SDAC - SECURE DATA STORAGE AND POSITION BASED ACCESS CONTROL IN CLOUD USING KEY SHARING SYSTEM

Dipa Dattatray Dharmadhikari
Research scholar, CSIT,
Babasaheb Ambedkar Marathwada University,
Aurangabad Maharashtra
431001

Dr Sharvari Chandrashekhar Tamane
Professor and HoD, IT, JNEC, MGM University,
Aurangabad
431001

Abstract

A health record is viewed as an essential component for managing and saving patients facts. Because the data will be accessed through interoperable devices and various owners, privacy and security are the most important processes to shield the health records in the public cloud platform. In the proposed, SDAC – secure data storage and position-based access control in cloud using key sharing system - patients manage and securely send their medical records in a unified manner in order to readily access the data in the cloud platform. Furthermore, before transferring the data to storage, each record was encrypted through chipertext and identity-based encryption mechanisms, as well as privacy access method also enabled. The data is kept by plentiful tables that are connected together depending on attributes and the tables that are reserved up to date are stated to as source tables. The source table is used to create the shared database instance for the cloud tenants. These shared tables and shared database instances STSI structures are created by combining data from numerous tables. During the download, the data is collected from the STSI table. Additionally, data between renters is mapped using the shared nearest neighbour method. During data storage and retrieval operations, encryption and decryption processes are carried out; the ciphertext is generated from the plaintext using the polynomial, encryption key, hash function, and policy. At the end of the decryption process, the secret key is revealed to obtain the plaintext.

Keywords: Storage; Attribute, Connected Tables; Privacy; Encryption; Decryption.

1. Introduction

Authors Cloud computing is viewed as a viable architype for deploying applications, software, and data over the Internet; additionally, hardware, applications, data, and software in data centres provide services. It is the technology deliver lots of services to the users. the services include the processor, memory, storage, application, database, software's, graphical utilization, and analysis over the internet. The resource sharing provides faster, flexible, innovative, economic scalable hardware components and software distributions depending on the user requirements. The advantage of cloud platform access is. the users can pay only for the requirements and period they are going to use. Also, according to the requirement, the users can change the hardware, software, platform usage and when they don't want to use then they can turn off the instance. The technology reduces the user purchasing cost and creates the infrastructure as they need as follows:

- Users can build hybrid cloud and multi cloud
- Data storage
- Big data analysis
- Developments and validations
- Disaster recovery
- Archiving and backup
- Social network
- Business infrastructure development

The data centers are the huge worldwide cloud network which is upgraded regularly with the current technology, it provides the cost reduction, minimum delay and scalability. According to the security system the transactions are protected by the service providers. But still, the security mechanism should be improved consistent with the day to day requirements and software developments. Users can decide to operate the cloud service as per the required content and time, this flexibility and operations are managed by the servers. The cloud offers to the users to save their documents and retrieve it by any accessible device and anywhere by anyone who authorized for it from web interface. So, the users can have maximum accessing speed, data viability, and security from anywhere.

Cloud is the technology and service in which users' network is hosted on cloud. The technology is centralized manage in which multiple computing resources share identical platform and users can enable to operate these resources to specific extent. Various sectors used the technology for speed process and resource management. Based on the cloud service users can improve the communication. The system provides globally positioned servers, and users move among the interconnected servers to save and retrieve the data. Because of the centralized service all the resources are visible to the required users called as tenants, thus, the technology needs utmost performance and security. The tasks are shared among the cloud environment. Security is given to get enter to the infrastructure, the gateway provides contextual access code and firewall of multi-layer, applications and other services are given to data centres.

The proposed SDAC - method focused to store and maintain the medical records securely in cloud environment as an outsourcing database as shown in Figure.1. The data was transferred to storage by the user through the providers. The data centre has numerous nodes, and data is saved and maintained at multiple remote servers via the functional dependence method. The service provider will handle active database maintenance, while a physical table will store dynamic user data. Medical data includes subtle information such as diseases and their roots, patient status, treatment specifics, doctor's information, and so on. Attributes are required to build the database in order to keep these records. These measurements are classified as substantial or non-substantial. The major substantial metrics are kept in the classic table, while the least significant metrics are kept in the ground table; ultimately, non-significant statistics are kept in the auxiliary table. These data are dynamically saved and retrieved by multiple users. To arrange the dynamic data, the attributes are clustered using the shared nearest neighbour method.

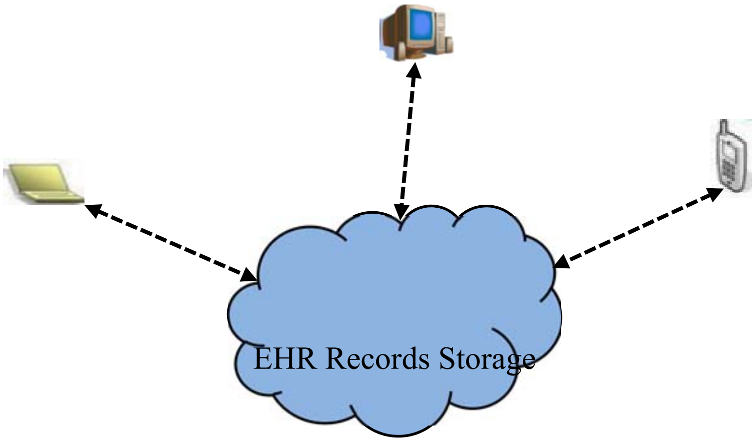


Figure.1 Cloud Storage

Then the database should be encrypted and then outsourced to the servers. Because the database can share with various systems, so the information in the database should be encrypted before stored in the cloud server, then the users will decrypt the data through the shared key.

2. Related Work

Cloud computing assign remote services with a user's data, computation, and software. It is a model which provide on demand access to a shared pool computing resource like servers, storage, networks, applications, and services. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It depends on sharing of resources to acquire coherence and economy of scale over a network [1].

