Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

SECURE DATA TRANSFER AND DELETION VIA COUNTING BLOOM FILTERS IN CLOUD COMPUTING

VINNAKOTA AKASH[1], Mr. SHAIK HIMAM BASHA[2]

#1 Pursuing M.C.A #2 Assistant Professor Department of Master of Computer Applications

QIS COLLEGE OF ENGINEERING & TECHNOLOGY

Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

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 storage, Data deletion, Data transfer, Counting Bloom filter, Public verifiability

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 percentof 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. To realize secure data migration, an outsourced data transfer app, Cloudsfer[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 securedata 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.

Literature Survey:

1. Changsong Yang et al. (2020) Title: Secure Data Transfer and Deletion from Counting Bloom Filter in Cloud Computing Journal: Chinese Journal of Electronics DOI: 10.1049/cje.2020.02.015 Merits: • Proposes a Counting Bloom Filter-based scheme for secure data transfer and permanent deletion in cloud environments. • Ensures public verifiability without requiring a trusted third party. • Demonstrates practicality and

efficiency through simulation. Demerits: • Limited scalability for large-scale cloud infrastructures. • Performance may degrade with increased data volume.

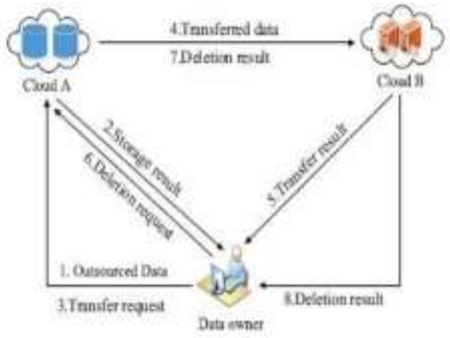
2. 2. Sabuzima Nayak & Ripon Patgiri (2021) Title: countBF: A General-purpose High Accuracy and Space Efficient Counting Bloom Filter Preprint: arXiv:2106.04364 Merits: • Introduces countBF, a Counting Bloom Filter variant offering high accuracy and space efficiency. lower • Experimental results show significant memory savings compared to standard Bloom Filters. • Achieves false Demerits: positive rates and execution times. • Primarily focused on theoretical analysis; practical implementation details are limited. • May require adaptation for specific cloud computing scenarios.
3. 3. B. Sravani et al. (2024) Title: Secure Data Transfer and Deletion from Counting Bloom Filter in Cloud Computing Journal: International Journal of Information Technology and Computer Engineering DOI: 10.1109/ICICI.2019.00080 Merits: • Focuses on enhancing security and privacy of data operations within cloud environments. • Employs Counting Bloom Filters for secure data transfer and deletion. • Integrates advanced cryptographic techniques to ensure confidentiality and integrity. Demerits: • Implementation details and performance evaluations are not provided. • Lacks comparative analysis with existing methods.ijitce.org

Analysis:

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 percentof 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. To realize secure data migration, an outsourced data transfer app, Cloudsfer[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 securedata transfer, integrity verification, verifiable deletion. These challenges, if not solved suitably, might prevent the public from accepting and employing cloud storage service.

System Architecture:



Modules:

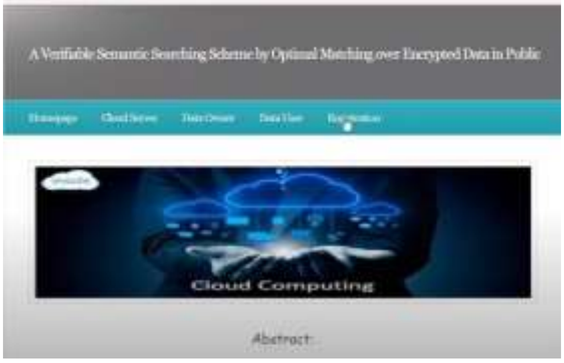
1. Secure Data Transfer: What are the primary security concerns during data transfer to and from the cloud? Think about confidentiality (preventing unauthorized access), integrity (ensuring data hasn't been tampered with), and availability (authorized users can access data when needed). What existing techniques are used for secure data transfer in the cloud? Common methods include encryption (like TLS/SSL for data in transit), secure protocols (like SFTP), and potentially techniques like data masking or tokenization depending on the sensitivity. How might Counting Bloom Filters contribute to secure data transfer? This is the interesting part! Perhaps they are used to: Verify the presence of data segments without revealing the actual data: This could be useful for integrity checks or ensuring all parts of a file have been transferred correctly without needing to transmit hashes of the entire dataset. Potentially in access control mechanisms: Could they be used to quickly check if a user has access rights to certain data without

