International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Bloom Filter for Secure Data Transfer and Deletion Counting in Cloud Computing

PUSULURI SRIDHAR[1], SK.MALINA [2]
#1Student, Dept of CSE, VelagaNageswaraRao College Of Engineering, Ponnur(Post),Ponnur(Md)Guntur(D.T)A. Andhra Pradesh.
#2Asst. Professor, Dept of CSE, VelagaNageswaraRao College Of Engineering, Ponnur(Post),Ponnur(Md)Guntur(D.T)A. Andhra Pradesh. malina.shaik30@gmail.com,

ABSTRACT_
With the fast improvement of cloud storage, an growing range of records proprietors pick to outsource their statistics to the cloud server, which can considerably decrease the neighborhood storage overhead. Because different cloud carrier vendors provide wonderful high-quality of statistics storage service, e.g., security, reliability, access pace and prices, cloud records switch has end up a quintessential requirement of the information proprietor to change the cloud provider providers. Hence, how to securely migrate the records from one cloud to any other and permanently delete the transferred records from the authentic cloud turns into a essential difficulty of information owners.To remedy this problem, we assemble a new counting Bloom filter-based scheme in this paper. The proposed scheme no longer solely can obtain impervious information switch however additionally can realise everlasting records deletion. Additionally,the proposed scheme can fulfill the public verifiability barring requiring any depended on 0.33 party. Finally, we also strengthen a simulation implementation that demonstrates the practicality and effectivity of our proposal.

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

1.INTRODUCTION

As a new computing paradigm, cloud computing is the fusion and development of parallel computing, distributed computing and grid computing. Cloud storage is one of the most attractive services offered by cloud computing, which can provide users with convenient data storage services and business access services by integrating a large number of distributed storage devices in network together. In cloud storage, users can outsource their data to the cloud server, which can greatly reduce the local hardware/software overhead and human resources investments. Due to the attractive advantages, cloud storage has been widely applied in the daily life and work. As a result, more and more resource constraint users, including individuals and corporations prefer to embrace cloud storage service. Despite tremendous advantages, cloud storage inevitably suffers from some new security problems because of the separation of outsourced data ownership and management, such as data confidentiality, data integrity, data availability and data deletion. These problems, specifically for data deletion, if not solved well, may impede the acceptance of cloud storage to the public. As the last phase of the data life cycle, data deletion directly determines whether the data life cycle can come to an end favourably, which is very important for data security and privacypreserving. However, data deletion attracts much less attention compared with data integrity, which has been well studied and solidly solved. Although some verifiable deletion schemes have been proposed for outsourced data in cloud computing environment, there are still some problems and challenges that urgently need to be solved solidly. To realize secure data migration, an outsourced data transfer app, Cloudsfer, has been designed utilizing cryptographic algorithm to prevent the data from privacy disclosure in the transfer phase.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

But there are still some security problems in processing the cloud data migration and deletion. Firstly, for saving network bandwidth, the cloud server might merely migrate part of the data, or even deliver some unrelated data to cheat the data owner. Secondly, because of the network instability, some data blocks may lose during the transfer process. Meanwhile, the adversary may destroy the transferred data blocks. Hence, the transferred data may be polluted during the migration process. Last but not least, the original cloud server might maliciously reserve the transferred data for digging the implicit benefits. The data reservation is unexpected from the data owners' point of view. In short, the cloud storage service is economically attractive, but it inevitably suffers from some serious security challenges, specifically for the secure data transfer, integrity verification, verifiable deletion. These challenges, if not solved suitably, might prevent the public from accepting and employing cloud storage service.

2.LITERATURE SURVEY

2.1 Practical Techniques For Searches On Encrypted Data

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query without loss of data confidentiality. In this paper, we describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; 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.

