A Fully Distributed Secure Approach using Nondeterministic Encryption for Database Security in Cloud

Mr.Srinu Banothu[1*] A. Govardhan[2] Karnam Madhavi[3]

[1]Research Scholar, JNTUH,
Assistant Professor, Dept of CSE, Vignan Institute of Technology and Science, Hyderabad, India
Email: srinub1307@gmail.com
[2]Professor & Rector, Dept. of CSE, JNTUH,Hyderabad, India
Email:govardhan_cse@jntuh.ac.in
[3]Professor, Deptof CSE,GRIET, Hyderabad, India
Email:bmadhaviranjan@yahoo.com
*Correspondence Author: Srinu Banothu

Summary:
Database-as-a-Service is one of the prime services provided by Cloud Computing. It provides data storage and management services to individuals, enterprises and organizations on pay and uses basis. In which any enterprise or organization can outsource its databases to the Cloud Service Provider (CSP) and query the data whenever and wherever required through any devices connected to the internet. The advantage of this service is that enterprises or organizations can reduce the cost of establishing and maintaining infrastructure locally. However, there exist some database security, privacychallenges and query performance issues to access data, to overcome these issues, in our recent research, developed a database security model using a deterministic encryption scheme, which improved query execution performance and database security level.As this model is implemented using a deterministic encryption scheme, it may suffer from chosen plain text attack, to overcome this issue. In this paper, we proposed a new model for cloud database security using nondeterministic encryption, order preserving encryption, homomorphic encryptionand database distribution schemes, andour proposed model supports execution of queries with equality check, range condition and aggregate operations on encrypted cloud database without decryption. This model is more secure with optimal query execution performance.

Keywords:
Cloud Computing,Database-as-a-Security(DaaS), Cloud Service Provider(CSP),Database Security.

1. INTRODUCTION

Cloud computing is a technology, provides various remote services on a pay and use basis. The cloud services are broadly categorized into three types: 1) Software-as-a-Service(SaaS) 2) Platform-as-a-Service(PaaS) 3) Infrastructure-as-a-Service(IaaS), the prime example of SaaS is Database-as-a-service (DBaaS), it allows organizations and end users to easily outsource their databases and computations and access data whenever and wherever required through any device connected to the internet. DBaaS provides organizations with unlimited data storage servicescost-effectively with higher availability and easy deployment.

A) DBaaS Architecture

The cloud database setup is shown in architecture that the cloud database is hosted by various cloud service providers and available over public cloud network to be rented out, use it as a service. The architecture of DBaaS is shown in figure 1, Cloud databases offerings bundle together a package of database management services, where organizations no need to deploy and manage their database servers and infrastructures, databases are hosted and managed by a third party and accessed by users on the cloud across the globe on pay and use basis. In which any organization or individual user run the application and upload or retrieve the data from cloud databases.

B) Benefits of DBaaS

There are many factors, demanded need for cloud database services and the following are benefits of it.

- Highly Scalable: Infinity data storage capacity

Manuscript received January 5, 2024
Manuscript revised January 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.1.16

- Cost-Effectiveness: this is a major advantage, only pay for what we use, cost of hardware and networking also eliminated
- For businesses struggling to manage their data, the cloud can provide a low cost alternative to investing in the infrastructure to manage it all at their sites
- For DBaaS, the organization pays for what it uses and time it uses, this is also a big advantage to the cloud database service users