revealing the exact permissions list? (This would need careful design to avoid security vulnerabilities).

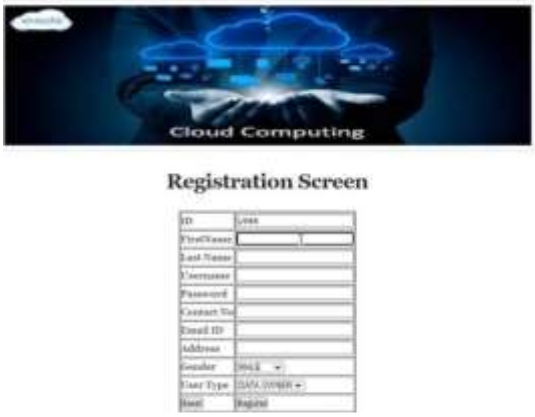
2. Secure Data Deletion: What are the challenges of ensuring data is truly deleted in a cloud environment? Cloud storage often involves distributed systems and data replication, making complete erasure complex. Simply "deleting" a file might not overwrite the physical storage immediately, leaving traces behind. What are some common techniques for secure data deletion in the cloud? These include cryptographic erasure (encrypting data with a key and then destroying the key), overwriting storage multiple times, and degaussing for magnetic media. How could Counting Bloom Filters be relevant to secure data deletion? This is where it gets innovative! Perhaps they could be used to: Track which data blocks have been targeted for deletion: A Counting Bloom Filter could efficiently represent the set of data chunks that need to be securely erased. Verify that deletion has been performed across all replicas: By querying the filter, the system could probabilistically check if a data block marked for deletion is still present in the storage system.

3. Counting Bloom Filters: What is a standard Bloom Filter? It's a probabilistic data structure used to test whether an element is a member of a set. It can have false positives (saying an element is in the set when it's not) but no false negatives (if an element is in the set, the filter will definitely say it is).

Implementation:


A Verifiable Semantic Searching Scheme by Optimal Matching over Encrypted Data in Public
Homepage
Cloud Server
Data Owner
Data User
Registration
Cloud Computing
Abstract

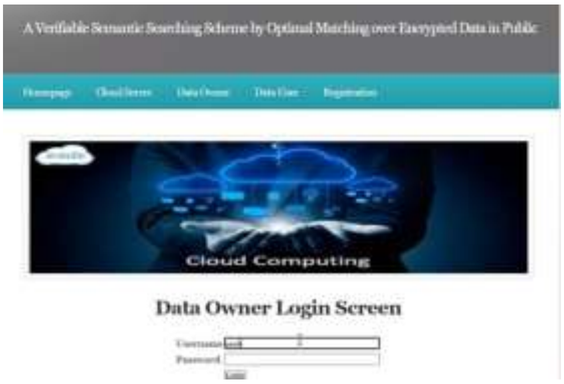
Home Screen



Registration Screen

ID	[illegible]
FirstName	
Last Name	
Username	
Password	
Contact No	
Email ID	
Address	
Gender	MALE
User Type	DATA OWNER
Reset	Register

