An Investigation Study on Secured Data Storage and Access Control in Cloud Environment

Chapter · January 2020

DOI: 10.1007/978-981-15-3284-9_26

2 authors:

P. Calista Bebe
New Prince Shri Bhavani Arts and Science College
6 PUBLICATIONS **9** CITATIONS
SEE PROFILE

Akila D.
Saveetha College of Liberal Arts and Sciences
112 PUBLICATIONS **489** CITATIONS
SEE PROFILE

An Investigation Study on Secured Data Storage and Access Control in Cloud Environment

P. Calista Bebe and D. Akila

Abstract Cloud computing is surroundings for imparting the information and resources which might be brought as the service to an end users over Internet on call for. Cloud allowed the users to get way into their stored information from any environmental places at any time. Cloud comprised of the key problems like safety, data confidentiality, network dependency and centralization. When storing the client sensitive information into cloud data storage, security plays an essential part. Providing the security to sensitive information is a key issue in cloud computing. In existing works, numerous methods were introduced for securely storing data into the cloud. But, the security level was not improved, and data accessing time was not reduced. Our research work concentrated on the cryptographic and data structure techniques for solving the existing problems during cloud storage and data access.

Keywords Cloud computing · Security · Data integrity · Geographical location · Data access · Cryptographic techniques

1 Introduction

Cloud computing is a type of figuring where the mutual assets and IT-related capacities are provided as the supplier to external customers by the utilization of Internet methodologies. Cloud computing is primarily based on data sharing and computing resources than the usage of local servers to manage there quests. Cloud computing allowed the users to receive benefit without any requirement for deep knowledge or expertise.

P. Calista Bebe (✉)
Department of Computer Science, School of Computing Sciences, Vels Institute of Science Technology & Advanced Studies (VISTAS), Chennai, India

D. Akila
Department of Information Technology, School of Computing Sciences, Vels Institute of Science Technology & Advanced Studies (VISTAS), Chennai, India

S.-L. Peng et al. (eds.), *Intelligent Computing and Innovation on Data Science*,
Lecture Notes in Networks and Systems 118,
https://doi.org/10.1007/978-981-15-3284-9_26

2 Literature Survey

A Dynamic Proof of retrievability method was designed in [1] for public auditability and for communication efficient restoration since information corruption [2]. A secure disintegration protocol (SDP) was introduced in [3] for protection of privacy on-site in cloud. Probabilistic analysis was carried out for finding the intrusion tolerance abilities. But, the key management method was not introduced for secure data integration in cloud. The designed method failed to utilize cryptography method effectively. A new large DAC-MACS scheme (NEDAC-MACS) was introduced in [4] to guarantee the secure attribute revocation. However, the attack detection rate was not increased by NEDAC-MACS scheme.

A new cloud storage encryption scheme was introduced in [5] to convince false client secrets and to improve the client privacy level. But, the encryption time was not minimized using new cloud storage encryption scheme. The multi-tenant networked cloud infrastructure architecture was introduced in [6] for securing the hosted services. The designed architecture was based on trusted virtual domains with security policies of tenant domains and security policies of virtual machines. But, the access control was not carried out in enhanced manner using multi-tenant networked cloud architecture. A new security assessment methodology was designed in [7] for examining the safety of critical services in cloud. But, the security level was not enhanced using security assessment methodology [10]. Broker-based structure was introduced in [8] [9]. However, the information confidentiality rate was not more suitable for using broker-based framework.

3 Secured Cloud Data Storage and Access Control Techniques in Cloud Computing

The main objective of designed scheme was to assure the redistributed information honesty and information accessibility in distributed storage. The key aim was to guarantee that cloud server stores the data in secured manner. The cloud storage systems were not used by peoples when his data changed randomly by CSP or different entities with no approval.

NEDAC-MACS assured safe quality revocation, information confidentiality and protection besides the stationary corruption of authorities. NEDAC-MACS enhanced security devoid of reducing the effectiveness.

The media cloud structure was introduced and used as manual in procedure of accumulation safety features or new media clouds. The designed structure was partitioned into three security limitations among every layer organizing the subsequent system safety characteristic on border to attain dissimilar levels of local safety protection.

4 Comparison of Techniques in Cloud Environment and Suggestions

4.1 Space Complexity

Space complexity is given by,

$$\text{SC} = \text{Total memory} - \text{unused memory space in cloud server} \tag{1}$$

From (1), the space complexity is calculated. When the space complexity is lesser, the approach is stated as greater efficient.

