**ABSTRACT**

In recent years, due to the appealing features of cloud computing, large amount of data have been stored in the cloud. Although cloud based services offer many  advantages, privacy and security of the sensitive data is a big concern. To mitigate the concerns, it is desirable to outsource sensitive data in encrypted form. Encrypted storage protects the data against illegal access, but it complicates some basic, yet important functionality such as the search on the data. To achieve search over encrypted data without compromising the privacy, considerable  amount of searchable encryption schemes have been proposed in the literature. However, almost all of them handle exact query matching but not similarity matching; a crucial requirement for real world applications. Although some sophisticated secure multi-party computation based cryptographic techniques are available for similarity tests, they are computationally intensive and do not scale for large data sources.

**Existing System**

In today’s data intensive environment, cloud computing becomes prevalent due to the fact that it removes the burden of large scale data management in a cost effective manner. Hence, huge amount of data, ranging from personal health records to e-mails, are increasingly outsourced into the cloud. At the same time, transfer of sensitive data to untrusted cloud servers leads to concerns about its privacy.

**Problems on existing system:**

1.     Transfer of sensitive data to untrusted cloud servers leads to concerns about its  privacy

2.     It does not provide more security and we get the files from only exact name required.

**Existing System**

In today’s data intensive environment, cloud computing becomes prevalent due to the fact that it removes the burden of large scale data management in a cost effective manner. Hence, huge amount of data, ranging from personal health records to e-mails, are increasingly outsourced into the cloud. At the same time, transfer of sensitive data to untrusted cloud servers leads to concerns about its privacy.

**Problems on existing system:**

1.     Transfer of sensitive data to untrusted cloud servers leads to concerns about its  privacy

2.     It does not provide more security and we get the files from only exact name required.

IMPLEMENTATION

             Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**Main Modules:-**

**1.KeyGeneration:**

                 The key generate from the authorized owner  for the file security. They provide a strong security definition and prove the security of the proposed scheme under the  provided definition.

                The dataowner who know the what kind of file this for make a key  It becomes Encrypt with  filename  for the purpose of Security.

**2.Indexconstruction:**

            The key of common Index can be made from the Index word given by the Dataowner and File. The secure index and a search scheme to enable fast similarity search in the context of encrypted data. In such a context, it is very critical not to sacrifice the confidentiality of the sensitive data while providing functionality. We provided a rigorous security definition and proved the security of the proposed scheme under the provided definition to ensure the confidentiality.

**3.DataEncryption:**

                Alice sends the encrypted collection along with the secure index to the remote server. Once data is outsourced, data users should be able to selectively retrieve data from the remote server. To do so, Alice shares the following information with data users:

           • Secret key of data collection encryption

           • Secret keys of index construction

           •Metric space translation function of index construction

           • Locality sensitive hash function of index construction Shared information

             enables data users to perform similarity search on the encrypted collection.

**4.Data Decryption:**

                         Once the encrypted items corresponding to the search request are retrieved, user decrypts them with the key to obtain their plain versions. Alice (data owner) can easily generate the trapdoors for the buckets of f and f0 and request the corresponding encrypted bit vectors from the server. Once received bit vectors are updated and encrypted by Alice, they can be sent back to the server. Note that, some buckets of f0 may not exist on the server. In such a case, Alice can ask server to replace some fake records with the new real records.To do so, Alice should keep identifiers of the fake records and generate trapdoors with them for replacement request. Similarly, if the content of some buckets for f becomes empty after an update, Alice can ask for replacement of the corresponding records with some fake records via a similar replacement request. Existence of both addition and removal of fake records hides their amount at a particular time. Finaly they provide Original Data.

**5.Search:**

               we provide a specific application of the proposed similarity searchable encryption scheme to clarify its mechanism.Server performs search on the index for each component  and sends back the corresponding encrypted bit vectors it makes by the respective  like commend. Finally, we illustrated the performance of the proposed scheme with empirical analysis on a real data.

**H/W System Configuration:-**

**Processor               -    Pentium –III**

**Speed                                -    1.1 Ghz**

**RAM                                 -    256  MB(min)**

**Hard Disk                          -   20 GB**

**Floppy Drive                     -    1.44 MB**

**Key Board                         -    Standard Windows Keyboard**

**Mouse                                -    Two or Three Button Mouse**

**Monitor                              -    SVGA**