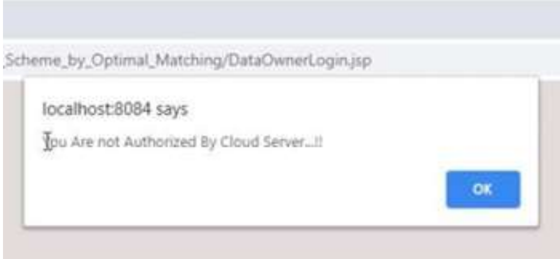
Sign Up


A Verifiable Semantic Searching Scheme by Optimal Matching over Encrypted Data in Public
Homepage
Cloud Server
Data Owner
Data User
Registration
Cloud Computing

Data Owner Login Screen

Username [illegible]
Password
Login

Data Owner Login

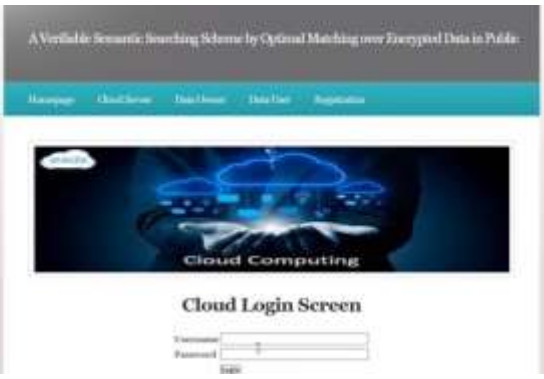


Scheme_by_Optimal_Matching/DataOwnerLogin.jsp

localhost:8084 says

You Are not Authorized By Cloud Server...!!

Authentication Failed



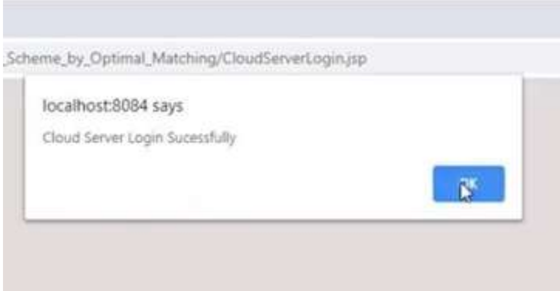
A Verifiable Semantic Searching Scheme by Optimal Matching over Encrypted Data in Public

Cloud Login Screen

Username

Password

Cloud Login

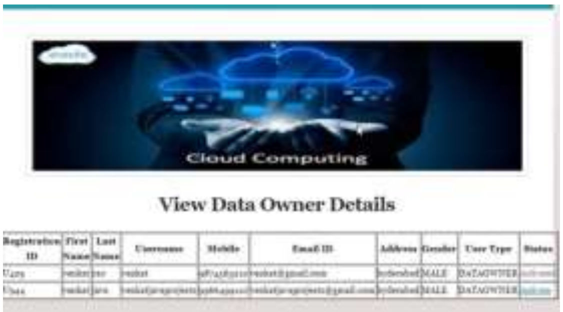


Scheme_by_Optimal_Matching/CloudServerLogin.jsp

localhost:8084 says

Cloud Server Login Sucessfully

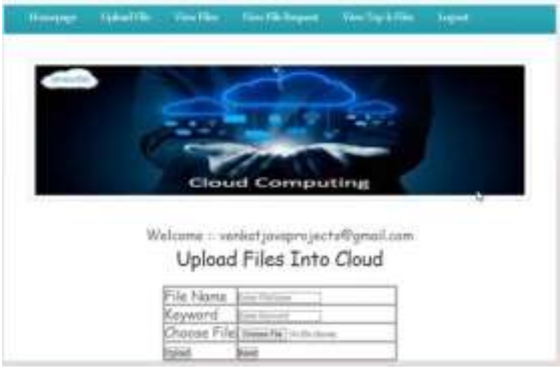
Authentication Success



View Data Owner Details

Registration ID	First Name	Last Name	Username	Mobile	Email ID	Address	Gender	User Type	Status
[illegible]	venkat	[illegible]	venkat	[illegible]	venkat@gmail.com	hyderabad	MALE	DATAOWNER	[illegible]
[illegible]	venkat	java	venkatjavaprojects	[illegible]	venkatjavaprojects@gmail.com	hyderabad	MALE	DATAOWNER	[illegible]

