IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue, 5, March 2019 E-ISSN: 2347-2693

A Review on Fragmented hash based Storage techniques for Query Processing in Cloud Data Storage

Jegadeeswari [1*], Dinadayalan [2], Gnanambigai [3]

[1]Bharathiar University, Coimbatore, Tamil Nadu, India
[2]Department of Computer Sci, Kanchi Mamunivar Centre for Postgraduate Studies, Puducherry, India
[3]Department of Computer Sci, Indira Gandhi College of Arts and Science, Puducherry, India

**Corresponding author: jega_sathya@yahoo.co.in*

DOI: https://doi.org/10.26438/ijcse/v7si5.225229 | Available online at: www.ijcseonline.org

***Abstract*—** Cloud Computing is a potential paradigm employed for the deployment of applications on the Internet. Cloud is an on-demand computing service that offers a dynamic environment for the users to guarantee Quality of Service (QoS) onjjjjj' data in cloud data centers. Security is an important role in cloud data storage while the services provided storing the data in the cloud. Most of the research works have been designed for secure cloud data storage. However, cloud users still have security issues with their outsourced data. In order to overcome such issues, we surveyed towards the fragmented hashing methods and data storage techniques in cloud. The main goal of this survey is to analysis the different method towards hashing and security methods to store data in cloud environment based on the metrics for different methods on the performance in terms of execution time and data retrieval efficiency.

***Keywords*—** Cloud data storage, Cloud users, Security, Confidentiality, Fragmented data, Query Processing

I. INTRODUCTION

Cloud Computing is a potential paradigm employed for deployment of applications on Internet. Cloud is an on-demand computing service that offers a dynamic environment for users to guarantee Quality of Service (QoS) on data for its secrecy in cloud data centers. Cloud applications utilize large data centers and efficient servers that host web applications and services. In addition, Cloud storage is a model of networked storage system in which data is stored in pools of storage that are usually hosted through third parties. There are numerous benefits to utilize cloud storage. The most significant is data accessibility. Data stored in the cloud can be accessed at any time from any place. Another benefit of cloud storage is data sharing among users.

The cloud users outsource their data to the remote cloud storage for reducing the storing cost. The third- party auditor is a partially trusted and independent entity that assesses the data and arbitration if necessary. The cloud users interrelate with cloud server for accessing and updating data stored in cloud. The key issues in cloud data storage is security owing to possible unauthorized access within cloud service providers. With the development and application of cloud computing, the security becomes more and more important. Due to the unauthorized access of cloud service providers, security is the main issue in a cloud environment.

Fragmentation is a technique in which the data can be stored in different cloud data centers by means of fragmenting the whole database into several pieces termed fragments. To implement confidentiality on data, the fragmentation is applied on the cloud data. A Fragment is a distributed database design technique to divide a single relation or a class of a database into two or more partitions such that a combination of the partitions provides the original database without any loss of information. The main purpose is to ensure the confidential data is protected from potential attackers.

The hashing technique allows the hash function to be modified dynamically to accommodate the growth or shrinking of the database. The dynamic hashing that grows to handle more items. The associated hash function must change as the table grows. A hash table or hash map is a data structure that uses a hash function to map identifying values, known as keys, to their associated values. The hash function is used to transform the key into the index (the hash) of an array. The hash function should map each possible key to a unique slot index. Hash table algorithms calculate an index from the data item's key and use this index to place the data into the array. The hash function calculates an index within the array from the data key. The data array length is the size of the array.

The survey is carried out in the following objectives,

- To achieve data security through confidentiality

- To provide multitenant access in cloud
- To attain the integrity trust assessment on cloud

The rest of this paper is organized as follows. Section II explains about related work done on the fragmentation and confidentiality. Section III and IV explains Fragmented hashing, Neural Network based Cryptography and secured data storage methods with merits and demerits table to analysis different technique. Finally, Section V concludes this paper.

II. RELATED WORK

The paper focuses on different methods to implement on the data security and data storage in the cloud which addresses the customers view towards data confidentiality. The main objective of the survey is to analysis the methods used to defend outsourced data from attackers and from curious cloud providers by using cloud data fragmentation model.

Several research works have been designed for cloud data security. For example, an efficient secure-channel free public key encryption with keyword search (SCF-PEKS) scheme was designed in [1] for improving the security of cloud data storage. However, the time taken for securing the data is higher. A multi-user searchable encryption scheme with keyword authorization (MSESKA) was intended in [2] for cloud storage. Though, the security was inadequate.

