DOI 10.29042/2018-3726-3730

Helix Vol. 8(5): 3726- 3730

Enhanced Privacy Preservation and Data Storage Security in Public Cloud

[*1]Prof. Rachana Deshmukh, [2]Prof. Rashmi Deshmukh, [3]Dr. Pallavi Chaudhari
[1, 3] Priyadarshini Institute of Engineering & Technology
[2]Priyadarshini Indira Gandhi College of Engineering
Email: rachana1509@gmail.com, rashmi_deshmukh86@yahoo.com, pallavichaudhari1@gmail.com

Received: 09th July 2018, Accepted: 14th August 2018, Published: 31st August 2018

Abstract
Cloud computing is an elegance of computing system where immensely scalable Information Technology-enabled capabilities are conveyed 'as a service' using Computer and Internet technologies to numerous outdoor clients. DaaS that provides various research challenges in associations to data storage security and cost related issues from user's view. The various security concerns are data intrusion, scalability, non-repudiation, data integrity, confidentiality, heterogeneity. In cloud database information can be leaked due to various reasons. The proposed method provides three level security using AES algorithm and secure private key. The method also provides data storage privacy preservation of large organization and sensitive data storage leak detection. The experimental outcome represented that our method is better for public cloud database security.

Keywords: Cloud Computing, Security, Privacy Preservation, AES, Data Storage

Introduction

Cloud computing [1] is the acceptance and development of present-day technologies and prototypes. The cloud computing resources are storage, networks, applications, servers, and services. There are four main types of cloud based computing facility system. These models are Database as a Service [3] abbreviated as DaaS, Software as a Service abbreviated as SaaS, Infra-structure as a Service abbreviated as IaaS and Plat-form as a Service abbreviated as PaaS. The cloud types are hybrid, public, community and private depends on their uses. The characteristics of cloud computing are location independent, elasticity and scalability [3], ubiquitous access, location independence, on-demand self-service.

Cloud database provides on demand data services to the client with privacy protection. DaaS is database management system over the cloud. Cloud storage allows customers to store data, and info in docs formats. iCloud, Google drive, Dropbox, etc. are most common and popular cloud storage services. The major issue with the cloud database is that it has need of a very great level safety. The cloud database should be secure in terms of audit, authentication and authorization. Confidentiality of information data is additional safety issue connected with cloud computing environment. The cloud database should be secure in terms of audit, authentication and authorization. Confidentiality of information data is additional safety issue connected with cloud computing environment. The different barriers of cloud database adoption are security, cost and availability. Privacy preservation of the cloud database from malicious attack is also main security issue in cloud database security.

The data leak detection and auditing in large organization are also necessary in cloud database. The different encryption techniques [4] that allow the execution of database actions on encoded data have some performance limits. And different types of encryption techniques must be implemented for every database operation and database column. Most of the encryption techniques regarding encryption for cloud-based database services are inappropriate to the database prototype for the cloud data storage.

The three level of security [5] should be provided in cloud database as a service. Some of the three level security issues are

- how to design a host assisted privacy preservation cloud database which ensures security of the information from unauthorized access?
- how to design and keep large organization cloud database from data security and misuse and
- how to provide auditing in cloud data storage?

The rest of the paper is presented in the following manner. Section 2 provides the details of related work done in cloud database security. Section 3 describes the proposed algorithm. Section 4 presents the implementation details of the proposed work with result analysis. Section 5 summarizes the work and also discusses the future research directives of the work.

Related Work

The author in [6] suggested a security and privacy preservation mechanism having two factor data

storage protection. The method also provides data recoverability for cloud data storage architecture. The method allows a cloud user to send encrypted message through a cloud data storage server. The data sender only essentials to identify the uniqueness of the receiver without his certificate or public key. On the other side the receiver essentials to retain two things to decrypt the encrypted message. The personal unique device which is used for security and sender secret key stored in server. If secure unique device is lost or stolen, then secure device is revoked.

Identity-based Encryption [7] is a kind of public key encryption in which key arrangement is repressed in the all keys should be in use from disparate identity divisions and with secure key accumulation. The advantage of IBE is great cipher text size and security. The author in [8] proposed a cloud system using single user key distribution and encryption mechanism for cloud data storage. The method is not suitable for large organizations. Cryptographic secure key circulation systems [9] intent to diminish the overhead in storing secret keys and managing for widespread cryptographic usage. In this suggested scheme a top-secret key for a specified node can be applied for its nodes. The system provides a process using hierarchical management system. The technique uses tree representation which consists of nodes. The top-secret key is allotted to the parental node the all nodes below parental node automatically provides the secret keys to all other nodes. This method is costly then symmetric keys [10].

Proposed Method

This section represents the proposed method steps. The proposed cloud data storage system consists of intermediate servers, clients, and cloud data storage. The client can be thin mobile client, desktop systems or middleware computer etc. The middleware servers are involved into system to make superior level of privacy. The data cloud storage servers are used to store database of large organizations.

The proposed steps are given below.

Step 1: Cloud data storage architecture setup

Step 2: Issue of private key by cloud data storage server.