View Data Owners

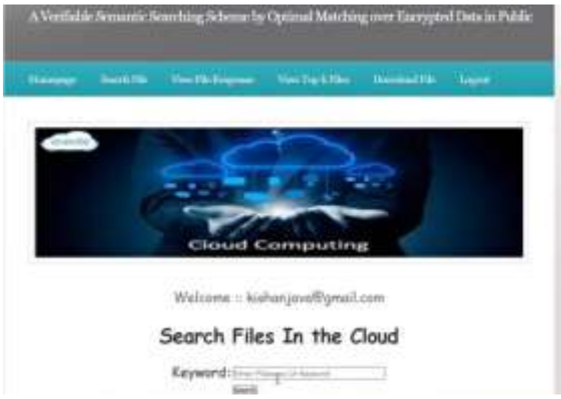


Welcome :: venkatjavaprojects@gmail.com

Upload Files Into Cloud

File Name	[illegible]
Keyword	[illegible]
Choose File	Choose File [illegible]
Upload	Reset

File Upload



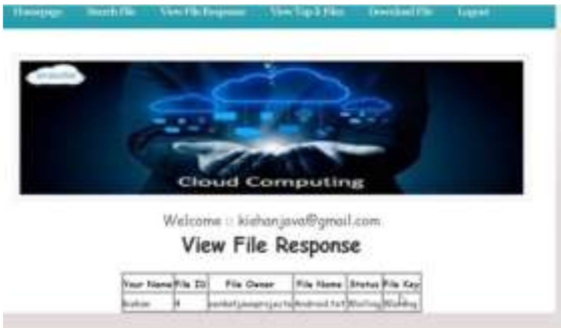
A Verifiable Semantic Searching Scheme by Optimal Matching over Encrypted Data in Public

Welcome :: kishanjava@gmail.com

Search Files In the Cloud

Keyword: [illegible]

File Search in Cloud

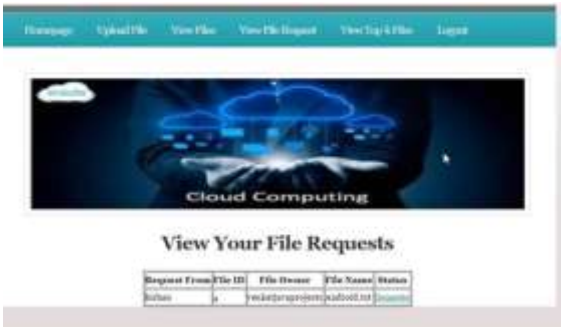


Welcome :: kishanjava@gmail.com

View File Response

Your Name	File ID	File Owner	File Name	Status	File Key
kishan	4	venkatjavaprojects	Android.txt	Waiting	Waiting

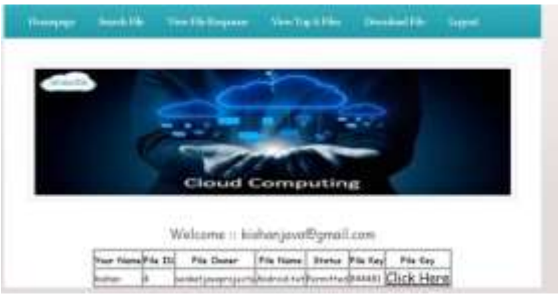
Search Response



View Your File Requests

Request From	File ID	File Owner	File Name	Status
kishan	4	venkatjavaprojects	[illegible].txt	[illegible]

Generate Key



Welcome :: kishanjava@gmail.com

Your Name	File ID	File Owner	File Name	Status	File Key	File Key
kishan	8	[illegible]	Android.txt	Permitted	[illegible]	Click Here

File Download Success

Conclusion

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 transferreddata 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] 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 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. [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] 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,Xi’an, China, pp.17–23, 2016. [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] 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] 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] 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] 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] 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] 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] 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] 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.