A Public Key Encryption with Keyword Search (PEKS) was developed in [3] for solving security vulnerability in cloud data storage. But, data confidentiality remained unaddressed. A new scheme was presented in [4] for encrypting the outsourced database and query points that protect key confidentiality and query controllability mutually with higher data privacy and query privacy. But, protecting the data access patterns from cloud server was not considered.

An efficient inner-product predicate encryption system was developed in [5] that support privacy preserving predicate encryption for Cloud storage. However, the execution time was higher. A Symmetric Encryption Algorithm (SEA) was applied in [6] for enhancing data security in the cloud storage. Though, SEA lacks security during data storage. A novel mechanism was designed in [7] by combining data fragmentation with encryption to protect the privacy of data.

An efficient data storage security model was developed in [8] for cloud service in which partitioning of data facilitates storing of the data in easy and effective manner. But, the security level was poor. The review of diverse encryption technique designed for protecting the cloud data storage was analyzed in [9]. A cryptographic tree-based key management and authentication system were presented in [10] to enhance the security and privacy of outsourced data in the cloud. However, data storage security level was not sufficient.

A privacy-preserving and auditing-supporting outsourcing data storage scheme was designed in [11] to achieve data integrity in the cloud computing environment. Though, data confidentiality was not achieved. A secure ciphertext self-destruction scheme with attribute-based encryption called SCSD was presented in [12] to enhance the security of cloud storage environment. But, the encryption performance was not efficient.

A Trust Enhanced Cryptographic Role-Based Access Control was employed in [13] to enhance the security of cloud storage systems. A two-factor data security protection mechanism with factor revocability was presented in [14] for cloud storage system to improve the confidentiality of the data. However, the security level was poor due to a potential practical risk.

A secure cloud storage system was intended in [15] that assist privacy-preserving public auditing for achieving higher storage security. An effective and flexible distributed Scheme with explicit dynamic data support was presented in [16] to authenticate the correctness of users' data in the cloud.

In [17], a secure, lightweight, robust, and efficient scheme was implemented for data exchange between the mobile users and the media clouds to achieve better cloud data storage security. A secure e-stream cipher-based encryption/decryption method was presented in [18] for providing security to the user's sensitive data at cloud data center. However, flexibility, reliability and scalability were not considered.

A probabilistic challenge-response scheme was intended in [19] to protect servers from collusion in cloud storage. Though, computation and communication overhead was more. A survey of the different type of cryptographic techniques designed for secure cloud data storage was analyzed in [20]. Data sharing method was developed in [21] with the aid of Oblivious random access memory (ORAM) for cloud data storage. However, the performance of cloud data storage was not efficient. An encryption method depended on keyword searchable attribute was presented in [22] for cloud storage. But, the data confidentiality level remained unaddressed in encryption method.

An integration of lattice signature and Bloom Filter theory was designed in [23] for preserving of user data privacy in cloud storage. Though, the security of data storage was not sufficient. In [24], cryptographic defense method was described for securing the cloud storage while accessing cloud data. But, the time consumption was not reduced.

III. ANALYSIS OF DIFFERENT METHODS FOR DATA FRAGMENTATION, HASHING AND NEURAL NETWORK CRYPTOGRAPHY

The different method of Data Fragmentation and Neural Network cryptography techniques are compared with the existing methods of fragmentation with merits and demerits. The review for the performance is analysis on the techniques with the following metrics such as execution time and data retrieval efficiency.

Secure-channel free public key encryption Method

Secure-channel free public key encryption with keyword search (SCF-PEKS) method was designed in [1] for improving the security of cloud data storage, in which two types of diversity, namely, a malicious server and a malicious user. A malicious server should not be able to distinguish which keyword corresponds to a given keyword ciphertext without the trapdoor from a receiver. A malicious user (including the receiver) should not be able to distinguish which keyword corresponds to a target ciphertext without the server's private key even s/he has the trapdoor of the keyword. Searchable encryption is an important cryptographic primitive that enables privacy-preserving keyword search on encrypted data.

Multi-user Searchable Encryption Scheme with Keyword Authorization Method

Multi-user Searchable Encryption Scheme with Keyword Authorization (MSESKA) Method was intended in [2] that allow a user to securely outsource its files and also allow some designated users to search its files in encrypted form on cloud storage. This method allows a user to encrypt its files in such a way that these files can be searched by other users that have been authorized by the data owner. This method satisfies the following properties: concise indexes, sublinear search time, security of data hiding and trapdoor hiding, and the ability to efficiently authorize or revoke a user to search over a file. The method enable a user to authorize other users to search for a subset of keywords in encrypted form. The asymmetric bilinear map groups of Type-3 and keyword authorization binary tree (KABtree) to construct this method that achieves better performance, but security is inadequate.