Step 3: Issue of secure device list

Step 4: Machine based user authentication by authentication server.

Step 5: Data transmission and access by using private key and secure machine address

Step 6: if any one security or both parameters are not valid then User will not decrypt data

Step 7: If user system lost or stolen then Permissions to access data revoked

Step 8: Data recovery process to recover original data.

Step 9: Audit report by data storage server

The proposed encryption algorithm is given below.

A. For Encryption

a) Verifier upload N no of data blocks.

b) For each data block 1 to N do

I. Generate N key for each data block.

II. Apply Encryption Algorithm (AES)

III. Key merger get data block ID & Key for each data block.

IV. Merge Keys into Super Key K.

V. Secure K (AES).

VI. Upload secure data block into cloud database.

VII. End for each.

To provide security in database the data is divided into blocks. If verifier wants to upload N number of blocks, then for each block key is generated and data block is encrypted using AES algorithm. The key manager gets data block ID and key for each data block. The key is merged into super key using AES algorithm. Using secure key, the data is uploaded into cloud database server.

The proposed decryption algorithm is given below.

A. For Decryption

a. Verifier download N no of data blocks.

I. Verifier search which data block to be downloaded

II. Split data block using AES search for download

III. A data block goes to AES decryption.

IV. Key manager send secure key.

V. Secure Key split into N no Key by Key Splitter.

VI. By the help of N no of key AES decrypt the data block.

b. Decrypted data block goes into file buffer.

Verifier search which data block to be downloaded. The verifier downloads the desired data from cloud database. Split data block using AES search for download. A data block goes to AES decryption. Key manager send secure key. Secure key splits into desired number of data blocks. With the help of secure key, the data can be decrypted using AES algorithm.

The steps involved in proposed work are represented below. The first step is to setup cloud data storage system for privacy preservation. The next step is to issue a private key by cloud data storage server to the authenticated user. The next step is to provide secure machine address to the cloud data storage user. Now every cloud data storage user has secure private key and security machine address for authentication. When user wants to access the cloud data then he/she has to authenticate by using secure machine address and secret key provided by authentication server. The secure key is generated by using AES 256-bit method. If any security or both parameters are not valid then user will not decrypt data. If user system is lost or stolen, then permissions to access data revoked. The next step is to recover original data.

The audit report by data storage server is also generated.

Implementation and Result Analysis

The simulation of the proposed work is performed in the Institute lab with CloudSim simulator. The algorithm is verified with different users and data with different volume. The Java environment and programming language is used for implementation of proposed algorithm.

The table 1 represents the different users with secure key.

USERS	**KEY**
User 1	FDe34434@#134D+$#2!44R5456Ueeey213Gwg2k5xD55gz
User 2	R5456U456U5UGuZnDp4 FDe34434@+$#2!4XnkGsw5xs
User 3	PVYXnkGswGwg2k5xDpUGuZn8KD iG+jL461J+TpG5IRo
User 4	UGu234Dp456U5UGuZnDp4+$#2!44 R5Gu45Gsw541190y
User 5	456U54UGuZnDpUGu234DpGu45Gs w541190y+$#2!44R5

Table 1: User with System Generated Key

When user data is of different volumes then total encryption duration (or data transfer duration) consumed by the proposed method is less as compare to the previous method. This comparison is shown in table 2. It represents the time in **milliseconds**.

S.No	Data Size (MB)	Total data transfer duration (Previous Method)	Total data transfer duration (Proposed Method)
1	5	41	32
2	8	55	48
3	20	67	60
4	50	72	69
5	125	82	73

Table 2. Total Encryption Time

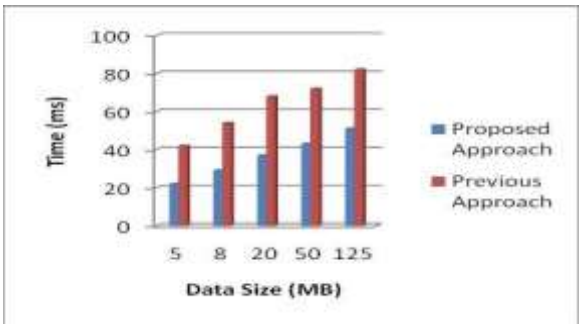

Figure 1. Performance Comparisons for Encryption

The above figure (Figure 1) represents the data size, encryption time in milliseconds for previous and proposed method.

The table 3 below provides the total decryption time in milliseconds. Also, represents the comparison between the data download time of previous approach and proposed approach.

S.No.	File Size (MB)	Total download Time (Previous Approach)	Total download Time (Proposed Approach)
1	5	43	28
2	8	55	36
3	20	70	43
4	50	85	56
5	125	91	82

Table 3. Total Decryption Time

S.No.	File Size (MB)	Total Decryption Key Management Time (ms) (Previous Approach)	Total Decryption Key Management Time (ms) (Proposed Approach)
1	5	3.326	2.438
2	8	8.857	8.231
3	20	26.167	24.692
4	50	31.396	29.372
5	125	37.248	35.541

Table 4. Total Key Management Time for Decryption

As provided in the table 3 above when user want to download database of dissimilar size then total decryption period used up by proposed method is less related to previous method and the comparison is given in above table 3.

