International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-12 Issue-02 Oct 2023
https://ijgst.com.2023.v12.i2.pp149-159

A Secured Data Migration Mechanism for Data Owners in Cloud Computing

B SUNIL KUMAR[1] S UDAYA LAKSHMI[2] K INDUMATHY[3] ERUGU SAI KUMAR[4]
[1]ASST.PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[2] ASSOC. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[3]ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[4] ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[1,2,3,4] SRI MITTAPALLI COLLEGE OF ENGINEERING

Abstract

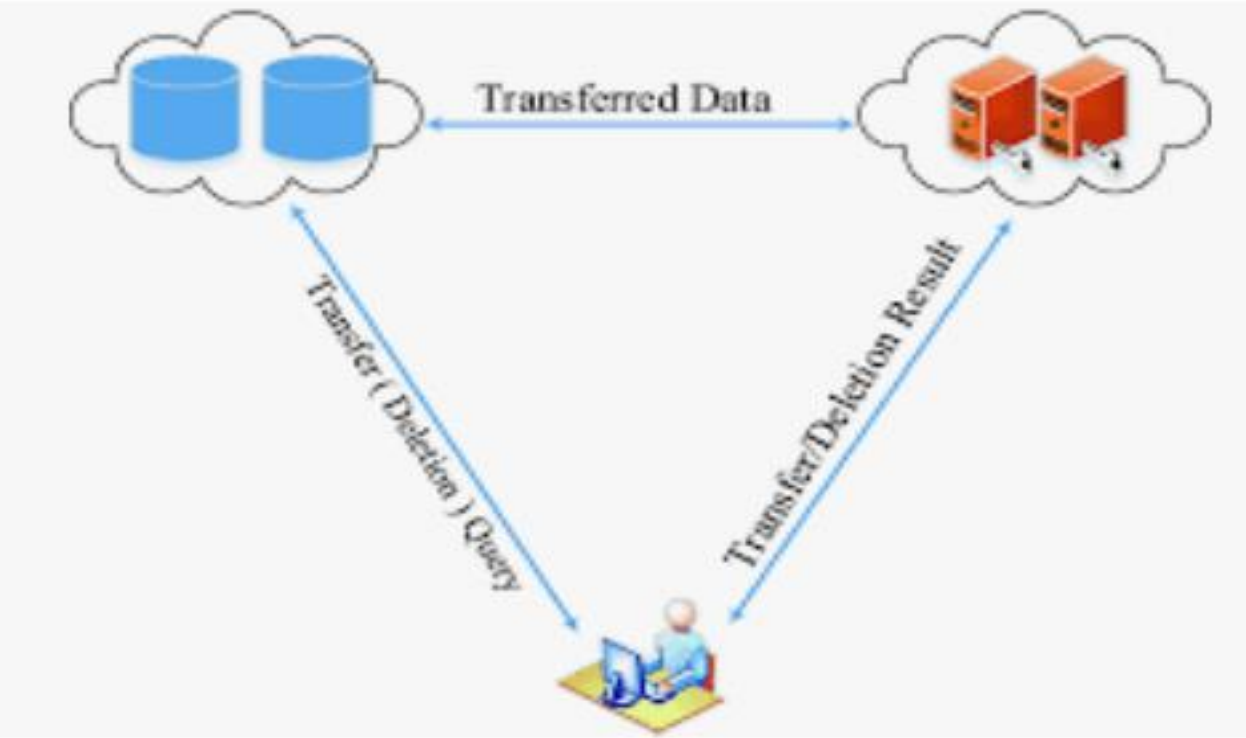
The rapid expansion of cloud capacity has attracted more and more data owners who are looking to re-appropriate their data to the cloud worker, which may drastically reduce the overhead of local storage. It is now an absolute necessity for data owners to switch cloud service providers due to the fact that different cloud providers provide different types of data storage management (e.g., security, reliability, access speed, and cost). Data owners are understandably concerned about the best practices for transferring data securely to a new cloud while permanently erasing it from the original. In this study, we provide an alternative approach to this problem, one that is based on the Bloom channel. Not only can the suggested conspiracy comprehend permanent data deletion, but it can also execute safe data transfer. The public evidence may be satisfied by the suggested approach as well, and no trusted third party is needed for this. Last but not least, we also encourage a recreation execution that proves our proposal is practical and sensible.

