PROTECTED INFORMATION MIGRATION AND REMOVAL VIA ENUMERATION BLOOMING FILTER IN CLOUD-BASED COMPUTING

[1]MRS. K. PRATHYUSHA, [2]T.LAKSHMI NARAYANA, [3]P.VIJAY KUMAR, [4]R.VENKATESH

[1](Assistant Professor) ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

[234]B,tech scholar ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

ABSTRACT

As cloud storage continues to grow quickly, more and more data owners are choosing to outsource their data to cloud servers, which can significantly cut down on the overhead associated with local storage. The ability to transfer data across cloud service providers is becoming a basic necessity for data owners switching between providers because different cloud service providers offer different quality of data storage services, such as security, reliability, access speed, and pricing. Therefore, one of the main concerns of data owners is how to safely move data from one cloud to another and permanently remove the transferred data from the original cloud. In this study, we develop a new counting Bloom filter-based approach to overcome this problem. The suggested plan is able to accomplish both permanent data deletion and secure data transfer. Furthermore, the suggested plan can meet public verifiability requirements without the need for a reliable third party. In conclusion, we also create a simulation application to show how our idea works and how effective it is.

Key words: public verifiability, cloud storage, counting bloom filter, data erasure, and data transport.

1.INTRODUCTION

1.1 PROBLEM STATEMENT

Large-scale dispersed storage resources, processing resources, and network bandwidths are connected through cloud computing, an up-and-coming and extremely promising computing paradigm[1,2]. It is capable of offering a wide range of excellent cloud services to tenants by utilizing these resources. Owing to the alluring benefits, the services—particularly the cloud storage service—have been extensively utilized[3,4].

This allows data owners with limited resources to outsource their data to the cloud server, significantly lowering their local storage expenses[5, 6]. A study by Cisco[7] projects that there will be over 3.6 billion Internet users worldwide in 2019—of whom roughly 55% will use cloud storage services. A growing number of businesses (such as Microsoft, Amazon, and Alibaba) are providing cloud storage services to data owners at varying costs, with varying levels of security, access speed, and other features, due to the potential market prospects. The data owners may switch cloud storage service providers to benefit from better cloud storage services. Because of this, they may move their outsourced data from one cloud to another before erasing the data that was moved from the original cloud. By the end of 2021, cloud traffic is predicted to account for 95% of all traffic, with traffic between separate cloud data centers accounting for over 14% of that total, according to Cisco[7]. The transfer of data that is outsourced is expected to become essential from the perspective of the data owners.An outsourced data transfer application called Cloudsfer[8] was created using a cryptographic technique to prevent data privacy disclosure during the transfer phase, enabling secure data movement. However, there 2 are still certain security issues with the way cloud data migration and deletion are handled. First off, the cloud server may just move a portion of the data in order to save network traffic, or it may even send some irrelevant data in an attempt to deceive the data owner[9]. Second, certain data blocks might be lost during the transfer process due to network instability.

The sent data blocks could be destroyed by the adversary in the interim[10]. Thus, during the migration procedure, the transferred data could become contaminated. Finally, but just as dangerously, the originating cloud server may keep the transferred data for uncovering the hidden advantages[11]. From the perspective of the data owners, the reserve of the data is unanticipated. To sum up, while cloud storage is a financially appealing option, it unavoidably faces significant security issues, particularly with regard to secure data transfer, integrity verification, and verifiable destruction. If these issues are not resolved appropriately, the general public may be discouraged from embracing and using cloud storage services.

1.2 DESCRIPTION

Contributions ,We investigate the issues of safe data deletion and transfer in cloud storage in this work, with an emphasis on achieving public verifiability. Next, we suggest a counting Bloom filter-based system that can do both publicly verifiable data deletion and proven data transfer across two distinct clouds. By examining the returned transfer and deletion evidences, the verifier—the data owner and the target cloud server—can identify malicious acts if the originating cloud server fails to migrate or remove the data in an honest manner. Furthermore, unlike the other options, our suggested plan does not require a trusted third party (TTP). Furthermore, we use security analysis to demonstrate that our new approach can meet the intended design goals. 3

2.LITERATURE SURVEY

1.Useful Methods for Data Encryption Searches :

To lower security and privacy threats, encrypted data should be stored on data storage servers, such as mail servers and file servers. 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 can be proven to be safe. They are provably secure in the following ways: they offer query isolation for searches, which prevents the untrusted server 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; they support hidden queries, which allow the user to ask the untrusted server to look up a secret word without disclosing it to the server; and they provide provable secrecy for encryption. Our presented algorithms are straightforward, quick (the encryption and search algorithms only require the use of stream cipher and block cipher operations for a document of a certain length), and introduce nearly no space and communication overhead, and hence are practical to use today.

