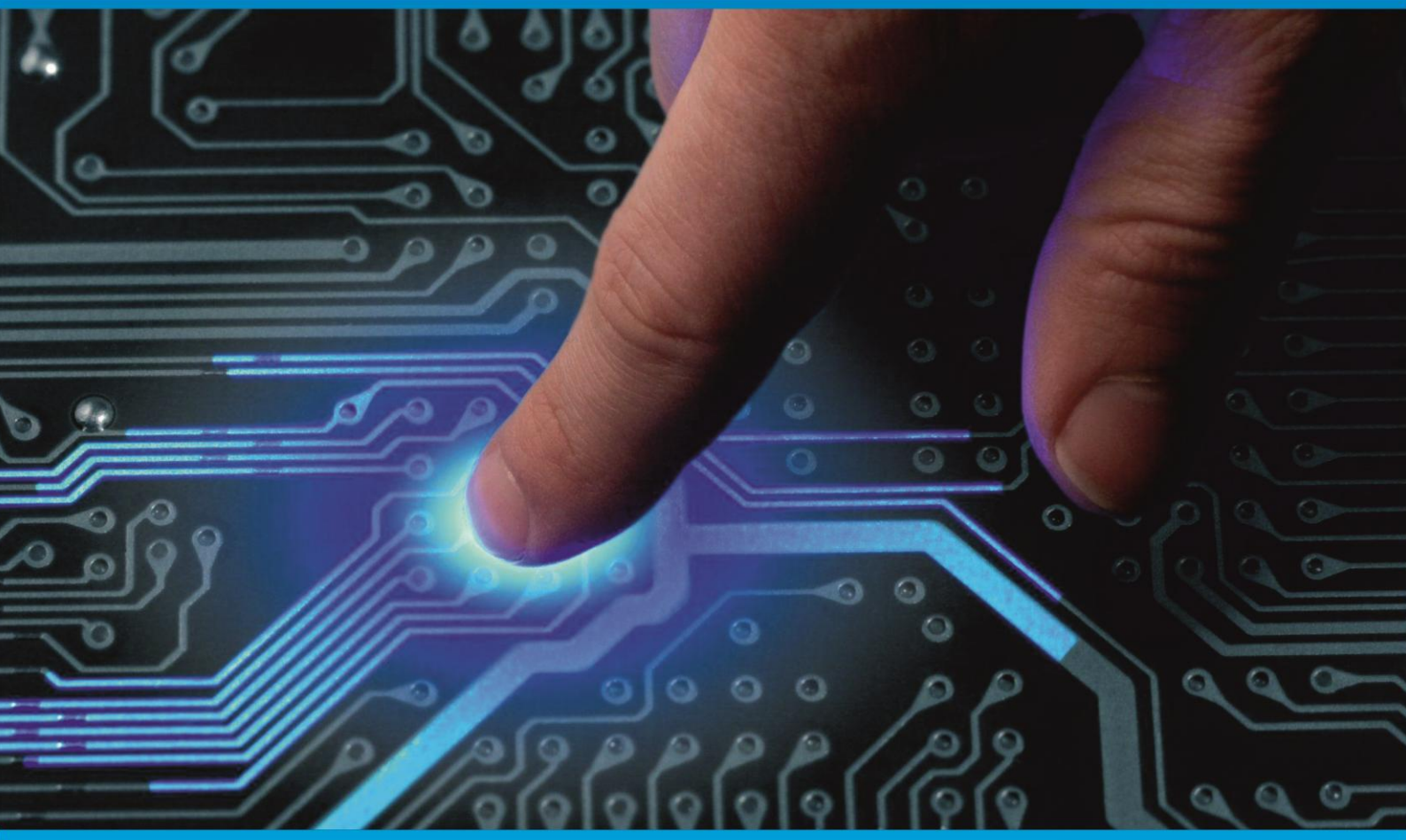
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006197 |

Novel Approach for Secure Transmission & Deletion of Data Using Counting Bloom Filters

Sushma Devi H R, Dr. Kanta D Devangavi

PG Student, Dept. of MCA., VIAT, Muddenahalli, Bangalore, India

Professor, Dept. of MCA., VIAT, Muddenahalli, Bangalore, India

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.

