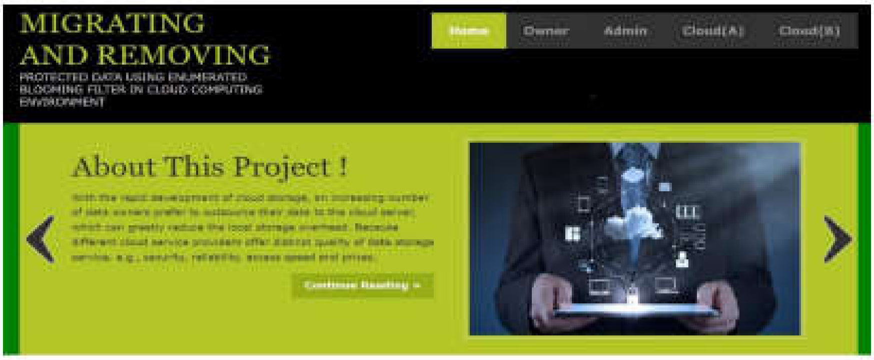
IV.RESULTS AND DISCUSSION


MIGRATING
AND REMOVING
PROTECTED DATA USING ENUMERATED
BLOOMING FILTER IN CLOUD COMPUTING
ENVIRONMENT
Home
Owner
Admin
Cloud(A)
Cloud(B)

About This Project !

With the rapid development of cloud storage, an increasing number of data owners prefer to outsource their data to the cloud server, which can greatly reduce the local storage overhead. Because different cloud service providers offer distinct quality of data storage service, e.g., security, reliability, access speed and prices.

Fig.1


MIGRATING
AND REMOVING
PROTECTED DATA USING ENUMERATED
BLOOMING FILTER IN CLOUD COMPUTING
ENVIRONMENT
Home
Owner
Admin
Cloud(A)
Cloud(B)

About This Project !

With the rapid development of cloud storage, an increasing number of data owners prefer to outsource their data to the cloud server, which can greatly reduce the local storage overhead. Because different cloud service providers offer distinct quality of data storage service, e.g., security, reliability, access speed and prices.

Fig.2

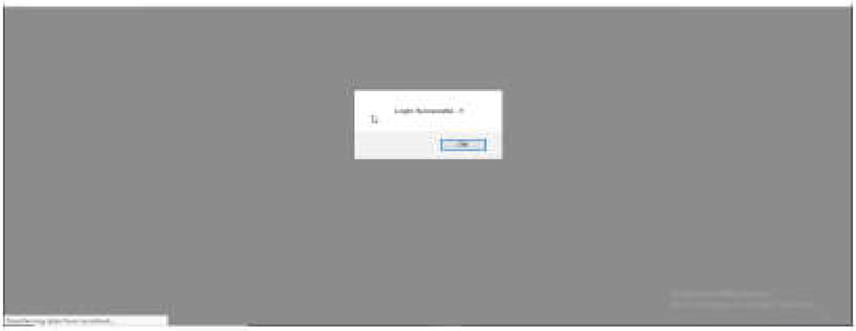
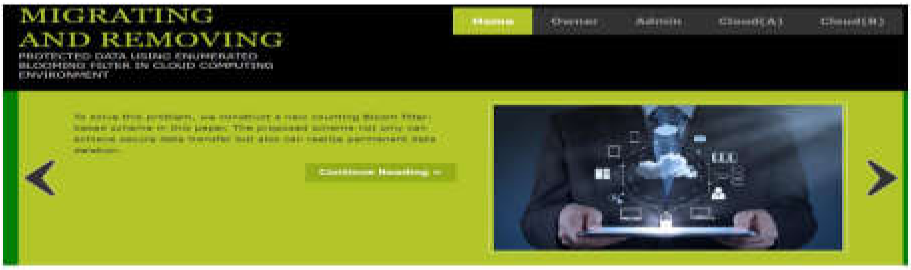

Login Successful...!!

Fig.3



MIGRATING AND REMOVING

PROTECTED DATA USING ENUMERATED BLOOMING FILTER IN CLOUD COMPUTING ENVIRONMENT

To solve this problem, we construct a new counting Bloom filter-based scheme in this paper. The proposed scheme not only can achieve secure data transfer but also can realize permanent data deletion.