2. Verifiable keyword-based semantic search over encrypted cloud data is provided by smart cloud search services.

Many cloud services are being pushed toward customers as the pay-as-youconsume cloud computing paradigm gains traction. Users of intelligent terminals benefit greatly from increased convenience, but they also face significant challenges when attempting to find the best services or goods available in the cloud. Therefore, one of the main issues with the consumer-centric cloud computing paradigm is how to provide a smart cloud search scheme. Sensitive data are always encrypted before being outsourced to preserve data privacy.

Users can search through encrypted data using the current searchable encryption systems, but they only support specific keyword searches, which has a significant impact on the usability of the data. Furthermore, the verifiability of search results is not supported by these approaches. The cloud server just performs a portion of the search operation or returns a portion of the result in order to save compute costs or download bandwidth, which is seen as self-serving and only partially honest but curious. Thus, a major problem is to guarantee the verifiability of search results while enhancing the flexibility of encrypted cloud data. This study proposes a clever semantic search technique to address the difficulty, which returns both the keyword-based exact match and the keyword-based semantic match result. The suggested plan also encourages the verifiability of search results.

The thorough performance and security analyses demonstrate that the suggested scheme is efficient and safe under the suggested paradigm. Pay for what you use The cloud computing paradigm is becoming more and more common since it offers users many 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 5 growing amount of private information from customers (such as email correspondence, picture albums, financial transactions, and personal medical records) is being moved to the cloud for more cost-effective storage and administration options. 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. Shahnaza along with others. suggested a practical IEEE 802.11e EDCA paradigm for differentiated multimedia mobile cloud services that are QoS aware. In a cloud environment, Cabarcos et al. suggested a middleware architecture that enables sessions started on one device to be smoothly transferred to another.

3. Providing efficient cloud search services: synonym query support for multi-keyword ranked searches via encrypted cloud data The use of cloud computing is growing in popularity.

Sensitive data should be encrypted by the data owner prior to outsourcing in order to protect data privacy. This renders the conventional and effective plaintext keyword search method meaningless. Semantically-based multi-keyword ranked search is not supported by the searchable encryption systems now in use; they only offer exact or fuzzy keyword search. When conducting a real search, cloud customers frequently provide synonyms for the predefined keywords rather than precise or approximate matching keywords. This is because they may substitute synonyms (reproducing information content) or may not have precise knowledge of the data. Consequently, synonym-based multi-keyword ranked search over encrypted cloud data continues to be an extremely difficult issue. For the first time, we provide in this work a practical solution to the multi-keyword 6 ranked search problem using synonyms over encrypted cloud data. Our primary areas of contribution are synonym-based search to accommodate synonym queries and multikeyword ranked search to obtain more precise search results.

To satisfy privacy requirements in two threat models of known background and known ciphertext models, two secure techniques are provided. Sensitive frequency data in the extended scheme can be adequately safeguarded by adding a few fake keywords, which are not used in the basic scheme. To support the accuracy and privacy-preserving assurance of the suggested systems, we provide security analysis. Extensive experiments on real-world dataset validate our analysis and show that our proposed solution is very efficient and effective in supporting synonym-based searching. A new paradigm of enterprise IT infrastructure called cloud computing uses a shared pool of configurable computing resources to deliver high-quality applications and services on demand [1]. On the other hand, there might have been unapproved operations on the outsourced data due to curiosity or financial gain. Before being outsourced, sensitive data should be encrypted by the data owner to safeguard privacy and prevent illegal access [2]. However, the conventional data usage service based on plaintext keyword search is rendered ineffective when dealing with encrypted data. It is evident that the straightforward and inconvenient process of downloading all the data and decrypting locally is impracticable, as the data owner and other authorized cloud customers will only be able to explore the material that interests them, not the entire collection. Furthermore, it is challenging to satisfy the demands of system usability and performance given the potentially enormous volume of outsourced data and large number of cloud clients [30]. Investigating effective and privacy-preserving search services using encrypted outsourced data is therefore extremely crucial.

4. Cloud computing's effective semantic search over encrypted data

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 both performance and storage needs. As such, compared to the previously presented systems, our created schemes are more realistic. Because cloud storage offers so many advantages over traditional storage systems, it has become a popular means of storing data. Instead of maintaining their own data storage infrastructures, organizations may use cloud storage by simply purchasing the necessary quantity of storage from the cloud storage provider (CSP) to meet their storage demands. They may trust CSP to take care of all data maintenance duties, including recovery and backup. Additionally, it enables remote access to all data, which helps to optimize operations across several locations. By simply outsourcing their 8 corporate data to cloud storage, firms may drastically save their operating expenses, thanks to all these advantages.