In a multi-tenant SaaS architecture fragments are allocated to the sites where they are most frequently accessed, aiming at maximizing the number of local accesses compared to accesses from remote sites. The cost of the read operation can be further reduced by the replication of fragments when beneficial. Fragmentation, allocation, and replication will be referred to as FAR in the rest of the paper [2].

Healthcare organizations generate a wide range of data and information. Big data in the field of health need infrastructure for better storage and management. Patient data availability is one of the most vital needs in the health and medical industry. Also, health researchers need easy access to extensive data for scientific analysis [3].

A cloud uses technology of multitenancy to share IT resources among multiple applications and tenants securely. Virtualization-based architectures is used by some clouds to isolate tenants, and some uses custom software architectures to get the job done. In this paper we have shown the proposed architecture for standing tenant placement for query request with sample HR benchmark design combined both approaches in memory and multitenancy [4].

Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [5].

In a multi-tenant SaaS architecture, different data layer designs have been proposed and used in different domains. The only difference between these designs is the level of the data separation for all tenants. Regardless of the design used for the data layers, service providers face enormous [6].

Cloud computing provides various facilities for the users like scalability, special computational mean and reducing workload and reducing capital expensive [7]. It consists of large-scale central servers, numerous edge servers deployed at the network edge, and a huge number of distributed end devices. Instead of considering them as separated parts, most applications require all of them to be well orchestrated for providing reliable services over different temporal and spatial scales [8].

The communication is, however, based on the ability of the communicating devices to encode and decode text messages and multimedia messages. The real challenge is converting the actual environment on the server to a remote environment on the cell phone. Several issues relate to the process but of concern is the generation of the scheduling and virtual environment [9].

Cloud computing is performing computing tasks via a network connection while remaining is isolated from the complex computing hardware and networking infrastructure' No User need to know about how cloud computing works, or how to control over the technology infrastructure in the cloud environment [10].

We propose an efficient framework for mobile edge-cloud computing networks, where the MEC and the cloud can share their computing resources with each other in the form of wholesale and buyback. We formulate the computing resource management at the MEC and the cloud as profit maximization problems, which are coupled by the wholesale and buyback process [11].

We start from the analysis of why we need edge computing, then we give our definition and vision of edge computing. Several case studies like cloud offloading, smart home and city as well as collaborative edge are introduced to further explain edge computing in a detailed manner, followed by some challenges and opportunities in programmability, naming, data abstraction, service management, privacy and security [12].

The resources has led to huge investment, at the same time; hiring skilled manpower was cumbersome as well as expensive. Non-IT Organizations, specifically small and medium enterprises were searching for cheaper and reliable computing environment. To cater the need of such users, a new paradigm popularly known as cloud computing has emerged [13].

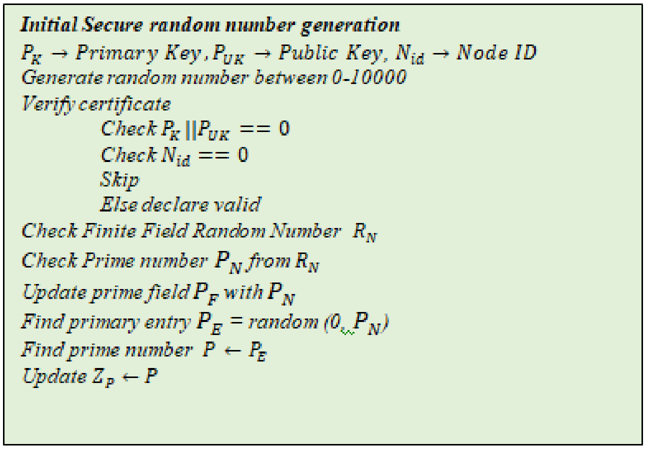
Cloud computing, massive computing capabilities are delivered as services using virtualization and service-oriented techniques to reduce cost, improve performance, or allow remote access. Mobile cloud computing enables large and powerful computing capabilities to be delivered as services. This allows mobile devices with limited resources to perform complex computations that require more powerful computing resources [14].

The tuples present in each tenant is loaded in its specific secluded tables designed after the base method and the storage is done in the private table in the common database case. The private tables that exist among various tenants are independent in nature. In this study, an adaptive database schema design technique for multi-tenant applications is proposed [15].

2.1. *SDAC Design and Implementation*

2.1.1. Network Model

The hierarchical cloud network constituted by user devices U_D (Tenants), access points A_P, internet gateways G_W, cloud host Servers C_S, and cloud storage devices S_D as shown in Figure:2 Cloud computation C_S, is a term used to describe the technological progress in distributed computing systems. Data is generated at the user end and transmitted to the cloud host via access points and gateways as well the server delivered data to the users. The same way U_D will send a query to the server to get response from it. The storage of the cloud database is maintained by efficient storage entities. The network was built with efficient data storage and safe data uploading and downloading mechanisms through chipper text. The bilinear map is used to construct a cryptosystem, which includes key sharing, identity-based encryption, short-term signatures, and other features. The following steps described the secure random number Z_P generation.



```
Initial Secure random number generation
$P_K$ → Primary Key, $P_{UK}$ → Public Key, $N_{id}$ → Node ID
Generate random number between 0-10000
Verify certificate
        Check $P_K || P_{UK} == 0$
        Check $N_{id} == 0$
        Skip
        Else declare valid
Check Finite Field Random Number $R_N$
Check Prime number $P_N$ from $R_N$
Update prime field $P_F$ with $P_N$
Find primary entry $P_E$ = random $(0, P_N)$
Find prime number $P \leftarrow P_E$
Update $Z_P \leftarrow P$
```

