**Efficient and Expressive Keyword Search Over Encrypted Data in Cloud**

**Abstract**

In this project Searchable encryption allows a cloud server to conduct keyword search over encrypted data on behalf of the data users without learning the underlying plaintexts. However, most existing searchable encryption schemes only support single or conjunctive keyword search, while a few other schemes that are able to perform expressive keyword search are computationally inefficient since they are built from bilinear pairings over the composite-order groups. In this paper, we propose an expressive public-key searchable encryption scheme in the prime-order groups, which allows keyword search policies (i.e., predicates, access structures) to be expressed in conjunctive, disjunctive or any monotonic Boolean formulas and achieves significant performance improvement over existing schemes. We formally define its security, and prove that it is selectively secure in the standard model. Also, we implement the proposed scheme using a rapid prototyping tool called Charm and conduct several experiments to evaluate it performance. The results demonstrate that our scheme is much more efficient than the ones built over the composite-order groups . Keyword research is one of the most important, valuable, and high return activities in the search marketing field. Ranking for the right keywords can make or break your website. By researching your market's keyword demand, you can not only learn which terms and phrases to target with SEO, but also learn more about your customers as a whole.

**EXISTING SYSTEMS:-**

However, the solution in as well as other existing PEKS schemes which improve on only support equality queries As such, our scheme is not only capable of expressive multi-keyword search, but also significantly more efficient than existing schemes built in composite-order groups. Using a randomness splitting technique, our scheme achieves security against offline keyword dictionary guessing attacks to the ciphertexts. Moreover, to preserve the privacy of keywords against offline keyword dictionary guessing attacks to trapdoors, we divide each keyword into keyword name and keyword value and assign a designated cloud server to conduct search operations in our construction.We formalize the security definition of expressive SE, and formally prove that our proposed expressive SE scheme is selectively secure in the standard model.

**Disadvantages:**

The approach based on set intersection leaks extra information to the cloud server beyond the results of the conjunctive query, whilst the approach using meta keywords require 2m meta keywords to accommodate all the possible conjunctive queries for m keywords. It is straightforward to see that compared to the existing ones, our construction make a good balance in that it allows unbounded keywords, supports expressive access structures, and is built in the prime-order groups

**PROPOSED SYSTEMS:-**

We propose an expressive public-key searchable encryption scheme in the prime-order groups, which allows keyword search policies (i.e., predicates, access structures) to be expressed in conjunctive, disjunctive or any monotonic Boolean formulas and achieves significant performance improvement over existing schemes. We formally define its security, and prove that it is selectively secure in the standard model.In order to tackle the keyword search problem in the cloud-based healthcare information system scenario, we resort to public-key encryption with keyword search (PEKS) schemes, which is firstly proposed in . In a PEKS scheme, a ciphertext of the keywords called “PEKS ciphertext” is appended to an encrypted PHR. To retrieve all the encrypted PHRs containing a keyword, say “Diabetes”, a user sends a “trapdoor” associated with a search query on the keyword “Diabetes” to the cloud service provider, which selects all the encrypted PHRs containing the keyword “Diabetes” and returns them to the user while without learning the underlying PHRs.

**ADVANTAGES:-**

The expressive SE scheme inherits the advantages of the Rouselakis-Waters scheme . Thus, it is straightforward to see that in our SE scheme, the size of the public parameter is immutable with the number of keywords, and the number of the keywords allowed for the system is unlimited and can be freely set. According to the analysis in terms of the pairing-friendly elliptic curves, prime order groups have a clear advantage in the parameter sizes over composite order groups. the advantage for a polynomial time adversary that can distinguish between the games Game0 and Game1 is negligible.

**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.

**Modules:**

In this project we have following Four modules

* Searchable Encryption,
* Cloud Computing,
* Expressiveness Keyword search
* Attribute-Based Encryption

**Cloud Computing:-**

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services) which can be rapidly provisioned and released with minimal management effort. Cloud-based healthcare information system that hosts outsourced personal health records (PHRs) from various healthcare providers. The PHRs are encrypted in order to comply with privacy regulations like HIPAA. In order to facilitate data use and sharing, it is highly desirable to have a searchable encryption (SE) scheme which allows the cloud service provider to search over encrypted PHRs on behalf of the authorized users (such as medical researchers or doctors) without learning information about the underlying plaintext. Note that the context we are considering supports private data sharing among multiple data providers and multiple data users.

**Attribute-based encryption:-**

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). The basic idea of our scheme is to modify a key-policy attributed-based encryption (KP-ABE) scheme constructed from bilinear pairing over prime-order groups. Without loss of generality, we will use the large universe KP-ABE scheme selectively secure in the standard model proposed by Rouselakis and Waters in [to illustrate our construction during the rest of the paper.

Expressiveness Keyword:-

The proposed scheme should support keyword access structures expressed in any Boolean formula with AND and OR gates. Efficiency. The proposed scheme should be adequately efficient in terms of computation, communication and storage for practical applications.

A ciphertext without its corresponding trapdoors should not disclose any information about the keyword values it contains to the cloud server and outsiders. Second, a trapdoor should not leak information on keyword values to any outside attackers without the private key of the designated cloud server.

We capture this notion of security for the SE scheme in terms of semantic security to ensure that encrypted data does not reveal any information about the keyword values, which we call “selective indistinguishability against chosen keyword-set .

**Architecture Digrams:-**



# System Configuration:

**HARDWARE REQUIREMENTS**:

Hardware - Pentium

Speed - 1.1 GHz

RAM - 1GB

Hard Disk - 20 GB

Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

**SOFTWARE REQUIREMENTS**:

Operating System : Windows

Technology : Java and J2EE

Web Technologies : Html, JavaScript, CSS

IDE : My Eclipse

Web Server : Tomcat

Tool kit : Android Phone

Database : My SQL

Java Version : J2SDK1.5

**CONCLUSION :-**

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the publickey setting, Boneh proposed a cryptographic primitive called public-key encryption with keyword search (PEKS). Since then, considering different requirements in practice, e.g., communication overhead, searching criteria and security enhancement, various kinds of searchable encryption systems have been put forth. However, there exist only a few public-key searchable encryption systems that support expressive keyword search policies, and they are all built from the inefficient composite-order groups . In this paper, we focused on the design and analysis of public-key sive searching formulas. Based on a large universe key-policy attribute-based encryption scheme given in , we presented an expressive searchable encryption system in the primeorder group which supports expressive access structures expressed in any monotonic Boolean formulas. Also, we proved its security in the standard model, and analyzed its efficiency using computer simulations.