5. Similarity ranking over encrypted private cloud data is supported by semantic search

Since the emergence of cloud computing, an increasing amount of data is being outsourced to public clouds for accessibility and cost savings. Nevertheless, in order to ensure security, the private data must be encrypted. It has shown to be quite difficult to search through encrypted cloud data in order to execute effective data usage. The query term that was supplied was the only factor taken into account by the current solutions, which ignored the keyword's meaning. As a result, the search algorithms lack intelligence and exclude certain pages that are semantically relevant. We aim to address the shortcoming by putting forth a semantic expansion based comparable search solution for encrypted cloud data. In addition to precisely matching files, our method could also return files that included phrases 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 cloud server initially uses SRL to determine whether keywords are semantically relevant to the query keyword after receiving a query request. The files are then retrieved using both the query keyword and the extensional terms. The overall relevance score determines the order in which the result files are returned. Ultimately, thorough security research demonstrates that, in accordance with the earlier searchable symmetric encryption (SSE) security criteria, our 9 technique is secure and preserves privacy.

The scheme's effectiveness and efficiency are demonstrated through experimental examination. Customers may take use of high-quality on-demand applications and services from a centralized pool of reconfigurable computing resources thanks to cloud computing. This new computing paradigm may 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 papers, private health information, 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. Regrettably, improper use of data encryption might lessen how effectively data is utilized. Instead of getting all the files back, a user often uses keyword search to get the files that interest them. We frequently employ keyword-based search techniques in our daily lives, such as Google's plaintext keyword search. But once the keywords are encrypted, the technologies become useless. In recent times, there has been significant development in searchable encryption (SE) techniques aimed at securing outsourced data searches. While some studies have concentrated on improving search efficiency, enabling multi-keyword search, and ensuring secure dynamic updating, they have primarily focused on exact keyword matching. To improve search flexibility and user-friendliness, other research has explored fuzzy keyword search, accommodating variations like minor typos and format inconsistencies such as "million" being mistyped as "milion", or "datamining" as "datamining". However, these methods predominantly assess structural similarity using edit distance, neglecting semantically related terms and consequently omitting many 10 pertinent files.

Furthermore, these fuzzy systems typically retrieve all relevant files based solely on the presence or absence of the keyword, without considering result ranking. Presented herein is a novel approach to similar search, centered on semantic query expansion while also supporting similarity ranking. This method enhances system usability by returning both exact matches and files containing semantically related terms to the query keyword. In our proposed framework, specific file metadata is created for each file, followed by uploading the encrypted metadata set and file collection to a cloud server.

Leveraging this metadata set, the cloud server constructs an inverted index and establishes a semantic relationship library

(SRL) for the keywords set, evaluating semantic relationships based on term co-occurrence within the SRL. Upon receiving a query request, the cloud server autonomously identifies terms semantically related to the query keyword according to the semantic relationship values in the SRL. Subsequently, both the original keyword and the semantically expanded terms are employed to retrieve files. Finally, the retrieved files are ranked based on their overall relevance score. Throughout this process, to ensure security and final result ranking, we adeptly adapt a cryptographic primitive, order-preserving encryption, to safeguard the relevance score. Detailed security analysis confirms the solution's efficacy in achieving semantic search goals while upholding privacy. Extensive experimental evaluation further validates the efficiency and effectiveness of our approach.

6. Secure semantic expansion-based search with similarity ranking support over encrypted cloud data

Since the emergence of cloud computing, an increasing amount of data is being 11 outsourced to public clouds for accessibility and cost savings. Nevertheless, in order to ensure security, the private data must be encrypted. It has shown to be quite difficult to search through encrypted cloud data in order to execute effective data usage. The query term that was supplied was the only factor taken into account by the current solutions, which ignored the keyword's meaning. As a result, the search algorithms lack intelligence and exclude certain pages that are semantically relevant. We aim to address the shortcoming by putting forth a semantic expansion based comparable search solution for encrypted cloud data.

In addition to precisely matching files, our method could also return files that included phrases 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 cloud server initially uses SRL to determine whether keywords are semantically relevant to the query keyword after receiving a query request. The files are then retrieved using both the query keyword and the extensional terms. The overall relevance score determines the order in which the result files are returned. In the end, a thorough security analysis demonstrates that our method satisfies the prior searchable symmetric encryption (SSE) security requirement while maintaining privacy. The effectiveness and efficiency of the plan are demonstrated by an experimental assessment.

7. Cloud computing: Semantically-aware encrypted data searching

As cloud computing becomes increasingly popular, more users are entrusting their datasets to cloud services. To safeguard privacy, these datasets are typically 12 encrypted before being outsourced. However, this encryption practice poses challenges for efficient data utilization, particularly in tasks like keyword-based searching within encrypted datasets. While existing schemes facilitate keyword-based searches, they often overlook the semantic context of users' queries, leading to suboptimal search outcomes. Addressing this challenge requires designing a content-based search approach that enhances semantic understanding and context awareness. In this paper, we introduce ECSED, a novel semantic search scheme that leverages concept hierarchies and semantic relationships within encrypted datasets. ECSED employs two cloud servers: one stores the outsourced datasets and delivers ranked results to users, while the other computes similarity scores between documents and queries, forwarding these scores to the first server. Additionally, we optimize search efficiency by employing a tree-based index structure to organize document index vectors. By building upon a multi-keyword ranked search framework, we propose two secure schemes. Experimental results using real-world datasets demonstrate the superiority of our scheme over previous approaches in terms of efficiency.

