IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 2 (February. 2019), ||S (III) || PP 08-10

Survey on keyword search over encrypted data in cloud

Mrs.Mukku Bhagya sri, Mr.V.B.Gaikwad
(Department of Computer Science, Mumbai University, Maharashtra
(Department of Computer Science, Mumbai University,Maharashtra
Corresponding Author: Mrs.Mukku Bhagya sri

Abstract: With development of cloud computing more and more data owners are outsourcing their data form local servers to cloud. By outsourcing data to cloud, the data can be accessed from anywhere at any-time. But the main concern in outsourcing the data is about privacy of data and also data owners feel that they might not have access over data. To protect data privacy, the sensitive data is encrypted while outsourcing it. Also the users are facing issues in searching data in cloud. To overcome such problem various searchable encryption schemes are used. The encrypted data is searched by authorized cloud service providers (CSP) without learning underlying texts. Most of the existing searchable encryption support only single keyword or conjunctive keyword search. They support only exact keyword search which greatly affects data usability. Also these schemes does not support verifiability of search result. In this paper various searchable encryption schemes are surveyed.

Keywords: Cloud service provider, Encryption, Search Encryption

Date of Submission: 03-02-2019 Date of acceptance:18-02-2019

I. INTRODUCTION

Due to recent developments in cloud, the outsourcing of data by data owners has increased to reduce the burden of maintaining the big data. However the data owners do not trust the cloud while outsourcing their data. They prefer to encrypt their data before outsourcing the data to protect privacy of data. This make data utilization more difficult than the data utilization made in traditional method. The encrypted data is accessed is accessed by authorized clod service provider (CSP) without learning the underlying text.

While searching the encrypted data in cloud various searchable encryption (SE) schemes are used. To retrieve encrypted keyword, user sends a trapdoor associated with the keyword. For example, a search query on keyword “Diabetes” is sent to the cloud service provider (CSP) which selects all encrypted documents related to diabetes without learning underlying texts.

II. LITERATURE SURVEY

Rongmao Chen [1] proposed a searrchable encryption scheme. They thoroughly investigated Public Key Encryption with Keyword Search (PEKS) which useful for many applications. But the proposed traditional method can be attacked by using Keyword Guessing attack (KGA) by malicious user. To address this security problem, proposes a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). They defined a new variant of the Smooth Projective Hash Functions (SPHFs) referred to as linear and homomorphic SPHF (LH-SPHF). Then they showed a generic construction of secure DS-PEKS from LH-SPHF. To explain the feasibility of the new framework, will provide an efficient instantiation of the general framework from a DDH-based LH-SPHF and prove that it can achieve the strong security against inside KGA.

Ning Cao [2] Considered large number of data users and documents in cloud to allow multiple keyword search request and return documents in order of their relevance to their keywords. Most of searchable encryption focus on single keyword search or Boolean keyword search and they rarely sort the search results. They defined a solution to solve privacy preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). Established a set of strict privacy requirements for secure cloud data utilization system. Between different multi keyword semantics choose an efficient similarity measure of "coordinate matching" to capture relevance of data documents to search query. Also use "inner product similarity" to quantitatively evaluate similarity measure. The basic idea of MRSE is based on secure inner product computation and give improved privacy.

Zhangjie Fu [3] recently consumer centric cloud computing has developed as smart electronic devices combined with emerging cloud computing technologies. Different types of cloud services are provided to consumers with effective and efficient cloud. They want to search relevant products or data which is highly

desirable in pay-as-you use cloud computing paradigm. The sensitive data like photo albums, Emails etc are encrypted before outsourcing to cloud. Most of existing search approaches over encrypted cloud data only support fuzzy keyword search but not semantics-based multi-keyword ranked search (MRSE). They proposed an effective approach to solve problem of multi-keyword ranked search over encrypted cloud data supporting synonym queries. It support multi-keyword ranked search (MRSE) to achieve more accurate search results and synonym-based search to support synonym queries.

