EXPRESSIVE KEYWORD SEARCH IN CLOUD OVER ENCRYPTED DATA

[1] Dayanada R B, [2] Dishika Ravindra, [3] Keerthi G Naidu, [4] L Vinith Kumar, [5] Lavanya M,

[1] Professor, Department of Computer Science & Engineering, K S Institute of Technology ,
[2,3,4,5] Undergraduate student, Computer Science & Engineering, K S Institute of Technology

Abstract: *:* Searchable encryption enables a cloud server to perform keyword search over scrambled information for the benefit of the information clients without learning the basic plaintexts. Notwithstanding, most existing accessible encryption plots just help single or conjunctive keyword look, while a couple of different plans that can perform expressive keyword search are computationally wasteful since they are worked from bilinear pairings over the composite-request gatherings. In this paper, we propose an expressive public key accessible encryption conspire in the prime-request gatherings, which permits keyword look arrangements (i.e., predicates, get to structures) to be communicated in conjunctive, disjunctive or any monotonic Boolean equations and accomplishes noteworthy execution improvement over existing plans. We formally characterize its security, and demonstrate that it is specifically secure in the standard model. The results show that our plan is considerably more productive than the ones worked over the composite-request gatherings.

Indexed Terms - Searchable encryption, cloud computing, expressiveness, attribute based encryption.

I. INTRODUCTION

Cloud Computing is a rapid growing technology which provides various of resources to the user on demand like storage resource, computing resources and so on. Basically, users store the data on cloud and retrieve the data when required. But the problem is unauthorized access of the data. Thus, searchable encryption (SE) allows a cloud server to performs keyword search over encrypted data without learning the underlying plaintexts on behalf of the data users. Consider a cloud-based social insurance data framework that has redistributed patient health records (PHRs) from different medicinal services suppliers. The PHRs are scrambled in request to conform to protection guidelines like HIPAA. In request to encourage information use and sharing, it is exceedingly alluring to have an searchable encryption plot which permits the cloud specialist organization to look over encoded PHRs for the benefit of the approved clients, without learning data about the basic plaintext. Multiple data sharing among multiple data users is the main context in the system. Hence, SE plans in the private-key setting , which expect that a single client who looks and recovers his/her very own information, are not appropriate. Hence, SE plans in the private-key setting , which expect that a single client who looks and recovers his/her very own information, are not appropriate. On the other hand, , private data recovery (PIR) protocols , which enable clients to recover a specific information thing from a database which openly stores information without uncovering the information thing to the database manager, are additionally not reasonable, since they require the information to be freely accessible. So as to handle the keyword search issue in the cloud-based human services data framework situation, we resort to open key encryption with keyword look (PEKS) plans, which is initially proposed in. . In a PEKS plot, a ciphertext of the keyword called "PEKS ciphertext" is added to an encoded PHR. To recover all the encoded PHRs containing a keyword, state "Diabetes", a client sends a "trapdoor" related 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. However, the solution in as well as other existing PEKS schemes which improve on only support equality queries . Set intersection and meta keywords1 can be used for conjunctive keyword search. . In order to address the above deficiencies in conjunctive keyword search, schemes such as the ones in were put forward in the public-key setting. Ideally, in the practical applications, search predicates (i.e., policies) should be expressive such that they can be expressed as conjunction, disjunction or any Boolean formulas of keywords. In the above cloud-based healthcare system, to find the relationship between diabetes and age or weight, a medical researcher may issue a search query with an access structure (i.e., predicate). SE schemes supporting expressive keyword access structures were presented in. In this paper, we propose an open key based expressive SE conspire in

prime-request gatherings, which is particularly reasonable for keyword search over scrambled information in situations of different information proprietors and numerous information clients, for example, the cloud-based medicinal services data framework that has re-appropriated PHRs from different social insurance suppliers.