KEYWORDS : cloud, Bloom filter

I. INTRODUCTION

Cloud computing, an emerging and very promising computing paradigm, connects large-scale distributed storage resources, computing resources and network bandwidths together[1,2]. By using these resources, it can provide tenants with plenty of high-quality cloud services. Due to the attractive advantages, the services (especially cloud storage service) have been widely applied[3,4], by which the resource-constraint data owners can outsource their data to the cloud server, which can greatly reduce the data owners' local storage overhead[5,6]. According to the report of Cisco[7], the number of Internet consumers will reach about 3.6 billion in 2019, and about 55 percent of them will employ cloud storage service.

Because of the promising market prospect, an increasing number of companies (e.g., Microsoft, Amazon, Alibaba) offer data owners cloud storage service with different prices, security, access speed, etc. To enjoy more suitable cloud storage service, the data owners might change the cloud storage service providers. Hence, they might migrate their outsourced data from one cloud to another, and then delete the transferred data from the original cloud. According to Cisco[7], the cloud traffic is expected to be 95% of the total traffic by the end of 2021, and almost 14% of the total cloud traffic will be the traffic between different cloud data centers. Foreseeably, the outsourced data transfer will become a fundamental requirement from the data owners' point of view.

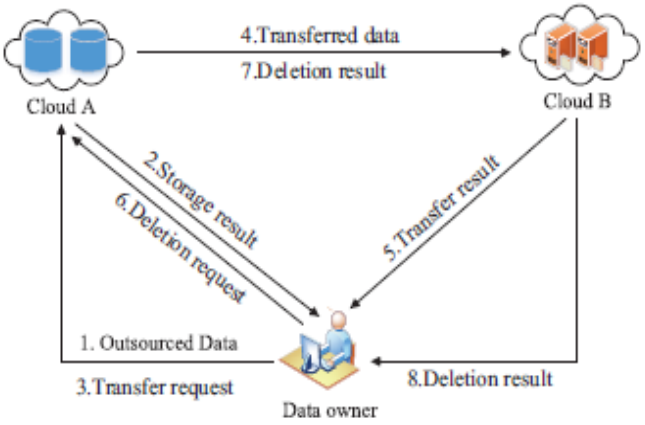


Figure 1: System Architecture

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006197 |

To realize secure data migration, an outsourced data transfer app, Cloud server [8], has been designed utilizing cryptographic algorithm to prevent the data from privacy disclosure in the transfer phase. 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[9]. Secondly, because of the network instability, some data blocks may lose during the transfer process. Meanwhile, the adversary may destroy the transferred data blocks[10]. 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[11]. 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.

Contributions In this work, we study the problems of secure data transfer and deletion in cloud storage, and focus on realizing the public verifiability. Then we propose a counting Bloom filter-based scheme, which not only can realize provable data transfer between two different clouds but also can achieve publicly verifiable data deletion. If the original cloud server does not migrate or remove the data honestly, the verifier (the data owner and the target cloud server) can detect these malicious operations by verifying the returned transfer and deletion evidences. Moreover, our proposed scheme does not need any Trusted third party (TTP), which is different from the existing solutions. Furthermore, we prove that our new proposal can satisfy the desired design goals through security analysis. Finally, the simulation experiments show that our new proposal is efficient and practical.

II. RELATED WORK

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.

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.

3. 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.

4. 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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006197 |

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.

5. Enabling central keyword based semantic extension search over encrypted outsourced data

In practice, search keywords have quite different importance when users take search operations. In addition, such keywords may have a certain grammatical relationship among them, which reflect the importance of keywords from the user's perspective intuitively. However, the existing search techniques regard the search keywords as independent and unrelated. In this paper, for the first time, we take the relation among query keywords into consideration and design a keyword weighting algorithm to show the importance of the distinction among them. By introducing the keyword weight to the search protocol design, the search results will be more in line with the user's demand.

III . SYSTEM ANALYSIS

Existing System

we study the problems of secure data transfer and deletion in cloud storage, and focus on realizing the public verifiability. Then we propose a counting Bloom filter-based scheme, which not only can realize provable data transfer between two different clouds but also can achieve publicly verifiable data deletion. If the original cloud server does not migrate or remove the data honestly, the verifier (the data owner and the target cloud server) can detect these malicious operations by verifying the returned transfer and deletion evidences. Moreover, our proposed scheme does not need any Trusted third party (TTP), which is different from the existing solutions. Furthermore, we prove that our new proposal can satisfy the desired design goals through security analysis. Finally, the simulation experiments show that our new proposal is efficient and practical.