Table 1 describes the space complexity with respect to range of cloud user requests ranging from 10 to 100. Space complexity comparison takes place on existing dynamic Proof of retrievability scheme, NEDAC-MACS and media cloud framework. The graphical analysis of space complexity is described in Fig. 1.

High coding granularity was achieved through encoding at information square dimension than part enormous information record. Information gets parceled into little information squares and encodes each datum square independently. With coding approach, a redesign inside information square influenced the current information square and connected images without refreshing huge information document. This in turn helps to reduce the space complexity. Therefore, the space complexity of dynamic Proof of retrievability scheme is 21% lesser than NEDAC-MACS scheme and 38% lesser than media cloud framework.

Table 1 Space complexity

Number of cloud user request (number)	Space complexity (MB)		
	Dynamic Proof of retrievability scheme	NEDAC-MACS scheme	Media cloud framework
10	25	33	42
20	28	36	45
30	31	40	49
40	29	38	47
50	27	35	44
60	25	31	42
70	22	28	38
80	26	32	43
90	30	36	46
100	34	41	50

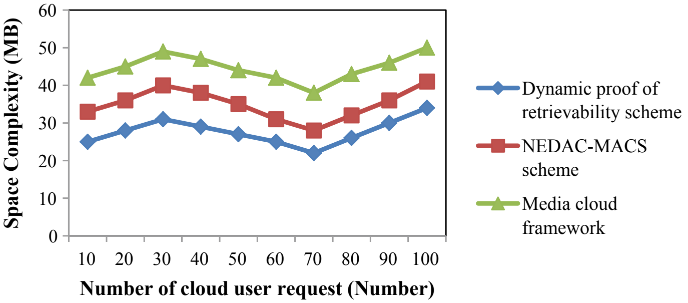

Fig. 1 Measure of space complexity

4.2 Security Level

Security level is defined as the ratio of number of cloud user data can be correctly accessed by authorized cloud users to the total number of cloud user data. It is calculated in terms of percentage (%). The formula can be

$$\mathrm{SL} = \frac{\text{Number of cloud user data correctly accessed by authorized cloud users}}{\text{Total number of cloud user data}} \quad (2)$$

From (2), the security level is calculated.

Table 2 illustrates the security level with the esteem number of cloud user data ranging from 10 to 100. The graphical analysis of security level is illustrated in Fig. 2.

Figure 2 explains the security level comparison for different number of cloud user data. From figure, it is observed that the security level using NEDAC-MACS

Table 2 Security level

Number of cloud user data (number)	Security level (%)		
	Dynamic Proof of retrievability scheme	NEDAC-MACS scheme	Media cloud framework
10	76	85	70
20	79	87	73
30	82	89	76
40	80	86	74
50	85	90	79
60	87	93	82
70	84	89	80
80	81	87	77
90	83	91	79
100	87	94	82

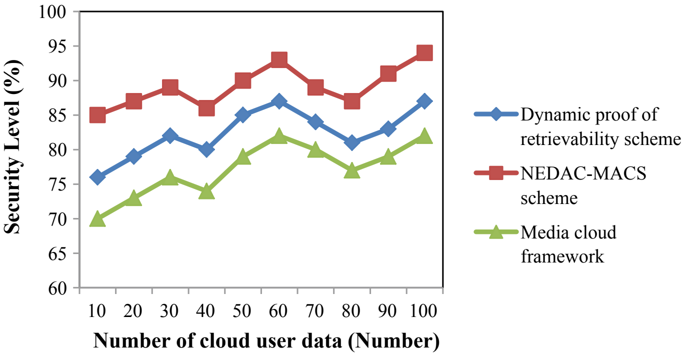

Fig. 2 Measure of security level

is higher when compared media cloud framework. NEDAC-MACS enhanced safety without reducing the performance. Therefore, the security level of NEDAC-MACS scheme is 8% higher than Dynamic Proof of retrievability scheme and 16% higher than media cloud framework.

4.3 Data Retrieval Time

The data retrieval time can be calculated in phrases of milliseconds (ms). It is given by,

$$\text{Data Retrieval Time} = \text{Ending Time} - \text{Starting time of data access} \quad (3)$$

When the data accessing time is lesser, the approach is believed as greater efficient (Table 3).

Data retrieval time comparison takes place on existing Dynamic Proof of retrievability scheme, NEDAC-MACS and media cloud framework. The graphical representation of data accessing time is explained in Fig. 3.

