*International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-7, Issue-1)*

**Research Article** | **January 2018**

# Secure Cloud Database Architecture for Data Leak Detection and Public Auditing using AES Algorithm

**Sanjay Kumar Sharma**
*PhD Scholar, Mewar University, Rajasthan, India*
Email: sanjaysharmaemail@gmail.com

**Dr. Manish Manoria**
*Director, Sagar Institute of Research Technology and Science, Ayodhya Bypass Road Bhopal, MP, India*
Email: manishmanoria@gmail.com

***Abstract—***

***Cloud computing is the self-motivated distribution of information and resources as a facility over the WWW. Confidentiality of information, detecting and preventing data privacy requires a set of different technique, which may include data-privacy, malware detection, and policy enforcement. The major dispute with the cloud computing database is that it have need of a very high level security. The cloud database security is ensured in terms of audit, authentication and authorization. Due to public nature of cloud database the information can be leaked. The three level of security should provided in cloud database as a service. We have created a secure architecture which provides data encryption using AES algorithm, and host assisted privacy preservation cloud database which ensures safety of the information from unauthorized access. The architecture provides audit report and data leak detection in cloud database. The experimental result illustrated that our system is fine appropriate for security in public cloud database. The proposed work also implement traceability i.e. ability to group manager or original user to preserve the identity.***

***Keywords— Cloud Database, Security, Privacy Preservation, Audit, Data leak Detection***

## I. INTRODUCTION

Cloud computing is the result of development and acceptance of current technologies and prototypes. The cloud computing resources are storage, networks,applications, servers, and services. The cloud computing architecture[2] is consists of four distribution systems, five important features, and three service prototypes.Massive evolution in better broadband conveniences, digital data, varying data storage necessities, and Cloud computing focused to the presence of cloud based databases.An essential objective[3] of cloud computing is to make available on-demand use to computer based resources such as network, database, applications and platform on pay-as you-go[4] basis alike to the way in which client get services from public usefulness services such as electricity, water, telephony, and gas. The Cloud based providers also called cloud service producers and Cloud consumers also called clients or cloud service consumers are the main pillars in cloud computing database. Cloud consumers can be either software service providers/ application [5]. A cloud service provider is a company that offers economically effective cloud based services using the devices[6] and programs.

Confidentiality of information is additional safety issue connected with cloud computing environment. The number of leaked confidential data records has increased throughout the past few years. The AES (Advanced Encryption Standard) algorithm is symmetric key algorithm mainly used for cloud database security.

How to design a host assisted privacy preservation cloud database which ensures security of the information from unauthorized access and how to design and keep large organizations cloud database from data leak and misuse is the key security issues in cloud database.

Our algorithms should be aimed to accomplish following objectives:

(1) Public Auditing: A public auditor or information verifier is capable of publicly audit the truthfulness of shared info without regaining the complete data from the cloud database.
(2) Accuracy: A public auditor is capable to verify accurately shared information integrity.

 

(3) Identity Privacy: A public auditor cannot discriminate the uniqueness of the signer on every info block in shared info throughout the method of auditing.
(4) Data leak detection: Data leak is also very common problem in public auditing. The proposed algorithm should detect data leak in cloud database

The paper is organized as follows. Section 2 represent the related work. Section 3 represent the proposed work and various steps in proposed work. Section 4 provides the implementation detail of the proposed system. Section 5 concludes the paper with future planning.

## II. RELATED WORK

Enormous progression in digital data, better broadband conveniences, altering data storage necessities, and Cloud system computing commanded to the appearance of cloud databases. The adoption of cloud computing database as fifth utility is failure because of cost, information and data privacy.