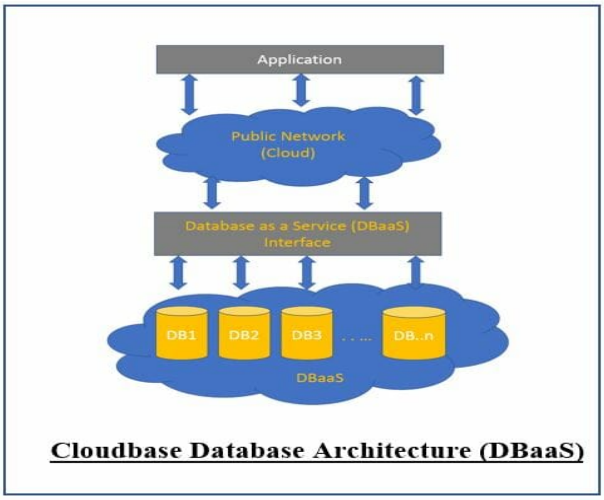

Figure 1. Database as-a-Service Architecture

Along with benefits, there are some challenges also in DBaaS, the biggest challenge is data security and privacy in the cloud environment. Now a day's most organizations or individuals are outsourcing their databases to the cloud environment, the amount of sensitive data stored in the cloud is increasing day by day; hence it should be protected from malicious parties.It introduces new challenges regarding database security and privacy. The major threats to user data are 1) protecting data from external attackers 2) protecting data from cloud service providers. Security and privacy to cloud databases can be provided using 1.Data Distribution Approaches and 2.Data encryption techniques. Authorscontributed their work to protect cloud databases from malicious attacks, few of them used data encryption methods and others used data distribution methods. In this paper we proposed a new model for cloud database security using a combination of data encryption and data distribution approaches, the basic idea of our proposed method is initially all the tuples of a relation are encrypted using AES-CBC-256 algorithm using random initialization vector and a secret key, it outputs nondeterministic cipher blocks for the same plaintext block and then the relation is partitioned vertically with selected columns into two or more fragments and store these fragments of tables into different database instances of the same cloud environment and also one additional index column is added to each table fragment, index column is encoded with the hash function, to retrieve the tuple values, a query will be sent to all database instances, processed on encrypted database tables, the result returned to the user is in an encrypted format, the user will decrypt the result using a secret key. Our proposed methodaddresses the data confidentiality and availability issues of the cloud database and reduces the query processing time to access the data from the cloud database.The remaining part of this paper discusses the concepts: section II covers related work, section III explains the proposed model methodology, section IV Results and Implementation and section V covers conclusion and future scope.

2. RELATED WORK

In 1978,Ronald L.Rivest et al.[1] Introduced encryption is a well-known technique for preserving the privacy of sensitive data, and also presented the limitations of the model. The authors also demonstrated an application that how to protect and access a small loan company data, which uses a commercial time-sharing system to store the records of loan company data bank. For data encryption, privacy homomorphism techniques are used in their model.Also introduced some sample privacy homomorphism, some of them are weak cryptographically and a "chosen ciphertext" attack may break them.

In 1981,George davida et al.[2] proposed a model for database encryption using sub-keys, the basic idea of this scheme is database is encrypted using the Chinese Remainder theorem which satisfies some of the required properties such as security, speed, record level encryption, and attribute based data access by users using distinct sub-keys.

In 2002,HakanHacigumus et al. [3] proposed a model to address the problem of data to be protected from database service providers and also proposed a technique to execute SQL queries over the encrypted database. Introduced adatabase encryption algorithm for the full SQL query. The basic concept of the algorithm is first, every tuple of a relationmust be encrypted with a secure encryption algorithm, then perform weak encryption to the some of the attribute values, it is performed by mapping attribute plain text values into a certain interval and encrypting that interval by a secrete permutation. Then these weakly encrypted attribute values are appended to the actual ciphertext.Therefore different plaintext values may be mapped to the same ciphertext. But the information available in the plaintext may be destroyed a little bit, but this is not the same as in an ordinary encryption scheme. With small post-processing,the remaining information (like the number of tuples of the table, or which tuples have similar values in which secret attributes) is sufficient to query the encrypted database.

In 2006,Evdokimov et al. [4] introduced a new security definition for Database Privacy Homomorphism, the idea is the construction of database Privacy Homomorphism based on a searchable encryption scheme, in this scheme initially, create some words, those are strings of the same length and then identify the attributes of the relation. Then bijectivelyconvert the tuples of the given relation to the sets of words or documents. The number of words in each document is the same as the number of attributes in the relation. The globally fixed word length is equal to the length of an attribute identifierplus the length of the longest attribute value. Then documents are stored on a remote server by encrypting using a searchable encryption scheme.To apply an exact select query on the encrypted relation, queries will be converted into the search operationand processed as a search operation, returning a setof encrypted strings. The strings are then decryptedand convertedinto the corresponding tuples. It is a generic construction for a databasePH, this can be proved to be secure in a relaxed way, but still requires rigorous and plausible sense under widely accepted cryptographic assumptions.

In 2012,DongxiShenluWang et al.[5], contributed work for secure query processing overthe encrypted database, it is named as programmable order-preserving indexing scheme. This scheme is built over simple linear expression of the form a*x+b, the form of expression in public, ‘x’ is the input value and coefficients ‘a’ and ‘b’ are kept secret (not known to attackers). By using linear expression the indexing scheme maps input value ’x’ to a*x+b+noise, where noise is a random value. If noise is carefully selected then the order of input values is preserved. This indexing scheme allows the programmability of basic indexing expressions, in which users can select different linear expressions for different input values for indexing input values. Programmability improves the robustness of the scheme against brute force attacks since there are more indexing expressions. This scheme is used to process range queries over the encrypted database and it only depends on linear expression, so that it is easy to understand by the users. The problem with this scheme is more processing overhead as different linear expressions are used to create indexing for different input values.

Authors in [6] proposed a model for cloud database security in Database-as-a-Service; it provides data privacy and security using data distribution techniques instead of data encryption. This technique is used by the existing netDB2 service. It is based on the multiple service providers and secret sharing algorithm, the basic idea of secrete sharing method is to distribute data to multiple servers to ensure the privacy of user queries. If the user wants to outsource data froma data source (D) to database service providers(DBS1,DBS2,……, DBSn), data is partitioned into *n* shares and *n* shares will be stored in *n* DBS. If the user wants to retrieve the data from DBS, the query will be sent to all DBS and data received from all DBS will be merged and the result will be sent to the user. To reconstruct secrete value Vs at data source D, the knowledge of any K can refer to Vs besides some secrete information X that is known only to the data source. Therefore with the full knowledge of (K-1), DBS will not have any knowledge of Vs, even if X is known to them.In this model, data source (D)selects a random polynomial equation q(x) of degree (K-1), where the constant is Vs. Each DBS has constant Vs and X which is a set of *n* random points.The problem with this model is the availability ofall DBS. If any one of the service provider’s server is down, data cannot be retrieved and another problem is the computational complexity of *n* random polynomial equations for different *n* values. Another issue identified in this model is authors only considered numeric data for encryption, doest talk about non-numeric data.