II. RELATED WORK

Public-Key Encryption with Keyword Search. The investigation of public key encryption with keyword search (PEKS), a few PEKS developments were advanced utilizing various systems or considering contrast circumstances. They expect to fathom two cruces in PEKS: (1) how to make PEKS secure against disconnected keyword reference speculating assaults; and (2) how to accomplish expressive looking predicates in PEKS. As far as the disconnected keyword reference speculating assaults, which necessitates that no enemy (counting the cloud looking server) can take in keyword from an offered trapdoor, supposedly, such a security thought is difficult to be accomplished in the public key setting . With respect to expressive inquiry, there are just couple of works in PEKS . Lamentably, the development in is based on inward item predicate encryption, and the developments in , are worked from the pairings in composite-request gathering. Along these lines, they are not adequately proficient to be embraced in the down to earth world . Additionally, the quantity of keyword permitted in these pursuit capable plans are predefined in the framework setup stage. It is direct to see that contrasted with the current ones, our development make a decent equalization in that it permits unbounded catchphrases, bolsters expressive access structures, and is worked in the prime-request gatherings.

Private-key Searchable Encryption. In a private-key SE setting, a client transfers its private information to a remote database and keeps the information private from the remote database promotion ministrator. Private-key SE enables the client to recover every one of the records containing a specific keyword from the re-bit database . Be that as it may, as the name proposes, private-key SE arrangements just apply to situations where information proprietors and information clients completely confided in one another.

Private Information Retrieval. Regarding open database, for example, stock statements, where the client is ignorant of it and wishes to scan for certain information thing without uncovering to the database manager which thing it is, private information recovery (PIR) conventions were presented, which enable a client to recover information from an open database with far littler correspondence then simply downloading the whole database. By the by, in our unique situation, the database isn't openly accessible, the information isn't open, so the PIR arrangements can't be connected.

III. OBJECTIVES

i. To provide security of the data stored in the cloud. Users store the data on cloud in encrypted form where only intended users can have the access to the data.
ii. To reduce the time for searching required data in cloud. Time efficiency is an important aspect in any system. Time required in searching the keyword in encrypted data is reduced when compared to other existing systems.
iii. Ensure stronger data accessibility. Users may require to access the data stored on cloud. Attribute based encryption is used where the data is retrieved based on the user attributes.

Various encryption techniques have been planned, actualized and created for searching data in the cloud. A system which supports efficient and expressive keyword search is one of the principal approaches that utilizes multi-keyword search when data is searched by the server without knowing the underlying plain text in the cloud. Thus, security and the privacy of the data is achieved by this system.

IV. DESIGN

System Architecture design-identifies the overall hypermedia structure for the WebApp. Architecture design consists of the goals established for a WebApp, the content that has to be presented, the users who can access the data , and the navigation of the system that has been established. Content architecture, mainly focuses on how the content objects are used and structured for presentation and navigation. WebApp architecture, addresses the manner in which the application is structure to manage user interaction, handle internal processing tasks, effect navigation, and present content. WebApp architecture is defined within the context of the development environment in which the application is to be implemented.

