# Assignment 1

**Problem statement:**
Use an academic web search to locate a journal paper which describes a design outcome in your field of interest (i.e. your engineering discipline).You must enter several keywords which relate to your topic. Read the paper and, using your own words, demonstrate your understanding of the paper by:

- Brief Contribution
- Performance metric, data set, comparative analysis and outcomes
- Writing out the major conclusions of the paper;
- Outlining the verification method(s) used to support these conclusions
- Describing the author's reflective comments on the quality of the design (positive and negative).
- The positive and negative environmental impacts;

After reading a published research paper, write down the research question you think the author have addressed in undertaking this research. Do you think the paper adequately supports the conclusions reached in addressing the question?

**Domain name:** Cloud Computing

**Theory:**

Cloud Computing is the storing of data and applications on remote servers and accessing them via the internet rather than saving or installing them on our personal or office computer. The term "cloud" is used because data and applications are stored on a cloud or connected web servers. The cloud can be accessed via the cloud computing system interface software that can be simple as using a web base service which helps all the applications and files that you will need for your job and personal life. The cloud is being used not only to store data but also inexpensive, efficient, flexible alternative to the computer to maintaining in-house computing equipment and software.

The cloud computing architecture is comprised of two parts. The front end and back end. The front end represents a computer that you as a client see, this side requires you to access the cloud computing system. The back end represents our cloud computing system is comprises computers, servers, and data storage system which store all your files and information.

Deployment models of Cloud Computing

- Private cloud: a cloud infrastructure operated by a single organization and it can be managed internally or by a third party.
- Community cloud: it is used by distinct groups (or communities) of organizations. The communities' benefits from public cloud capabilities and also know their neighbors.

- Public cloud: the capability resources are shared with the provider's other customers. No awareness of their neighbors.
- Hybrid cloud: it is a composition of two or more clouds. It uses the public cloud for general computing and stores customer's data in private clouds.

Service models of Cloud Computing

- Iaas (Infrastructure-as-a-service): Iaas cloud offers virtual machines, file storage, firewalls, load balancers and IP addresses.
- Paas (platform-as-a-service): Paas cloud provides an operating system, execution runtime, database, web server and dev tools.
- Saas (software–as-a-service): Saas cloud provides Email, CRM, virtual desktop, communication, and games.

**A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data**

This paper is been published in *International Journal of Advance Research, Ideas and Innovations in Technology , which has* **ISSN: 2454-132X and Impact factor: 4.295**
***(Volume3, Issue1)***

1) **Brief Contribution**

The major aim of this paper is to solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) at the time of protecting exact method wise privacy in the cloud computing concept. For this author has completely studied existing system and to overcome problems in existing system author proposed new system with the architecture of ranked search over encrypted cloud data . The existing system proposes a secure tree-based search scheme over the encrypted cloud data, which supports multi-keyword ranked search and dynamic operation on the document collection. To face the challenge of cooperating such multi keyword semantic without privacy breaches, we propose a basic idea for the MRSE using secure inner product computation, which is modified from a secure k-nearest neighbor (kNN) method, and then give two considerably improved MRSE method in a step-by-step way to accomplish different severe privacy needs in two risk models with enlarged attack competence.

2) **Performance metric, data set, comparative analysis and outcomes**

**a) Performance metric**

Author has implemented the proposed scheme using C++ language in Windows 7 operation system and tests its efficiency on a real-world document collection: the Request for Comments (RFC). The test includes

1) The search precision on different privacy level, and

2) The efficiency of index construction, trapdoor generation, search, and update.

Data users can accomplish different requirements on search precision and privacy by adjusting the standard deviation σ, which can be treated as a balance parameter.

**b) Data set**:

The data set used by author as follows:

- Precision rank privacy
- Precision of different standard deviation σ
- Multi-keyword Ranked Search Over Encrypted(MRST)
- BDMRS- Basic dynamic multi-keyword ranked search table
- EDMRS -enhanced dynamic multi-keyword ranked search table

**c) Comparative analysis**

Author has also provided efficiency in Index Tree Construction ,Trapdoor Generation, Search Efficiency, Update Efficiency.