In 2017, authors in [7] recently proposed a model for cloud database security to improve security level, this model provides security to a cloud database using a combination of data distribution and data encryption techniques. This model uses two types of clouds one is master cloud and another is slave cloud, the master cloud stores the entire database encrypted using some encryption algorithms and the slave cloud stores the extended columns (i.e. vertically fragmented columns)of relation. Keys are not revealed to master cloud service providers. In this model, when a relation for master cloud is created, one additional column is added for storing the indexes of each tuple in that relation. The index column stores the indexes of the tuple in plain text format so that the user can query the relation through that index to access the desired tuples. The index is replicated in each fragment stored in the slave cloud. Here master cloud is a private cloud because it is available within the enterprise limits, it actslike a proxy server, the task of the proxy server is to create relations, insert, delete, encrypt, decrypt and process the queries. The problem with this model is that since it maintains a private cloud locally in the enterprise environment, the same infrastructure has to be established and maintained locally as public cloud, so there is no benefit of cloud service reflected. Another issue is all slave cloud servers must always be available to retrieve the data by users. If any one of the slave cloud servers is down data can't be retrieved, so losing on-demand cloud service. And also increases query processing time to access the data as the query has to be split forwarded to all the slave clouds.

3. METHODOLOGY

In our model, three entities are involved 1. Data Owner 2. Data user and 3. Cloud Service Provider (CSP) or Cloud vendor and the basic architecture of secure Database-as-a-Service (DaaS) modelis shown in figure 2, in which the Data owner outsources databases encrypted using the secure secret key to CSP, then data owner shares the secret key securely to data users through a secure channel, CSP stores the encrypted database, and process the query requests received from data owner or user on an encrypted database. Data users send the query to process on the encrypted database without decryption to CSP, then CSP processes the query and returns the results to the data user.

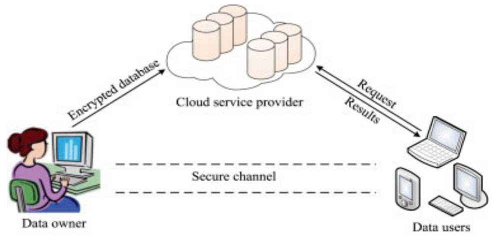

Figure 2: Basic Architecture of Secure Database-as-a-Service (DaaS) model.

In our proposed model we are using the following database encryption schemes in combination with the data distribution approach for enhancing database security in the cloud.

A. Encryption Schemes

Traditional Encryption schemes provide strong security guarantees, such as symmetric encryption algorithms like AES, DES, etc. However, when these traditional encryption schemes are used for database encryption, leads to unavoidable database search and processing problems, those are mainly three types: Equality check, Order Checking and Computability.

Equality Checking: Whenever plaintext data in the database are encrypted using a traditional encryption scheme, the same plaintext blocks may be mapped to different ciphertext blocks if different keys or initialization vectors are used. So that it is very difficult to search text.

Order Checking: When numeric data values are encrypted using a traditional encryption scheme, it losses the order of numeric data, so it is very difficult to search order of data, due to this range queries cannot be applied tothe database.

Computational problem:When plaintext data is encrypted using traditional encryption algorithms, we cannot perform operations like addition or multiplication on ciphertext data. Due to this queries with aggregate functions cannot be applied tothe database.

To overcome the aboveissues, we are using three categories of algorithms in our proposed model, so that we can execute range and aggregate queries on encrypted cloud databases without decrypting the database tables.

- Nondeterministic Encryption
- Order Preserving Encryption
- Homomorphic Encryption

Nondeterministic Encryption: The non-deterministic encryption scheme maps the same plaintext blocks to different ciphertext blocks, wheneverplaintext is encrypted using traditional encryption algorithmslike AES-CBC-256 using a secret key and a random initialization vector value using Cipher Block Chaining (CBC) or Cipher Feedback (CFB) modes. So that it is protected from Chosen Plaintext Attack(CPA). In our proposed model, we used the AES-CBC-256 algorithm for database table encryption, since it is more secure and efficient.

Order Preserving Encryption: The order preserving encryption scheme is used for encrypting numeric data in database relations because it preserves the order of data in the ciphertext. For example if v1,v2 are two integer values and if v1< v2, then it holds the order that Enc(k,v1) <Enc(k,v2), where 'k' is a secret key and Enc(k,v1) is the encrypted values of v1 using secrete key 'k'. So that rage queries can be executed efficiently and securely on the encrypted database without decrypting.It avoids the order checking problem. We used the most popular order preserving encryption scheme used in [8-10], in our model for numeric data encryption.