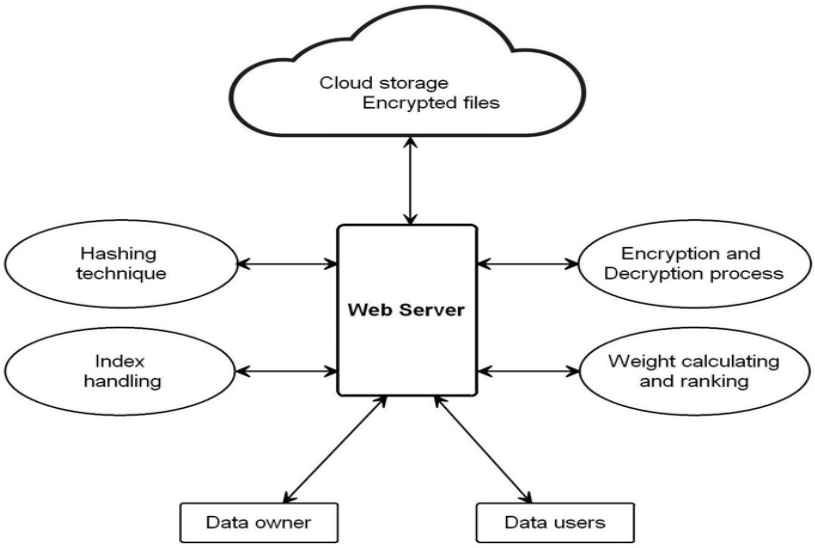

Fig 1 : System Architecture

Our expressive SE conspire comprises of a trusted trapdoor age focus which distributes an open framework parameter what's more, keeps an key stealthily, a cloud server which stores and hunts scrambled information in the interest of information clients, various information proprietors who transfer scrambled information to the cloud, and various information clients who might want to retrieve scrambled information containing certain keywords.. To re-appropriate a scrambled record to the cloud, an information proprietor attaches the scrambled record with keywords encoded under the open parameter and transfers the consolidated scrambled record and scrambled keywords to the cloud. To recover all the scrambled records containing keywords fulfilling a specific access structure (i.e., predicate or approach) an information client initially acquires a trapdoor related with the entrance structure from the trapdoor age focus and at that point sends the trapdoor to the cloud server.

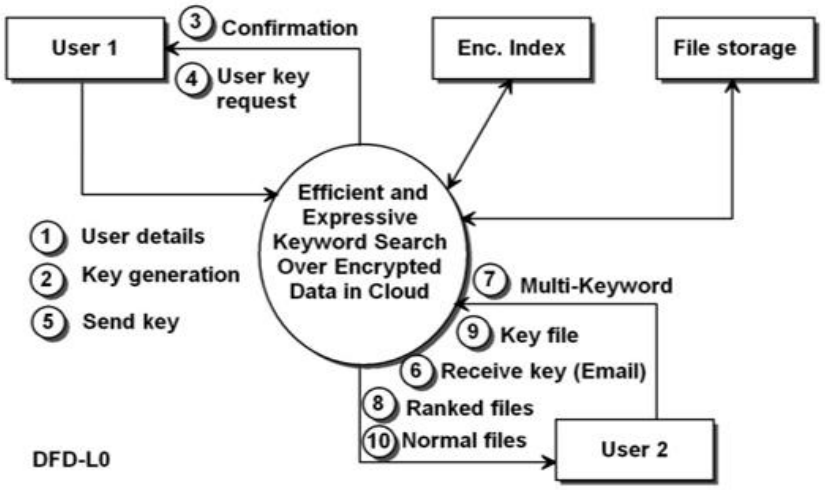

Fig 2 : Data Flow Diagram

Initially data owner uploads the file with the attributes. The file is taken and searched for the keywords by removing punctuation, pronouns and unnecessary words. Weight for each keyword in that particular file is calculated which is called the rank of the keyword. Each of these keyword is then hashed using any of the hashing techniques and this hash value of the keyword is stored in the cloud along with the encrypted file and the encrypted keyword. Thus the data stored in the cloud is in encrypted form. Users can access the data stored on the cloud based on their attributes by keyword search. When the user searches a particular file by giving certain keyword, if the attributes of the user is matching the attributes of the file stored on the cloud then the file is returned in the decrypted form.

V. RESULTS

A snapshot is the state of a system at a point in time. The actual copy of the state of a system or to a capability provided by certain systems can be referred.

The snapshots of the system are shown below :

