CHAPTER 4

QUERY BASED USER SEGREGATION

4.1 OBJECTIVE

The cloud computing provides virtualization services which assist the likelihood for adaptation and collaboration of diverse internet based enterprises migration over the universe. The semantic web scheme is designed simultaneously which makes use of RDF as storage formats for saving the information serving the applications which make of cloud computing. The adoption to cloud semantic web technique on cloud platforms provides an effective means for managing the information for the applications employing cloud environment. Numerous databases for storage applications have been designed for the computing environment.

There is a need for an effective technique which allows segregating the users based on the requirement and serving them accordingly based on their search semantics for gaining access to the information hoarded into the cloud server. The focus is to use the queries of the users to segregate them based on their search terms and offer them only the requested information thus retarding to gain access to the other information stored over the web.
4.2 PREAMBLE

The cloud computing is a crucial research topic and is widely implemented technology in the present scenarios. The databases are also merged into the cloud systems which are offered as an element of the cloud as software as a service (SaaS) called the database as a service. The cloud offers enormous space for storage in a scattered manner aimed to offer performance at the expected levels. The storage services can be made use by the consumers which are offered by service providers like amazon web services and it can hoard the databases over the cloud and allows the users to utilize the service as many times as they can base on their requirements. The semantic web is an attractive package for the forthcoming generation web-based models. The extremely formless information prevailing over the web based source gives rise to disputes to the present days prevailing search engines.

The semantics could be viewed as a part of optimization. The key element linked with the semantic structure is resource description framework (RDF) generally employed to describe each and every object over the web independently and in a planned method. The work represents the connection of semantic web along with the cloud computing. The semantic web is the focused research topic dealing with the varied semantics along with semantic associations. The semantic web provides an insight of the ways to represent the information individually over the internet with the help of RDF and ontology language. The semantic web addresses the issues of varied semantics and allows for association of domain information from various sources. Along with semantic web, the cloud computing is also a major research topic in present days.

The work offers association of semantic web with cloud services. The associations of cloud services and the semantic web offer a better working
environment for many business sectors. The focus of the work is to segregate the users to offer a better service to access the database only based on their queried request on – demand. The information is available over the internet massively and the greatest issue with this information is that they are not homogeneous i.e. the data differs in terms of semantics and structure. This is based on the reason that different sectors will generate information uniquely based on their own demands and there are no regular schemes for making this data look alike. It is necessary to introduce a mechanism which allows the users to utilize this scattered information based on their requirements over the internet for which the semantic web offers a better solution.

4.3 GENESIS

The information over the internet is not dependable and there are no sources which can carry out information verification. There is a no need for offering dependability for data so that an individual can have belief over the data. The scheme employs a broadcast technique which offers belief for the information. It makes use of both static and scattered technique to offer belief over the data. The services prevailing are virtualized resources over the cloud. It remains a great dispute and it is employed by various organizations for incorporating their diverse services into a single service for offering functionality. It makes use of cloud registration to access the registered entry and from there individual can gain access to the provided data a greater suppleness for the individuals as it exists on the cloud.

These services serve as a forthcoming generation search engine based on the semantics prevailing within the data. The search engine makes use of a penetration technique for systematizing the information. The approach allows the user to search some data by using various exact keywords and it offers a better way for exploring data. The technique offers a suggestion
regarding the system implementation. It aids the individuals to offer a better search and routing methods. Presently, only the individuals can recognize the content of the data but not the machine but the amalgamation of web semantics will permit the machine to recognize and process the data. It will offer information analysis and format a platform for understanding for the machine in order to process the information quickly. It is essential for an RDF to manage the information over the cloud infrastructure. The scheme is employed over amazon cloud services where the information is stored in the form of RDF and it employs SPARQL for querying the information in a scattered fashion. This scheme makes use of scattered data over the cloud in a machine recognizable format and the query is also offered in a scattered fashion.

The present situation makes the individuals employ web interfaces to access the information. There is a need of incorporated access to the services for the individuals to make it effective. By employing web portals the individuals not only desires to access the information but also several services offered by these portals. But for the conventional amalgamation of web services, it is quite impossible. Assume that there are two web services where one offers data about a movie booking service in a city and the second offers the booking capability. In case if an individual needs to view the existing booking services within the city employing first web service and to reserve a ticket by employing the second one which offers a better integration of the services. It is capable to the extent the queries across the data but to assimilate the services is quite complex. In order to attain the objective, there is a need for a base free high-level web portal incorporated structure which offers a way for dealing with dissimilar information.