I. Introduction

One emerging and promising computing paradigm, known as "cloud computing," integrates computer resources, organisation transmission capabilities, and wide-area conveying capacity assets [1,2]. Using these resources, it can provide residents with several excellent cloud services. Asset limitation information owners can reevaluate their data to the cloud worker, which can significantly reduce the owners' neighbourhood storage overhead[5,6]; this is one of the many appealing benefits of the administrations, which have led to their widespread application [3,4]. Cisco predicts that by the end of 2019, the number of Internet users will reach 3.6 billion, with around 55% of that figure using cloud storage services. With the economy looking up, more and more companies (including Alibaba, Microsoft, and Amazon) are offering cloud storage services to data owners at varying prices, levels of security, and with varying levels of access speed, among other factors. Cloud storage specialist co-ops are an option for data owners looking for better cloud storage management. Thus, criminals may

copy their stolen data to a different cloud, then delete it from the original cloud. Cisco predicts that by the end of 2021, cloud traffic will account for 95% of all traffic, with inter- a crucial need. A redesigned data transfer program, Cloudsfer[8], has been developed to provide safe data transfer by using cryptographic computation to prevent security disclosure during the exchange process. Nevertheless, when getting ready to move data to the cloud, there are still certain security concerns. addition to that, deletion. To start, in order to save money, the cloud worker may just transfer a portion of the information, or they may intentionally send some irrelevant data in an effort to trick the owner of the data [9]. Some information squares may also be missing during the exchange interaction due to organisational vulnerability. And all the while, the bad guys .

cloud traffic accounting for about 14% of that total. From the point of view of the data owners, the reevaluated data transfer will inevitably become
may wipe out the relocated data blocks [10]. It follows that the transferred data may get contaminated as a result of the movement contact. Finally, the first cloud worker could have malicious intent by hoarding the transferred data in order to reap certain advantages [11]. As far as the data owners are concerned, the data reservation is shocking. Therefore, although cloud storage is financially attractive, it does encounter some real security issues, particularly with regard to the transfer of sensitive data, reliability checks, and cancellations. If these problems aren't solved rationally, cloud storage management could not be accepted or used by the general public



II. Literature Survey

1. Techniques for Searching Encrypted Data That Are Actually Useful
Encrypting data stored on data storage workers, such mail workers and record workers, is appealing since it reduces security and protection threats. But this usually means you have to sacrifice some functionality for security. For example, what if a client wants to get just reports that include a certain set of words? Up until now, there hasn't been a solution that allows the data warehouse worker to search and answer the question without compromising data confidentiality. Our cryptographic strategies for decrypting data during searches are detailed in this article, along with proofs of security for the crypto frameworks that emerge from them. Several immediate advantages are associated with our methods. Their security may be proven: Among their features are the following: provable mystery in encryption, which means that an untrusted worker cannot decipher the plaintext even when provided with the ciphertext; query isolation in searches, which means that an untrusted worker cannot decipher the plaintext beyond the search result; controlled searching, which prevents the untrusted worker from searching for a self-assertive word without the client's permission; and covered up questions, which allow the client to ask the untrusted worker to search for a mysterious word without divulging the word. We offer simple, fast, and practically space-and communication-efficient algorithms that may be used today with little to no overhead (for a lengthy report, the encryption and search algorithms only need stream code and square code operations).

2. Cloud computing technologies that are smart: semantic search using validated keywords
As the pay-as-you-go paradigm of cloud computing gains traction, customers are being inundated with cloud services. Although this is very helpful for intelligent terminal users, selecting the right cloud services or solutions may be a significant issue. The goal of consumer-driven cloud computing has a fundamental issue in enabling a smart cloud search conspire. Encryption is a standard practice for protecting sensitive data before transmission. Although existing searchable encryption solutions do enable clients to search across encrypted data, the fact that they only permit narrow keyword searches drastically restricts data convenience. The aforementioned tactics also don't promise a specific result from a search. In order to decrease processing cost or download data transmission, cloud workers typically execute partial search operations or offer partial findings. This makes them seem self-centred, semi-honest, and inquisitive. Finding a way to make encrypted cloud data more adaptive while yet guaranteeing the consistent veracity of search results is a major task. The authors of this study provide a clever semantic search method for test management that provides the actual and semantic results of a keyword-based match. The search result and the conspiracy theory are both supported by the

evidence. All of the performance and security tests run under the provided model show that the proposed design accomplishes the purpose of keyword-based semantic search.