Asymmetric key fragmentation Method

Asymmetric key fragmentation (AKFS) was designed in [17] for improving the security of private data in a cloud environment. This method divides up the encryption key into multiple fragments and that can designate a single fragment as the mandatory fragment. Here it is implemented by designating a single fragment for the encryption key and for defragmentation among multiple fragments and also it can block the defragmentation without that mandatory fragment. This method is used to manage encryption key safely when it comes to ownership guaranteed security framework. This is designed for a secure cloud data storage and to improving the security of private data in a cloud environment. It can resolve both threat from the malicious insider and the user's mistake in same time. The security level of private data is not sufficient.

A two-factor data security protection Method

A two-factor data security protection mechanism was designed in [8] for cloud storage system and to improve the confidentiality of the data in cloud. But, storage complexity was higher. This system allows a sender to send an encrypted message to a receiver a server. The sender only knows the identity of the receiver but no other information (its public key). The receiver possesses two things in order to decrypt the ciphertext. The first secret key and second thing is a unique personal security device. It is to decrypt the ciphertext without either piece. It cannot be used to decrypt any ciphertext. This can be done by the cloud server which will immediately execute some algorithms to change the existing ciphertext to be un-decryptable by this device. The process is completely transparent to the sender and the cloud server cannot decrypt any ciphertext at any time. The security and efficiency analysis show that this method is not only secure but also practical. Even security device is stolen or lost, this device is revoked and cannot be used to decrypt any ciphertext.

Fragmentation Method

Fragmentation technique is the normalized data tables are regarded as standalone fragments that are then distributed at different Cloud storage providers. This procedure is applied to relational databases where the tables are treated as independent fragments. Additional confidentiality constraints depend on the data's domain into account. Fragmentation technique which is efficiently stores the data on CSP servers using the minimum possible amount of encryption. Appropriate numbers of Cloud Service Provider (CSP) are determined, to design the fragments according to user requirements and confidentiality level. Decent testing on the cloud environment is not carried out in Fragmentation technique.

Indexing encrypted Data based on direct encryption and hashing method

Indexing encrypted Data based on direct encryption and hashing uses hash function to compute values of two attributes of different tables on which the equality predicate is evaluated in the context of a join query. Determine the proper balance between index efficiency and protection. Measure of inference exposure on the indexed data that nicely models the problem in terms of graph auto morphisms. This method increases the ability to select a set of tuple in response to a query and associated with each encrypted tuple a number of indexing attributes. Hash-based method for database encryption is suitable for selection queries. Direct

encryption provide an adequate level of security against inference attacks and still encryption needs to protect the data integrity on the cloud infrastructure. Data confidentiality and integrity together put us into risk by outsourcing data storage and management

Fragmentation and Encryption method

Fragmentation and Encryption method approach is allowing the protection of confidentiality of sensitive information in outsourced multi-relational databases by improving on combination of fragmentation and encryption improve the security of the querying technique in order to protect data confidentiality under collaborative Cloud storage service providers. This method that have used to decompose multi-relational databases in the aim to protect sensitive associations querying technique to optimizes and executes queries in distributed system the security of the querying technique in order to protect data confidentiality under a collaborative Cloud storage. The query optimization and execution techniques to overcome processing of nested queries are limitations of this approach.

IV. DATA FRAGMENTATION BASED NEURAL NETWORK CRYPTOGRAPHY TECHNIQUE FOR CLOUD DATA SECURITY

The Data Fragmentation methods are dividing the user data into a number fragments and Neural Network Cryptography method is to implement security in storing data. These are the objectives to improve data security and confidentiality in a cloud environment.

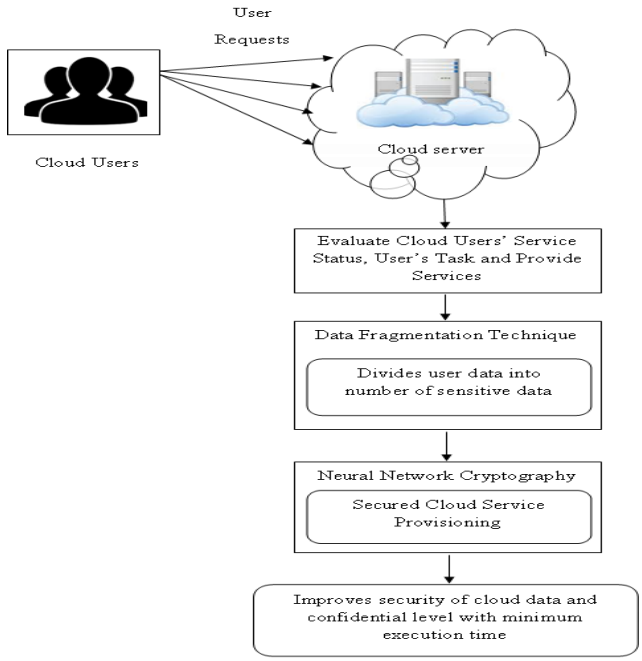

Figure 1 Architecture Diagram of Data Fragmentation Based Neural Network Cryptography for Cloud Data Security

