**Result-Pattern Hiding Searchable Encryption for Conjunctive Queries**

**E.GANSHKUMAR Reg no:4317109a**

**Abstract:**

Cloud computing is an on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet. Previously “partially hiding” predicate encryption scheme for functions that compute an arithmetic branching program on public attributes followed by an inner product predicate on private attributes. This constitutes the first “best of both worlds” result in bilinear groups that simultaneously generalizes existing attribute-based encryption schemes and inner product predicate encryption. Now Public key encryption with equality test (known as PKE-ET) enables anyone to perform equivalence test between two messages encrypted under distinct public keys. Attribute-hiding predicate encryption is a paradigm for public key encryption that supports both attribute-hiding and fine-grained access control. In this paper, we first initialize the concept of attribute-hiding predicate encryption with equality test (shorten as AH-PE-ET) by incorporating the notions of PKE-ET and PE, and then propose a concrete AH-PE-ET scheme. Inheriting the merits of predicate encryption, versatile access control can be achieved such that the cipher texts and the secret key are respectively associated with the descriptive attributes x and the Boolean functions f and decryption can only be done if f(x) returns true. In the AH-PE-ET scheme, one data receiver can calculate a trapdoor using his/her private key and deliver this trapdoor to an un-trusted cloud server, who in turn compares the cipher texts from this receiver with other receivers’ cipher texts

**Existing system**

In the existing system, ABE-based access control mechanisms cannot preserve the privacy of user’s attributes. To be more specific, although the outsourced data are stored in the form of ciphertext, the attributes associated with the ciphertext are clearly exposed to the malicious adversary. These attributes usually contain sensitive privacy information about users. This seriously disgraces the privacy of users if attribute disclosure happens.

**Disadvantages**

* In this system leakage of some data occurs.
* Less security.

**Proposed system**

In the proposed scheme, it is the first such scheme which meanwhile deals with these issues on both privacy protection of user attributes and flexible data search. Additionally, the rigorous security proof clearly states to prove that our scheme is IND-CPA secure in the standard model under decisional bilinear Diffie-Hellman assumption. Finally, we present theoretical comparisons and experimental simulations of the existing ABE-ETs and our AH-PE-ET scheme to indicate the feasibility and practicability of our proposed scheme.

**Advantages**

* Controls the leakage of information.
* More secure.

**S/W System Configuration**

**Software Requirements**

* Operating System : Windows 8
* Application Server : Tomcat 7.0
* Front End : HTML, JSP,CSS
* Scripts : JavaScript.
* Backend Language : Java
* Database : MySQL 6.0
* IDE : Eclipse(2019-3)

**Hardware Requirements**

# Processor - Intel i3

* RAM - 4GB
* Hard Disk - 500 GB