International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Secure Search Scheme over Encrypted Cloud Data Using Greedy Depth First Search Algorithm

L.Prabhat , E.Swetha , P.Sahithi , P.Sai Chandra

[1] (internal guide), Asst.Professor, -prabhat.ou@gmail.com

[2] (BTECH) -edamswetha222@gmail.com

[3] (BTECH) -sahithiparne@gmail.com

[4] (BTECH) -saichandrarox2k15@gmail.com

[1,2,3,4] Department Of Information Technology, Teegala Krishna Reddy Engineering College, Medbowli, Meerpet, Saroornagar (M), Hyderabad-500097

Abstract:

Secure pursuit methods over encrypted cloud data enable an approved client to query data records of enthusiasm by submitting encrypted query keywords to the cloud server in a protection saving way. In any case, by and by, the returned query results might be erroneous or inadequate in the untrustworthy cloud condition. For instance, the cloud server may deliberately overlook some qualified outcomes to spare computational assets and correspondence overhead. Accordingly, a well-working secure query framework ought to give a query comes about check system that enables the data client to confirm comes about. we display a safe multi-keyword ranked hunt plot over encrypted cloud data, which at the same time underpins dynamic refresh tasks like cancellation and addition of records. In particular, the vector space demonstrate and the broadly utilized TF _ IDF show are consolidated in the index development and query age. We develop a unique tree-based index structure and propose a "Greedy Depth-first Search" calculation to give productive multi-catchphrase ranked inquiry. The safe kNN calculation is used to scramble the index and query vectors, and in the interim guarantee precise significance score estimation between encrypted index and query vectors. With a specific end goal to oppose factual assaults, ghost terms are added to the index vector for blinding query items. Because of the utilization of our exceptional tree-based index structure, the proposed plan can accomplish sub-straight pursuit time and manage the cancellation and addition of reports adaptably. Broad tests are directed to exhibit the productivity of the proposed conspire..

Keywords

Encrypted, Cloud, Data, Query, Server, Greedy, Depth, First, Multi, Ranked, Index.

1. Introduction

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high--end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and

security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

Software protection and simulation on oblivious rams by O. Goldreich and R. Ostrovsky. Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM.A machine is oblivious if the sequence in which it accesses memory locations is equivalent for any two inputs with the same running time. For example, an oblivious Turing Machine is one for which the movement of the heads on the tapes is identical for each computation. (Thus, the movement is independent of the actual input.) What is the slowdown in the running time of a machine, if it is required to be oblivious? In 1979, Pippenger and Fischer showed how a two-tape oblivious Turing Machine can simulate, on-line, a one-tape Turing Machine, with a logarithmic slowdown in the running time. We show an analogous result for the random-access machine (RAM) model of computation. In particular, we show how to do an on-line simulation of an arbitrary RAM by a probabilistic oblivious RAM with a polylog arithmetic slowdown in the running time. On the other hand, we show that a logarithmic slowdown is a lower bound.

Practical techniques for searches on encrypted data by D. X. Song, D. Wagner. It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the un trusted server cannot learn anything about the plaintext when only given the cipher text; they provide query isolation for searches, meaning that the un trusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the un trusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the un trusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

Computationally private information retrieval with polylogarithmic communication by C. Cachin, S. Micali. He presented a single-database computationally private information retrieval scheme with polylogarithmic communication complexity. Our construction is based on a new, but reasonable intractability assumption, which we call the Φ-Hiding Assumption (ΦHA): essentially the difficulty of deciding whether a small prime divides Φ(m), where m is a composite integer of unknown factorization.

Single database private information retrieval implies oblivious transfer by G. D. Crescenzo, T. Malkin. A Single-Database Private Information Retrieval (PIR) is a protocol that allows a user to privately retrieve from a database an entry with as small as possible communication complexity. We call a PIR protocol non-trivial if its total communication is strictly less than the size of the database. Non-trivial PIR is an important cryptographic primitive with many applications. Thus, understanding which assumptions are necessary for implementing such a primitive is an important task, although (so far) not a well-understood one. In this paper we show that any non-trivial PIR implies Oblivious Transfer, a far better understood primitive. Our result not only significantly clarifies our understanding of any non-trivial PIR protocol.

Public Key Encryption with keyword Search by D. Boneh, G. D. Crescenzo. We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword \urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We done and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word \urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server

to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

2. System Analysis

i. Existing System:

After Boneh et al. initiated the study of public-key encryption with keyword search (PEKS), several PEKS constructions were put forth using different techniques or considering different situations. They aim to solve two cruces in PEKS: (1) how to make PEKS secure against offline keyword dictionary guessing attacks; and (2) how to achieve expressive searching predicates in PEKS. In terms of the offline keyword dictionary guessing attacks, which requires that no adversary (including the cloud searching server) can learn keywords from a given trapdoor, to the best of our knowledge, such a security notion is very hard to be achieved in the public-key setting. In a private-key SE setting, a user uploads its private data to a remote database and keeps the data private from the remote database administrator. Private-key SE allows the user to retrieve all the records containing a particular keyword from the remote database

Disadvantages Of Existing System:

KPABE schemes are not designed to preserve privacy of attributes (keywords) associated with cipher texts.