These methods used in Data Fragmentation Technique to divide the sensitive datasets into a number of fragmented sensitive data for efficient data isolation. Besides, neural technique employed Neural Network Cryptography to encrypt and decrypt the fragmented sensitive data. For performing encryption and decryption, the Neural Network Cryptography used to feed forward and back propagation concepts. Therefore, neural methods achieve higher cloud data security during the service provisioning. As a result, these techniques are efficient and effective for all types of user's queries and also provide a higher level of data confidentiality for cloud service provisioning. The data flow of this te**c**hnique for cloud data security is shown in above Figure 1. Initially a user request is sent to the cloud server. The cloud server analyzes cloud users' service status, user task for providing services to the cloud user. After that, data fragmentation technique is used for dividing the user data into a number of sensitive data in order to obtain the high confidential sensitive data for encryption. In research many technique are used to implement. The high confidential sensitive data is encrypted by using the Neural network Cryptography to improve the security of cloud data service and confidentiality has been implement efficiently with the neural concepts with lower execution time.

V. CONCLUSION

In this discussion we found various solutions to implement the hashing and security methods for data storage on cloud. An effective survey on Data Fragmentation towards hashing and cryptography methods is analyses to provide higher security and confidentiality while accessing data from a cloud server. However, despite of this it also have some weak area to work upon. The various survey hashing and security mechanisms are implemented using Data Fragmentation. The effectiveness of these techniques has been analyses with the metrics such as execution time, data confidential level, cloud data security and storage space. With these methodologies, it is expressive that the cloud data security and data confidential level provides more precise results for cloud service provisioning when compared to state-of-the-art works.

REFERENCES

[1] Lifeng Guo, Wei-Chuen Yau, "Efficient Secure-Channel Free Public Key Encryption with Keyword Search for EMRs in Cloud Storage", Journal of Medical Systems, Springer, Volume 39, Issue 11, Pages 1-11, 2015.

[2] Zuojie Deng, Kenli Li, Keqin Li and Jingli Zhou, "A multi-user searchable encryption scheme with keyword authorization in cloud storage", Future Generation Computer Systems, Elsevier, Pages 1-25, 2016.

[3] Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo, Xiaofen Wang, "Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 4, Pages 789 – 798, April 2016.

[4] Youwen Zhu, Zhiqiu Huang, Tsuyoshi Takagi, "Secure and controllable k-NN query over encrypted cloud data with key confidentiality",