Homomorphic Encryption: Cipher outputs from homomorphic encryption are more secure and all aggregate operations like sum, sub, min, max and average operations are performed on them without decrypting.For example, if x1,x2 are two plaintext values then E(k,x1)*E(k,x2) is equal to E(k,(x1*x2)) and D(k, E(x1*x2)) is equal to x1*x2, where E(k, x) is the encryption of plaintext values using secrete key 'k' and D(k,C) is the decryption of ciphertext C using secrete key 'k'. So it holds the multiplicative homomorphic property.This encryption scheme is designed for executing aggregate SQL queries on ciphertext blocks without decrypting them. In our model, we used the homomorphic encryption scheme in[7]. This homomorphic scheme is very efficient

B. Proposed model Methodology

First, database relations are encrypted using appropriate encryption schemes,then relations are vertically fragmented with selected columns of relations(i.e. column selection for table partition is based on data sensitivity level) and stored in cloud databases. Two types of databases are used, one is a master database and another is a slave cloud database, master database is used to store the metadata information in the data owner environment, slave cloud databases are used to storethe fragmented tables. The metadata in the master database includes the relations with fields likerelation name, column names and database name; this is required for data owners and data users for easy retrieval of data from cloud databases.For data encryption, AES-256-CBC uses a secret key and a random initialization vector is used for nondeterministic ciphertext blocks so that the same plaintext blocks are mapped to different ciphertext blocks using the same secret key.It provides very good data confidentiality and high security to the data with optimal database encryption time, and we used Order Preserving Encryption (OPE)scheme forexecuting range queries over encrypted cloud database,homomorphic encryption for aggregate query execution over encrypted cloud database and also used the hashing encryption scheme for equality condition checking i.e.blind index, this model is called as fully secure distributed approach(FSDA) using the blind index. The methodologyof my proposed model:

- First,additional columns are added in cloud database relations, one for the blind index for equality check, one column for storing the values encrypted using Order preserving encryption for range condition checking and another column for storing domain values encrypted using homomorphic encryption for aggregate query processing.
- The data owner encodes the primary key column domain values of the table using the hash encoding scheme and stores them in the blind index column of the cloud database table, here the SHA-256 encoding scheme is used.

- Then all numeric column domain values are encrypted using the Order Preserving Encryption scheme [7] and stored in additionally added columns of cloud database for executing range queries over encrypted database table without decryption.
- Data owner also encrypts the domain values of columns using a homomorphic encryption scheme on which aggregate queries are to be processed and store them in additionally created columns in the cloud database.
- Finally, the data owner encryptsall the column values of a relation in a database using AES-256-CBC encryption algorithm, a secret encryption key and a random initialization vector (IV), this key is known only to the data owner and it should be securely shared to the data users.
- Then the encrypted database tables or relationsare vertically partitioned into two or more fragments with selected columns by considering data sensitivity criteria and also add index column for each vertically fragmented relations, this index value must be replicated in all fragments for the tuple of un-partitioned relation so that the user can retrieve the tuple data easily and reduces the query execution time.
- Uploads the encrypted and vertically fragmented table in multiple databaseinstances ofthe samecloud service provider environment.
- Data owner maintains metadata inthe owner-private environment to know the locations of fragments stored in cloud databases.
- Data owners must authenticate users to perform operations on a cloud database, for authentication users must register with the data owner with their details.
- The data owner will share the user credentials with cloud service providers(CSP), so that CSP verify the user credentials with credentials already shared by the data owner to CSP, if a user is valid then CSP grant permissions to the user to access data.
- Data users can send the query request tothe data owner for the metadata information.
- The data user can retrieve the encryption key fromthe data owner and perform operations on databases like selection, insertion, deletion and updating.
- The data owner or user retrieves the data from the cloud database in encrypted form only and performs decryption at the client environment using the secret key. So CSP doesn't have any knowledge about the data stored in the cloud.
- When the user sends the SELECT query to retrieve the data from the database, it must include the JOIN clause with a predicate on the index column.

C) Proposed Model summary steps

Database outsourcing process:

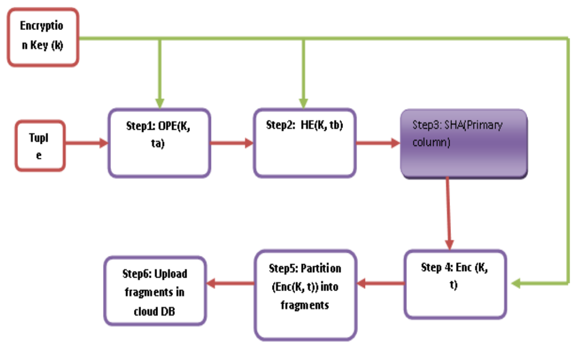

Figure 3: Shows the steps for secure outsourcing of database to cloud environment

Let R (A1, A2, A3…An) be a relation schema of relational database, where R represents relation, A1, A2, An, are columns in relation R. let Aa be a column with numerical values on which range queries are to be executed and Ab be a column on which aggregate queries are to be executed and K represents the encryption key of length 256 bit length.