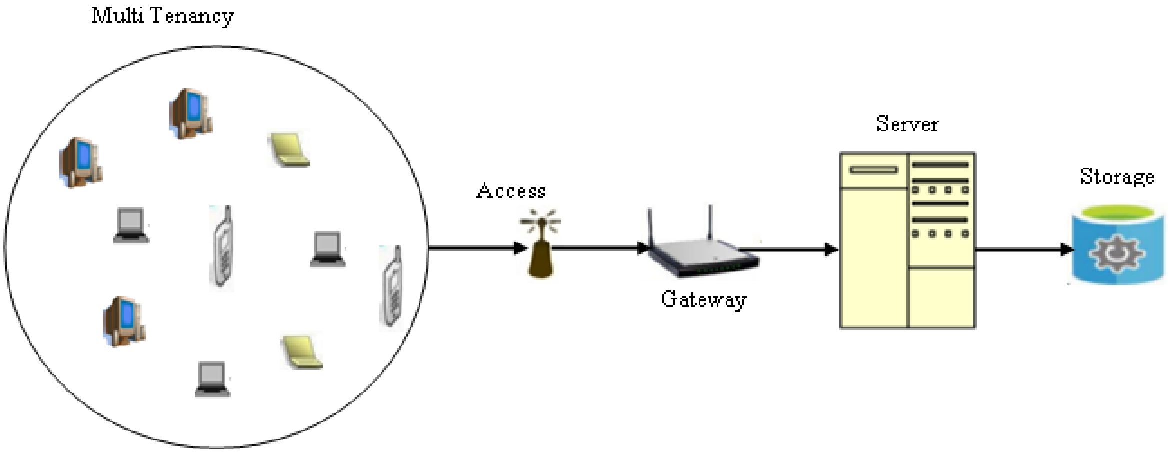


Figure 2 Cloud Network

2.2. *Active Storage Formation*

The most significant aspect of cloud network is effective database creation, the database has several tables $T = t_1, \dots. t_n$ that are linked together also they are called as source tables, The database is available in the private, public, or hybrid cloud platform, and it should be well-organized in order to access easily. The network is created with the dynamic database that can add, delete, and update the contents in response to environmental changes. To preserve the confidentiality of private health records, the strategy focused on storing health data in a safe way based on a privacy-based security-preserving mechanism. The network was designed with multi-tenancy, database confidentiality, and scalability method, here, the core database is created with the set of attributes A_T and objects to build the active storage as shown below here we are maintaining five set of medical information at each table called as source, in addition conversion table called as physical table.

Doctor Details	Patient History	Patient Details	Prescription	Medicine
Doctor Name	Patient ID	Patient Name	Prescription ID	Inventory ID
ID	Hospital Name	S.no	Patient ID	Name
Gender	Disease Name	Gender	Medicine Name	Manufacture
Age	Completion Duration	Age	Number of days	Price
Specialization Designation	Visiting Start Date	Position		Quantity and Expired date
Hospital Name	Visiting Last Date	Phone.no		
Correspondence Address	Current Status	Address		
City and Zip		City and Zip		

Table.1 Attributes and Objects

A collection of tables designed to keep health records in the most scalable form through the shared table and shared data instances STSI. A single cloud instance in the network serves numerous users; to serve a larger number of users, several databases need be developed to handle the performance. The data is taken from the STSI structured table during the download, and the join operation is avoided. The ground table of the STSI structure is formed from the classic table. The auxiliary table is then built from the other fields of the ground table by deleting the additional fields. It provides a dynamic framework for the tables that are stored in several cloud tenants.

The Pearson method is used to calculate the coefficient correlation based on the properties of the table entries. Furthermore, data between tenants is mapped through shared nearest neighbor approach as shown in Figure. 3.. The data distance between the tenants is used to create the distance matrix. The distance matrix is used to get the optimal value for each row.

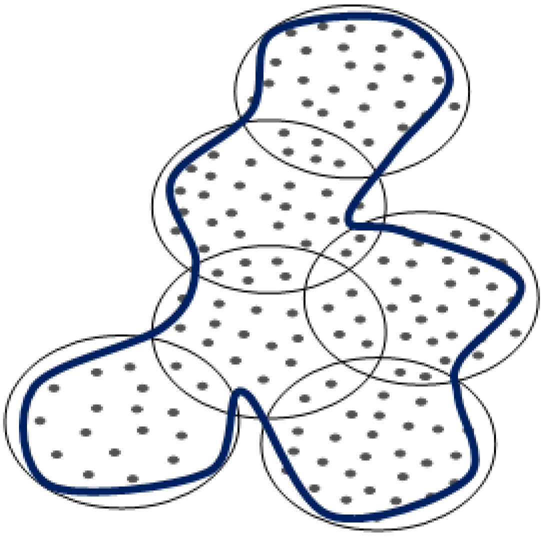


Figure.3. Shared Nearest Neighbor

Because data generation in the network is dynamic, it requires dynamic updates on a regular basis; additionally, the update should be classified according to the attribute in cluster $\boldsymbol{C}$ form. The cluster set is produced depending on the size, density $\boldsymbol{D_S}$, and shape of the data as shown in Figure.4. The shared nearest neighbor $\boldsymbol{S_{NN}}$ clustering approach is used to cluster the data according to the attribute from the dynamic collection, here $\boldsymbol{C_T}$ is the cloud count, $\boldsymbol{M_P}$ is minimum points. The algorithm computed the utmost similar data points to build the $\boldsymbol{K}$ neighbors set from $\boldsymbol{C_{Ti}}$, $\boldsymbol{C_{Tj}}$. Here, $\boldsymbol{C_{DCi}}$ is the data records and $\boldsymbol{C_{TCi}}$ is the tenant records.