Journal of Parallel and Distributed Computing, Elsevier, Volume 89, Pages 1–12, March 2016.
[5] Xu An Wang, Fatos Xhafa, Weiyi Cai, Jianfeng Ma, Fushan Wei, "Efficient privacy preserving predicate encryption with fine-grained searchable capability for Cloud storage", Computers and Electrical Engineering, Elsevier, Volume 56, Pages 871–883, November 2016.
[6] Ramalingam Sugumar and Sharmila Banu Sheik Imam, "Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage", Indian Journal of Science and Technology, Volume 8, Issue 23, Pages 1-5, 2015.
[7] Valentina Ciriani, Sabrina De Capitani Di, Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati, "Combining fragmentation and encryption to protect privacy in data storage", ACM Transactions on Information and System Security (TISSEC), Volume 13 Issue 3, Pages 1-33, July 2010.
[8] Swapnil V.Khedkar , A.D.Gawande, "Data Partitioning Technique to Improve Cloud Data Storage Security", International Journal of Computer Science and Information Technologies, Volume 5, Issue 3, Pages 3347-3350, 2014.
[9] R.Kirubakaramoorthi, D. Arivazhagan and D. Helen, "Survey on Encryption Techniques used to Secure Cloud Storage System", Indian Journal of Science and Technology, Volume 8, Issue 36, Pages 1-7, 2015.
[10] Pothula Sujatha, "An Authentication Based Secure Data Storage in Cloud Computing", International Journal of Advanced Computing and Electronics Technology (IJACET), Volume 1, Issue 1, Pages 8-13, 2014.
[11] Xinyue Cao, Zhangjie Fu and Xingming Sun, "A Privacy-Preserving Outsourcing Data Storage Scheme with Fragile Digital Watermarking-Based Data Auditing", Journal of Electrical and Computer Engineering, Hindawi Publishing Corporation, Volume 2016, Article ID 3219042, Pages 1-7, 2016.
[12] Tonghao Yang, Junquan Li, and Bin Yu, "A Secure Ciphertext Self-Destruction Scheme with Attribute-Based Encryption", Mathematical Problems in Engineering, Hindawi Publishing Corporation, Volume 2015, Article ID 329626, Pages 1-8, 2015.
[13] Lan Zhou,Vijay Varadharajan,and Michael Hitchens, "Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage", IEEE Transactions on Information Forensics and Security, Volume 10, Issue 11, Pages 2381 – 2395, 2015.
[14] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, Yang Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System", IEEE Transactions on Computers, Volume 65, Issue 6, Pages 1992 – 2004, 2016.
[15] Wenjing Lou, Kui Ren, Qian Wang, Sherman S.M. Chow, Cong Wang, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, Volume 62, Issue 02, Pages 362-375, 2013.
[16] Yogesh V. Bhapkar, Rakesh S. Gaikwad, Milind R. Hegade, "Providing Security and Privacy to Cloud Data Storage", International Journal of Computer Science and Information Technologies, Volume 6, Issue 2, Pages 969-971, 2015.
[17] Muhammad Usman, Mian Ahmad Jan, Xiangjian He, "Cryptography-based secure data storage and sharing using HEVC and public clouds", Information Sciences, Elsevier, Volume 387, Pages 90–102, 2017.
[18] Dharavath Ramesh, Rahul Mishra, Damodar Reddy Edla, "Secure Data Storage in Cloud: An e-Stream Cipher-Based Secure and Dynamic Updation Policy", Arabian Journal for Science and Engineering, Springer, Pages 1–11, 2016.
[19] Tao Jiang, Xiaofeng Chena, Jin Li, Duncan S. Wong, Jianfeng Ma, Joseph K. Liu, "Towards secure and reliable cloud storage against data re-outsourcing", Future Generation Computer Systems, Elsevier, Volume 52, Pages 86–94, November 2015.
[20] Peng Yong, Zhao Wei, Xie Feng, Dai Zhong-Hua, Gao Yang, Chen Dong-Qing, "Secure cloud storage based on cryptographic techniques", The Journal of China Universities of Posts and Telecommunications, Elsevier, Volume 19, Supplement 2, Pages 182–189, October 2012.
[21] Dandan Yuan, Xiangfu Song , Qiuliang Xu , Minghao Zhao, Xiaochao Wei , Hao Wang and Han Jiang, "An ORAM-based privacy preserving data sharing scheme for cloud storage", Journal of Information Security and Applications, Elsevier, Volume 39, Pages 1-9, April 2018.
[22] Shangping Wang, Jian Ye and Yaling Zhang, "A keyword searchable attribute-based encryption scheme with attribute update for cloud storage", PLOS One, Volume 13, Issue No.5, Pages 1-19, May 2018.
[23] Yunxue Yan, Lei Wu, Ge Gao, Hao Wang and Wenyu Xu, " A dynamic integrity verification scheme of cloud storage data based on lattice and Bloom filter", Journal of Information Security and Applications, Elsevier, Volume 39, Pages 10-18, April 2018.
[24] Nesrine Kaaniche and Maryline Laurent, "Data Security and Privacy preservation in Cloud Storage Environments based on Cryptographic Mechanisms", Computer Communications, Elsevier, Volume 111, Pages 120-141, October 2017.

Authors Profile

S.Jegadeeswari received her M.Sc Computer Science degree from Kanchi Mamunivar Centre For Post Graduate Studies, Puducherry during 2005, M.Phil in Computer Science in Bhathidasan University during 2006 and currently a research scholar in Bharathiar University, Coimbatore, India. Her research interest includes parallel and distributed computing, and network. She has 10 years of teaching experience.

Dr. P. Dinadayalan received Ph.D in Computer Science, M.Phil in Computer Science, M. Tech in Computer Science & Engineering and Master of Computer Applications. He is having 19 Years of Experience in Teaching and working as Assistant professor in Computer Science, Mahatma Gandhi Government Arts College, Mahe, India. His research interests include Artificial Neural Networks, Distributed Systems and Cloud Computing.

Dr. N. Gnanambigai received Ph.D in Computer Science, M.Phil in Computer Science and Master of Computer Science. She is having 17 Years of Experience in Teaching and working as Assistant professor in Computer Science, Indira Gandhi college of Arts and science College, Puducherry, India. His research interests include Artificial Neural Networks, Distributed Systems, networking and Cloud Computing.