The XML is another based free information swapping standard over the web. XML carts the information in the form of a tree based structure
but two semantically equal documents could have diverse structures and the two XML can have the same information but diverse structures. For combining the data from two semantically similar but diverse structures for the XML documents there is a need to implement semantic amalgamation.

The database administration can be offered as a cloud service where the information can be scattered over the cloud and the resource sharing, the software could be carted out because of which the rising interests in outsourcing database and the database administration behaviors can be viewed in the present scenarios. The performance of the database over the cloud offers the users a better way for accessing the on-demand information.

The semantic web offers an understanding of data for the machine as evaluated with HTML pages and on other hand the performance for accessing this fresh arrangement of data must be effective so that the performance will not weaken. The information management concepts deal with large storage of RDF triplets and the ways an individual can preserve such large storages effectively through several features of query generation and strewn query processing.

Several accesses to the data elements in a cloud environment is possible by a mechanism called access token rows based on the access token, entities, attribute types and attribute name. The access type can be cataloged based on several sub – types like information access, predicate access and object access. The token allotments are achieved based on the access token allotment and based on described time stamps.
SECURITY ISSUES IN CLOUD COMPUTING

The cloud computing is an emerging computing platform where the application can execute over the linked cloud servers rather on the local servers. The cloud computing offers services like effective data storage, resource distribution, and services in a scattered manner easily. The cloud computing is defined as the utilization of computing resources like hardware and software over the internet. There is several resources available namely software as a resource (SaaS), platform as a resource (PaaS) and infrastructure as a resource (IaaS). Every individual can gain access to the resources through internet either using computing devices like mobile, laptop, tablet, etc.

Gaining access to those resources through the web is a key issue and it improves safety. The access control offers approval to the individuals to gain access to the resources that are freely available to the individuals. Previously, there were several access control schemes prevailing for safeguarding the data access. The access control depends on the safety of the system and provides access to the objects. It is to note that the cloud computing faces issues like safety and confidentiality of information when a susceptible information are stored using a third party cloud service providers. Several access control models have been devised to address the safety-related issues in cloud computing.

The conventional access control schemes are discretionary access control (DAC), mandatory access control (MAC) and role-based access control (RBAC). The intention of the access control over cloud computing is to retard the illegal access to the elements of the cloud for improving the security features. The access control mechanisms are employed to reconcile each and every effort of specific users to the object based on the access rights governing the system. The conventional access control believes indication
examine has the approval database and this database considers the user approval. It might be employed in computer science and automation because security remains a bigger dispute in the cloud. The safeguarding of information system either directly or indirectly influences the organizations.

The access control is commonly referred as a policy which permits or restricts the access to the system. It also discovers the intrusion of unprivileged users into the system. The common access control schemes are identity-based control schemes. These access controls rely on the cloud storage and its information safety and the choice of access are very crucial over cloud computing. The access control is very crucial in information center for governments and business. It is also vital to understand that the access control itself is not a solution for safeguarding the information for some other measures are also required. There exists a difference between the choice of policies and the schemes. The access policies are high-level choices which verify the way for managing the access and its associated decisions.

4.4.1 Access Control Techniques

The different types of access control mechanism are presented below.

a) Discretionary Access Control (DAC)

This is a conventional access control where the individual has the entire control over all the programs. The DAC (Figure 4.1) is based on granting access to the individual on the basis of user’s characteristics and approval which is described for open policies.

The DAC possess and implements along which it verifies the permission to specific individuals to the object. The DAC policies consider the
access of the individuals to the object which is based on the characteristics of
the individual and the approval which indicates each individual's access
mechanism and the object which is being requested by the individual. Every
user requests an object which is been verified. For DAC access method
elasticity is needed. Here, mostly the approval is indicated openly and also the
approvals of the users are locked. During the open approval then it is
perceived as open policies.