Figure 3 illustrates the data retrieval time comparison for different number of cloud user requests. From figure, it is clear that the data accessing time using media cloud framework is lesser when compared to NEDAC-MACS. This is because the designed framework uses three protection limitations with every layer arranging equivalent system protection events on border to attain different local security protection level. By this way, the data accessing time gets reduced. As a result, the data retrieval time consumption of media cloud framework is 38% lesser than Dynamic Proof of retrievability method and 45% lesser than NEDAC-MACS scheme.

Table 3 Tabulation for data retrieval time

Range of cloud user request (number)	Data accessing time (ms)		
	Dynamic Proof of retrievability scheme	NEDAC-MACS scheme	Media cloud framework
10	25	33	13
20	28	35	15
30	32	38	19
40	36	40	21
50	39	43	24
60	42	46	27
70	45	49	30
80	41	45	28
90	44	49	31
100	47	52	33

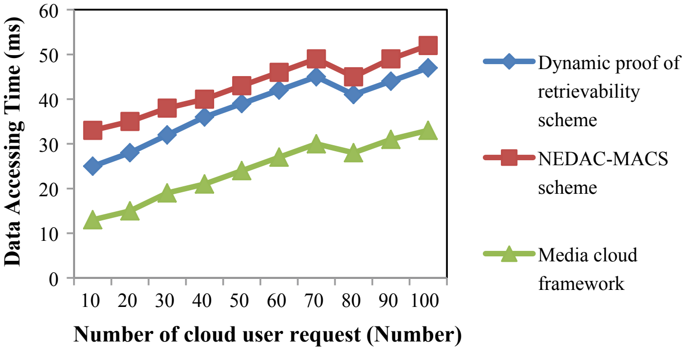

Fig. 3 Measure of data retrieval time

5 Discussion on Limitation of Secured Cloud Data Storage and Access Control Techniques in Cloud Computing

The data confidentiality rate was not improved using Dynamic Proof of retrievability scheme. NEDAC-MACS addressed two vulnerabilities though the nonrevoked users disclosed obtained key update keys to the revoked user. But, the attack detection rate was not enhanced using NEDAC-MACS scheme.

A security media cloud framework was introduced for preserving the multimedia data and services. The existing media cloud structure comprised of three protection limitation in media cloud to guarantee cloud protection. Sec-ABAC access manage protocol guaranteed the access manage of cloud resources. The operation of structure on Amazon Web Services failed to examine exact performance of Sec-ABAC protocol. The space complexity was not reduced using security media cloud framework.

6 Conclusion

A comparison of different existing secured data storage and access control techniques for improving the security is studied in cloud computing. This survey paper also discussed the methodologies and different methods to store the data in efficient manner. From the study, it is clear that the existing techniques failed to improve the data confidentiality rate. In addition, the attack detection rate was not improved using NEDAC-MACS scheme. The huge range of experiments on current techniques calculates the relative overall performance of many secured data storage and access control techniques with its restrictions. The future research can be carried out using cryptographic and data structure techniques for performing the secured data storage and access control in cloud computing.

References

1. Ren Z, Wang L, Wang Q, Xu M (2018) Dynamic proofs of retrievability for coded cloud storage systems. IEEE Trans Serv Comput 11(4):685–698
2. Du M, Wang Q, He M, Weng J (2018) Privacy-preserving indexing and query processing for secure dynamic cloud storage. IEEE Trans Inf Forensics Secur 13(9):2320–2332
3. Rawal BS, Vijayakumar V, Manogaran G, Varatharajan R, Chilamkurti N (2018) Secure disintegration protocol for privacy preserving cloud storage. Wirel Pers Commun 103(2):1161–1177
4. Wu X, Jiang R, Bhargava B (2017) On the security of data access control for multi-authority cloud storage systems. IEEE Trans Serv Comput 10(2):258–272
5. Chi P-W, Lei C-L (2018) Audit-Free Cloud storage via deniable attribute-based encryption. IEEE Trans Cloud Comput 6(2):414–427
6. Varadharajan V, Tupakula U (2018) Securing services in networked cloud infrastructures. IEEE Trans Cloud Comput 6(4):1149–1163
7. Hudic A, Smith P, Weippl ER (2017) Security assurance assessment methodology for hybrid clouds. Comput Secur 70:723–743 (Elsevier)
8. Halabi T, Bellaiche M (2018) A broker-based framework for standardization and management of cloud security-SLAs. Comput Secur 75:59–71 (Elsevier)
9. Li H, Yang C, Liu J (2018) A novel security media cloud framework. Comput. Electr. Eng. 1–11 (Elsevier)
10. Sudha C, Akila D (2019) Detection of AES algorithm for data security on credit card transaction. Int J Recent Technol Eng (IJRTE) 7(5C):283–287