Author has given comparative analysis in

- Time cost for trapdoor generation for different sizes of dictionary with the fixed number of query keywords, t = 10, and for different numbers of query keywords with the fixed dictionary, m = 4000
- The efficiency of a search with ten keywords of interest as input for the different sizes of document collection with the same dictionary, m = 4000, and for different numbers of retrieved documents with the same document collection and dictionary, n=1000, and m = 4000.
- For deletion of a document ,when the size of dictionary is fixed, the deletion of a document takes nearly logarithmic time with the size of document collection and the update time is proportional to the size of dictionary when the document collection is fixed

**d) Outcomes**

- It includes Time cost for index tree construction, The efficiency of a search with ten keywords of interest as input, Time cost for trapdoor generation, Time cost for deletion of a document.

The generation of a trapdoor incurs a vector splitting operation and two multiplications of a (m × m) matrix, thus the time complexity is O (m2). Due to the dimension extension, the time cost of EDMRS scheme is a little higher than that of BDMRS scheme.
The space complexity of each note for data deletion is increased from O(m) to O(mlogn).

3) **Writing out the major conclusions of the paper**

Author has described and solves the problem of multi-key word ranked search over encrypted cloud data, and set up a range of privacy requirements. Among various multi-keyword semantics, we can select the efficient similarity measure of "coordinate matching," i.e., as many equivalent as possible, to effectively capture the Relevance of outsourced documents to the query Keywords

4) **Outlining the verification method(s) used to support these conclusions**

Author has compared existing systems and formulated the proposed system. They have also provided performance matrix to observed values in proposed system to check system behavior. With the help of Time cost for index tree construction, The efficiency of a search with ten keywords of interest as input, Time cost for trapdoor generation, Time cost for deletion of a document we can A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data.

5) **Describing the author's reflective comments on the quality of the design**

Among various multi-keyword semantics, we select the efficient similarity measure of "coordinate matching," i.e., as many equivalent as possible, to effectively capture the Relevance of outsourced documents to the query Keywords, and utilize "inner product similarity" to quantitatively calculate such comparison measure. In order to acquire the test of supporting multi-keyword semantic without privacy violation, we offer a basic idea of MRSE using secure inner product calculation. Then, we give two improved MRSE schemes to attain various severe privacy needs in two different threat models. The further enhancements of our ranked search method, including supporting more search semantics, i.e., TF×IDF, and dynamic data process detailed analyses in investigating privacy and efficiency assurance of proposed schemes are mentioned, and testing on the real-world data set demonstrate our proposed schemes which introduces low transparency on both calculation and communication.

6) **The positive and negative environmental impacts**

As per authors perspective this system supports A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data but if ranked search system fails entire system will collapse and there may be data security issue and data storage issue.

After considering all the points paper adequately supports the conclusions reached in addressing the question

1. Is privacy maintained in encrypted cloud data?
2. How the multi-key word rank search is performed over encrypted cloud data?
3. Which encryption algorithm allows users to occupy in the ranking over the encrypted cloud data?
4. Is data leakage is avoided and data security is achieved?

Using a basic idea of MRSE using secure inner product calculation, the author has solved the problem of multi-key word ranked search over encrypted cloud data, and set up a range of privacy requirements. The DES encryption algorithm allows user to occupy in the ranking while

the popularity of computing work is done on the server side by process only on cipher text. Thus, data leakage can be eradicated and data security is guaranteed

5. How data is secured/retrieve data in terms of cloud server crash?
6. How the ideal time complexity of O(n) MRSE operations is achieved with regards to O(n2)?

    There has been no method that could protect the data from cloud server crash. Also, the time complexity of the MRSE operations is O(n2) as compared to ideal O(n).