![Diagram of Discretionary Access Control](image)

Figure 4.1  Discretionary Access Control

The DAC consists of access rules and access elements. The
access elements permit the system to describe numerous different levels of
approval and the access rules offer the methods for the cloud to retard illegal
access of the susceptible information. The DAC allows controlled distribution
of objects among diverse subjects. The DAC is a mechanism which instructs
which user access which resources. Here, the creator of the object can select to
offer access permission to rest of the users.
The access control list is linked with every other file system. A common form of DAC can either be a password which grants access to the approved users. The DAC mostly deals with the legacy of permissions, user based approvals, inspecting events of the system and managerial rights.

The below stated are the possible merits of the discretionary access control mechanism.

- The DAC method offers elasticity in information utilization.
- The method will preserve the approved database which contains several approved individuals.

The setbacks of the discretionary access control mechanism are stated below.

- The method offers no guarantee for information flows and there are no constraints on the information regarding the utilization and this will create uncertainty in information usage and also the information will vanish.
- The information is vulnerable to third party users.
- The information is unreliable.
- It is also possible to embezzle a copy of created message without the knowledge of the message creator.
- The owner of the message might modify the DAC policies by appending suspicious programs.
b) Mandatory Access Control (MAC)

The scheme (Figure 4.2) is based on the access of the objects to several subjects and the mandatory access control is mainly based on the safety levels. Here, the users are not authorized to modify the access controls. The conventional MAC schemes are mainly linked with some safety concerns. It is based on the two below stated schemes.

i) Read Down

The present safety levels of the individuals should control the access of the read objects.

ii) Write Up

The present safety level of the individuals must control the access of the written objects.

![Diagram of Mandatory Access Control](image_url)

**Figure 4.2  Mandatory Access Control**

The MAC is based on the object categorization and the subjects present in the cloud environment. The access to a specific object is permitted.
only if several associations are fulfilled. Every object and subject within the cloud environment are allocated with several safety levels which aid to locate the present access state of the object. The safety level is linked with the user are called permission. The MAC is used to safeguard the network and the file system, retard the users from accessing without proper approval. Here, the users are not allowed to modify the access control and its safety levels. The MAC label is a safety element which may pertain to the subjects and objects all through the system.

The individuals can be linked with the object based on the belief levels and safety. The MAC usually takes the tree-based approach for managing the access to the cloud data. This tree-based approach is based on the safety levels and usually, the MAC contains a safety label. This safety label is allocated to all the subjects based on the demanding objects. The safety label of two data as detailed below.

- **Catalog**
  
  It contains top undisclosed and private information.

- **Group**
  
  It is based on the safety levels.

  It verifies the information access from cloud MAC and it verifies the identity of the individuals based on the catalog and groups. It imposes the managerial safety policies and it is estimated that the MAC is safer than DAC. For DAC the flow of data is irregular rather in MAC it is managed based on the safety levels allotted and also it allows safety permissions to each individual. All the individuals can read from bottom levels based on the authorization from the creator and also the individuals have the authorization to write to the top levels based on the permissions.
The merits of mandatory access control mechanism are stated below.

- The information reliability will be elevated and it retards the flow from bottom level to the upper-level objects.
- It is employed in military and government applications.
- It offers multiple levels of safety.
- It retards the illegal individuals from modifications.
- When the information is in perpendicular order and it will offer the multiple levels of safety.
- Here, the every access to the individual will be arbitrated so that the data is accessed through the cloud is safer.
- The access is approved or retarded to the objects based on the time based on the safety levels of resources and the permission of the users.
- The expandability of the scheme is minimal and it will not adjust to all application types.

The setback of the mandatory access control mechanism is the safety levels are recognized to a specific subject within the tree structure and it won’t alter the safety levels.

c) **Role – Based Access Control (RBAC)**

The role-based access control (Figure 4.3) access choices based on the roles performed by the users and their duty within the cloud environment. It devises the access of the individuals to the system based on the actions performed by the individuals over the cloud. It needs task detection for the users performing on the system. The tasks can be a collection of objects or activities linked with the subject. The task differs based on the priority of
the user and the RBAC offers safety for web based applications. The duties are allotted based on the specific cloud managerial structure with their safety policies. Each task within the business outline involves all the approved users, authorities, contracts and permissible information access. The roles can be allotted based on the least rights. The recognized tasks can be shifted and utilized based on suitable methods and safety policies. The tasks can be controlled centrally.