3. Developing efficient cloud search services: ranking multi-keyword searches over encrypted cloud data with synonym query assistance

Using the cloud is turning out to be more commonplace. The conventional and effective plaintext keyword search approach is rendered useless by the fact that sensitive data should be encrypted by the data owner prior to outsourcing in order to guarantee data security. Unfortunately, semantics-based multi-keyword ranked search is currently not supported by any searchable encryption schemes. The only options available are cautious or fluffy keyword searches. There is a good chance that cloud clients' searching input will be synonyms of the predefined keywords rather than specific or fluffy matching keywords in a real search scenario. This is due to the possibility of synonym substitution (reproduction of information content) and her lack of thorough data knowledge. Consequently, there is still a difficult problem with synonym-based multi-keyword ranked search using encrypted cloud data. For the first time in this work, we provide a solution to the problem of encrypted cloud data searching using synonyms and multiple keywords. Our primary areas of contribution are synonym-based search and multi-keyword ranked search. The former helps with synonym queries while the latter produces more precise search results. The two risk models—" the known ciphertext model and the realised foundation model—are addressed by two safe strategies. While basic plot does not accept the use of bogus keywords, enhanced plot does, greatly ensuring the sensitive recurrence information. We validate the offered plans' correctness and protection-preserving certainty by conducting a security analysis. Our analysis is supported by extensive testing on real-world datasets, which demonstrate the high efficiency and effectiveness of our suggested approach for synonym-based searching.

4. Efficient semantic search over encrypted data in cloud computing

The many benefits that cloud storage offers over more conventional capacity options have contributed to its meteoric rise in popularity. Despite the many benefits of cloud storage, several security concerns have also surfaced, discouraging organisations from transferring their data to the cloud. So, before putting sensitive information on the cloud, owners encrypt it. Data security is improved by encryption, but searchability and search efficiency are negatively affected. A number of strategies that enable keyword searching on encrypted data in the cloud have recently become the subject of investigation. Regardless, these strategies have flaws that render them impractical when put into practice. In this research, we proposed a framework—named "Synonym-Based Keyword Search (SBKS)," "Wikipedia-Based Keyword Search (WBKS)," and

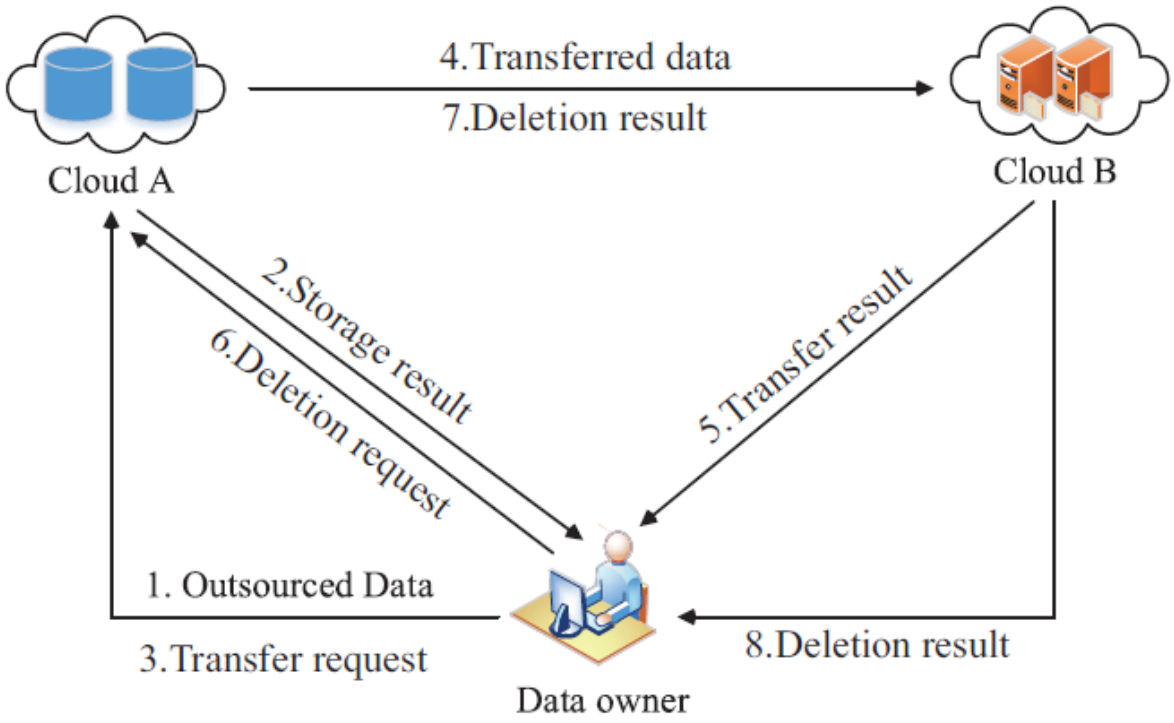
Wikipedia-Based Synonym Keyword Search (WBSKS)"—to facilitate semantic search on encrypted data stored in the cloud. Our results showed that compared to the previous designs, ours are more efficient in terms of performance and capacity requirements. Thus, compared to the earlier ideas, ours have greater potential for success.