Furthermore, we provide proofs of security under both known ciphertext and known background models. Cloud computing represents a mature model for enterprise IT infrastructure, offering high-quality applications and services. By migrating complex local data systems to the cloud, customers can mitigate management overhead and local storage constraints. However, the security of outsourced data remains a concern, given that Cloud Service Providers (CSPs) exert complete control over the data. Encrypting data before outsourcing to the cloud is essential for protecting sensitive information. While encryption safeguards privacy against unauthorized access, it complicates effective data 13 utilization, including search operations within encrypted data. Li et al. [58] proposed a secure, privacy-preserving outsourced classification solution for cloud computing. Nonetheless, the encryption of outsourced data presents significant challenges for tasks like search operations

8. Enabling semantic extension search based on core keywords over encrypted data that is outsourced

When consumers do searches, search terms really have quite varied priorities. Additionally, there could be a specific grammatical connection between these terms, which intuitively reflects the significance of the keywords from the user's perspective. Nonetheless, the search terms are treated independently and unrelatedly by the current search algorithms. For the first time, we explore the relationship between query keywords in this work and develop a keyword weighting method to illustrate the significance of the differences between them.

The search results will be more in line with user desire by adding the term weight to the design of the search protocol. Furthermore, we create a unique core keyword semantic extension ranking system on top of this. Our technique strikes a fair balance between search efficiency and functionality by expanding the primary query term rather than all keywords. We additionally introduce the TF-IDF rule when constructing trapdoors and the index in order to properly communicate the relation between queries and files. Specifically, our system leverages the sub-matrix technique to accommodate both data set and keywords modifications. After providing an overview of the fundamentals of the core keyword semantic extension ranking method, our study proposes two safe searchable encryption techniques that satisfy various privacy needs under two distinct threat scenarios. 14 Because of the cloud's flexibility and limitless resources, more individuals are choosing to outsource their data to it as cloud computing gains popularity. It can also lower the expenses associated with maintaining local data and provide a practical means of communication for resource sharing between authorized data users and data owners.

Thus, a lot of data—from emails to private medical records, among other things—is being sent to public clouds like Google App Engine [4], Apple iCloud [3], Microsoft Azure [2], Amazon Web Services [1], and Apple iCloud [3]. But as cloud servers are seen as "semi-trusted" or "honest but curious," keeping data on them likewise jeopardizes data privacy [5]. Data owners must thus encrypt their (perhaps) sensitive data before outsourcing due to privacy concerns. But this invalidates conventional search strategies in the plaintext realm. The data owner outsources both the encrypted data and the index structure to the cloud server in order to enable efficient searches across encrypted data. The encrypted index is built using the extracted keywords from data files and the accompanying index-based keyword matching algorithm. The cloud server uses index information and keyword trapdoors to search over encrypted files before providing the target files to data consumers.

3.SYSTEM DESIGN

A complicated project or system's system design phase is crucial to its development and implementation. In order to accomplish certain goals and needs, it entails specifying the architecture, parts, modules, interfaces, and data flow of a system. It is impossible to exaggerate the significance of system design since it is essential to the accomplishment, effectiveness, and longevity of every project. In this piece, we'll examine the primary arguments for system design's importance and its effects on different fields.

● **Fulfilling User needs:**

The capacity to convert user needs into a well-organized and logical system is fundamental to system design. Through meticulous examination and comprehension of end-user requirements, system designers are able to develop a design that successfully satisfies these demands. By doing this, you can be confident that the finished system or product will live up to user expectations, which will increase user happiness and adoption.

● **Efficiency and Optimization:**

System design makes it possible to optimize hardware, software, and human resources, among other resources. Designers may avoid bottlenecks, decrease redundancy, and simplify operations by making intelligent architectural selections. This results in better resource usage, lower operating costs, and increased system performance.

● **Adaptability and Scalability:**

Robust systems possess the capacity to adjust to dynamic demands and developing technological landscapes. In the fast-paced world of today, where technical developments happen quickly, scalability is essential. A system that is built with scalability in mind may readily handle expansion and adjust to new 19 difficulties without needing to be completely redone.

● **Robustness and dependability:**

ISSN: 2366-1313

In crucial systems like those utilized in healthcare, aircraft, banking, and other industries, robustness and dependability are essential. Redundancy and fault tolerance techniques are incorporated into system architecture to guarantee that the system keeps working even in the event of a hardware breakdown.

