IJDCST @October Issue- V-1, I-6, SW-47
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Ranked Search Result Authentication on Secure Cloud Data

Jyothsna Rentapalli[1], P.Radha Krishna[2]

[1]Student, Nova College of Engineering and Technology for Women, Ibrahimpatnam,Krishna Dist, Andhra Pradesh, India

[2] Associate Professor, HOD, Nova College of Engineering and Technology for Women, Ibrahimpatnam,Krishna Dist, Andhra Pradesh, India

Abstract: Now a day's Cloud computing is the main data source for storing information. The only problem is data security. In other words more number of approaches is introduced for secured data in cloud. In previous techniques we define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Specifically, we explore the statistical measure approach, i.e. relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information. The resulting design is able to facilitate efficient server-side ranking without losing keyword privacy. Thorough analysis shows that our proposed solution enjoys "as-strong-as-possible" security guarantee compared to previous searchable encryption schemes, while correctly realizing the goal of ranked keyword search. In this we propose Authentication Schema based on ranking with each keyword search results. By using this enhanced schema we are propose the cloud server internally wants to do so for saving cost when handling large number of search requests from internal are external attacks. Using our proposed work to utilize the one way hash chain technique, this can be added directly on top of the previous RSSE design.

Index Terms: Ranked search, searchable encryption, confidential data, cloud computing, Ranked Authentication.

I. INTRODUCTION

Cloud Computing is a commercial expression used to describe the different types of computing concepts that involve a large number of computers connected through a real-life communication network. Cloud computing is a jargon term without a commonly accepted non-ambiguous scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The phrase is also, more commonly used to refer to network based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines. Several virtual servers are do not exist physically they are developed around fly with affecting the end user like a cloud. The benefits through new computing model include but are not limitation: Relief of the burden for storage management universal data access with independent geographical representation locations and avoidance of capital expenditure on hardware, software maintenances. To protect data privacy and combat unsolicited accesses in the cloud and beyond, sensitive data, e.g., emails, personal health records, photo albums, tax documents, financial transactions, etc., may have to be encrypted by data owners before outsourcing to the commercial public cloud this, however, obsoletes the traditional data utilization service based on plaintext keyword search. The trivial solution of downloading all the data and decrypting locally is clearly impractical, due to the huge amount of bandwidth cost in cloud scale systems.

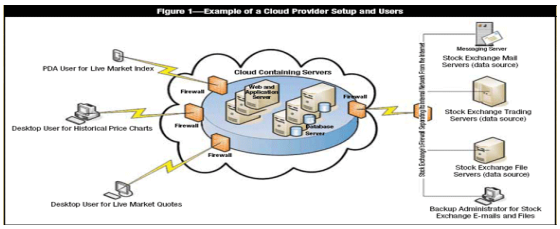

Figure 1: Authority in cloud computing process.

Considering the potentially large number of on-demand data users and huge amount of outsourced data documents in the cloud, this problem is particularly challenging as it is extremely difficult to meet also the requirements of performance, system usability and scalability. On the one hand, to meet the effective data retrieval need, the large amount of documents demand the cloud server to perform result relevance ranking, instead of returning undifferentiated results. On the other hand, to improve the search result accuracy as well as to enhance the user searching experience,
it is also necessary for such ranking system to support multiple keywords search, as single keyword search often yields far too coarse results. As a common practice indicated by today's web search engines (e.g., Google search), data users may tend to
Provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. One of the most popular ways to do so is through keyword-based search. Such keyword search technique allows users to selectively retrieve files of interest and has been widely applied in plaintext search scenarios. Unfortunately, data encryption, which restricts user's ability to perform keyword search and further demands the protection of keyword privacy, makes the traditional plaintext search methods fail for encrypted cloud data.