Trapdoors are subject to the offline keyword dictionary guessing attacks.

They are not sufficiently efficient to be adopted in the practical world

Private-key SE solutions only apply to scenarios where data owners and data users totally trusted each other.

ii. Proposed System:

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.

First, to preserve keyword privacy in an access structure, we adopt the method to divide each keyword into a generic name and a keyword value. Since keyword values are much more sensitive than the generic keyword names, the keyword values in an access structure are not disclosed to the cloud server, whereas a partial hidden access structure with only generic keyword names is included in a trapdoor and sent to the cloud server.

We equip this designated server with a public and private key pair of which the public key will be used in trapdoor generation such that it is computationally infeasible for anyone without knowledge of the privacy key to derive keywords information from the trapdoor.

We propose the first expressive SE scheme in the public-key setting from bilinear pairings in prime order groups. 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 cipher texts. 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.

Advantages Of Proposed System:

In addition to hiding keywords in cipher texts, we also need to preserve keyword privacy in a trapdoor which contains an access structure as a component.

We formalize the security definition of expressive SE, and formally prove that our proposed expressive SE scheme is selectively secure in the standard model.

We implement our scheme using a rapidly prototyping tool called Charm, and conduct extensive experiments to evaluate its performance. Our results confirm that the proposed scheme is sufficiently efficient to be applied in practice.

3. Design and Implementation

i. Modules:

- Data Owner
- Data User
- Cloud
- TGC

Modules Description:

- ***Data Owner:***

In Data Owner module, Initially Data Owner must have to register their detail and TGC will authorize the registration by sending user id, name through email. After successful login data Owner can upload files into cloud server with File access policy. He/she can view the files that are uploaded in cloud.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

- ***Data User:***

In Data user module, Initially Data user must have to register their detail and TGC will authorize the registration by sending user id, name through email. After successful login he/ can search all the files upload by data owners. He/she can send search request to TGC then TGC will send the trapdoor key. After entering the Trapdoor key he/she can view the file.

- ***Cloud:***

In Cloud module, Cloud can view all the Data owners and data user's details. Cloud can able see the files in cloud uploaded by the data owners.

- ***TGC:***

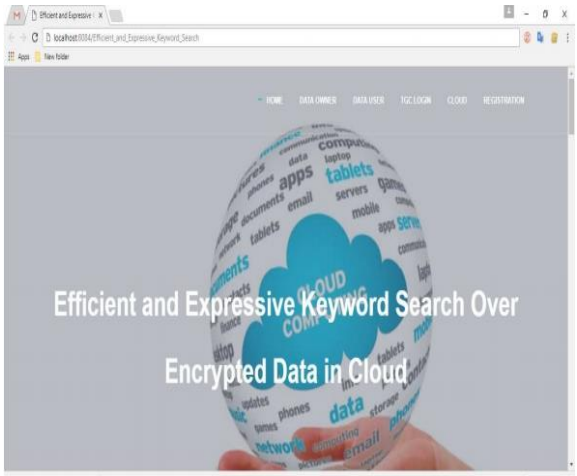
In TGC module, TGC can view all the Data owners and data user's details. TGC will authorize data owners and data users. Also TGC will approve and send the Trapdoor key to the users. TGC can able see the files in cloud uploaded by the data owners.