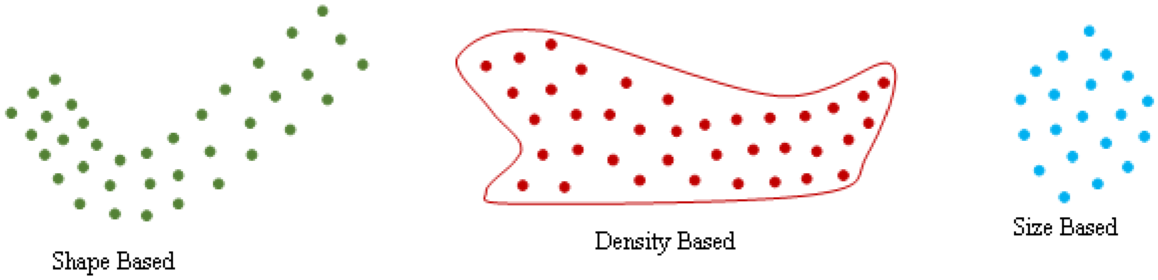


Figure.4. Data Parameter

The distance D_{ist} computation provide the distance from i and j. Here i contains the data points and j provides the tenant information. From these calculations we found the essential data points and noise data points, based on the essential point attributes the cluster will form, C_{Cj} is the minimum density value. The M_P and D_S are computed from neighbors who shared the A_T frequently to form the clusters and the cluster count will vary based on the network access and the K value will be balanced among these clusters.

$$C = M_P$$
$$D_S = \min(C, C_T)$$
$$S_{NN} = [C_{DCi}][C_{TCj}]$$
$$K = C_T$$
$$Update\ C_{Ti} and\ C_{Tj}$$
$$D_{ist} = (i - j^2)$$
$$S_{NN}[i][j] = D_{ist}$$

$$If\ D_{ist} < D_S\ Update\ K$$
$$if\ D_{ist} < D_{ST}$$
$$Update\ M_{DS} \pm D_{ist}K$$
$$If\ M_P \to 0||M_P < K$$
$$M_P = K$$

$$XY = X_{[i]}Y_{[i]}$$
$$S_X \pm X_{[i]}, S_Y \pm Y_{[i]}$$
$$S_{X2} \pm X_{[i]}X_{[i]}, S_{Y2} \pm Y_{[i]}Y_{[i]}$$
$$r = \frac{\dfrac{X,Y - (\,S_X,\,S_Y)}{n}}{\sqrt{\dfrac{|\,S_{X2} - \,S_X{}^2|}{n}\dfrac{|\,S_{Y2} - \,S_Y{}^2|}{n}}}$$

Then, prepare the DSSN list and validate the count in it, as well as the verify the PSSN list to authorize the patient information. Then, along with random numbers R_{ND}, check the doctor's count, specialization, and ID in the DSSN list. Check the patient counts and R_{ND} for them in the patient list - PSSN list as well. Then, create the patient's information and history as follows.

Position based Random number	***Specilization based Random number***	***Disease based Random number***
$Select\ Random\ number\ R_{ND}(0-1)$ $If\ R_{ND} < 0.333 \to Junior$ $If\ R_{ND} < 0.666 \to Senior$ $else \to Trainer$	$Select\ Random\ number\ R_{ND}(0-1)$ $If\ R_{ND} < 0.14 \to$ General $If\ R_{ND} < 0.28 \to$ Cardiology $If\ R_{ND} < 0.42 \to$ Dermatology $If\ R_{ND} < 0.56 \to$ Ophthalmology $If\ R_{ND} < 0.7 \to$ Gynecology $If\ R_{ND} < 0.84 \to$ Pediatrician $else \to$ Dental	$Select\ Random\ number\ R_{ND}(0-1)$ $If\ R_{ND} < 0.14 \to$ Headache $If\ R_{ND} < 0.28 \to$ HeartAttack $If\ R_{ND} < 0.42 \to$ SkinItching $If\ R_{ND} < 0.56 \to$ CataractOperation $If\ R_{ND} < 0.7 \to$ Pregnancy $If\ R_{ND} < 0.84 \to$ Pneumonia $else \to$ CavitiesCleaning

Check the patient ID and position from the cloud list to identify the patient's status. Gender can be classified as male or female, and age should be divided into minimum and maximum age ranges. The medication information and prescription are then updated periodically.

The data is then saved in a cloud bucket. It is useful for saving and deleting content from it. It has a distinct name and access restrictions. We may allocate who can access the data and to what extent they can access it using access control. To secure the content, it will provide position-based access control. Each object in cloud storage has a number of entries. Because the cloud data is accessed by many users, so, the cloud network stores the following user information:

Device ID	Device Type	User ID

The data bucket has the following data accessing information:

Device ID	Cloud ID	Data Content	Accessed Port ID	Access Counts

The network cloud centre contains the cloud host, which encompasses the user devices. The host is constructed with a host ID, a cloud ID, and current data, the host list keeps track of each host's information. The internet service provider class keeps track of the access point's ID, accessed data, maximum access, accessed device ID, number of device accessing, and maximum accessed port. The access point list keeps track of the number of available access points.

The source tables are separated into numerous tables, and table entries are kept in each tenant. The STSI structure is carried out using the existing data by merging it from multiple tables. It contains DSSN, name, address, age, gender, position, specialist, and phone, check the counts C and data limits, as like patient information also updated. The data stored in cloud table as given below. Here, D_L , P_L, C_C are the data limit, patient limit, and cloud count.

$$If\ C > \frac{iD_L}{C_C}\ andC < \frac{(\,i+1)D_L}{C_C}$$

$$Update\ STSI\ Count\ and\ ID$$

$$If\ C > \frac{iP_L}{C_C}\ and\ C < \frac{(\,i+1)P_L}{C_C}$$

$$Update\ STSI\ Count\ and\ ID$$

$$If\ C > \frac{iH_L}{C_C}\ and\ C < \frac{(\,i+1)H_L}{C_C}$$

$$Update\ STSI\ Count\ and\ ID$$

$$If\ C > \frac{iR_L}{C_C}\ and\ C < \frac{(\,i+1)R_L}{C_C}$$

$$Update\ STSI\ Count\ and\ ID$$

$$If\ C > \frac{iM_L}{C_C}\ and\ C < \frac{(\,i+1)M_L}{C_C}$$

$$Update\ STSI\ Count\ and\ ID$$

Update STSI Structure

$$If\ C > \frac{iD_L}{C_C}\ and\ C < \frac{(\,i+B)D_L}{C_C}$$

$$If\ C > \frac{iP_L}{C_C}\ and\ C < \frac{(\,i+B)P_L}{C_C}$$

$$If\ C > \frac{iH_L}{C_C}\ and\ C < \frac{(\,i+B)H_L}{C_C}$$

$$If\ C > \frac{iR_L}{C_C}\ and\ C < \frac{(\,i+B)R_L}{C_C}$$

$$If\ C > \frac{iM_L}{C_C}\ and\ C < \frac{(\,i+B)M_L}{C_C}$$

$$if\ C == 0 \rightarrow NULL$$

$$B = M_{DF}$$

Here, $M_{DF}$is the maximum data fetching and all the entries are updated in the cloud table, then create new tables as X and Y.