Jiguo Li [4], with development of cloud computing many data owners are interested in outsourcing their data and also retrieval of data when required. But the main concern is security and privacy of data stored in cloud. Attributed based encryption is used for fine grained access control which provides security to data. But the computation cost and the size of cipher text grows rapidly with increase in complexity of access control. To overcome this issue outsourced attribute based encryption (OR ABE) is proposed. But the amount of encrypted files are becoming large in cloud which arises problem for query processing. To solve above problem a new cryptographic primitive called attribute based encryption scheme with outsourcing key-issuing and outsourcing decryption which implements keyword search function (KS-OABE). It provide security against chosen plaintext attack (CPA). Also, cloud service providers (CSP) perform encrypted keyword search without knowing the underlying text.

Wenhai Sun [5], the data is outsourced from different sources and data is encrypted before outsourcing to cloud. The search over encrypted data is difficult. Man secure search encryption techniques are focussing on single contributor scenario where the encrypted data are managed by single owner based on symmetric cryptography. An efficient attributed based keyword search with efficient user revocation (ABKS-UR) which enables scalable fine-grained search authorization.

Table 1: Survey Table

Sr.No	Title of paper	Author	Methods Used
1	Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage	Rongmao Chen, Guomin Yang, Fuchun Guo	New PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS).
2	Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data	Ning Cao, Cong Wang, Ming Li	Coordinate matching to capture relevance of data documents to search query.
3	Achieving Effective Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query	Zhangjie Fu, Xingming Sun, Nigel Linge, Lu Zhou	An effective approach to solve problem of multi-keyword ranked search over encrypted cloud data supporting synonym queries.
4	KSF-OABE:Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage	Jiguo Li, Xiaonan Lin	Outsourced Attribute Based Encryption (OR- ABE) is proposed.
5	Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud	Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou, Hui Li	An efficient attributed based keyword search with efficient user revocation (ABKS-UR) which enables scalable fine-grained search authorization.

III. PROPOSEDMETHOD

With the development of cloud computing, more and more data owners are outsourcing their data. But they are concerned about the security of data. To protect the privacy of data, the data is encrypted before outsourcing the data. The main concern is searching over encrypted data.

The search encryption (SE) scheme consists a trusted trapdoor generation centre which publishes public system parameter and also keeps master key in secret. The cloud server which stores and searches encrypted data on behalf of data owners as well as multiple data owners who uploads the encrypted data to cloud and different users to retrieve data which have certain keywords. To outsource encrypted document to

cloud, a data owner appends the encrypted document with encrypted keywords and also uploads the encrypted document and also respective encrypted keywords to cloud. A trapdoor is used to obtain data.

IV. CONCLUSION

In this paper various searching techniques over encrypted data is summarized. The survey on different techniques solves the problem of search over encrypted data. All this different techniques helps in searching over encrypted data by providing privacy and security. The data is encrypted before outsourcing the data and encrypted data is searched by sending request to cloud service providers without learning the underlying text. This techniques helps in maintaining the security and privacy of data.

REFERENCES

[1]. Rongmao Chen, Guomin Yang, Fuchun Guo, "Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage".
[2]. Ning Cao, Cong Wang, Ming Li, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data".
[3]. Zhangjie Fu, Xingming Sun, Nigel Linge, Lu Zhou, "Achieving Effective Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query"
[4]. Jiguo Li, Xiaonan Lin, "KSF-OABE:Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage".
[5]. Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou, Hui Li, "Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud".
[6]. O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams.
[7]. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data".
[8]. Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system".
[9]. B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search".
[10]. Z. Lv, C. Hong, M. Zhang, and D. Feng, "Expressive and secure searchable encryption in the public key setting".

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Mrs.Mukku Bhagya sri. "Survey on keyword search over encrypted data in cloud." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 02, 2019, pp. 08-10.