Steps for secure outsourcing of database to cloud environment:

Step1: Encrypt tuple column t_{a1} value using OPE algorithm i.e. OPE(K, t_a).

Step2: Encrypt tuple column t_{a2} value using Homomorphic algorithm HE(K, t_b).

Step3: Find the hash of primary key column using SHA256 hash algorithm for equality check.

Step 4: Encrypt tuple data using AES-256-CBC using Enc (K, t(a1,a2…aj, ak,..,an))

Step 5: Distribute the encrypted tuple values into multiple database instances.

Step 6: Insert distributed column values into fragmented table columns of cloud databases.
Step 7: Repeat steps 1-5 until all records are uploaded in cloud database tables.

So the advantage of our proposed cloud database security model is that 1) it is strongly protected from Chosen Plaintext Attack(CPA) because, in this model we used a random initialization vector in AES-CBC-256 Algorithm for database relation encryption, it maps the same plaintext into different ciphertext blocks. 2) As database relationsare partitioned vertically and distributed into multiple database instances if the attacker compromises the data in one fragment, cannot get the complete information.The cloud service providers will be unaware of the data stored in the database because all attribute values of records in database relations are stored in ciphertext format.

4. IMPLEMENTATION AND RESULTS

A. Cloud Computing Tools

For simulation of our model, we designed an application using PHP and My-SQL server, also used HTML for front end design, for this installed the XAMPP tool and application is deployed on local system.Then we created a public cloud computing account at cloud clusters.io, which provides an open-source cloud computing service. We have created a My-SQL server managed with PhpMyadmin for experimental purposes and then created two slave databases in the cloud for storing fragments of database relation. The configurations of servers created on the cloud are 3(core) Processors,4GB RAM, 100GB SSD. Then run my application on my local system configured with IntelCore i5 processor,10GB RAM and 360GB hard disk space.The network speed is 150mbps.

B. Results and Performance Evaluation

For ourexperimental work, we have taken employee datasets and stored them in cloud databases.For simulation purposes,we have created two databaserelations onour local system one for storing metadata and another for storing employee records with fields id, emp_id, emp_name, emp_email, emp_salary, and emp_age., this is called data at data owner side, we also created two slave databasesin cloud environment each one for storing fragmented relations and also note that we can create more number of slave databases, which may be equivalent to several fields in data owner base table. We have created a fragmented table schema in slave database1 with fields id, emp_id,emp_name,emp_email and blindindex, here the blindindex column is used to store the hash encoded values of emp_id field,and here we have taken emp_id filed as the primary key. Also created another fragmented table in slave database2 with two columns i.e. emp_salary, and emp_age. Then1000 records of employeesare encrypted using a suitable encryption scheme and inserted into the cloud databases, the results are shown in figures. Figure 4 shows the data stored in the data owner local system, it is in plain text format. Figure 5 shows the data stored in a vertically fragmented table in cloud database server 1, in which field values emp_id, emp_name and emp_ email are encrypted by data owner using the AES-256-CBC algorithm and secure encryption key and stored in cloud, bindex column values are encoded values of emp_id column using an SHA-256 encoding scheme, bindex column values are required for executing select queries with equality check condition on encrypted database relation without decryption in the cloud environment. Figure 6 shows the data stored in a vertically fragmented table in cloud database server2, these column values are encrypted by the data owner using the AES-256-CBC algorithm and secure encryption key and stored in the cloud.

Emp ID	Employee Name	Email Id	Salary	Age
cse_01	Manoj	manoj@gmail.com	24000	34
cse_02	Jasmitha	jasmitha@gmail.com	15000	21
cse_03	srinu	srinu@gmail.com	34000	40
cse_04	padma	padma@gmail.com	18000	32
cse_05	praveen	praveen @gmail.com	29000	39
cse_06	venkat	venakt@gmail.com	40000	40
cse_07	raju	raju@gmail.com	45000	45
cse_08	rani	rani@gmail.com	12000	40
cse_09	sonu	sonu@gmail.com	33000	34
cse_10	JUNAID ASHRAF SOFI	JUNAIDASHRAF 02018@GMAIL. COM	54000	28
cse_100	NANJUTI VARSHITHA	varshitha@gmail. com	108500	53
cse_101	NIDRA UDAYA SREE	nidrapaemaiah12 3@gmail.com	110000	51
cse_102	NIMMALA GANESH	ganesh@gmail.com	111500	49
cse_103	NYAVANANDI SURAJ	suraj@gmail.com	113000	47
cse_104	YELLAMCHERV U ALEKHYA	alekhya@gmail.c om	114500	45
cse_105	PAMIREDDY MONIKA	venkatareddy185 4@gmail.com	116000	43
cse_106	SEEMA TABASSUM	mdjunaid.464@g mail.com	29178	41
cse_107	SHRIYA GURRAM	SHRIYA@GMAI L.COM	26476	39
cse_108	THATIKONDA AKHIL KUMAR	tsksridhar1@gm ail.com	67527	60
cse_109	ALAMPALLY NIKHIL	rkumar@gmail.c om	90296	32
cse_11	ANDELA RAHUL	RY1318297@G MAIL.COM	52000	34
cse_110	ALE VINAY	vinay99@gmail.c om	26388	31
cse_111	ALUGULA HARSHA VARDHAN REDDY	mattareddy.alugu @gmail.com	24053	59
cse_112	ARRAGONI BALARAM	balaram99@gma il.com	55635	62
cse_113	AYYALASOMAY AJULA ADITYA SUDEEP SAI	sudeep280700@ gmail.com	75658	45
cse_114	BUJJI ASHRITH	bujji_bnr43@redi ffmail.com	48521	49
cse_115	BOLISETTY NIKHIL GUPTA	NIKHILGUPTA@ GMAIL.COM	20726	28
cse_116	GUNUPUDI VENKATAPAVA NMANIDEEP	manideep pvana@gmail.co m	50676	63
cse_117	BATTULA ASHISH GOPI	gopi99@gmail.co m	60966	66
cse_118	BEERELLI SADASHIVA REDDY	madhukarreddy @gmail.com	48156	37