The data D is generated and placed in the database table based on the attribute types. The data packet contains device ID I[0] , packet cloud ID I[1], IP address of device I[2] and IP address of packet cloud IDs I[3], pseudonym I[4], content, port and bucket information. Here, pseudonym is generated through the random numbers between 0 to1. The unique primary key field identifies each table row, hence, each attribute of the table reliant on DSSN, Patient ID, PSSN, MInventory ID and Prescription ID.

$$I = I[]$$

Based on the attribute types, data is stored in the database as physical table. The A_T are classified as substantial and non-substantial records. Each table row is identified by its unique primary key field P_{KF}. The P_{KF} and foreign key entities are used to link the data in these tables. During data upload U_L and download D_L operations, the operation is determined by a probability P_B and update U_L , D_L user counts U_C and total devices T_D, also update the number of instances N_I. Here, N_D is the number of devices per instance.

$$U_L = U_C, D_L = U_C$$
$$N_D = U_C + T_D$$

During the upload operation, the table row entry is retrieved R_T from the user and transferred to the local cloud bucket on the user's end. Total data processing D_P is computed based on the minimum M_{RT} and maximum M_{XRT} count, total execution count T_C is computed based on the processing count and instances.

$$D_P = M_{RT} + M_{XRT}$$
$$R_T = N_D N_I$$
$$T_C = T_C + D_P N_I$$

The doctor, paycheck, patient, patient history, medicine, and prescription information are all null at the start. Then if the random number is less than 0.2, the new doctor's name, pay check, doctor ID, gender, age, position, specialist, phone number, and address are updated. Afterwards verify the doctor ID, name, position, check number, salary, bonus, and pay date, if the random number is less than 0.1. subsequently update the patient, patient name, patient ID, gender, age, disease, phone number, address, and doctor ID if the random number is less than 0.4. Next verify the patient history, hospital name, patient ID, completion duration, current status, disease name, hospital visiting start date, last date of visiting, and next visiting date if the random number is less than 0.6. If the random number is less than 0.8, it should update medicine details including medicine ID, medicine inventory ID, manufacturer, medicine name, price, quantity, and expiry date. If not, obtain a patient ID, a fresh prescription, a prescription ID, the number of days the medicine will be available, and the name of the medication. Then, upload the following details to the cloud bucket, such as doctor's information, medication information, prescription, patient history, and patient information. Then, based on the set of identities and access structure, create the mono and non-mon structures. If the access criteria are not met with the identities then it is non-mono N_M structure, else it is mono structure. In $\mathrm{mono} - \mathrm{A}$ is the doctor entry that includes the DSSN, age, gender, name, position, specialty, phone, and address. The patient information is then filled up with PSSN, age, gender, name, position, phone, address, and patient DSSN, and it is known as $\mathrm{mono} - \mathrm{B}$. In $\mathrm{mono} - \mathrm{C}$, the patient history is kept with the ID, completion data, current status, disease name, hospital name, visiting start length, and visiting last data. Drug inventory ID, manufacturer, price, name, quantity, and expiry date are all filled out in $\mathrm{mono} - \mathrm{D}$ medicine information. The prescription data with ID, patient ID, number of days medicine details, and medicine name are all included in $\mathrm{mono} - \mathrm{E}$. The cloud bucket data is then sent to the cloud server via hierarchical communication. When these data are received by the cloud server, they are stored in the data center database. The same set of operations is carried out for all data received from diverse users.

$$N_M = mono - A + mono - B + mono - C + mono - D + mono - E$$

The network offered security measures through attribute parameters and identity gathering. The cloud database structure is used to provide dynamic data support, the tables that are kept up to date are referred to as source tables and the tables are divided into multiple tables. The shared database instance for the cloud tenants is constructed from the source table.

The core points are chosen from the M_P based on the number of neighbours who shared the characteristics. Then, between the data mapping clusters are produced. Based on the significance of data attribute in the mapped cluster, the data is placed in the different tables. The table structure is redesigned based on the new attributes. The data base operations are performed based on the redesigned table structures. During the data storing and retrieval operations the encryption and decryption operations are performed. Using the elliptic curve parameter, create a security for data access, so, initiate keypair generator K_{PG} for each instance. The elliptic curve parameter E_{CP} was filled into the keypair generator. Select the private P_K and public keys P_{UK} from the K_{PG} and build a hash code for the P_K.

The access structure for both operations are created in monotone and non-monotone access structures. The access structure is created for the set of authorized users can access the data. In the setup phase, bilinear map is created and the security parameter is adopted from the prime fields P_F . For each user device, the identity I information is generated by taking the $I[0]$, $I[1]$, $I[2]$, and $I[3]$.