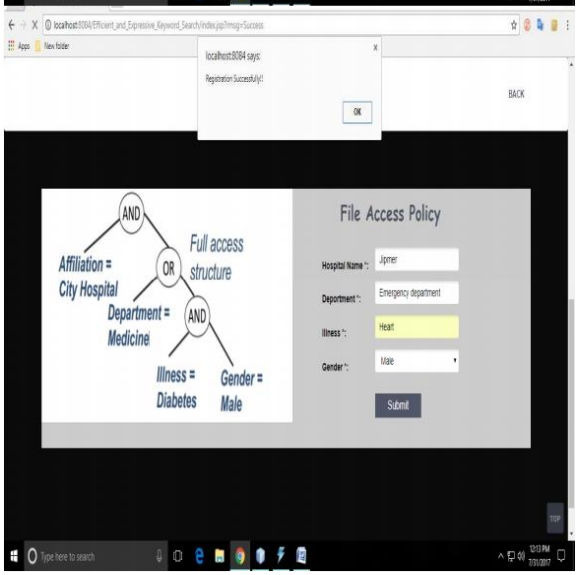
ii. System Design

Data Flow Diagram

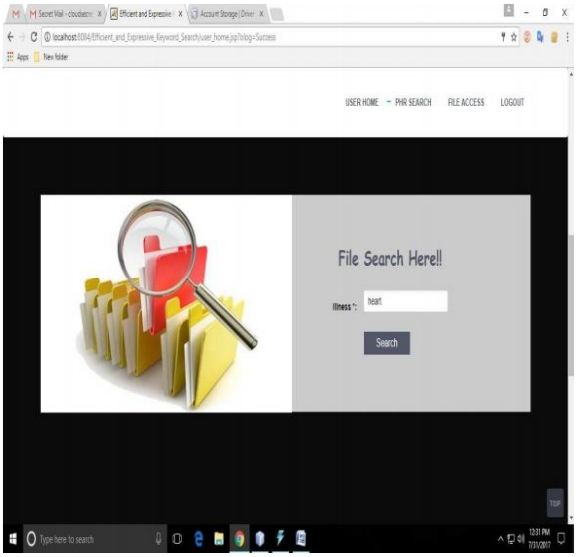
1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

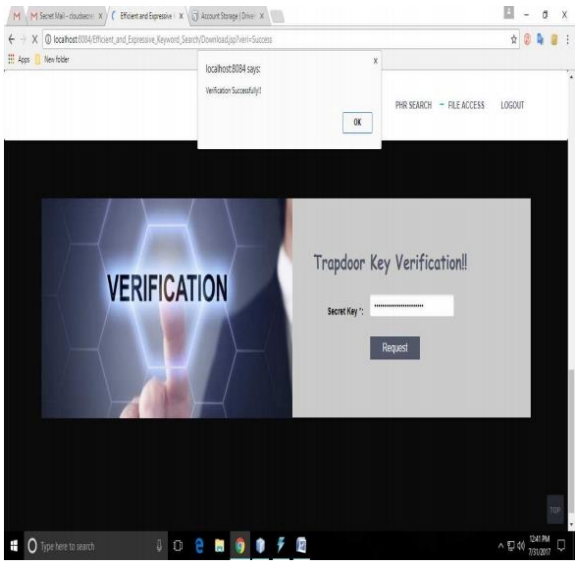
iii. Results





International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018





4. Conclusion

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the public key 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 searchable encryption systems in the prime-order groups that can be used to search multiple keywords in expressive searching formulas. Based on a large universe key-policy attribute-based encryption scheme given in, we presented an expressive searchable encryption system in the prime order 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.

5. References

[1] O. Goldreich and R. Ostrovsky, "Software protection and simulation oblivious rams,"
J. ACM, vol. 43, no. 3, pp. 431–473, 1996.

[2] 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 14-17, 2000. IEEE Computer Society, 2000, pp. 44–55.

[3] E. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol.2003, p. 216, 2003.

[4] C. Cachin, S. Micali, and M. Stadler, "Computationally private information retrieval with polylogarithmic communication," in Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding, ser. Lecture Notes in Computer Science, vol. 1592. Springer, 1999, pp. 402–414.

[5] G. D. Crescenzo, T. Malkin, and R. Ostrovsky, "Single database private information retrieval implies oblivious transfer," in Advancesin Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding, ser. Lecture Notes in Computer Science, vol. 1807. Springer, 2000, pp. 122–138.

[6] W. Ogata and K. Kurosawa, "Oblivious keyword search," J. Complexity, vol. 20, no.
2-3, pp. 356–371, 2004.

[7] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Publickey encryption with keyword search," in Advances in Cryptology- EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May2-6, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol.3027. Springer, 2004, pp. 506–522.

[8] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, "Expressive search on encrypted data," in 8th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '13,

Hangzhou, China - May 08 - 10, 2013. ACM, 2013, pp. 243–252.

[9] P. Golle, J. Staddon, and B. R. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security, Second International Conference, ACNS 2004, Yellow Mountain, China, June 8-11, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol. 3089. Springer, 2004, pp. 31–45.

[10] D. J. Park, K. Kim, and P. J. Lee, "Public key encryption with conjunctive field keyword search," in Information Security Applications,5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers, ser. Lecture Notes in Computer Science, vol. 3325. Springer, 2004, pp. 73–86.

[11] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Pairing-Based Cryptography - Pairing 2007, First International Conference, Tokyo, Japan, July 2-4, 2007, Proceedings, ser. Lecture Notes in Computer Science, vol. 4575. Springer, 2007, pp. 2–22.

[12] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," J. Network and Computer Applications, vol. 34, no. 1, pp. 262–267, 2011..