Figure 4. Data to be outsourced by the data owner

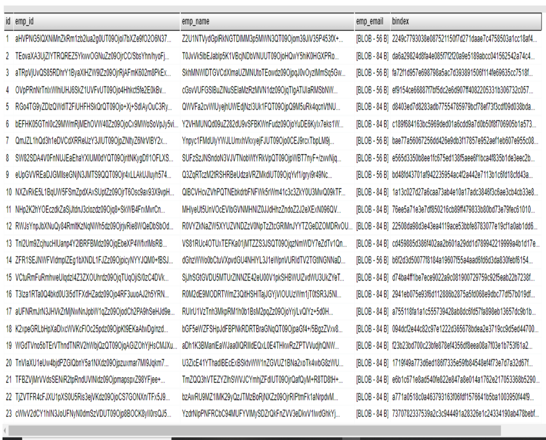

Figure 5. Fragmented data stored in cloud database server1

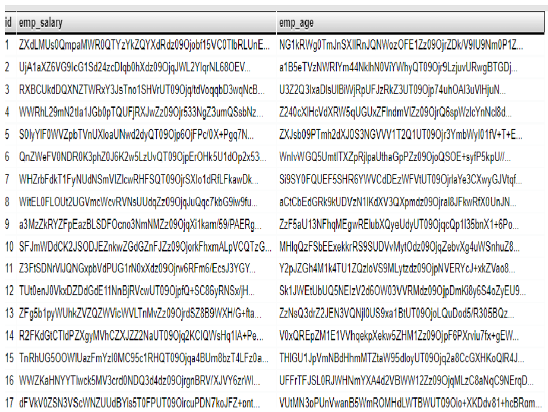

Figure 6. Fragmented data stored in cloud database server2

Figure 7. Emp_age field values encrypted using homomorphic encryption

id	OPE(K,Salary)
1	656206284
2	1309397157
3	1634916838
4	980842854
5	1181804128

Figure 8. Emp_salary encrypted using Order Preserving Encryption

Figure 7 shows the emp_age column values encrypted using a homomorphic encryption schemeby the data owner and stored in a cloud database for executing SQL queries with aggregate functions on an encrypted cloud database without decryption. Figure 8 shows the emp_salary column values encrypted using an order preserving encryption scheme by the data owner and stored in a cloud database for executing SQL queries with rangeconditions on encrypted cloud database without decryption.In our proposed model we have stored these column values in an isolated cloud server, these records are retrieved using the replicated id column values in each fragmented table.

We evaluated the performance in terms of a time delay to encrypt and upload the data in cloud databases and to retrieve from a cloud database, decrypt at the client-side and show the result to the user. The performance of our method is compared with the existing methods. For performance testing of our proposed model, the first 106 records are encrypted and inserted in cloud databases then 206,306,406,506 and 606.

Table 1: Time delay in seconds to encrypt and insert the records in cloud databases

Time delay to upload Data in Cloud database(Seconds)		
No. of Records	SCA(sec)	FDSA(sec)
106	58.87	87.39
206	114.22	184.69
306	177.63	265.06
406	243.00	349.15
506	297.23	442.66
606	423.89	473.61

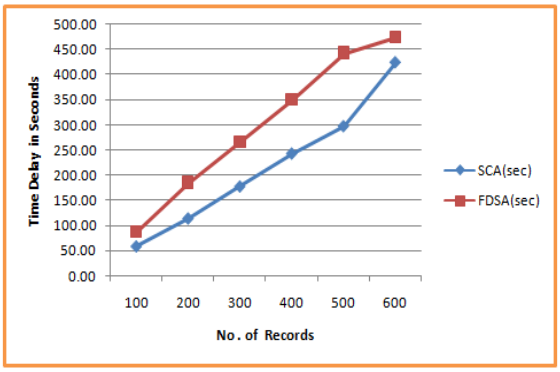

Figure 9:Time delay in seconds to encrypt and insert the records in cloud databases of FDSA and SCA models

Table 1:shows the performance in terms of the time delay of Secure Centralized Approach (SCA) and Fully Distributed Secure Approach (FDSA) using nondeterministic encryption (i.e. our proposed model)) for encrypting and inserting the records in cloud databases. The data recorded in table 1 areused to compare the time delay ofthe existing model with our proposed model for encrypting and executing INSERT/UPDATE query to insert or update data in the cloud database.