- **Cost-Effectiveness:**

Systems with poor design might incur needless expenses during development and maintenance. A well-considered system design can assist in locating affordable solutions and preventing needless spending. This is especially important for businesses that want to get the most out of their investments.

- **Security:**

In the digital era, security is a major problem. Security measures are incorporated into effective system design from the beginning, increasing its resistance to cyber attacks and weaknesses. Sensitive data may be safeguarded, the system's integrity can be preserved, and unwanted access can be avoided with a secure system design.

- **Maintainability and Manageability:**

Systems are dynamic and always changing. An effective system design considers administration and maintenance simplicity of use. It should be simple to identify problems, implement fixes, and make modifications without disrupting the entire system.

- **Interoperability:**

Systems frequently need to interact and communicate with one another in the connected world of today. Interoperability is taken into account in effective system design to ensure that the system can easily interchange functionality and data with other systems, facilitating integration and data sharing.

- **Documentation and Knowledge Transfer:**

Developers, administrators, and stakeholders can benefit much from the system design documentation. It facilitates knowledge transfer and guarantees that the system can be efficiently managed and 20 maintained over time by giving a clear roadmap of the system's design, parts, and functionality. To sum up, the foundation of each successful project or system is system design. It offers the framework that all subsequent stages of development are built upon. System

ISSN: 2366-1313

designers are essential because they prioritize user requirements, efficiency, scalability, dependability, cost-effectiveness, security, maintainability, interoperability, and documentation in determining a system's longevity and performance. A well-designed system is an essential component of contemporary development and innovation since it not only satisfies current demands but also guarantees durability and adaptability in a constantly evolving technological landscape.

3.1 SYSTEM ARCHITECTURE

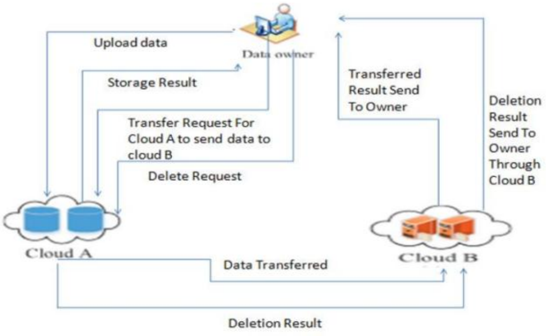

Upload data
Data owner
Storage Result
Transfer Request For Cloud A to send data to cloud B
Delete Request
Transferred Result Send To Owner
Deletion Result Send To Owner Through Cloud B
Cloud A
Cloud B
Data Transferred
Deletion Result

FIG:1 System Architecture

3.2 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

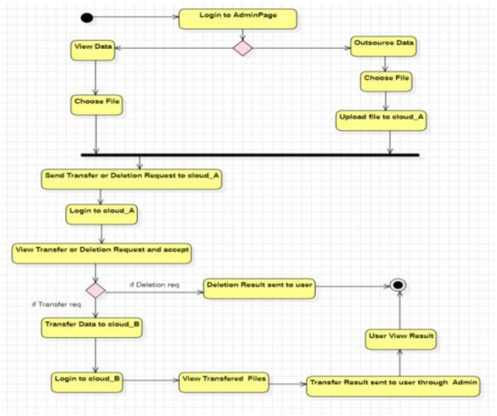
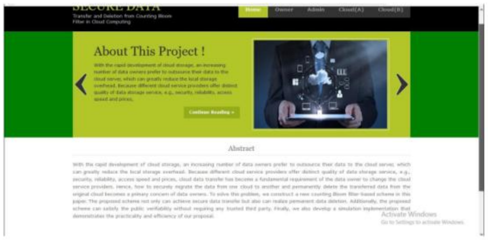


FIG:2 Activity Diagram

4.OUTPUT SCREENS

Home screen: The homepage screenshot serves as a snapshot of the project's initial interface, providing a quick and tangible overview for stakeholders, team members, and users. This image encapsulates the design, layout, and key elements of the homepage at a specific point in time.



SECURE DATA

Transfer and Deletion from Counting Bloom Filter in Cloud Computing

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,

Abstract

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, cloud data transfer has become a fundamental requirement of the data owner to change the cloud service providers. Hence, how to securely migrate the data from one cloud to another and permanently delete the transferred data from the original cloud becomes a primary concern of data owners. 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. Additionally, the proposed scheme can satisfy the public verifiability without requiring any trusted third party. Finally, we also develop a simulation implementation that demonstrates the practicality and efficiency of our proposal.

FIG:3 Output Screen-1

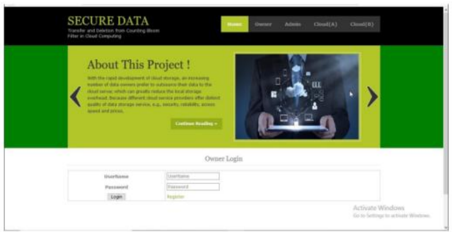


FIG:4 Output Screen-2

Login status: The Login Status Page is a vital application component, providing real-time authentication status information for a secure and seamless login experience.