2.2 Smart cloud search services: verifiable keyword-based semantic search over encrypted cloud data

With the increasing popularity of the pay-as-you- consume cloud computing paradigm, a large number of cloud services are pushed to consumers. One hand, it brings great convenience to consumers who use intelligent terminals; on the other hand, consumers are also facing serious difficulties that how to search the most suitable services or products from cloud. So how to enable a smart cloud search scheme is a critical problem in the consumer-centric cloud computing paradigm. For protecting data privacy, sensitive data are always encrypted before being outsourced. Although the existing searchable encryption schemes enable users to search over encrypted data, these schemes support only exact keyword search, which greatly affects data usability. Moreover, these schemes do not support verifiability of search result. In order to save computation cost or download bandwidth, cloud server only conducts a fraction of search operation or return a part of result, which is viewed as selfish and semi-honest-but-curious. So, how to enhance flexibility of

encrypted cloud data while supporting verifiability of search result is a big challenge. To tackle the challenge, a smart semantic search scheme is proposed in this paper, which returns not only the result of keyword-based exact match, but also the result of keyword-based semantic match. At the same time, the proposed scheme supports the verifiability of search result. The rigorous security analysis and performance analysis show that the proposed scheme is secure under the proposed model and effectively achieves the goal of keyword-based semantic search. Pay-as-you-consume cloud computing paradigm has become more and more prevalent, due to its benefits for consumers, including a large number of convenient service, relief of the burden for storage, flexible data access, reduction of cost on hardware and software. A lot of companies have set up and provided various cloud computing services. More and more sensitive data from consumers (e.g., photo albums, emails, personal health records and financial transactions, etc.) have been centralized into the cloud for its flexible management and economic savings. Meanwhile, many technical schemes related to cloud computing service are proposed by researchers. Noh et al. proposed a flexible communication bus model for multimedia services in cloud environment. Shahnaza et al.proposed a realistic IEEE 802.11e EDCA model for QoS-aware differentiated multimedia mobile cloud services. Cabarcos et al. proposed a middleware architecture that allows sessions initiated from one device to be seamlessly transferred to a second one under a cloud environment.

2.3 Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query

Cloud computing becomes increasingly popular. To protect data privacy, sensitive data should be encrypted by the data owner before outsourcing, which makes the traditional and efficient plaintext keyword search technique useless. The existing searchable encryption schemes support only exact or fuzzy keyword search, not support semantics-based multi-keyword ranked search. In the real search scenario, it is quite common that cloud customers' searching input might be the synonyms of the predefined keywords, not the exact or fuzzy matching keywords due to the possible synonym substitution (reproduction of information content) and/or her lack of exact knowledge about the data. Therefore, synonym-based multi-keyword ranked search over encrypted cloud data remains a very challenging problem. In this paper, for the first time, we propose an effective approach to solve the problem of synonym-based multi-keyword ranked search over encrypted cloud data. We make contributions mainly in two aspects: synonym-based search for supporting synonym query and multi-keyword ranked search for achieving more accurate search result. Two secure schemes are proposed to meet privacy requirements in two threat models of known ciphertext model and known background model. In enhanced scheme, the sensitive frequency information can be well protected by introducing some dummy keywords, which is not adopted in basic scheme. We give security analysis to justify the correctness and privacy-preserving guarantee of the proposed schemes. 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.

3.PROPOSED SYSTEM

In the proposed work, the gadget research the issues of impervious records switch and deletion in cloud storage, and center of attention on realizing the public verifiability. Then the device proposes a counting Bloom filter-based scheme, which now not solely can realise provable information switch between two exclusive clouds however

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

additionally can acquire publicly verifiable records deletion. If the unique cloud server does no longer migrate or dispose of the information honestly, the verifier (the records proprietor and the goal cloud server) can notice these malicious operations with the aid of verifying the again switch and deletion evidences. Moreover, our proposed scheme does no longer want any Trusted 0.33 birthday celebration (TTP), which is specific from the present solutions. Furthermore, we show that our new idea can fulfill the preferred layout desires thru safety analysis. Finally, the simulation experiments exhibit that our new concept is environment friendly and practical.

3.1 IMPLEMENTATION

1.DATA OWNER:

In this application the owner is one of the main module for uploading the files and view the uploads file which are uploaded by the owner before do all these operations the owner should register with the application and the owner should authorized by the cloud.Owner can Able to Send transfer data request,delete request.

2.Admin

In This Application admin is one of the main modules he can able view data owner requests like transfer,delete .