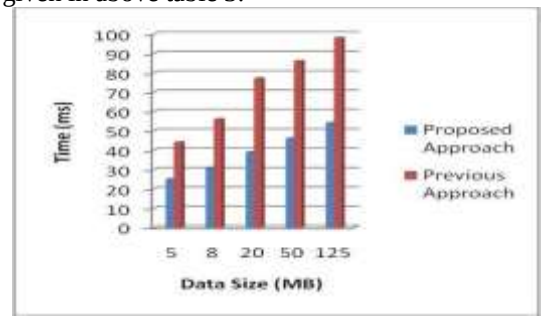

Figure 2. Performance Comparison of Data Decryption Techniques

The figure 2 above provides the data size, and decryption time in milliseconds for proposed and previous approaches.

Key Management Duration (Decryption)
As represented in table 4, total decryption duration of key for the proposed method is less as compared to the total decryption duration of the previous method.

Total Key Management Time (Encryption)
As provided in the table 5 total encryption duration of the proposed method is less as compared to encryption duration of the previous method.

S.No.	File Size (MB)	Total Encryption Key Management Time (ms) (Previous Approach)	Total Encryption Key Management Time (ms) (Proposed Approach)
1	5	2.014	1.173
2	8	9.875	8.998
3	20	21.146	20.362
4	50	26.384	25.481
5	125	32.031	30.731

Table 5 Total Key Management Time for Encryption

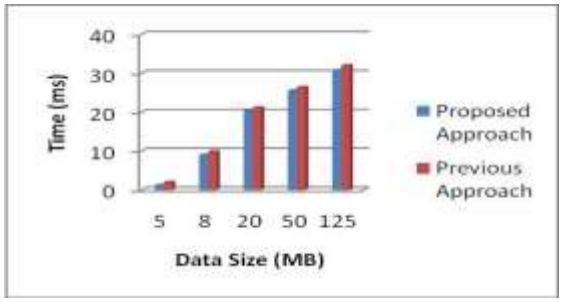

Figure 3. Performance Comparison for Key Management Time (Encryption)

The above figure (Figure 3) represents the comparison between proposed and previous method. It gives the clarification about how much is the total encryption key management time required when a user want to upload a file in cloud environment.

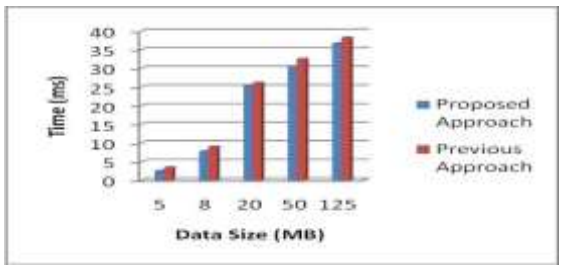

Figure 4. Performance Comparisons for Key Management Time (Decryption)

The above figure (figure 4) provides the comparison between proposed and previous method's total decryption key management time i.e. when any user wants to download any database in cloud data storage environment then how much time is consumed for key management in decryption.

Conclusion
Cloud data storage allows consumers to store information, in docs and relational formats. Data protection and privacy is main safety issue associated with cloud data storage system. The paper proposed three level data protection technique. The system provided a secure cloud data storage which provides data encryption, security and privacy preservation which ensures security of the data from unapproved access. The experimental outcome illustrated that the proposed method is fine applicable for privacy preservation in public cloud data storage. We are furthermore planning to introduce data freshness and public auditing for improving in cloud data storage.

References
[1] Rajkumar Buyya, "Introduction to the IEEE transactions on cloud computing" IEEE transactions on cloud computing, vol. 1, no. 1, January-June 2013

[2] H. Hacıgumus, B. Iyer and S. Mehrotra, "Providing database as a service," in Proc. 18th IEEE Int. Conf. Data Eng., Feb. 2002, pp. 29–38.

[3] Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and *M*. Zaharia, *"*A View of Cloud Computing," Communications of the ACM, Vol. 53, No. 4, 2010, *pp. 50-58.*

[4] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, May 2000, pp. 44– 55.

[5] Y. Sun, J. Zhang, Y. Xiong, G. Zhu, "Data Security and Privacy in Cloud Computing" International Journal Of Distributed Sensor Networks, 2014.

[6] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System",IEEE transactions on computers, vol. 65, no. 6, june 2016, pp1992-2004

[7] Boyang Wang, Baochun Li and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data

in the Cloud", IEEE transactions on cloud computing, vol. 2, no. 1, january-march 2014, pp.43-57

[8] Jianyongchen, Y. Wang, X. Wang, "On-demand Security Architecture for cloud computing" IEEE, 2012.

[9] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services", in Proc. 17th ACM Conf. Comput. Commun. Security, 2010, pp. 735–737.

[10] Xiaokui Shu, Danfeng Yao, and Elisa Bertino, Privacy-Preserving Detection of Sensitive Data Exposure, IEEE transactions on information forensics and security, vol. 10, no. 5, may 2015, pp-1092-1112