5. Secure private cloud data semantic search with similarity ranking

More and more people are transferring their data to the public cloud as a result of cloud computing because of the convenience and cost advantages it offers. Still, encryption is a necessary for protecting sensitive data. Searching encrypted cloud data has proven to be a formidable challenge when it comes to implementing optimal data utilisation. The provided query keyword was the only determinant in the previous methods, which ignored the meaning of the word. Consequently, the search strategies lack intelligence and fail to include reports that are semantically relevant. With this shortcoming in mind, we provide a similar search solution based on semantic expansion that operates over protected cloud data. In addition to returning records that are directly related to the query, our solution might also provide documents that include phrases that are semantically related to the query. For every record, the suggested conspiracy builds a matching document metadata. Once the collection of documents and encrypted information are ready, they are sent to the cloud worker. Cloud workers take a collection of information and use it to build an inverted index and a semantic relationship library (SRL) for a set of keywords. The first thing a cloud worker does after getting a query demand is look up the SRL-identified keywords that are semantically related to the query keyword. The documents are retrieved using a combination of the query term and extensional words. Based on the overall relevance score, the requested result records are returned. Ultimately, our method is safe and preserves data according to the previous searchable symmetric encryption (SSE) security specification, as shown by thorough security assessment. Findings from an exploratory assessment show how well the strategy works.

International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-12 Issue-02 Oct 2023
https://ijgst.com.2023.v12.i2.pp149-159

III. The Proposed Scheme : We lay forth our new plan for you. Take note that the organisation specialising in distributed storage has to verify the owner of the data. The data owner has become



a genuine resident of both cloud A and cloud B, and we will assume this for the sake of simplicity.

1. Overview

In our situation, In the same vein as Ref.[26], we want to achieve irrefutable data transmission and destruction. Figure 4 depicts the basic cycles. Before sending the encrypted data to cloud A, the data owner must first encrypt it and then assess the ciphertext. After that, he deletes the neighbourhood reinforcement and verifies the capacity result. After that, the data owner may switch to cloud B and transfer some data from cloud A by changing the cloud capacity specialist cooperative. The data owner must next verify the successful completion of the transfer. Finally, after a successful data transfer, the data owner requests that cloud A delete the transmitted data and verifies that the deletion was successful.

2. The concrete scheme

Our new proposed scheme contains the accompanying six calculations.

1) Initialization

Create separate ECDSA public private key sets for the data owner, cloud A, and cloud B, respectively, using the formats PKO, SKO, PKA, and PKB. Next, the data owner selects k safe hash functions g1, g2, •, gk, all of which map each index from 1 to N to distinct cells in CBF, i.e., gi : [1,N] → [1,m]. In addition, before uploading a document to cloud A, the data owner chooses a memorable tag.