Fig.4

V. CONCLUSION AND FUTURE WORK

The owner of the data does not think that the cloud server would transfer and delete data in an honest manner when it comes to cloud storage. Our solution to this issue is a secure data transport mechanism based on CBF that can also achieve verifiable data deletion. As per our plan, cloud B has the ability to verify the integrity of the transferred data, ensuring that the data has been migrated completely. Additionally, cloud A ought to employ CBF to provide deletion evidence following deletion, which the data owner will use to confirm the deletion outcome. Hence, the cloud A cannot behave maliciously and trick the data owner successfully. Lastly, the results of the simulation and security analysis verify the viability and security of our idea, respectively.
Like every other solution now in use, our plan takes into account the data transfer between two distinct cloud servers. As cloud storage has advanced, the data owner may wish to move their outsourced data from one cloud to two or more target clouds at the same time. Nevertheless, the multi-target clouds may conspire to deceive the data owner in a harmful manner. Therefore, we need to investigate the verifiable data movement among three or more clouds further.

REFERENCES

[1] C. Yang and J. Ye, “Secure and efficient fine-grained data access control scheme in cloud computing”, Journal of High Speed Networks, Vol.21, No.4, pp.259–271, 2015.

[2] CHARY, D. C. N., BABU, M. R., & MORE SADANANDAM, S. K. (2023). Leveraging Deep Learning Techniques for the Stability Principles of Current Artificial Neural Networks Are Emerging Into Their Activation Functions.

[3] X. Chen, J. Li, J. Ma, et al., “New algorithms for secure outsourcing of modular exponentiations”, IEEE Transactions on Parallel and Distributed Systems, Vol.25, No.9, pp.2386–2396, 2014.

[4] CH, N. C., Chintha, S., Rajendra, E., & Srinivas, S. Generalized Flow Performance Analysis of Intrusion Detection using Azure Machine Learning Classification.

[5] P. Li, J. Li, Z. Huang, et al., “Privacy-preserving outsourced classification in cloud computing”, Cluster Computing, Vol.21, No.1, pp.277–286, 2018.

[6] CHARY, D. C. N., BABU, M. R., & MORE SADANANDAM, S. K. (2023). Leveraging Deep Learning Techniques for the Stability Principles of Current Artificial Neural Networks Are Emerging Into Their Activation Functions.

[7] B. Varghese and R. Buyya, “Next generation cloud computing: New trends and research directions”, Future Generation Computer Systems, Vol.79, pp.849–861, 2018.

[8] W. Shen, J. Qin, J. Yu, et al., “Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage”, IEEE Transactions on Information Forensics and Security, Vol.14, No.2, pp.331–346, 2019.

[9] R. Kaur, I. Chana and J. Bhattacharya J, “Data deduplication techniques for efficient cloud storage management: A systematic review”, The Journal of Supercomputing, Vol.74, No.5, pp.2035–2085, 2018.

[10] Cisco, “Cisco global cloud index: Forecast and methodology, 2014–2019”, available at: https://www.cisco.com/c/en/us- /solutions/collateral/service-provider/global-cloud-index-gci/ white-paper-c11-738085.pdf, 2019-5-5.

[11] CH, D. (2021). NARASIMHA CHARY,”. COMPREHENSIVE STUDY ON MULTI-OPERATOR BASE STATIONS CELL BINARY AND MULTI-CLASS MODELS USING AZURE MACHINE LEARNING”," A JOURNAL OF COMPOSITION THEORY, 14(6).

[12] Chary, C. N., Krishna, A., Abhishek, N., & Singh, R. P. (2018). An Efficient Survey on various Data Mining Classification Algorithms in Bioinformatics. International Journal of Engineering and Techniques,

[13] Shobarani, R., Sharmila, R., Kathiravan, M. N., Pandian, A. A., Chary, C. N., & Vigneshwaran, K. (2023, April). Melanoma Malignancy Prognosis Using Deep Transfer Learning. In 2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1) (pp. 1-6).