Figure 4.3  Role – based Access Control (RBAC)
The RBAC permits the individuals to implement several tasks at the same time and the tasks are the useful approach to business like a cloud, grid and peer – to – peer environments. For some cases, only the tasks can be allotted to an individual user and it identifies the similar tasks to other individuals together. After the DAC and MAC schemes, the RBAC serves as an effective control mechanism. It is to be noted that safeguarding the information over the cloud is same as safeguarding information over the web.

The RBAC over the web is a user pull framework and it is used to offer services and allocated tasks to each individual based on the characteristics of the users and its tasks are based on the implementation environment in the cloud. The RBAC over the web is implemented with a server pull framework. The RBAC authorizations are linked with the tasks and the individuals are allotted to specific tasks. The system manager can only be able to generate the tasks and offers authorizations to those tasks. Lacking of RBAC it is quite hard to decide the level of authorization allotted to the users.

The RBAC can be employed based on the user pull architecture where the individuals can pull their respective tasks from the server and the server pull framework refers pulling their corresponding tasks from the server. These methods are employed in RBAC models.

The below described are the merits of the role – based access control mechanism.

- It offers ladder tasks for access based on several applications.
- The tasks are allotted based on the least rights for the specific objects for reducing the breakdown of data by the attackers.
• The segmentation of tasks will be preserved in order to retard the exploitation of data because each individual is allotted with specific responsibilities.

• This segmentation of responsibilities can either be fixed or autonomous.

• The RBAC offers categorization of the individuals based on their performing environment.

The setbacks addressed the role – based access control mechanism are stated below.

• Occasionally, it is not possible to accomplish the rights linked with the individuals with specific tasks.

• The authorization linked with each task can be removed or modified based on the rights for modifying the responsibilities.

• The responsibilities are allotted based on the least rights but still modification of responsibilities might create uncertainty for judging the authorizations of each individual linked with that tasks.

4.4.2 Disputes Faced By Conventional Schemes in Cloud Databases

The below stated are the disputes faced by the conventional scheme in cloud environments.

a) Expandability

The major feature in the cloud is its scalable nature which literally means that the cloud resources can either possibly extended or shrink autonomously without any possible hindrance to the services offered. It places
a big dispute for the developers to extend the databases in order to offer a limitless number of parallel users and data expansion.

**b) High Accessibility and Error Lenience**

The accessibility of database means that the database is live and running. It becomes quite essential to imitate the information across huge geographic distance in order to offer high accessibility to data, stability and error lenience.

**c) Diverse Environments**

The individual requires accessing different applications from diverse sites with the help of devices like mobiles, tablets, notepads and computers. The user applications and the information differ in nature and it becomes quite complex to instruct the mechanism for accessing the system by the users.

**d) Data Reliability and Confidentiality**

The reliability is a major significant necessity for all types of business applications and is preserved through database restrictions. The lack of confidentiality among the data results in unpredicted outcomes and it becomes hard to preserve the reliability.

**e) Easy Query Interfaces**

The cloud databases are scattered. The querying of this scattered database is a great dispute encountered by the cloud developers. A scattered query has to access several nodes of cloud databases. There must be an easy and consistent query interface for querying the databases.

**f) Data Safety and Confidentiality**
The information is physically stored in a specific place and is confined to the local rules and guideline of that place. If the data is encrypted using a key which is not in the possession of the host, then it offers little safety.

g) Data Movements and Interoperability

The data movement is the capability to execute elements written for one cloud service providers into another cloud provider’s surrounding.

4.5 VARIED SEMANTICS

The majority of the information produced over the internet is by different sectors for processing their demand based on their requirements. These sectors generate this information using their own standards and they are not understood by the machines i.e. the machines will be incapable of identifying the information as facts and could not process the information for which the information has to be made machine understandable so that the machines could process the data and it will be available for usage.

4.5.1 Semantic Web

The Semantic Web is a collection of knowledge for characterizing, storing, and querying information. These technologies can be used to hoard text-based information such as text in a Word document or PDF file which are used to stock up data as smaller bits. The Semantic Search is focused largely on the text based information. The Semantic Web also comprises of numbers, dates, figures, and other data in addition to text.
The semantic web is a technique that permits the web index to snatch the meaning for the words given as input by the user for revealing the results depending upon their importance. The search using semantics is provided by enhancing the search precision for the user context and the results retrieved after performing the search. The results of the search could create a lot of similar results but the semantic search recognizes a number of other things into the search including searching the context, area, goal, change in expressions, synonyms, universal and focused queries. These results try to match the queries entered by the users in their natural language for extracting important query items. The internet searching tools like google, bing integrates some function of semantic search.