II. RELATED WORK

In our earlier technologies for providing security to that data stored in cloud is the main aspect in present days. For this technique we have to implement the over technologies for doing that aspect in the cloud. Earlier numbers of approaches are introduced for accessing services in the real-life applications. Traditionally searchable encryption techniques are developed for studying cryptographic primitives. They proposed schema in the symmetric key setting, in that each file is encrypted where each word was encrypted. Further enhance search efficiency Curtomola was proposed per-keyword based approach. In their construction every any one can write the public key with in server with authorized private key search process.

They choose the principle of "coordinate matching", i.e., as many matches as possible, to capture the similarity between a multi keyword search query and data documents, and later quantitatively formalize the principle by a secure inner product computation mechanism. One disadvantage of our earlier approach is that cloud server has linearly traversed the whole index of all the documents for each search request.

III. PROBLEM STATEMENT

We consider an encrypted cloud data hosting service involving three different entities.

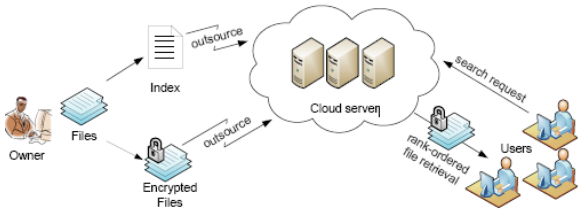

Figure 2: Encrypted Cloud data search results.

As shown in above figure Data owner has a collection of n data files C = (F1; F2; : : : ; Fn) that he wants to outsource on the cloud server in encrypted form while still keeping the capability to search through them for effective data utilization reasons.

To search the file collection for a given keyword w, an authorized user generates and submits a search request in a secret form a trapdoor Tw of the keyword w—to the cloud server. Upon receiving the search request Tw, the cloud server is responsible to search the index I and return the corresponding set of files to the user.

we have the following goals: i) Ranked keyword search: to explore different mechanisms for designing effective ranked search schemes based on the existing searchable encryption framework; ii) Security guarantee: to prevent cloud server from learning the plaintext of either the data
Files or the searched keywords, and achieve the "as strong as-possible" security strength compared to existing searchable encryption schemes; iii) Efficiency: above goals should be achieved with minimum communication and computation overhead. Due to these goals we are solving the complexity errors. We are calculating the each individual data assurance in the commercial order. In that we are finding the relevance of the data assurance in the individual aspects. a ranking function is used to calculate relevance scores of matching files to a given search request. The most widely used statistical measurement for evaluating relevance score in the information retrieval community.

IV. PROPOSED APPROACH

Compared to earlier approaches for data security in the cloud we are using searchable symmetric data encryption schemes. By using these references we describe the cloud data security efficiently but there is a problem on providing top-k searchable security on keyword based techniques. For those reasons we are introducing the efficient encryption technique for cloud data. So a better technique is need for doing above wok.

We propose Ranked searchable Encryption Scheme and Ranked Search Results Authentication Schemes. Our proposed algorithm consists of four algorithms.

1. Key Gen
2. Build Index
3. Trapdoor Gen
4. Search Index

Using these four algorithm aspects we are implementing security analysis for One-to-Many mapping applications.

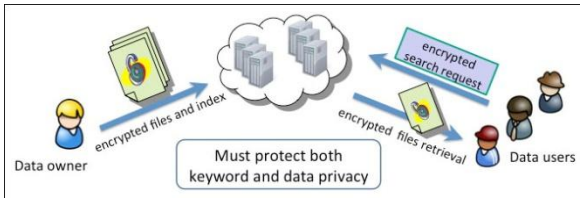

Figure 3: Cloud security issues with comparative values in cloud.

In this achievement we will find the preserving applications in symmetric order. Order-preserving mapping technique for our purpose to protect that sensitive weight information, while providing efficient ranked search functionalities.

As shown in above figure (figure 3) data owners encrypted files with index references and they must be increased in the commercial way and to protect their data in the individual assurance prospectories. Our approach also includes the efficient results in authenticate a new user details. In this achievement we are encouraging the individual keyword search process for doing protection of user's data.