2Encryption of data Before sending the revised document, the data owner uses a safe encryption algorithm to encrypt it.

i) The owner of the data first stores the encryption key k = H(tagf ||SKO) and then uses it to encrypt the document C = Enck(F), where Enc is an IND-CPA safe encryption solution. In order to make sure that the CBF remains valid after data transmission and deletion, the data owner first divides the ciphertext C into n′ blocks. While doing so, they insert n−n′ irregular squares into the n′ blocks at random places. After then, these random occurrences are documented in table PF by the data owner.
ii) The owner of the data blocks (Ci) randomly selects an integer representing Ci and processes the hash values (Hi) as H(tagf ||ai||Ci). Therefore, D = ((a1,C1), •, (an,Cn)) may be used to represent the revised dataset. Finally, using the document tag tagf, the data owner transmits D to cloud A.

3) Data outsourcing

The data owner transfers certain data blocks, or even the whole document, from cloud A to cloud B whenever he chooses to change service providers.

i) step in determining which data blocks should be moved is for the data owner to create a file containing a sequence of block lists (ώ). At this point, the data owner determines a signature sigt = SignSKO(transfer||tagf ||ϕ||Tt), where Tt is a timestamp. After that, the data owner sends a transfer request to cloud A using the formula Rt = (transfer, tagf, ϕ, Tt, sigt). At the same time, cloud B receives the hash values {Hi}i∈ϕ from the data owner.
ii) Cloud A checks the legitimacy of the transfer demand Rt upon receipt. Cloud A sends the input data blocks {(ai,Ci)}i∈ϕ, the mark sigta, and the transfer demand Rt to cloud B. Cloud A will halt and express displeasure if Rt is invalid. In every other case, cloud A adds a mark sigta = SignSKA(Rt||Tt).

4) Data transfer

When the data owner decides to switch service providers, he moves certain data blocks—or perhaps the whole document—from cloud A to cloud B.
i),in order to identify which data blocks need to be relocated, the data owner generates a series of block lists (ώ) in a file. The data owner then works out a signature sigt = SignSKO(transfer||tagf ||ϕ||Tt), where Tt is a timestamp. Following this, the data owner generates a transfer request Rt = (transfer, tagf, ϕ, Tt, sigt) and then transmits it to cloud A. Meanwhile, the owner of the data transmits the hash values {Hi}i∈ϕ to cloud B.
ii) When cloud A receives the transfer demand Rt, it verifies its authenticity. The data blocks {(ai,Ci)}i∈ϕ, the mark sigta, and the transfer demand Rt are sent to cloud B by cloud A. If Rt is not valid, cloud A pauses and returns disappointment. Otherwise, cloud A processes a mark sigta = SignSKA(Rt||Tt).

5) Transfer check

The cloud B needs to check the accuracy of the transfer and returns the transfer result to the data proprietor.

i) Cloud B verifies the authenticity of the transfer request (Rt) and the mark (SigTA) before proceeding. Cloud B will terminate and produce disappointment if none of them is significant. Otherwise, it will verify whether the condition Greetings = H(tagf ||ai||mi) holds, where I is an element of. If Hi is equal to or greater than H(tagf ||ai||Ci), then cloud B requests that cloud A transmit (ai,Ci) again; otherwise, cloud B proceeds to Step ii).
ii) With the use of the files {ai}i∈ϕ, cloud B creates an additional tallying Sprout channel CBFb and stores the squares {(ai,Ci)}i∈ϕ. Sigtb = SignSKB(success||tagf ||ϕ||Tt||CBFb) is the signature that cloud B figures out afterwards. Data owner receives the transfer proof π = (sigta,sigtb,CBFb) from cloud B finally.
iii) After receiving π, the transfer outcome is checked by the data owner. The data owner verifies the authenticity of the mark sigtb, to be clear. At the same time, to verify that the tallying Bloom channel CBFb is accurate, the data owner randomly selects half of the records from set ϕ. The owner of the data believes the confirmation of transfer is significant and that cloud B retains the transmitted data honestly if and only if all of the tests pass.