The two basic forms of search are navigation and investigation.

a) **Navigation**

The navigation uses the online searching tools to assist the user to attain their intention by serving as a travel guide. The semantic search does not work with directions.

b) **Investigation**

In analysis search, the user is provided with an internet searching tool which provides results to the context about which the user is trying to explore information more precisely. The search tool does not hold any records for representing user knowledge in prior. Rather the user attempts to discover different reports and tries to perceive the needed information.

**4.5.2 Semantic Association**

The semantic search is a solution of varied semantics and it is to be noted that offering varied semantics itself is a major job and it necessitates
supplementary efforts like applying standards or alterations in fundamental concepts of tools and languages.

The semantic search addresses for scattered and semantically varied information and make it easy to distribute the information as per the domain request of the users. The Figure 4.4 represents the semantic web which offers user segregation. The semantic search allows the users to pick the corresponding information and avoiding unnecessary information. The semantic search allows the users to segregate the requested information based on the differences between the vocabularies among different sources of data. The below stated are the major problems which have to address during performing a semantic search.

- The technique for associating two diverse platforms and the protocols for interchanging the information among them.

- The segregation of user requests between two diverse systems which make use of similar data.

The solution can be addressed by estimating and locating a specific way for connecting diverse assorted information so that these systems can effectively relay the requested information to the user. The communication between these systems for segregating the users based on their queries or requirements are based on the request / response model.
4.6 SETBACKS ADDRESSED

The individual receives the results which are not intended for his purpose. This might possibly make some other information over the web vulnerable. The users not intended to access this information might gain access to this information as a result, the confidentiality of the message gets compromised.
• This is due to the reason that the queries are misunderstood by the system i.e. the meaning of the work is assumed wrong by the system. Differently meaning words in diverse contexts and indexing used within the keyword fails to maintain the associations between the queried words.

• The usage of words that are not possibly used for queries which can be addressed by appending a few associated words into the queries.

4.7 CLOUD COMPUTING VS SEMANTIC WEB

The cloud computing is been widely employed for diverse applications due to their flexibility, expandability and error lenience. The web service is a present evolution of cloud computing. It has merged diverse applications, platforms, remote services, etc. The semantic characteristic of web service offers an advantage of context conscious, QoS conscious, performance conscious web-based service detection mechanism.

The semantic computing links and combines different domains like software engineering, natural language processing, artificial intelligence, grid computing and pervasive computing. Due to which the semantic maintenance and data processing related to the real – time applications becomes convenient. Consequently, there is a need to preserve and process semantic data for real-time applications over the cloud environment. Figure 4.5 depicts the development of information formats and figure 4.6 depicts the efficient service discovery for serving users query in cloud computing.
Figure 4.5  Development of Data Storage for Semantic Web Precise Data
4.8 PROPOSED SOLUTION

The semantic web services are any services readily available over the internet which makes use of regular XML messaging system and it is not bound to any specific operating systems or a programming language. This can be identified using service entries. The steps of web service detection method for segregating the users based on queries in cloud computing scenario are as stated below.

Procedure

Step 1: The cloud service provider executes the services and makes it accessible to the cloud environment which can be accessed through the Internet.
**Step 2:** It is a reasonably administrated index of services preserved within the cloud environment. It is a administrated storage for organizations and their offered services.

**Step 3:** The individuals are the users of these web services. These users request for a particular set of services for which the users must be segregated based on their queries based on conventional web services by opening a network association and forwarding an XML request message.

**Step 4:** The XML request is semantically matched in the UDDI entries and an XML response message is generated holding the description of the related entries of the particular web services.

**Step 5:** The cloud server forwards the XML reply message on the same network to the requestor of the web-based services based only on their demands.

**Step 6:** The requestor of the service extorts only the position of their requested and desired web service and summons it preserved over the cloud environment.

4.9 **PROPOSED ARCHITECTURE**

Figure 4.7 depicts the designed framework for the cloud-based semantic incorporation for cross area resources.