The elliptic curve group G and elliptic curve E_{CC} is created over the finite field. From the finite field, the random keys α, K_{E1} and K_{E2} are generated. The security parameters P, Q and R are generated by taking the α, K_{E1} and

$\mathrm{K_{E2}}$ as inputs with the prime field, and the three levels of collision resistance hash functions are generated using complex multiplication as $\mathrm{H_1}$, $\mathrm{H_2}$,$\mathrm{H_3}$.

$$\alpha = R(0, Z_P), \alpha^i = \alpha$$
$$K_{E1} = K_{E2} = R(0, Z_P)$$
$$K_1 = K_{E2}, K_2 = K_{E2}$$

Then the final master secret key $\mathrm{M_{SK}}$ and the master public key $\mathrm{M_{PK}}$ both are generated from the Generator, P, Q, R and the hash functions.

$$M_{SK} = \alpha + K_1 + K_2$$
$$M_{PK} = G + P_i + Q_i + R_i + H_1 + H_2 + H_3 + I$$

In the encryption phase, the arbitrary number is selected and the hash value is generated from the first level hash functions $\mathrm{H_1}$. Here, i is the number of users.

$$P_i = \alpha^i P$$
$$Q_i = K_1 \alpha^i P$$
$$R_i = K_2 \alpha^i P$$
$$m = (K_{E1} + K_{E2})\alpha$$
$$F_P = R(0,1,m)$$
$$H_1 = F_P \rightarrow Hashcode$$
$$e = H_1 +$$
$$H_2 = e \rightarrow Hashcode$$
$$g = H_2 +$$
$$H_3 = g \rightarrow Hashcode$$

From the plaintext the ciphertext is generated from the polynomial, encryption key, hash function H_2 and policy. At the decryption end, the secret key is generated with third level hash function H_3 and n-degree complex function. Here R is the random number. Generate signature S through the SHA256 with digital signature algorithm and select the P_K from the S.

$$em = R(0, m)$$
$$D = Bucket \rightarrow toString + M_{PK}$$
$$D \rightarrow .hashcode$$
$$rm = P + D + em$$
$$r = rm \rightarrow hashcode$$
$$KD = rm + P$$
$$i = i(1 - P)$$
$$x = x + i \rightarrow hashcode$$
$$P_{mi} = rP_i$$
$$Encrypt \rightarrow (D + P_{mi} + x)$$

The generated secret key is used to complete the decryption process as shown in Figure.5.

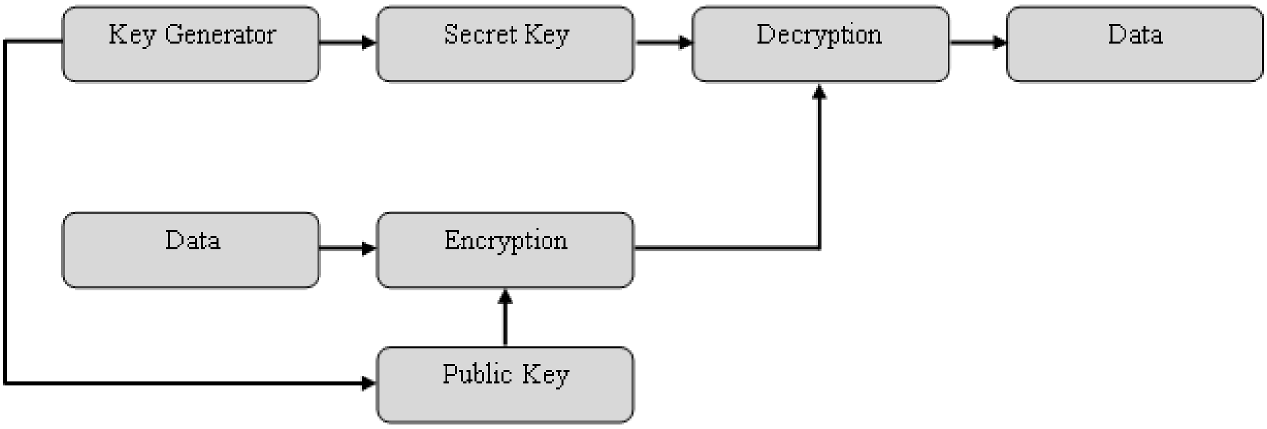


Figure.5 Secure Access in Network

3. Results and Discussion

The database is created in the network with attacker probability, age limits for patients and doctors, gender, medicine, prescriptions, required tables to process the data, number of instances, cloud hosts, number of devices, private key, public key, pair key, virtual machine lists, and other things to keep the secure storage and maintenance. Several tables were created and updated as classic, group, and axillary tables to keep doctor, patient, and medicine information up to date, as shown below:

3.1 Classic Table

Doctor Entry							
DSSN	**Name**	**Address**	**Age**	**Gender**	**Position**	**Specialist**	**phone**
100	Qjus	Pscdiofaffr	52	Male	1	3	68285
8448	Tduwdrm	Elenmty	38	Female	1	3	50719
1732	Wsfe	Vtcuvxtew	46	Female	1	2	93307
196	Bclgssybk	Yiauihum	12	Male	2	3	64727
6727	Nmlq	Hjftqxjx	9	Male	2	3	57026

Patient Entry							
PSSN	**Name**	**Address**	**Age**	**Gender**	**DSSN**	**phone**	**Position**
8577	Gkwmnt	Alqyrexv	33	Male	3596	57373	7
9948	Xgtcnjke	Wusoei	67	Female	7499	14215	4
8057	Cabb	Psswdgnv	17	Male	9159	93262	6
4646	Kpfch	Epijquya	19	Male	1732	84855	2
3365	Pmcjlbtq	Jijsdqr	40	Male	100	60355	3

Patient History						
Patient ID	**Hospital Name**	**Disease Name**	**Completion Duration**	**Visiting Start date**	**Visiting last date**	**Current Status**
9575	Qpmevkiv	Uyussvmy	37	2020-7-13	2020-10-20	5
6843	Cgsin	Huapmd	15	2021-6-16	2021-9-21	7
7988	Fces	Ctmfbqe	95	2021-8-26	2021-12-4	6
76	Lklo	Ytrrbu	27	2020-10-11	2020-12-6	0
6589	Qlrxofuwk	Mlrjao	80	2020-12-3	2021-1-12	0

Patient History			
PId	**Patient Id**	**Medicine Name**	**No of Days**
1427	76	Dssuwgk	6
3727	9575	Skdrfuoahuhv	11
3024	6567	Wdjmcxtpqlxs	67
5180	5927	Wbhvqqfrqxma	76
5467	9948	Ephopyh	99

