International Journal of Advanced and Innovative Research (2278-7844) / Volume 7 Issue 4

A HIGH SECURITY APPROACH WITH FAST INDEXING OVER CLOUD STORAGE HLMS

Varsha Sadhwani[1]*, Mr. Sunil Malviya*[2]

[1]***Research Scholar, CSE Department, SIRT College, Bhopal, INDIA***

[2]***Guide, CSE Department, SIRT College, Bhopal, INDIA***

Abstract - **In the field of cloud computing the approach for sharing of data and storage between a groups of people requires efficient approach with cost cutting and low maintenance procedure. Sharing of outsourced files assures security and ensures data veracity according to the frequent changes in shared data files. Issues like preserving privacy of data among the group stored data shared in common cloud storage. Prominent attacks within the cloud requires scheme of defense mechanisms use key distribution mechanism in secured communication channels. Some of the existing system use fine grain access control with revoked user that protects prominent attacks for original data achieving security. In our proposed paper we inculcate a Cloud Storage Controller (CSC) that manages the allocation of group of data stored and it can only referenced and cannot download any database from cloud. The data will be blended together into one of two sets for example if two users storing data of 2 megabyte and 3 megabyte each then that will be merged together as two datasets with 1 megabyte of first user and 1 megabyte of second user. In the second data set it merges 1 megabyte of first user and 2 megabyte of second user using Fusing Data Technique (FDT). Every dataset will be bookmarked which symbolizes the user that dataset belongs to and that will be indexed in the Cloud Storage controller (CSC). It helps in fast and highly secured datasets storage management in cloud storage system. It achieves efficient database privacy and revokes user data swiftly and securely.**

Keywords—*Big-Data; Network Traffic Monitoring and Analysis; Network Attacks; Machine Learning; High-Dimensional Data; MAWILab.*

Introduction

While estimating the cloud data sharing of essential data sharing in storage system with low maintenance cost that provide maintenance for utilizing the resources [1]. It provides abstract of cloud service providers with abstract and infinite data storage space that offers clients for data group. It helps in cutting down the costs and database management over various locations of cloud servers [2].

The control for security concerns made to outsource data with big data storage that has very reactive and responsive cloud database providers. The database preserving data privacy that encrypts cloud stored data that is uploaded by the users [3]. It has secured and efficient data sharing for Special dynamic cloud data group. Cloud based multiuser services with worldwide web services in cloud storage accessing and managing the cloud services [4]. It reduces costs with set of rules which has secure and fast operations. They normally have rule based order of information that has regulations for sending and receiving information stored in cloud data. They have redundant values causing security by protecting the problems with redundant database storage. The efficient mechanism for controlling the open source for hindering system process has computation speed. They improvise their processing speed along with packet travelling methods in core system using hashing functions. In our proposed paper we are going to discuss about how the secured cloud storage is possible using Fusing Data Technique and describes the utilization of Cloud Storage Controller for indexing the bookmark reference indicates the actual user and actual set of data. It also enhances fine grained access control for revoking the user appropriate data again. Before all we are going to discuss about the security threat that comprehends the importance of security protection technique for cloud based common storage system.

Literature Review

Hongwei Li ; Yi Yang ; Yuanshun Dai ; Jian Bai ; Shui Yu ; Yong Xiang, IEEE 2017 [5]

The author of this latest work discussed about the symmetric encryption technique over the cloud and working towards the cloud data storage and processing of data. They have discussed about how the medical cloud and data processing can be executed over the cloud environment.

J. H. Abawajy and M. M. Has [6]

The Author of this paper introduced a technique where a data pouring and buffering paradigm to address the data dissemination problem in medical cloud. In Data Pouring (DP) and data accessing scenario, data are periodically broadcasted to vehicles on the road. In DP-IB, data poured from the source are buffered and rebroadcasted at the intersections.

Mohammad Ali Salahuddin [7], IEEE2015

In this paper an POF based calculation and an cloud based infrastructure is proposed by author for RSU based cloud and vehicle monitoring framework. They have worked on CRM which is cloud resource management for the vehicle and data monitoring.

Xingliang Yuan, Student Member [8]

In this paper author proposed technique for health care cloud system and security approach for processing storage access. The working scenario provided towards the algorithm execution. Data compression is performed using compressive sending algorithm and further the symmetric encryption algorithm is used for security approach.

In a cryptographic network system that ensures data storage security defined by Kallahalla for untrustworthy server using techniques that shares data files and file groups equally by encrypting them with file block of key. They used for distributed approach that revokes the overheads for key distribution with untruthful database for overcoming the data sharing and data storage system [9]. Data sharing schemes have more complexities towards increment with data revocation for which it increase its number of data owners and revoke their users again.

In another paper represented by Yu blends key policy techniques with attribute based encryption methodology for proxy key re-encryption along with idle re-encryption data access control for fine grained knowledge of data [10]. The user based system hindering the implementation of applications over the group of cloud service data stored and shared in other data files. A secure provenance planning for Lu that leverages the group signature data and cipher text attribute based methodologies based on data encryption techniques. They secure several keys by securing attributes based privacy preserving along with group signature keys used for tractable privacy preserving where the plan does not supports revocation of data files.

Liu is another author who presents secure multi owner data storage system for acclaiming fine grained access control for retracted users that may not be able to contact the data sharing once again when they revoke prominent attack oriented systems [11]. They suffer attacks using private key for decrypting and encrypting data by using private and public access towards decrypted data file. They revoke file confidentially responding to the prominent attacks caused by sharing and accessing the data that suffers conspiracy in revoking private key in cloud with sequence of data base substantiates the list of revocation files. The withdraw user can calculate the decryption key that leads to attack the conditions followed by sharing data that corresponds to the attack algorithm. The attack that leads to revoked users for sharing and revealing data confidentiality towards other legitimate users.