Fig 3 : Login Page

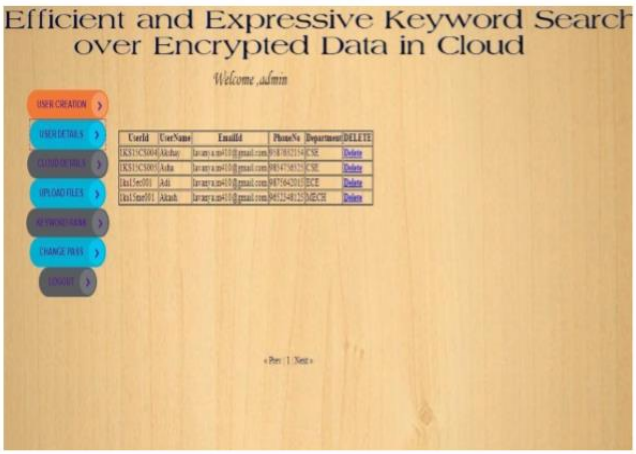

Fig 4 : User Details

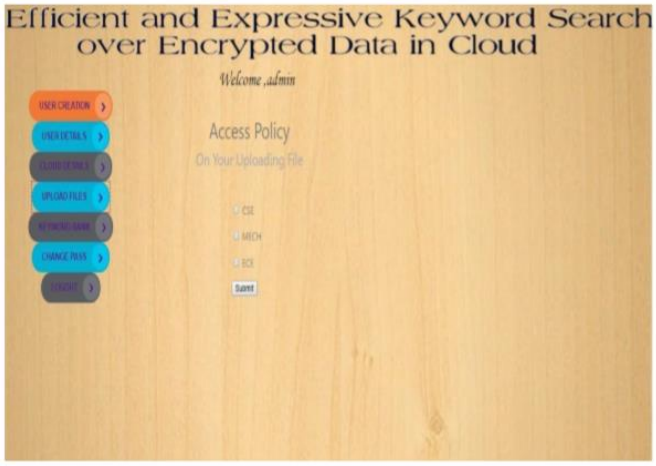

Fig 5 : File Upload

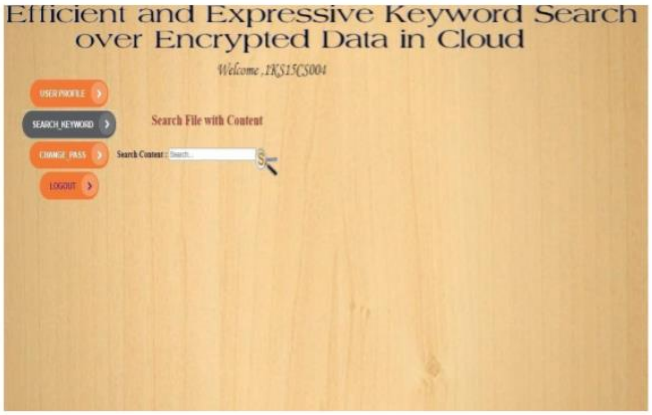

Fig 6 : Keyword Search

VI. CONCLUSION

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the public key setting, 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. . In any case, there exist just a hardly any public key accessible encryption frameworks that help expressive keyword search arrangements, and they are altogether constructed from the composite-request bunches . In this paper, we concentrated on the plan and examination of public key accessible encryption frameworks in the prime-request gatherings that can be utilized to look through various keywords in expressive looking equations. . In light of a vast universe key-strategy property based encryption conspire given in we presented an expressive accessible encryption framework in the prime- request bunch which underpins expressive access structures communicated in any monotonic Boolean recipes. Likewise, we demonstrated its security in the standard model, and dissected its proficiency utilizing PC enactments.

ACKNOWLEDGEMENT

The successful project execution would have not been possible without the people who made it possible and whose constant guidance crowned our effort with success. We take this opportunity to express our sincere gratitude to Management K S Institute of Technology, Bengaluru. We would like to express our gratitude to Dr. K.V.A. Balaji C.E.O. K.S. Institute of Technology, Bengaluru, for facilitating us to build and present the project. We would like to extend our gratitude to Dr.T.V.Govindaraju, Principal/Director, K.S. Institute of Technology, Bengaluru, for providing opportunity to publish this paper.

We thank Dr. Rekha.B.Venkatapur, Professor and Head, Department of Computer Science and Engineering, K.S. Institute of Technology, Bengaluru, for her encouragement.

We would also like to thank, Mr. K. Venkata Rao, Associate Professor, Department of Computer Science and Engineering, K.S. Institute of Technology, Bengaluru, for his constant guidance and inputs.

We wholeheartedly thank our project mentor Dr. Dayananda R B, Professor, Department of Computer Science and Engineering, K.S. Institute of Technology, Bengaluru, for his support and guidance throughout.

Finally, we would like to thank all the teaching and non-teaching staff of the college for their cooperation. Moreover, I thank all my family and friends for their invaluable support and cooperation.

REFERENCES

[1] https://en.wikipedia.org/wiki/Counterfeit_medications

[2] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advances in Cryptology - EUROCRYPT 2004,

[3] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in 2000 IEEE Symposium on Security and Privacy, Berkeley, California, USA, May 1417, 2000. IEEE Computer Society, 2000, pp. 44–55

[4] W. Ogata and K. Kurosawa, “Oblivious keyword search,” J. Complexity, vol. 20, no. 23, pp. 356–371, 2004.