**a) Non – Traversed Area Information Resources**

For the designed framework the lower layer symbolizes the non – traversed information resources. These sources are with diverse data plans and equipment and their own standards and frameworks. These resources inquiries with their local query language and obtains the outcomes in the local standard formats based on which the users are segregated.
b) Query Conversion

The query conversion is employed for converting the query from one standard to the other. It performs as an intermediary between the diverse source and the RDF entries. Here, D2RQ serves as a query converter which converts the query from local data standards to RDF based standard query.
The D2RQ base is employed for accessing the associated databases as RDF graphs. It offers an RDF-based access to the associated database. The D2RQ server is employed for carrying out features like non-RDF database based on SPARQL queries, access to associated data, generating routine deposit into the database in the form of RDFs.

c) RDFs

There are two steps associated with incorporating relations such as schema conversion and separating the relations.

Here, RDFL is employed to design each XML schema as local RDF segregations for a uniform demonstration. The prime focus of this method is to conserve the structure of an XML schema. In the subsequent step, the local schemas are separated from the universal relations. Here, supplementary domain precise knowledge is employed. A mapping table is also being employed which holds the mapping between the local and universal relations. It is assumed that the mappings between these two XML schemas are equal because for some cases they appear dissimilar. Two different roles are performed by the global ontology and it offers the users to access the data with consistent query interface and subsequently it serves as an arbitration mechanism for accessing the scattered data through any of the XML sources as depicted in figure 4.7.

- Information Segregation

The system converts the RDF query into several sub-queries i.e. one for each XML source.
**Peer to Peer Segregation**

Here, the query raised by the user against the XML schema is communication to all arbitrates scattered resources.

### 4.10 WORKING OF THE SYSTEM

The designed scheme must offer a solution for query based user partition for real-time applications. Though the users of the systems still view a single schema, the queries are converted to suitable sub – queries for independent data sources and the outcomes are provided to those requested users appropriately in order to avoid intrusion of unwanted participants to access the attained results. Therefore, the results delivered to the individuals are always fresh and for any information sharing framework segregation of semantic diversity is important.

No matter whether the query is raised on demand the differences are predicted semantically between the data sources. Normally, these differences are accepted by the semantics. These are used to detail the mechanism for splitting the semantics of the data and reformulate them based on the raised queries.

**Procedure**

**Step 1:** The services are requested by the users through the accessing devices through possible interfaces. These details are forwarded to the platform-specific message structures.

**Step 2:** The request is handled by the semantic web service for access and recovery from RDF data stores.
Step 3: The details of the queries are then passed to SPARQL query evaluator which estimates the query and arranges the result set.

Step 4: The results are then passed on to semantic web service in XML format.

Step 5: The web service communicates the results of the query to only those end users requested for the service.

Step 6: The user application process this XML and exhibits the outcomes of the posted queries only to those intended users.

For much simpler means the simplified procedure steps are stated below.

Initially, users are with requirements

User enters a keystroke for initiating search

if (search = requirements)

Catalog users based on requirements

Else

Retard user to gain other data

Return requested data

let $A_{ij}$—associations between the fetched data

let $R_{ij}$—associations between the concepts fetched

Let $q_p = A_{ij}$ is the number of associations relating the concepts i and j between the fetched information.

Let $q_p = R_{ij}$ is the number of associations relating the concepts i and j from the concepts fetched.
for (i=0; i<q_p; i++)

if (q_p == 0)
user’s try to access unrelated data

else
needed data are fetched
return
cataloged users

4.11 SEMANTIC VECTOR ALGORITHM

A query is specified by giving a set of keywords, possibly linked through logic operators and enriched with additional constraints. The Semantic based search are capable of exploiting concepts hidden behind each keyword. The core step that consists of identifying the mapping between keywords and concepts can be performed in a semi-automated way. For avoiding ambiguities, the user can be requested, during query definition, to specify the concept a keyword refers to. The user specifies a query by entering a keyword and selecting a concept. A semantic search would take into account keyword-concept associations and would return a page only if both keywords are present within the page and they are related to associated concepts.
Algorithm

Vector Cut Arc,

Cut Arc( )
{
    //begin with one arc, we segment arc each times add by one
    for(i=1,i<=|Cut Arc|,i++)
        getsubset(int n, vector Cut Arc);
}