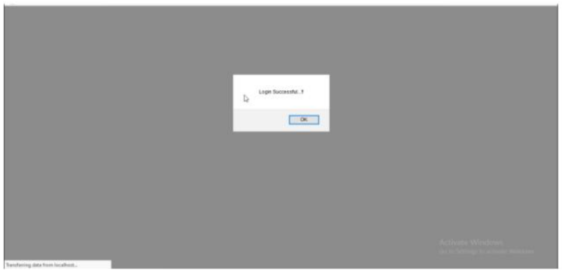


FIG:5 Output Screen-3

Owner home screen: The Owner Home Screen is a crucial interface for property owners, providing a central hub for managing listings and monitoring key metrics.

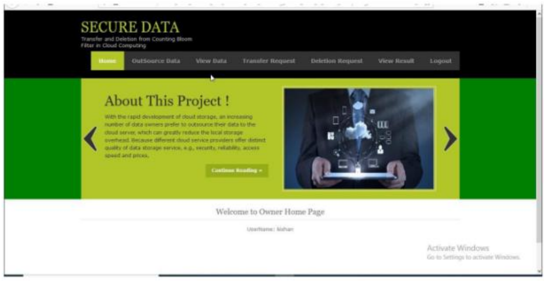


FIG: 6 Output Screens-4

Out source data:

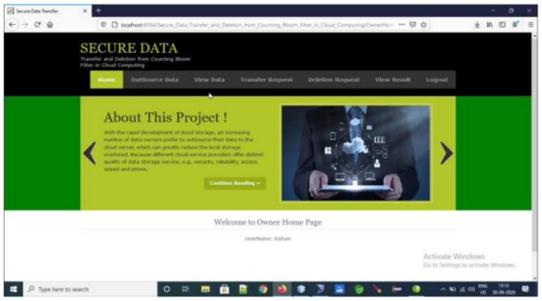


FIG:7 Output Screen-5

Divide data into blocks:

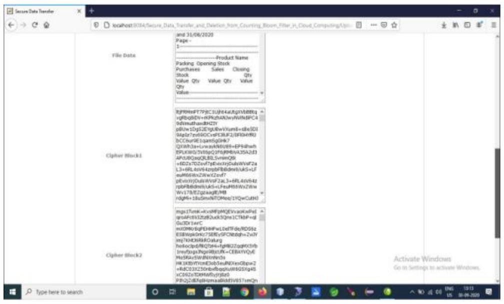


FIG:8 Output Screens-6

Upload status: The screenshot above depicts the Upload Status Page, a crucial component of our project's user interface. This page serves as a real-time indicator of file upload progress, offering userstransparency and feedback during the data submission process.

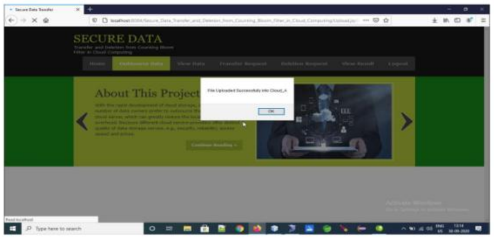
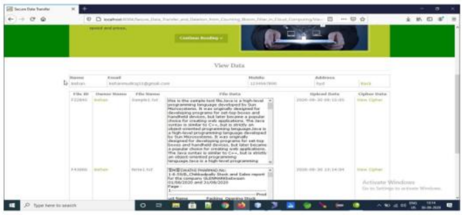


FIG:9 Output Screen-7

Selected user details:



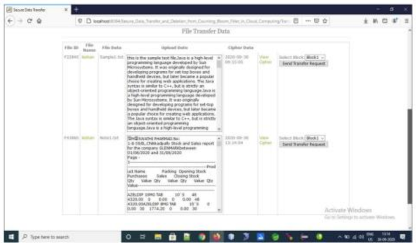
View Data

Name	Email	Mobile	Address	
kishan	kishanmudiraj11@gmail.com	1234567890	hyd	Back

File ID	Owner Name	File Name	File Data	Upload Date	Cipher Data
[illegible]	kishan	Sample1.txt	this is the sample text file.Java is a high-level programming language developed by Sun Microsystems. It was originally designed for developing programs for set-top boxes and handheld devices, but later became a popular choice for creating web applications. The Java syntax is similar to C++, but is strictly an object-oriented programming language.Java is a high-level programming language developed by Sun Microsystems. It was originally designed for developing programs for set-top boxes and handheld devices, but later became a popular choice for creating web applications. The Java syntax is similar to C++, but is strictly an object-oriented programming language.Java is a high-level programming	2020-09-30 09:15:05	View Cipher
[illegible]	kishan	Note1.txt	[illegible] Chikkadpally Stock and Sales report for the company GLENMARK between 01/06/2020 and 31/06/2020 Page : 1	2020-09-30 13:14:04	View Cipher