Boyang Wang et al. in [7]Provides privacy preservation for shared data in cloud computing using public auditing method. The auditing method used ring signature to provide verification process. The system consists of public verifier, group of users and cloud server. In this method the distinctiveness of the signer on every block in collective data is retained private from public verifiers, the verifiers are able to capably validate shared info truthfulness without reclaiming the complete file. The method is able to accomplish numerous inspecting tasks all together in its place of confirming them one by one. The method improves the efficiency and effectiveness of method in auditing shared information integrity. The data owner in the beginning generates shared info in the cloud. The info is shared through group users. Both the group users and original user are associates to the group. Every single member of the created group is permissible to modify and access shared info. Shared info and its authentication metadata are both put in storage in the cloud database server. A public authenticator, such as a third party examiner providing professional info inspecting services or a info user external to the group expecting to make use of shared data, is capable to openly validate the truthfulness of shared info stored in the cloud database server. When a public verifier needs to check the truthfulness of shared info, it primarily directs an inspecting challenge to the cloud database server. Afterward acceptance the auditing challenge, the cloud database server answer back to the public auditor with an inspecting evidence of the ownership of shared info. Then, this public auditor checks the precision of the complete info by confirming the precision of the auditing proof. Principally, the method of public auditing is a challenging task and reply protocol amongst the cloud database server and a public verifier.

Two categories of security threats associated to the integrity of shared info are possible privacy and integrity threats. In integrity threats an opponent may attempt to corrupt the truthfulness of shared info or the cloud database service provider possibly will carelessly remove or even corrupt the info in its storage because of human errors or to hardware failures. In some cases the cloud database service providers can economically inspired, that is it might be unenthusiastic to notify users about such exploitation of info in order to protect its status and circumvent trailing revenues of its services.In privacy threats the uniqueness of the signer on every block in shared info is trustworthy and private Search operators are too not entirely maintained by encrypted database. Some encryption procedure support comparison operations but not select operators like minus, union, intersect.

The disadvantage of encryption technique is that this scheme is not proper for lengthy operations. This scheme also very complex to implement because database administrator does not every operations related to each database column. The overhead difficulty is somewhat astounded by [9]. The adaptive encryption technique worked using proxy and intermediate proxy. The resolution for above difficulty is offered in [7]. The system allows multiple client database to execute concurrent SQL operations.

Adaptive Encryption Scheme[11]consists of client, encryption algorithm, encryption engine, and cloud database. The figure below represent the encrypted cloud database. The main modules of adaptive encryption scheme are plain text data, user application, encrypted database interface, encryption engine, master key, cached plain metadata, database engine, encrypted metadata, encrypted data.

## III. PROPOSED METHOD

The data owner in the beginning generates shared info in the cloud. The info is shared through group users. Both the group users and original user are associates to the group. Every single member of the created group is

 

permissible to modify and access shared info. Shared info and its authentication metadata are both put in storage in the cloud database server. A public authenticator, such as a third party examiner providing professional info inspecting services or a info user external to the group expecting to make use of shared data, is capable to openly validate the truthfulness of shared info stored in the cloud database server.When a public verifier needs to check the truthfulness of shared info, it primarily directs an inspecting challenge to the cloud database server. Afterward acceptance the auditing challenge, the cloud database server answer back to the public auditor with an inspecting evidence of the ownership of shared info. Then, this public auditor checks the precision of the complete info by confirming the precision of the auditing proof. Principally, the method of public auditing is a challenging task and reply protocol amongst the cloud database server and a public verifier.

**ALGORITHM**

The steps involved in the proposed work is given below.
Data owner Application
Authentication using login detail, password and Internet Address
Security key generation by intermediate server
Security key distribution by intermediate server
Key authentication using intermediate server
Data auditing, data auditing and leak report generation
The user be able to work with the cloud system database using application.

Master key generation: In first step the system generate the secure key which is mainly used for authentication purpose. The subsequent stage is to generate multiuser key which is used for various groups for security purpose. In next step is distribution of the multiuser key to other user participating in cloud database services. The verifier will login to the system using user ID and password provided by the cloud database provider. After authentication process performed by server the intermediate server will validate Internet address of the verifier. If ID, password and IP address of the verifier is authenticated then intermediate sever will generate the security key using AES and provided to the verifier. Verifier's public and private keys will be authenticated by intermediate server and access is provided to the verifier. The verifier's activities is audited by intermediate server. Auditing report and data leak report is also provided by the system to provide security to the system.The proposed architecture consists of clients, intermediate servers, and cloud database. The client can be mobile client, desktop computer etc. The intermediate servers are included into architecture to offer advanced level of safety. The database servers are used to store database of organizations.