Proposed System

we aim to achieve verifiable data transfer between two different clouds and reliable data deletion in cloud storage. Hence, three entities are included in our new construction,

In our scenario, the resource-constraint data owner might outsource his large-scale data to the cloud server A to greatly reduce the local storage overhead. Besides, the data owner might require the cloud A to move some data to the cloud B, or delete some data from the storage medium. The cloud A and cloud B provide the data owner with cloud storage service. We assume that the cloud A is the original cloud, which will be required to migrate some data to the target cloud B, and remove the transferred data. However, the cloud A might not execute these operations sincerely for economic reasons. because they belong to two different companies. Hence, the two clouds will independently follow the protocol. Furthermore, we assume that the target cloud B will not maliciously slander the original cloud A.

IV. IMPLEMENTATION

Data confidentiality

The data confidentiality means that adversary cannot get any plaintext information without the corresponding data decryption key. In our scheme, the data owner uses IND-CPA secure AES algorithm to encrypt the file. Hence, the adversary cannot forge a valid data decryption key successfully. Furthermore, the data owner keeps the data decryption key secret. That is, any adversary cannot obtain the decryption key to further get the plaintext information.

Data integrity

The data integrity means that the transferred data must be intact, or the cloud B refuses to accept the data. Upon receiving the transferred data (ai , Ci) from the cloud A and the hash values Hi from the data owner, the cloud B checks the equation $H_i = H(tagf \| ai \| Ci)$, where $i \in \phi$. Note that $\{Hi\}i\in\phi$ are computed by the data owner with a secure hash function. Thus, the cloud A and other adversaries cannot forge a new data block (ai , C′ i to make the equation $H_i = H(tagf \| ai \| C'_i)$ hold. That is, if the cloud A does not honestly migrate the data to cloud B, or the transferred data blocks are tampered by the attackers during the migration process, the cloud B can detect these malicious behaviors and will not accept the received data. Hence, the integrity of the transferred data is guaranteed.

Public verifiability

We analyze the verifiability of the transfer result and the deletion result, respectively. The verifier who owns transfer proof π and transfer request Rt can verify the transfer result. Specifically, the verifier first checks the validity of Rt. If Rt is valid, it means that the data owner indeed requested to migrate the data to cloud B. Then the verifier further verifies the validity of the signatures sigta and sigtb. Note that the cloud B will not maliciously collude with the cloud

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006197 |

A to mislead the data owner. Hence, the verifier can trust the returned transfer result if and only if both the signatures are valid. Besides, the verifier checks that whether the cloud B maintains the transferred data honestly by verifying the counting Bloom filter CBFb.

V. SIMULATION RESULTS

We simulate our scheme and previous schemes[26,32] with the OpenSSL library and the PBC library on the same windows machine equipped with 4 G main memory and Intel(R) Core(TM) i5-4590 processors that running at 3.30GHz. In storage phase, the computation overhead comes from storage proof generation and storage result verification.

In encryption phase, we increase the file from 1MB to 8MB with a step for 1MB, and the number of the data blocks is fixed in 8000, then the time cost comparison is shown in Fig.5. We can find that the time cost of the three schemes will increase with the size of the encrypted data. However, the growth rate of our scheme is relatively lower.

In storage phase, the computation overhead comes from storage proof generation and storage result verification. Fig.6 shows the time cost of storage proof generation. We find that the time of our scheme is much less than that of Yang et al.'s scheme of Ref.[26], and the growth rate of Yang et al.'s scheme of Ref.[26] is relatively higher than that of our scheme. To simulate the data transfer, we increase the number of transferred data blocks from 10 to 80 with a step for 10. For simplicity, we fix n = 400 and ignore the communication overhead, as shown in Fig. 8. The time cost increases with the number of transferred data blocks. Moreover, Yang et al.'s scheme of Ref.[26] costs much more time since it needs to execute many bilinear pairing calculations to verify the data integrity, however our scheme only needs to compute some hash values. Finally, the data owner wants to delete the transferred data from cloud A, and we fix n = 400, then the performance evaluation is presented in Fig.9. The time overhead of Hao et al.'s scheme of Ref.[32] is almost constant. However, the time cost of our scheme and Yang et al.'s scheme of Ref.[26] will increase with the number of deleted data blocks, and the growth rate of Yang et al.'s scheme of Ref.[26] is relatively higher. Meanwhile, Yang et al.'s scheme of Ref.[26] costs much more time when the deleted data blocks are more than 20. So, we think that our scheme is more efficient to delete the transferred data blocks.