FIG:10 Output Screen-8

Transfer Request:

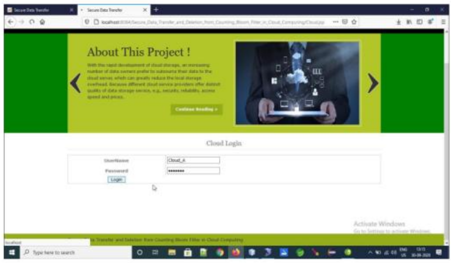


File Transfer Data

File ID	File Name	File Data	Upload Date	Cipher Data		
[illegible]	kishan	Sample1.txt	this is the sample text file.Java is a high-level programming language developed by Sun Microsystems. It was originally designed for developing programs for set-top boxes and handheld devices, but later became a popular choice for creating web applications. The Java syntax is similar to C++, but is strictly an object-oriented programming language.Java is a high-level programming language developed by Sun Microsystems. It was originally designed for developing programs for set-top boxes and handheld devices, but later became a popular choice for creating web applications. The Java syntax is similar to C++, but is strictly an object-oriented programming language.Java is a high-level programming	2020-09-30 09:15:05	View Cipher	Select Block: Block1 Send Transfer Request
[illegible]	kishan	Note1.txt	[illegible] 1-8-59/B, Chikkadpally Stock and Sales report for the company GLENMARK between 01/06/2020 and 31/06/2020 Page : 1 ... Product Name Packing Opening Stock Purchases Sales Closing Stock Qty Value Qty Value Qty Value Qty Value ...	2020-09-30 13:14:04	View Cipher	Select Block: Block1 Send Transfer Request

FIG:11 Output Screen-9

Cloud_a login: The login page serves as the initial point of entry for users to access the Cloud-based platform. To enhance user experience and security, we have designed a sleek and intuitive login interface. Users are required to enter their credentials, including a unique username and password, to gain access to the system.



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.

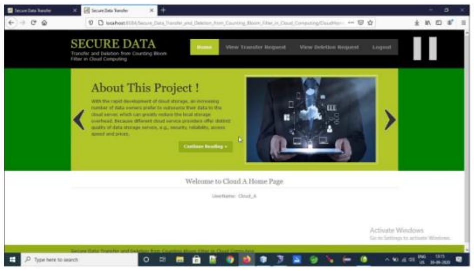
Cloud Login

UserName: Cloud_A

Password: ********

FIG:12 Output Screen-10

Cloud a home page:



SECURE DATA
Transfer and Deletion from Counting Bloom Filter in Cloud Computing

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.

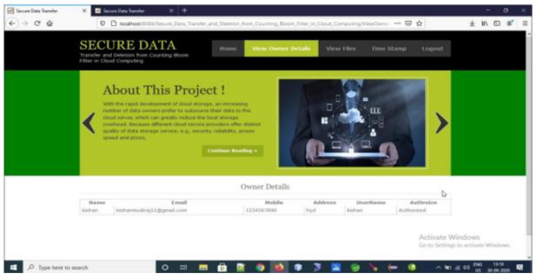
Welcome to Cloud A Home Page

UserName: Cloud_A

FIG:13 Output Screen-11

Admin login: The administrator dashboard is a crucial backend component that provides administrators with tools to manage user accounts, monitor system analytics, and configure settings.

View owner details:



SECURE DATA
Transfer and Deletion from Counting Bloom Filter in Cloud Computing

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.

Owner Details

Name	Email	Mobile	Address	UserName	Authroize
kishan	kishanmudiraj11@gmail.com	1234567890	hyd	kishan	Authorized

FIG:14 Output Screen-12

Time stamp in graph:

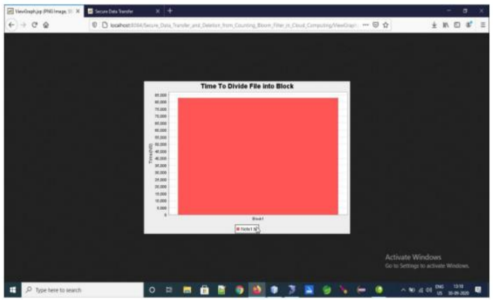

ViewGraph.jsp (PNG Image, 5…
Secure Data Transfer
localhost:8084/Secure_Data_Transfer_and_Deletion_from_Counting_Bloom_Filter_in_Cloud_Computing/ViewGraph
Time To Divide File into Block
85,000
80,000
75,000
70,000
65,000
60,000
55,000
50,000
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
Time(MS)
Block1
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
US
13:10
30-09-2020

FIG:15 Output Screen-13

5.CONCLUSION

To sum up, the counting Bloom filter-based plan that has been suggested tackles the crucial problems of safe data deletion and transfer in cloud storage, emphasizing the attainment of public verifiability. The work's contributions are found in its capacity to guarantee publicly verifiable data erasure and demonstrable data transit between various cloud service providers. The plan provides a way around issues including the possibility of data modification, integrity checks, and the danger of the original cloud server retaining dangerous material. The independence of the suggested approach from Trusted Third Parties (TTP) sets it apart from other options and is one of its main advantages.