6) Data deletion

Following a successful transfer to cloud B, the data owner may request that cloud A delete certain data blocks.

i) tamp Td is appended to the data owner's mark sigd by using the SignSKA function on delete, tagf, ϕ, and Td. The data owner then generates a data deletion request Rd = (erase, tagf, ʕ, Td, sigd) and sends it out, but it's not A.
ii) Cloud A verifies Rd after receiving it. Cloud A will terminate and return disappointment if Rd is invalid; else, it will delete the data blocks.

IV. Security Analysis

1. Protecting personal information Data confidentiality ensures that no one other than the comparing data unscrambling key can access any plaintext data. As part of our strategy, the data owner encrypts the file using the IND-CPA safe AES algorithm. Data unscrambling key k = H(tagf ||SKO) is recorded in the meanwhile, where H is protected hash capacity and SKO is the secret private key. Because of this, the adversary is unable to successfully generate a large data decoding key. In addition, the owner of the data maintains the key to decrypting it a secret. If an adversary were to get their hands on the decryption key, they would also have access to the plaintext data.

2. Data integrity

To ensure data integrity, make sure the sent data is error-free; otherwise, cloud B would reject it. Cloud B tests the condition Hi = H(tagf ||ai||Ci), where I ∈ ϕ, after receiving the hash values Hi from the data owner and the transferred data (ai, Ci) from cloud An. Please be informed that the data owner uses a protected hash function to determine {Hi}i∈ϕ.

3. Public verifiability

We dissect the cancellation result and the exchange outcome separately to see how verifiable they are.
The possession of move verification and move demand Rt allows the verifier to verify the outcome of the exchange. In instance, before doing anything further, the verifier ensures that Rt is legitimate. Assuming Rt is true, it means the data owner explicitly requested to transfer the data to cloud B. Next, the verifier double-checks the sigta and sigtb markings to make sure they're legitimate. Keep in mind that cloud B will not conspire with cloud A in an evil way to trick the data owner. Thus, the returned move result may be trusted by the verifier, provided that both marks are authentic. In addition, the verifier confirms the checking Bloom channel CBFb to see whether cloud B really maintains the sent data. In addition, the cancellation outcome may be confirmed by the verifier who has erasure evidence τ and erasure demand Rd. The verifier first ensures that Rd is legitimate. Assuming Rd is not valid, it means the data owner never needed to delete the data; nonetheless, the verifier double-checks the mark sigda's authenticity and the correctness of the counting Bloom channel CBFd. The verifier will accept the cancellation proof τ as correct if and only if all the tests are passed. Keep in mind that the verifier is not required to have access to any sensitive data in order to certify the outcomes of the exchange and deletion. Our proposal is able to meet the requirements of public verifiability.

V. Conclusion

When using distributed storage, the data owner has no guarantee that the cloud worker will act honestly when transferring or erasing data. We provide a CBF-based secure data transfer method that can also recognise irrefutable data deletion as a solution to this problem. Our strategy calls for using cloud B to verify the integrity of the sent data, which will guarantee its complete transfer. Cloud An should also use CBF to generate an erasure cancellation proof that the data owner may use to verify the cancellation outcome. Therefore, cloud A is unable to successfully do malicious acts in order to deceive the data owner. Finally, our proposal has been independently validated as secure and feasible by the results of the security analysis and the reenactment.Our strategy, like other existing ones, takes into account the transfer of data between two separate cloud workers. Regardless, as events unfold with dispersed storage, the data owner may simultaneously have to move the re-appropriated data from one cloud to another, perhaps involving at least two separate goal mists. All the same, the multi-target mists may plot vengeful fraud against the data owner. We must thus do more research on the transfer of demonstrable data over a minimum of three fogs.

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 deduplicationtechniques 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.
[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*,
[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 cloudstorage 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] LAKSHMI, MANNAM SWARNA, and KALE MASTHAN RAO. "Dynamic Audit Services for Cloud Outsourced Storages with Key Updates." (2017).

[21] GUPTA, DR K. GURNADHA. "A PRODUCTIVE IBPRE MODEL FOR SECURE DATA SHARING IN BLOCKCHAIN TECHNOLOGY BASED IOT."