//procedure getsubset

//n is the number of arc to be segmented
getsubset(int n)
{
    //define a stack temporarily store the arc will be pop out of the Arc stack;
    for(int i=0,i<|Cut Arc|,i++)
    {
        j=i;
        Arcstack push(Cut Arc(j));
        While(!Arcstack empty( ))
        {
            if(Arcstack size( )==n)
            {
                //additional code
            }
        }
    }
}
//when the number of arc in stack a set of arc is got
//we can process these arc process_subgraph( );

//pop the top of stack

}

else
{

if(++j!=Vec Arc, size( ))

// if the position of pointer j do not reach top of vector arc then push it into stack

Arcstack push(Cut Arc[j]):

else
{

//if the pointer reach the arc at top then get the position as top of stack.

j=getposition(Arcstack gettop( ));

Arcstack pop( );

}

}

}//end while

}//end for

}//end procedure

The users are segregated based on the input query and it is possible that at least some sort associations exists between the queries due to which all these data are extracted. But most of the times these are not intended
for the users and this information are not of use of the users which must not be accessed by the users. The algorithm assists the users to merely utilize only those results that are intended for the user requirements.

4.12 PERFORMANCE ANALYSIS

The performance estimation is done for estimating the association the fetched information and the relation among the concepts fetched. Here, the search is performed for five diverse categories based on which the relevance among the fetched queries is estimated for the proposed system and conventional access control mechanism. The outcomes are depicted in Figure 4.8 and 4.9.

Table 4.1 Associations based on fetched data

<table>
<thead>
<tr>
<th>Categories</th>
<th>User Segregation</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No. of Queries Fetched</td>
<td>No. of Queries Fetched</td>
</tr>
<tr>
<td>Education</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>Health</td>
<td>30</td>
<td>28</td>
</tr>
<tr>
<td>Travels</td>
<td>60</td>
<td>30</td>
</tr>
<tr>
<td>Hotels</td>
<td>60</td>
<td>42</td>
</tr>
<tr>
<td>Sports</td>
<td>90</td>
<td>25</td>
</tr>
</tbody>
</table>
The performance analysis depicts that the proposed user segregation scheme attains elevated levels of enhancement when compared to the existing access control mechanism.

Table 4.2 Associations based on concepts

<table>
<thead>
<tr>
<th>Categories</th>
<th>User Segregation</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No. of Queries Fetched</td>
<td>No. of Queries Fetched</td>
</tr>
<tr>
<td>Education</td>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>Health</td>
<td>45</td>
<td>28</td>
</tr>
<tr>
<td>Travels</td>
<td>57</td>
<td>45</td>
</tr>
<tr>
<td>Hotels</td>
<td>59</td>
<td>48</td>
</tr>
<tr>
<td>Sports</td>
<td>68</td>
<td>57</td>
</tr>
</tbody>
</table>
The performance analysis depicts that the proposed user segregation scheme attains elevated levels of enhancement in associations for concepts in user queries as compared to the existing access control mechanism.

**Figure 4.9  Associations based on concepts**

The above illustrated graphs depicts the associations of the information fetched based on the queries in terms of data and concepts. It is important that the data must be extracted matching to the concepts which is very well executed and on comparison it is evident that the user segregation scheme acquires 78% efficiency as estimated against the conventional access control mechanism as depicted in Figure 4.10.
**4.13 EXPERIMENTAL SETUP**

For performing analysis the analysis employs the use specific model of cloud computing architecture with specific service running on it. As mentioned before, it is evident that cloud computing architecture may diverse in implementation both for public or private cloud computing. Generally, the users of public cloud computing will spread in different places geographically. In the context of some specific business model, cloud computing users can originate from the same network or region. The concept of using cloud computing services like this can be described as shown in fig. 4.11, 4.12 and 4.13.
Figure 4.11 Users Search

Figure 4.12 Categorizing Users
4.14 CHAPTER SUMMARY

The chapter portrayed an insight to the user segregation based on the queries i.e. the requirements of the users which have to be served by the suppliers of the cloud. For minimizing the security problems the users are segregated based on their queries based on which they will be served. The forthcoming chapter describes the message inspector which attempts to audit the results given to the users as a result of the posted queries.