V. PERFORMANCE ANALYSIS

As mentioned in the above description of our proposed work, firstly we are maintaining one-to-many mapping for preserving in the sequential order.

Algorithm 1 One-to-many Order-preserving Mapping-$\mathcal{OPM}$

procedure $\mathcal{OPM}_K(\mathcal{D}, \mathcal{R}, m, \mathrm{id}(F))$
  while $|\mathcal{D}| != 1$ **do**
    $\{\mathcal{D}, \mathcal{R}\} \leftarrow \mathrm{BinarySearch}(K, \mathcal{D}, \mathcal{R}, m)$;
  end while
  $coin \xleftarrow{R} \mathrm{TapeGen}(K, (\mathcal{D}, \mathcal{R}, 1||m, \mathrm{id}(F)))$;
  $c \xleftarrow{coin} \mathcal{R}$;
  return c;
end procedure

procedure $\mathrm{BinarySearch}(K, \mathcal{D}, \mathcal{R}, m)$;
  $M \leftarrow |\mathcal{D}|$; $N \leftarrow |\mathcal{R}|$;
  $d \leftarrow \min(\mathcal{D}) - 1$; $r \leftarrow \min(\mathcal{R}) - 1$;
  $y \leftarrow r + \lceil N/2 \rceil$;
  $coin \xleftarrow{R} \mathrm{TapeGen}(K, (\mathcal{D}, \mathcal{R}, 0||y))$;
  $x \xleftarrow{R} d + \mathrm{HYGEINV}(coin, M, N, y - r)$;
  if $m \leq x$ **then**
    $\mathcal{D} \leftarrow \{d+1, \ldots, x\}$;
    $\mathcal{R} \leftarrow \{r+1, \ldots, y\}$;
  else
    $\mathcal{D} \leftarrow \{x+1, \ldots, d+M\}$;
    $\mathcal{R} \leftarrow \{y+1, \ldots, r+N\}$;
  end if
  return $\{\mathcal{D}.\mathcal{R}\}$:

Algorithm 1: One-to-many mapping distributions.

As illustrates Following the same example of keyword "network" in Fig. 3, where max=_ = 0:06 (i.e., the max score duplicates is 60 and the average length of the posting list is 1000), one can determine the cipher text range size jRj = 246, when the relevance score domain is encoded as 128 different levels and c is set to be 1.1.

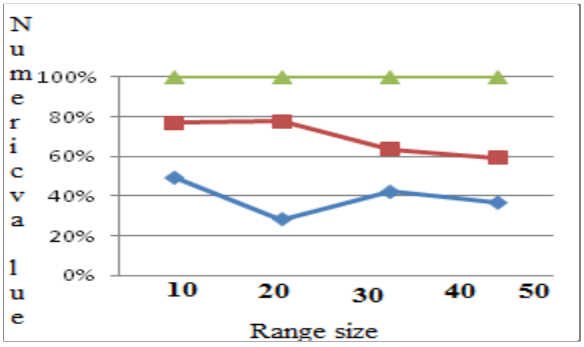

Figure 4: Representation of the search results with equivalent numerical value and range of that keyword search.

As shown in figure 4, we consider the individual range size of the object representation.

VI. CONCLUSION

In this paper, we are introducing the Ranked Search results Authentication for data retrieval from cloud in easiest way. In previous approach like searchable symmetric data encryption methods were worked for protection on cloud. In this region various applications were proposed but they are not giving the efficient results for accessing required results. Our proposed approach also includes the multi keyword search results process were developed. Further development of the cloud applications in Hash based searching is the future process for that work.

VII. REFERENCES

1)http://en.wikipedia.org/wiki/Cloud_computing.
2) Cong Wang, Ning Cao, Kui Ren," Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", Ieee Transactions On Parallel And Distributed Systems Vol.23 No.8 Year 2012.
3) Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou," Secure Ranked Keyword Search over Encrypted Cloud Data", in Proc. of ICDCS'10,2010.
4) Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou," Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data ", in Proc. of INFOCOM'11, 2011.