A secured access control scheme for encrypting the cloud storage data presented by Zhou invokes the role based encryption technique. The scheme that develops efficient user revocation for combining the role based access control for encryption based policies that secure huge set of database storage in cloud. The entity verification for defense of attacks towards data base enclosure leverages polynomial design towards the secured way for controlling the dynamic group of data. Private Key disclosing supports portability and confidentiality between user and the cloud storage system obtaining attackers details through secret key discloser [12]. Privacy preserving policy yet again proposed by Nabeel for content based sharing of public cloud policies. They are usually not secure leads to weak security and protection scheme that issues identity based tokens for securing data storage.

TABLE 1: ANALYSIS OF THE AVAILABLE RECENT ALGORITHMS.

AUTHORS	ALGORITHM/TECHNIQUE	ADVANTAGES	DISADVANTAGES	REMARK/ FURTHER EXTENSION
Hongwei Li ; Yi Yang [5]	Symmetric encryption technique.	The encryption techniques provide the security of the data.	It is quite slow in nature.	They have discussed about how the medical cloud and data processing can be executed over the cloud environment.

J. H. Abawajy and M. M. Has [6]	Data pouring and buffering paradigm.	Data pouring and buffering paradigm to address the data dissemination problem in medical cloud.	Buffering time is slow.	In Data Pouring (DP) and data accessing scenario, data are periodically broadcasted to vehicles on the road.
Mohammad Ali Salahuddin [7]	POF based calculation.	Worked on the data monitoring.	Monitoring of the data sometimes get failed.	They have worked on CRM which is cloud resource management for the vehicle and data monitoring.
Xingliang Yuan, Student Member [8]	Proposed technique for health care cloud system and security approach for processing storage access.	It provides the security for the data.	Encryption technique converted the text into non-readable form.	Data compression is performed.
Kallahalla [9]	Files and file groups equally by encrypting them with file block of key.	They used for distributed approach that revokes the overheads for key distribution with untruthful database.	Data sharing schemes have more complexities towards increment with data revocation.	Data revocation for which it increase its number of data owners and revoke their users again.
S. Yu, C. Wang, K. Ren [10]	Proxy key re-encryption along with idle re-encryption data access control for fine grained knowledge of data.	The user based system hindering the implementation of applications over the group of cloud service data stored and shared in other data files.	Slow in performance.	They secure several keys by securing attributes based privacy preserving along with group signature keys.
X. Liu, Y. Zhang [11]	Secure multi owner data storage system for acclaiming fine grained access control for	The withdraw user can calculate the	They suffer attacks using private key for decrypting and	The attack that leads to revoked users for

	retracted users.	decryption key that leads to attack the conditions followed by sharing data.	encrypting data.	sharing and revealing data confidentiality towards other legitimate users.
L. Zhou, V. Varadharajan [12]	A secured access control scheme for encrypting the cloud storage data presented.	Secure huge set of database storage in cloud.	They are usually not secure leads to weak security and protection scheme.	The entity verification for defense of attacks towards data base enclosure leverages polynomial design towards the secured way.

In the comparison table 1 above, some existing recent algorithms are discussed, their advantages, disadvantages, limitation and further extension is discussed in the given table.

Problem Definition

The existing system does not provide any sort of algorithm of approach in which a proper auditing can be provided.

- In Existing system, there are following associate problems which are worked on our proposed work
- AES-256 is quite common and easily available for hacker activity in case it desire to break.
- Existing accessing and storage scheme is slow in terms of computation time and process. Thus it exhibit high cost while storage of data, providing its availability to access.
- The existing algorithm use model which is still extension is required for proper loose coupling.
- Previous approach having limitation of accessing data from large structure of dataset.
- Highly indexed data structure is not taken in the base paper, which further need analysis of high end access.

Experiment Execution & Efficiency

- The proposed work can be done in accordance of working with security and storage over the various available component. Data optimization over the network and to work on reducing better resource management and CRM investigation can be done in further proposed methodology.
- An advance accessing mechanism with process security is going to process in proposed approach with lexical storage and HECC security approach.
- The above algorithm pseudo code is executed at our implementation end and further the modules and sub algorithm which is being implemented at server end is discussed here.

CONCLUSIONS

This paper discuss about the survey of various cloud computing health care communication technique. The proposed scheme permits the user to efficiently perform search over the encrypted cloud data. To do so, the data owner generates the cluster index and document index. The documents are encrypted and outsourced to the cloud. After performing experiments using synthetic data it can be easily inferred that the proposed search scheme reduces the time and number of comparisons required to retrieve the desired documents.

ACKNOWLEDGMENT

The authors are thankful to our college Principal and Management for giving us the research lab to direct this investigation.

REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2]. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136– 149.

[3]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[4]. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.

[5]. Hongwei Li ; Yi Yang ; Yuanshun Dai ; Jian Bai ; Shui Yu ; Yong Xiang, "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data", IEEE 2017.

[6]. J. H. Abawajy and M. M. Hassan, "Federated internet of things and cloud computing pervasive patient health monitoring system," IEEE Communications Magazine, vol. 55, no. 1, pp. 48–53, 2017.

[7]. Mohammad Ali Salahuddin, "Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles", April 2015.

[8]. X. Yuan, H. Cui, X. Wang, and C. Wang, "Enabling privacy-assured similarity retrieval over millions of encrypted records," in Proc. of ESORICS, 2015.

[9]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[10]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[11]. X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[12]. L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure rolebased access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.