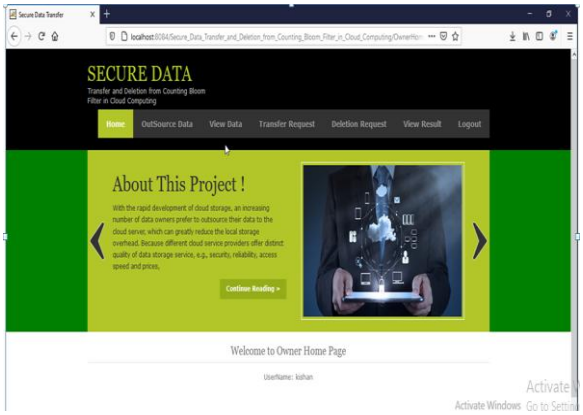


Fig.1.Owner home screen

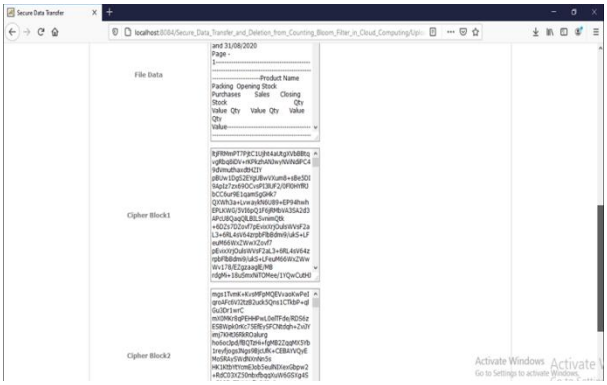


Fig. 2. Data Divide into blocks

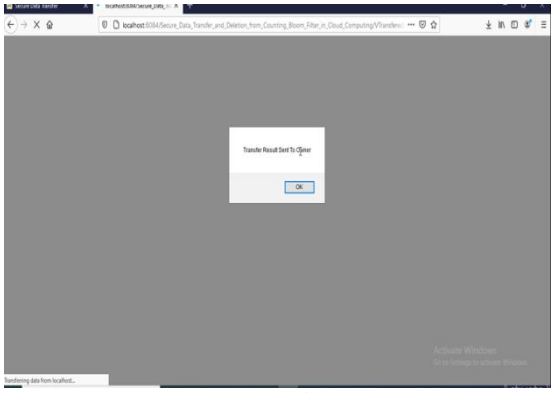


Fig. 3. View transfer request

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006197 |

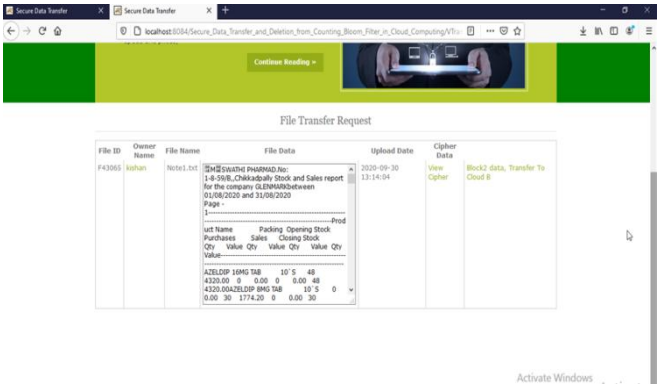


Fig 4 Result sent to owner

III. CONCLUSION AND FUTURE WORK

In cloud storage, the data owner does not believe that the cloud server might execute the data transfer and deletion operations honestly. To solve this problem, we propose a CBF-based secure data transfer scheme, which can also realize verifiable data deletion. In our scheme, the cloud B can check the transferred data integrity, which can guarantee the data is entirely migrated. Moreover, the cloud A should adopt CBF to generate a deletion evidence after deletion, which will be used to verify the deletion result by the data owner. Hence, the cloud A cannot behave maliciously and cheat the data owner successfully. Finally, the security analysis and simulation results validate the security and practicability of our proposal, respectively. Future work Similar to all the existing solutions, our scheme considers the data transfer between two different cloud servers. However, with the development of cloud storage, the data owner might want to simultaneously migrate the outsourced data from one cloud to the other two or more target clouds. However, the multi-target clouds might collude together to cheat the data owner maliciously. Hence, the provable data migration among three or more clouds requires our further exploration.

REFERENCES

[1] [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] [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] [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] [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] [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] [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] [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] [8] Cloudsfer, "Migrate & backup your files from any cloud to any cloud", available at: https://www.cloudsfer.com/, 2019-5-5.

[9] [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.

[10] [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.

[11] [11] Y. Luo, M. Xu, S. Fu, et al., "Enabling assured deletion in the cloud storage by overwriting", Proc. of the 4th ACM International Workshop on Security in Cloud Computing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006197 |

[12] [12] C. Yang and X. Tao, "New publicly verifiable cloud data deletion scheme with efficient tracking", Proc. of the 2th International Conference on Security with Intelligent Computing and Big-data Services, Guilin, China, pp.359–372, 2018.