Figure 9: shows that our proposed model performance in terms of time delay for encrypting and inserting the data in cloud database is a little bit slower than the existing model, but as security is a concern our model is more secure than the existing models.

Table 2: Time delayfor Select query execution to retrieve all records from cloud database and data decryption at client side

Time delay to Retrieve Datafrom cloud database (seconds)		
No. of Records	SCA(sec)	FDSA(sec)
106	1.02	1.04
206	1.89	1.82
306	2.74	2.76
406	3.50	3.03
506	4.29	4.18
606	4.62	5.18

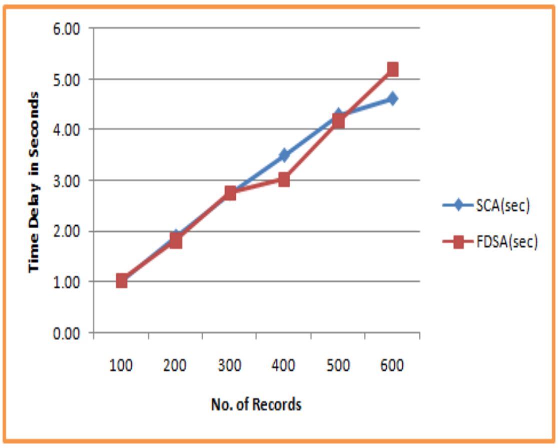

Figure 10:Shows time delay for Select query execution to retrieve all records from cloud database and data decryption at client side of SCA and FDSA models

Table 2: shows the data recorded for testing the performance in terms of time delay forSELECT query execution to retrieve all records from cloud database and data decryption at the client-side with a varied number of

records such as 106,206,306,406,506 and 606 recordsof our proposed model and SCA models.

Figure 10: shows that our proposed model performance in terms of time delay for SELECT query execution on cloud database servers and decrypting the results returned by the query at the user side is almost the same as the existing model, but as security is a concern our model is more secure than the existing models.

5. CONCLUSION AND FUTURE SCOPE

In this paper, we proposed a model for cloud database security using data distribution and nondeterministic encryption approach, in our model we used AES-256-CBC algorithm, order-preserving encryption and homomorphic encryption schemes for database encryption and distributed database vertical fragmentation technique is used for data distribution, in which databasetables are vertically partitioned with selected columns based on the data sensitivity level.For implementing our model, designed a web application using PHP and My-SQL, we run our application using the XAMPP tool on the local machine and created a database server on open source cloud service provider cloudcluster.io and evaluated the performance of SELECT query execution with equality check, range check predicates in WHERE clause on encrypted cloud databases and measured the time delay to access the data from the cloud.In our research, we have compared the performance of our model with existing methods and found our model is more secure with optimal query execution time. Our future research is to introduce novel methods to further enhance the data upload performance.

References

[1] Ronald L. Rivest Len Adleman, Michael L. Dertouzos "On Data Banks And Privacy Homomorphisms" Massachusetts Institute of Technology Cambridge, Massachusetts Copyright © 1978 by Academic Press, Inc

[2] George I. Davida, David L. Wells, "A Database Encryption System with Sub-keys", ACM Transactions on Database Systems, Vol. 6, No. 2, June 1981, Pages 312-328.

[3] Hakan Hacıgum, Bala Iyer, Chen Li, Sharad Mehrotra "Executing SQL over Encrypted Data in the Database-Service-Provider Model", ACM SIGMOD '2002 June 4-6, Madison, Wisconsin, USA Copyright 2002 ACM 1-58113-497-5/02/06 ...}.

[4] Elisa Bertino, and Ravi Sandhu, "Database Security—Concepts, Approaches, and Challenges", IEEE Transactions On Dependable And Secure Computing, VOL. 2, NO. 1, January-March 2005

[5] Evdokimov, S. Fischmann, M. Gunther, "Provable Security for Outsourcing Database Operations", Proceedings of the 22nd International Conference on Data Engineering (ICDE'06) 8-7695-2570-9/06 $20.00 © 2006 IEEE

[6] Sergei Evdokimov, Oliver Gunther, "Encryption Techniques for Secure Database Outsourcing", ESORICS 2007. LNCS, vol. 4734, Springer, Heidelberg (2007) (http://www.springerlink.com/content/978-3-540-74834-2/)

[7] Dongxi Liu, Shenlu Wang, "Programmable Order-Preserving Secure Index for Encrypted Database Query", IEEE Fifth International Conference on Cloud Computing, 978-0-7695-4755-8/12 $26.00 © 2012 IEEE

[8] Dongxi Liu, Shenlu Wang, "DEMO: Query Encrypted Databases Practically", CCS'12 October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10.