Medicine Description					
MInventory Id	**Medicine name**	**Manufacturer**	**Price**	**Quantity**	**Expiry date**
4951	Vkkfydxodf	Qncxehy	385	939	2021-8-4
4999	Engbmep	Jkhhvhl	673	392	2020-10-2
1949	Nxpnaff	Vulbmc	195	648	2020-9-7
321	Dvkjgncy	Xqubsimph	389	691	2020-3-3
3318	Chkdv	Ejprmxpcm	285	499	2021-4-18

3.2 Ground Table

Doctor			
DSSN	**Age**	**Position**	**Specialist**
8027	58	2	7
5587	33	2	5
966	28	2	3
3880	8	1	2
3895	16	2	1

Patient			
PSSN	**Age**	**DSSN**	**Position**
9575	53	4182	5
6843	39	3596	7
7988	69	4816	6
7622	16	1732	2
970	62	7499	4

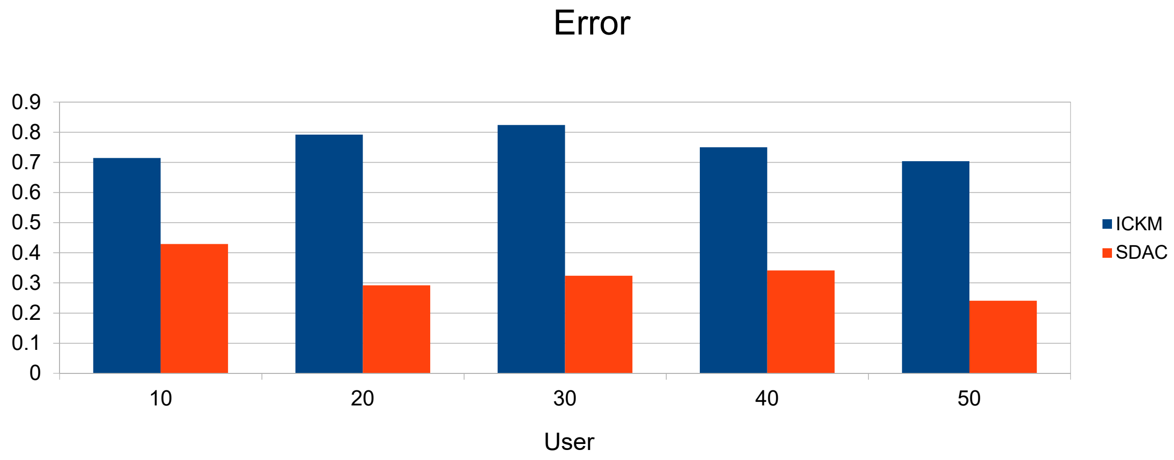
Patient		
Patient Id	**Disease Name**	**Current Status**
756	Ddxfxsgoqafd	0
7988	Kqeorbdmipg	6
9575	Uyussvmynamem	5
7619	Awkkbjgru	7
7764	Gnwvqncliw	0

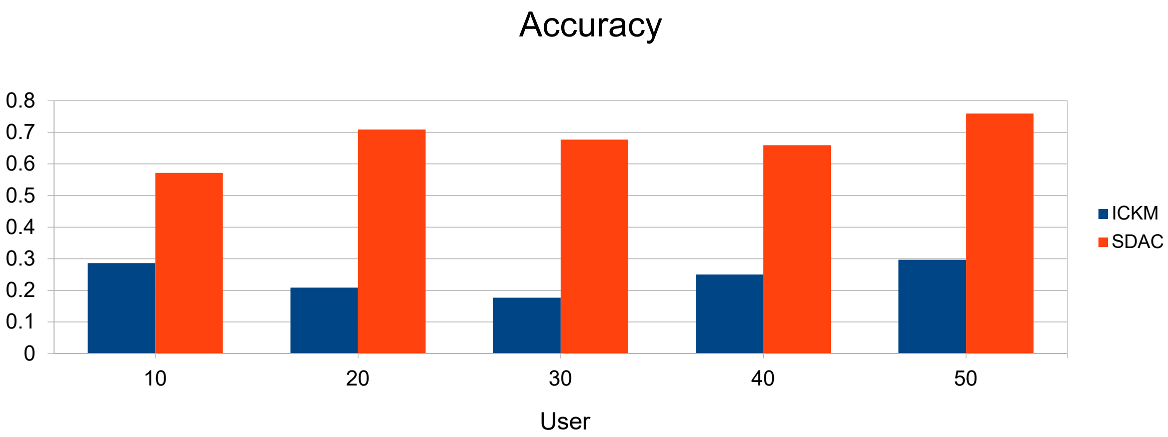
3.3 Auxiliary Table

Doctor				
D_SSN	Name	Address	Gender	Phone
3596	Lpat	Itucvkpcexpxd	Female	44609
3880	Qkfqrk	Cqgvqwsrhpb	Female	29331
8027	Lwixax	Ickciqwugp	Female	61881
5587	Pxuuglgxa	Trtxwybn	Male	90386
966	Yjpdw	Wkgnodnnfssck	Female	70267

Patient				
P_SSN	Name	Address	Gender	Phone
6843	Abixarmc	Qxfdwdyx	Female	79253
7988	Jeqtjtime	Wymxknhv	Female	12481
7622	Ojtodngef	Iesnaaai	Female	11196
970	Nyxb	Fsyltuey	Male	57843
3644	Qisdn	Hcnjqdxm	Male	58988

Patient				
Patient Id	Hospital Name	Completion Duration	Visiting Start Date	Visiting Last Date
756	Llcl	94	2021-12-2	2022-4-2
7988	Bnunidbid	40	2021-9-30	2021-11-24
9575	Qpmevkiv	37	2020-7-13	2020-10-20
76	Lklo	27	2020-10-11	2020-12-6
7619	Cmdd	11	2021-5-7	2021-7-14





Accuracy and error are metrics used to assess the performance of patient history maintenance in a secure cloud storage environment. It also calculated the precise performance of all processing. This specifies how many times the algorithm performs the correct processing during execution. If the classification was correct, the true count will be increased; otherwise, it will be treated as false counts. It is calculated by dividing the number of correct received packets by the total number of sent packets. Furthermore, the error was calculated based on the loss packets based on the transmissions. Due to heterogeneous communication and security threats, packet loss will occur in cloud networks; more packet loss reduces the performance of data storage and processing. In this case, the SDAC performed better than the base model. Because the SDAC includes precise storage and secure maintenance methods. It reduces errors in the process and improves accuracy.