3.CLOUD A

The cloud is the main module to operate this project in the users activation s , owner activation and also the cloud can check the following operations like search permission provides to the users, can check the top-k searched keyword, top-k similarity in chart, top-k searched keyword in chart. Primarily the cloud should login. Then only the cloud can perform the above mentioned actions.

4.CLOUD B

The cloud is the main module to operate this project in the users activation s , owner activation and also the cloud can check the following operations like search permission provides to the users, can check the top-k searched keyword, top-k similarity in chart, top-k searched keyword in chart.Primarily the cloud should login. Then only the cloud can perform the above mentioned actions.

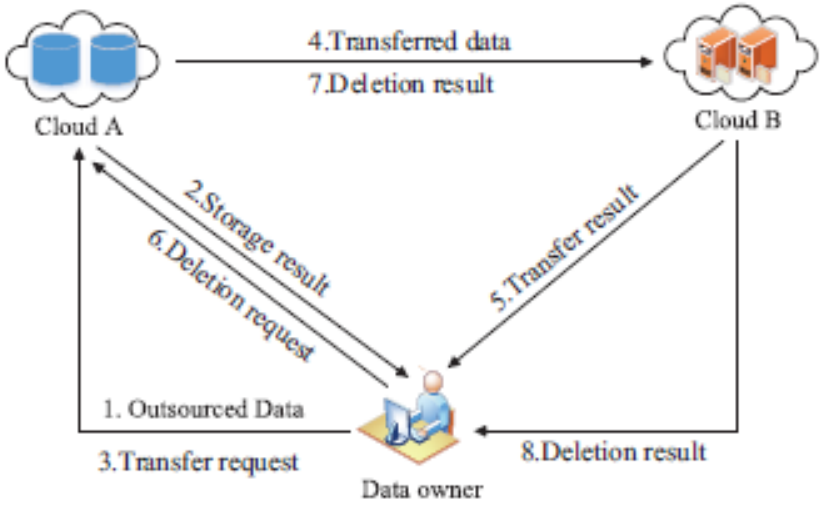

Fig: 4.1. System Model

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

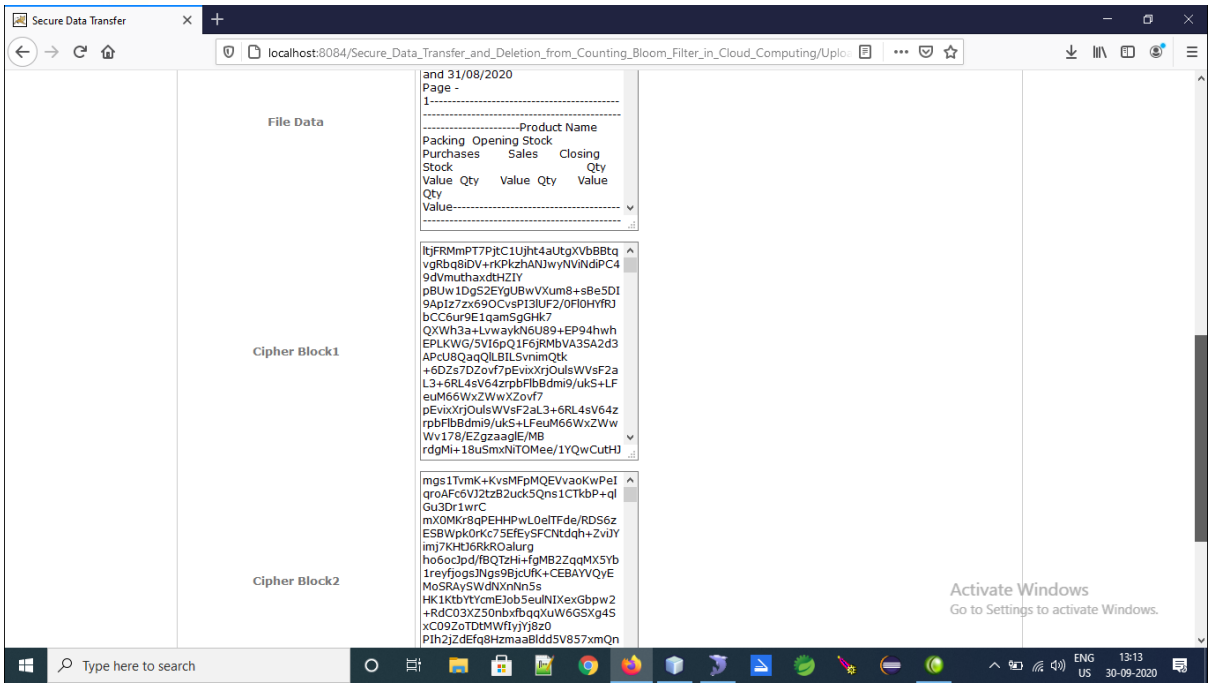

Fig 4.1 Information Divided Into Blocks For Security

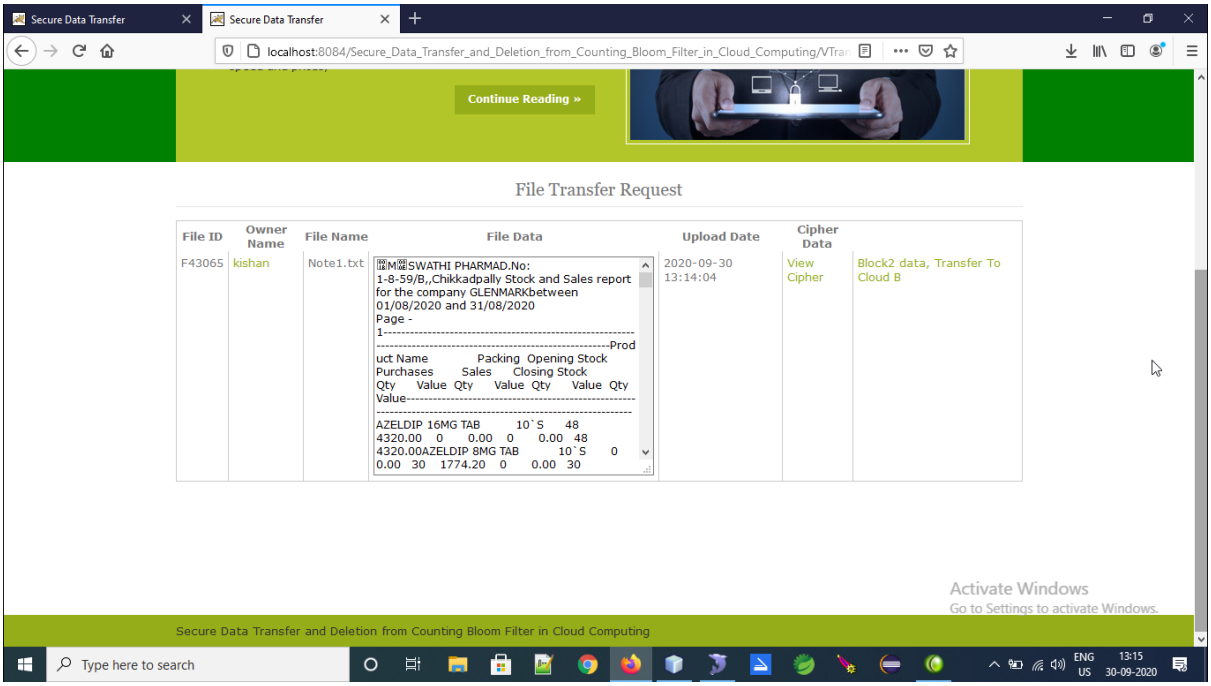

Fig 4.2 File Transferred From One Cloud To Another Cloud