[9] Lei Xu, Xiaoxin Wu, Hub: HeterogeneoXs Bucketization for Database Outsourcing, Cloud Computing'13, May 8, 2013, Hangzhou, China. ACM 2013 978-1-4503-2067-2/13/05 ...$15.0

[10] Luca Ferretti, Michele Colajanni, and Mirco Marchett, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", IEEE Transactions on Parallel and Distributed Systems, VOL. 25, NO. 2, FEB 2014.

[11] Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian, and Jinguang Han, Member, IEEE, Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing, IEEE Transactions On

Services Computing, VOL. 10, NO. 5, SEPTEMBER/OCTOBER 2017

[12] Cheng Guo, Ruhan Zhuang, Yingmo Jie, Yizhi Ren, Ting Wu3, Kim-Kwang and Raymond Choo, "Fine-grained Database Field Search Using Attribute-Based Encryption for E-Healthcare Clouds" J Med Syst(2016) 40:235 DOI 10.1007/s10916-016-0588-0

[13] Md Abdullatif ALzain and Eric Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", Proceedings of the 44th Hawaii International Conference on System Sciences – 2011, 1530-1605/11 $26.00 © 2011 IEEE, Pg. No: 1-9

[14] Amjad Alsirhani, Srinivas Sampalli, Peter Bodorik, "Improving Database Security in Cloud Computing by Fragmentation of Data", International Conference on Computer and Applications (ICCA), 978-1-5386-2752-5/17/$31.00 2017 IEEE

[15] Youssef Gahia * and Imane El Alaoui, "A Secure Multi-User Database-as-a-Service Approach for Cloud Computing Privacy", International Workshop on Emerging Networks and Communications (IWENC 2019) November 4-7, 2019, Coimbra, Portugal, Science Direct Available online at www.sciencedirect.com Procedia Computer Science 160 (2019) 811–818

[16] K. Madhavi, G. Ramesh, K. Sowmya, **CICIT,** pp 630-636 (2019).

[17] Srinu Banothu, A.Govardhan, Karnam Madhavi, Performance Comparison of Cryptographic Algorithms for Data Security in Cloud Computing, Journal of Information and Computational Science, ISSN: 1548-7741, Volume 11 Issue 9 – 2021,Pg.No 1-8.

[18] Srinu Banothu, A.Govardhan, Karnam Madhavi, Performance Evaluation of Cloud Database Security Algorithms, E3S Web of Conferences 309 in *ICMED 2021.*

[19] Bih-Hwang Lee,Ervin Kusuma Dewi, Muhammad Farid Wajdi,Data Security in Cloud Computing Using AES Under HEROKU Cloud,The 27th Wireless and Optical Communications Conference (WOCC2018).

[20] Mr. Manish M Poteya, Dr C A Dhoteb, Mr Deepak H Sharmac,Homomorphic Encryption for Security of Cloud Data,7th International Conference on Communication, Computing and Virtualization 2016.

[21] S.Rajeswari,R.Kalaiselvi, Survey of Data and Storage Security in Cloud Computing,Proceedings of 2017 IEEE international conference on circuits and systems(ICCS2017).

[22] Nishit Mishra, Tarun Kumar Sharma, Varun Sharma and Vrince Vima,Secure Framework for Data Security in Cloud Computing,©Springer Nature Singapore Pte Ltd. 2018.

[23] Krishna Keerthi Ch,Lakshmi Muddan,Rajani Kanth A,Performance Analysis of various Encryption Algorithms for usage in Multistage Encryption for Securing Data in Cloud,2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017.

[24] P.Y.A.Ryan,Preta Voter with Paillier encryption, Mathematical and computer modelling,Elsevier pg.No 1646-16662,2008

[25] Mbarek Marwan, Ali Kartit and Hassan Ouahmane,Applying Homomorphic Encryption For Securing Cloud Database,978-1-5090-0751-6/16/$31.00 ©2016 IEEE

[26] Radjab Harerimana,Syh-Yuan Tan and Wei-Chuen Yau, A JAVA IMPLEMENTATION OF PAILLIER HOMOMORPHIC ENCRYPTION SCHEME 2017 Fifth International Conference on Information and Communication Technology (ICoICT). ISBN: 978-1-5090-4911-0 (c) 2017 IEEE

[27] Si Chen, Lin Li, Wenyu Zhang, Xiaolin Chang, Zhen Han,BOPE: Boundary order-preserving encryption scheme in relational database system,IEEE Open Access Journal 2017.

[28] Rivest R.L. (1993) Cryptography and machine learning. In: Imai H., Rivest R.L., Matsumoto T. (eds) Advances in Cryptology — ASIACRYPT '91. ASIACRYPT 1991. Lecture Notes in Computer Science, vol 739. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-57332-1_36