Through the verification of transfer and deletion evidence, the scheme allows the data owner and the destination cloud server to identify any dishonest migration or deletion actions by employing the counting Bloom filter. This gives data owners looking to switch cloud service providers more confidence by improving the security and transparency of the data movement process. The suggested scheme's ability to achieve the intended design goals is confirmed by the security analysis. Additionally, simulation studies support the proposal's applicability in realworld applications by demonstrating its effectiveness and practicality. Given the increasing importance of cloud storage in contemporary computing, it is critical to address security issues related to data erasure and transmission. This paper presents a counting Bloom filter-based system that makes a substantial contribution to the development of verifiable and secure cloud data management. The plan, based on its unique data migration and deletion approach and public verifiability, is a significant addition to the cloud computing industry, paving the way for secure data management.

6.FUTURE SCOPE

It is admirable that the suggested method concentrates on resolving significant issues with safe data deletion and transmission within cloud storage, and the addition of a counting Bloom filter-based approach brings a fresh perspective to the area. For a system to be deemed robust, any potential flaws should be recognized and fixed, just like with any other system. The potential for false positives or negatives while counting Bloom filters is one important issue. These filters work well for membership queries that are approximate, although they might not be 100% accurate. Future research may focus on improving the counting Bloom filter's implementation to reduce errors and boost accuracy overall. This improvement could involve investigating hybrid techniques that incorporate several data structures for a more dependable result, or it could involve optimizing the hash functions.

The possible influence of the suggested strategy on performance is another factor to take into account. Even though counting Bloom filters is effective, there could be computational overhead. To comprehend the system's scalability and resource requirements, in-depth performance testing would be beneficial, particularly in large-scale cloud systems.

The results of this testing may guide modifications or new strategies aimed at preserving the harmony between system effectiveness and security. Strategically, the system is designed to reduce dependencies and promote decentralization without relying on a Trusted Third Party (TTP). It's crucial to recognize, nevertheless, that this strategy can create new challenges for the cloud service providers and data owners in terms of communication and building confidence. Subsequent investigations may 74 examine techniques to optimize these exchanges and augment the user experience in general, all the while preserving the intended degree of security. Future developments may bring the system's functionality beyond the counting Bloom filter. Investigating cutting-edge cryptographic methods could improve data secrecy even further during the transfer and deletion procedures. Techniques such as homomorphic encryption or zero-knowledge proofs may be considered to provide an additional layer of protection for sensitive data. Furthermore, it is critical to continuously adapt to new security requirements and cloud technology advancements.

The system must keep up with new trends, security threats, and industry best practices due to the dynamic nature of the cloud computing environment. To guarantee the system's continued relevance and efficacy throughout time, frequent upgrades and improvements will be required. In conclusion, even though the suggested approach seems like a good way to address the issues with safe data transfer and deletion in cloud storage, it is important to recognize any potential drawbacks and make plans for future improvements. Enhancing the counting Bloom filter implementation, attending to performance issues, investigating sophisticated cryptographic methods, and keeping abreast of industry advancements will all help ensure the system's continued success in the ever-changing world of cloud computing. The method aims to ensure secure data transfer and deletion in cloud storage using a counting Bloom filter-based scheme, despite potential drawbacks like false positives and performance impact. Future work should focus on scalability testing, cryptographic algorithms, and adapting to changing cloud technologies.

7.REFERENCES

References Made From:

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. 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.

3. 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.

4. B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions", Future Generation Computer Systems, Vol.79, pp.849–861, 2018.

5. 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.

6. 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.

7. 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-indexgci/white-paper-c11-738085.pdf, 2019-5-5.

8. Cloudsfer, “Migrate & backup your files from any cloud to any cloud”, available at: https://www.cloudsfer.com/, 2019-5-5.

9. Y. Liu, S. Xiao, H. Wang, et al., “New provable data transfer from provable data possession 76 and deletion for secure cloud storage”, International Journal of Distributed Sensor Networks, Vol.15, No.4, pp.1–12, 2019.

10. Y. Wang, X. Tao, J. Ni, et al., “Data integrity checking with reliable data transfer for secure cloud storage”, International Journal of Web and Grid Services, Vol.14, No.1, pp.106–121, 2018.