[13] [13] Y. Tang, P.P Lee, J.C. Lui, et al., "Secure overlay cloud storage with access control and assured deletion", IEEE Transactions on Dependable and Secure Computing, Vol.9, No.6, pp.903–916, 2012.

[14] [14] Y. Tang, P.P.C. Lee, J.C.S. Lui, et al., "FADE: Secure overlay cloud storage with file assured deletion", Proc. of the 6th International Conference on Security and Privacy in Communication Systems, Springer, pp.380-397, 2010.

[15] [15] Z. Mo, Y. Qiao and S. Chen, "Two-party fine-grained assured deletion of outsourced data in cloud systems", Proc. of the 34th International Conference on Distributed Computing Systems, Madrid, Spain, pp.308–317, 2014.

[16] [16] M. Paul and A. Saxena, "Proof of erasability for ensuring comprehensive data deletion in cloud computing", Proc. of the International Conference on Network Security and Applications, Chennai, India, pp.340–348, 2010.

[17] [17] A. Rahumed, H.C.H. Chen, Y. Tang, et al., "A secure cloud backup system with assured deletion and version control", Proc. of the 40th International Conference on Parallel Processing Workshops, Taipei City, Taiwan, pp.160–167, 2011.

[18] [18] B. Hall and M. Govindarasu, "An assured deletion technique for cloud-based IoT", Proc. of the 27th International Conference on Computer Communication and Networks, Hangzhou, China, pp.1–8, 2018.

[19] [19] L. Xue, Y. Yu, Y. Li, et al., "Efficient attributebased encryption with attribute revocation for assured data deletion", Information Sciences, Vol.479, pp.640–650, 2019.

[20] [20] L. Du, Z. Zhang, S. Tan, et al., "An Associated Deletion Scheme for Multi-copy in Cloud Storage", Proc. of the 18th International Conference on Algorithms and Architectures for Parallel Processing, Guangzhou, China, pp.511–526, 2018.

[21] [21] C. Yang, X. Chen and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage", Journal of Network and Computer Applications, Vol.103, pp.185–193, 2018.

[22] [22] Y. Yu, J. Ni, W. Wu, et al., "Provable data possession supporting secure data transfer for cloud storage", Proc. of 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications(BWCCA 2015), Krakow, Poland, pp.38–42, 2015.

[23] [23] J. Ni, X. Lin, K. Zhang, et al., "Secure outsourced data transfer with integrity verification in cloud storage", Proc. of 2016 IEEE/CIC International Conference on Communications in China, Chengdu, China, pp.1–6, 2016.

[24] [24] L. Xue, J. Ni, Y. Li, et al., "Provable data transfer from provable data possession and deletion in cloud storage", Computer Standards & Interfaces, Vol.54, pp.46–54, 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details