AES Encryption process
Key Expansions: The requirement of AES is 128 bit round key + 1
The Initial Round steps
In AddRoundKey step xor is used to combine each byte
Rounds In subbytes phase each byte is replaced with another
In shiftrows phase last 3 rows shifted for number of steps
In mixcolumns steps add 4 bytes to every column.
In addround phase subkey is combined with state

AES Decryption process
Step 1: Add round key phase
Step 2: Mix columns phase
Step 3: Shift rows phase
Step 4: Byte substitution phase

After getting the security key the user can access cloud database and can implement dissimilar instructions and get the desired information. All the data stored in the cloud database are in encrypted form. The application designed for testing the proposed architecture can execute statements select, insert, delete, and update to the encrypted database. Data transferred between cloud database and application are not encrypted. The data always scrambled before storing keen on the cloud system database. When an application issue

 

instructions select, delete, insert, and update, the encrypted database interacts with encryption engines with the help of main secure key. After getting the multiuser security key the user can access cloud database and can perform many instruction and get the desired information. Unapproved user cannot be accessed the cloud system database without the security key generated by cloud system. The intermediate system perform the authentication, and auditing operation. The audit report is also generated using intermediate server. The private info or data cannot be retrieved by others.

Database creation: The database administrator setup the database. In database creation phase database administrator creates the database with required tables. The column of a tables may have number, varchar and date data types. The database administrator allocates the secure key to all the cloud database clients.

SQL statements execution: SQL statements insert, delete, select and update are executed on database. When an application or user executes SQL operations on the cloud database encryption engine determines the table, SQL operations and column of database and decrypt the desired result and provide the output data to the clients. The application or user uses master key for decryption process.

## IV. IMPLEMENTATION

Java programming language is used for the implementation of the architecture and algorithm. Oracle 11g enterprise server is used as the cloud database server. The implementations are performed in lab, which make available with a cluster of machines in Oracle 11g database and Java environment. Every client computer executes the Java client prototype of structural design on an Intel i3 machine having a single 3 GHz processor, 2 GB of RAM and 1200 RPM 1TB SCSI hard disks. The database server is Oracle 11g running on Intel machine having an i3 3.5 GHz processor, 4GB of RAM and a 7,200 RPM 1 TB SATA disk. The database used for experiment is college training and placement database. We have collected training and placement data from college of different years. We have also collected various company data in which students are placed. We have tested our system with plaintext data as well as encrypted data. We have implemented the assessment for every database i.e. for plaintext and encrypted. The test is performed for plaintext and encrypted database for different clients from 5 to 20. In experiments the transactions are performed and response time and throughput are recorded with different number of clients and different time interval.

The different cloud server established in our proposed work is given in table below.

**Table 1: Cloud database server**

| MODE | Multiple |
|---|---|
| IP | 210.132.122.1 |
| serverCommon | cloudserver |
| ipIT | 210.132.122.2 |
| serverIT | cloudit |
| ipCS | 210.132.122.3 |
| serverCS | cloudcs |
| ipET | 210.132.122.4 |
| serverET | Cloudet |
| ipEX | 210.132.122.5 |
| serverEX | cloudex |

Computational Comparison Running Time

**Table 2: Running time computation**

| Schemes | [7] Method | Our work |
|---|---|---|
| SecretKey Generation | 0.007311 | 0.006981 |
| Machine Generation | 0.006164 | 0.006001 |
| Cipher text Generation | 0.010380 | 0.010213 |
| Security Machine Update | 0.06606 | 0.06606 |
| Data recovery (Original) | 0.049095 | 0.049018 |
| Data recovery (Updated) | 0.032797 | 0.032898 |