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

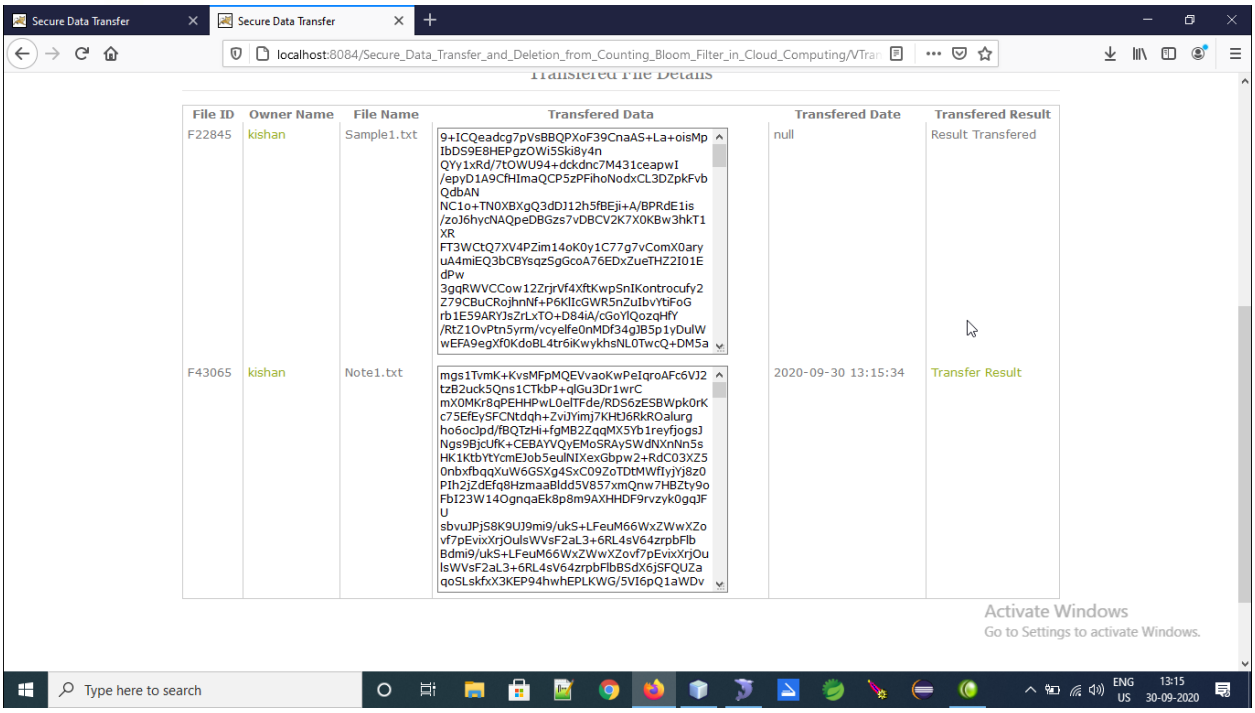

Fig 4.3 File Transfer Result sent to owner

5.CONCLUSION

In cloud storage, the information proprietor does now not trust that the cloud server might execute the facts switch and deletion operations honestly. To clear up this problem, we advocate a CBF-based impenetrable information switch scheme, which can additionally understand verifiable statistics deletion.

In our scheme, the cloud B can take a look at the transferred statistics integrity, which can warranty the statistics is totally migrated. Moreover, the cloud A ought to undertake CBF to generate a deletion proof after deletion, which will be used to affirm the deletion end result via the information owner. Hence, the cloud A can't behave maliciously and cheat the information proprietor successfully. Finally, the safety evaluation and simulation outcomes validate the protection and practicability of our proposal, respectively.

FUTURE SCOPE

Similar to all the present solutions, our scheme considers the facts switch between two distinct cloud servers. However, with the improvement of cloud storage, the facts proprietor would possibly desire to concurrently migrate the outsourced statistics from one cloud to the different two or extra goal clouds. However, the multi-target clouds may collude collectively to cheat the statistics proprietor maliciously. Hence, the provable records migration amongst three or greater clouds requires our similarly exploration

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] 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-index-gci/ 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 and deletion for secure cloud storage", International Journal of Distributed Sensor Networks, Vol.15, No.4, pp.1–12, 2019.

Author Profiles

Pusuluri Sridhar pursing M. Tech in Computer Science and Engineering from VelagaNageswaraRao College Of Engineering, Ponnur. Affiliated to JNTUK, KAKINADA.

SK.MALINA
Design: Asst.Prof,qual: MTECH(CSE) with having 3 years of experience in Teaching, current working : VNR college of Engineering, Affiliated to JNTUK, KAKINADA.
malina.shaik30@gmail.com, phone: 9666247505