4. Conclusion

The data in the proposed work is generated at the user end and communicated to the cloud host. It has several tables that are linked together. The data is generated and placed in the database table based on the attribute types. The unique primary key field identifies each table row. These table data are linked together using the primary and foreign key entities. The table row entry is fetched from the user and generated as a local cloud bucket in the user end during the upload procedure. The cloud bucket data is then sent to the cloud server via hierarchical communication. The tables that are kept up to date are referred to as source tables. The shared database instance for the cloud tenants is constructed from the source table. The source tables are separated into numerous tables, and table entries are kept in each tenant. The STSI structure is carried out using the existing data by merging it from multiple tables.

The data is taken from the STSI structured table during the download, and the join operation is avoided. The ground table in the STSI structure is formed from the classic table. The auxiliary table is formed from the other fields of the ground table by eliminating the other available fields. It provides a dynamic structure for stored tables across multiple cloud tenants. Furthermore, data between tenants is mapped utilising the shared nearest neighbour approach. The data is divided into tables based on the importance of each data attribute in the mapped cluster. Encryption and decryption processes are carried out during data storage and retrieval operations. Both operations have access structures that are built in monotone and non-monotone access structures. The ciphertext is created from the plaintext using the polynomial, encryption key, hash function, and policy. The secret key is generated at the decryption end using a third level hash function and an n-degree complex function. The secret key generated is used to finish the decryption process.

References

[1] Deepak Kumar Verma, Tanya Sharma, “Issues and Challenges in Cloud Computing”, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 8, Issue 4, April 2019.

[2] Ahmed E. Abdel Raouf, Nagwa L. Badr, and Mohamed Fahmy Tolba, “Dynamic Distributed Database over Cloud Environment”, 13 January 2016.

[3] Mohammad Mehrtak, SeyedAhmad SeyedAlinaghi, Mehrzad MohsseniPour, Tayebeh Noori, Amirali Karimi, Ahmadreza Shamsabadi, Mohammad Heydari, Alireza Barzegary, Pegah Mirzapour, Mahdi Soleymanzadeh, Farzin Vahedi, Esmaeil Mehraeen, Omid Dadras, “Security challenges and solutions using healthcare cloud computing”, Journal of Medicine and Life. Vol: 14 Issue: 4 July August 2021.

[4] Arpita Shah, and Narendra Patel, “Efficient and scalable multitenant placement approach for in-memory database over supple architecture”, Computer Science and Information Technologies, Vol. 1, No. 2, pp. 39, July 2020.

[5] Dr. N. Krishna Murthy, Dr. R. Selvam, “Security Issues and Challenges in Cloud Computing”, International Advanced Research Journal in Science, Engineering and Technology(IARJSET), Vol. 2, Issue 12, December 2015.

[6] Ahmed E. Abdel Raouf, Alshaimaa Abo-alian, Nagwa L. Badr, “Multi-Tenant RDBMS Migration in the Cloud Environment”, International Journal of Intelligent Computing and Information Sciences, Vol.21, No.2, 2021.

[7] A. Stephen, A. Arul Anitha, L. Arockiam, “Cloud Computing: Opportunities and Challenges”, ReTeLL, Vol. 21, June 2019.

[8] Ju Ren, Deyu Zhang, Shiwen He, and Yaoxue Zhang, "A Survey on End-Edge-Cloud Orchestrated Network Computing Paradigms: Transparent Computing, Mobile Edge Computing, Fog Computing, and Cloudlet", ACM Computing Surveys, Vol. 52, No. 6, October, 2019.

[9] Alshamaileh Mohammad, Li Chunlin, "Evaluating Mobile Cloud Computing Models", 4th International Conference on Machinery, Materials and Computing Technology (ICMMCT 2016).

[10] Trilochan, Anjali Verma, "Cloud Computing: Evolution and Challenges", International Journal of Engineering Science and Computing, April 2017.

[11] Yongmin Zhang, Xiaolong Lan, Ju Ren and Lin Cai, "Efficient Computing Resource Sharing for Mobile Edge-Cloud Computing Networks", IEEE/ACM Transactions on Networking, Vol. 28, No. 3, June 2020.

[12] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu, "Edge Computing: Vision and Challenges", IEEE Internet of Things Journal, Vol. 3, No. 5, October 2016.

[13] Jitendra Singh, "Study on Challenges, Opportunities and Predictions in Cloud Computing", I.J. Modern Education and Computer Science, 2017.

[14] Talal H. Noor , Sherali Zeadally , Abdullah Alfazi , Quan Z. Sheng, "Mobile cloud computing: Challenges and future research directions", Journal of Network and Computer Applications, 2018.

[15] J.M. Naveen and B. Muthu Kumar, "A Multi-Tenant Web Application Framework for Software as a Service", European Journal of Applied Sciences, 2016.

Authors Profile

.

Dipa Dattatray Dharmadhikari, has completed her Bachelor's degree from Terna Public Charatable Trust College of Engineering Osmanabad and later on pursued Master Degree from Government Engineering College Aurangabad Babasaheb Ambedkar Marathwada University,Aurangabad. Her area of interest includes Cloud Computing., Database technologies and Security.

.

Sharvari Chandrashekhar Tamane currently working as Professor & HoD at the Information Technology, Jawaharlal Nehru Engineering College, MGM University Aurangabad, Maharashtra Sharvari does research in Big Data Analytics, Cloud Security etc. Her current project is to get CFC for Big Data, IoT, Smart Cities to be published by Elsevier or Taylor and Francis.

.