 

The table above represent the Computational Comparison Running Time of the system. As compared to the base paper running time our scheme represent quite improvements. The secret key generation time will decrease in our proposed work as compared to base paper computational time. The security key machine generation time is decreased in our proposed work as compared to base paper computational time. It will improve performance of the system in cloud database. The different computational time of base paper and proposed work w.r.t. secret key generation, Security Machine Generation, Cipher text Generation, Security Machine Update, Data recovery

(Original) and Data recovery (Original) is represented in table above.

Computational Comparison Length of size in bits

**Table 3: Computational comparison key Length size**

| Schemes | [7] Method | Our work |
|---|---|---|
| Secret Key Size | 160 | 256 |
| Machine Generation | 640 | 680 |
| Original Ciphertext size | 1600 | 1622 |
| Updated Ciphertext size | 2144 | 2102 |

The table above represent the Computational Comparison Length of size in bits of the system. As compared to the base paper Length of size in bits our scheme represent quite improvements. The secret key size time will increase in our proposed work as compared to base paper Length of size in bits. The security key machine generation time is increased in our proposed work as compared to base paper Length of size in bits. It will improve performance of the system in cloud database. The different Length of size in bits of base paper and proposed work w.r.t. secret key size, Security Machine Generation, original Cipher text, updated cipher text size is represented in above.

## V. CONCLUSIONS

The cloud computing resources are storage, networks, applications, servers, and services. The prospective encounters connected with cloud system database are high availability, scalability data consistency and fault tolerance, integrity, confidentiality and many more. Although data encryption appears the ultimate in-built way out for data privacy. The information and data should be preserved and protected. By using AES key cloud database can guarantee more safety and privacy upgraded performance can be achieved in terms of encryption. We have design a host assisted privacy preservation cloud database which ensures security of the info from illegal access. The audit report is providing by the algorithm when query to the cloud intermediate server. The proposed architecture keep large organization cloud database from data leak and misuse. The experimental result illustrated that our system is fine appropriate for secrecy safeguarding and data leak prevention in cloud database. As direction of future investigation we are planning to introduce machine learning mechanism to improve the data leak detection and audit generation in our algorithm. The machine learning mechanism automatically cluster the user, auditor according to audit report and access control and performance of the system will also improve.

## REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud computing and emerging it platforms: Vision, hype, andreality for delivering computing as the 5th utility," Future GenerationComput. Syst., vol. 25, no. 6, pp. 599–616, 2009.

[2] Peter Mell, Timothy Grance," The NIST definition of cloud computing", http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] RajkumarBuyya,"Introduction to the IEEE transactions on cloud computing" vol 1,januarry-june 2013

[4] M.Armbrust, "A view of cloud computing, communications of the ACM", vol 53, no. 4, (2010).

[5] H. Hacig€um€u¸s, B. Iyer, and S. Mehrotra, "Providing database as a service," in Proc. 18th IEEE Int. Conf. Data Eng., Feb. 2002, pp. 29–38.

[6] B. Sosinsky, "Cloud Computing Bible" Wiley Publishing, Inc., Indianapolis, Indiana 2011

 

[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] Lucca Ferretti,FabioPierazzi,MichelColajani and Micro Marchetti "Performance and cost evaluation of an adaptive encryption architecture for cloud databases" IEEE transactions on cloud computing, vol 2,no.2,April-June 2014

[9] K. Rajasrika, P.S. Smitha "Achieving Cloud Data Sharing Using Key Aggregate Searchable Encryption" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2015

[10] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting confidentiality with encrypted query processing," in Proc. 23rd ACM Symp. Operating Systems Principles, Oct. 2011, pp. 85–100.

[11] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. De Rose, and R. Buyya, "Cloudsim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," Software: Practice and Experience, vol. 41, no. 1, pp. 23–50, 2011.

 