A Survey on Security in Encryption based Cloud Data Search

M.Haritha[1] Mr.C.Thirumalai Selvan[2] Dr. V.Venkatachalam[3]
[1,2,3]Department of Computer Science & Engineering
[1,2]K.S.R College of Engineering, Tamilnadu, India [3]The kavery Engineering College, Tamilnadu, India

Abstract— Cloud computing is the internet based service where the services are provided to the users on remote servers. The advantage of cloud computing is to store and create data on cloud servers. But the cloud storage contains drawback of privacy vulnerabilities and data securities. Hence there is many number of techniques to control these issues. In this paper a survey on several techniques such as order preserving encryption (OPE), privacy preserved index (PPI), searchable encryption (SE), identity based encryption (IBE), multi-keyword ranked search over encryption (MRSE), searchable attribute based encryption (SABE), fuzzy keyword search and privacy preserving semantic search are the techniques we surveyed for security in cloud.

Key words: Encryption, Cloud Data Search, Security

I. INTRODUCTION

Cloud computing is a large group of computers connected via internet. In cloud server users data are usually accessed directly in all machines using web services. Cloud services are provided in users request basis and operate on increased flexibility, reliability and scalability at low cost for business users and individuals alike.

Cloud computing provides always enabled convenient demand on network access on a shared pool of computing environment. This can be accessed with the existing and new technologies. These technologies get into serious problems that reduces the trust between the client and the provider in all computer systems.

In cloud computing sensitive data values are protected and shared in encrypted form. Data encryption is carried out before outsourced to a commercial public cloud. And user privacy is ensured with encrypted search methods in cloud data centers. The cloud can be of private, public or hybrid cloud. Public cloud can be mutual by various enterprises. Private cloud data is mutual by particular enterprises and it is expensive and secured when compared to public cloud. Public cloud is a combination of both public and private cloud hence it is a critical application may host by enterprises. Hybrid cloud is less secure.

A. Secured Data Search

Secured data search is a control based technologies and policies and designed to adhere the regulatory compliance rules and protect the information. Cloud computing security process should address the security controls will incorporate to maintain the customers data security, privacy and compliance with necessary regulations.

B. Privacy

Involves the handling and protection of sensitive personal information that individuals provide in the course of every day transactions. The providers should kept their privacy data in protected manner this helps the authorizers to access the data in its entity.

C. Keyword Search

Keyword search is a type of search that looks for matching documents in the server that contains one or more words specified by the user.

II. TECHNIQUES

A. Order Preserving Encryption (OPE)

OPE [1] is used to preserve the cipher text whose the natural ordering of plain text and allow the efficient range of query processing over outsourced encrypted data without giving decryption to encrypted keys.OPE is apparently, a method of encrypting data so that it is possible to make efficient of quality of comparisons on encrypted data items without decrypting them.

OPE supports the fast ranked search in a practical way. It is used to solve encrypted query problems in a database. And also it is used to encrypt the relevance score of inverted index .OPE has the direct access with the keywords randomly and flatterns the distribution.

B. Privacy Presrved Index (PPI)

Data sharing is an emerging data transmission technique in cloud server which has the potential to transform the IT operations of corporations. We can able to find privacy threats in data in server by outsourcing trust in the service provider is limited. Specifically, we examine the data split up technique [2] to build privacy-preserving index on perceptive attribute of a relational table. Such index enables an untreated server to evaluate range queries with minimal information leakage. We analyze the worst-case scenario of assumption attacks that can potentially lead to violate of privacy and find size of data sedution in the framework of these attacks [7].

C. Searchable Attribute based Encryption

Searchable Attribute-Based Encryption (SABE) is a type public key encryption [6] in which privacy key and the ciphertext are reliant upon attributes. The decryption of a secret message is possible only if the set of attributes of the user key coincide the attributes of the ciphertext key.

A security feature of Searchable Attribute-Based Encryption in participant conflict: An challenger that can holds several keys should only control data at small key access individually.

Searchable attribute-based encryption (SABE) can be used for record encryption. Instead of encrypting each part of a records, it is possible to encrypt the record only with attributes which is used to reduce the key usage. This early also it can be used for relay encryption to reduce the usage of number of keys.

D. Searchable Encryption

Searchable encryption [1] is an encryption technology for searching data in an encrypted state. This type of encryption is only done in the server machine. Although various

methods for searchable encryption have been used, schemes that use data-retrieval indexes and tags to determine whether data correspond to the server have been widely adopted.

Searchable encryption is to store only encrypted data on the server and to encrypt and decrypt them by client machines. Since it can handle not only retrieval-target data but also search keywords in an encrypted state, searchable encryption [3] is gaining considerable attention as a useful technology for safe and secure utilization of data on the cloud. Hence it can also be accessed with the query processing.

E. Fuzzy Keyword Search

In fuzzy keyword search, large number of privacy information are being found in the middle of the cloud server. For the protection of privacy data, privacy data usually have to be encrypted before retrival, which makes effective data development a very challenging mission. Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and countably retrieve files of own concentration, these techniques support only exact keyword search. Fuzzy keyword search [1] is adopted only for traditional search patterns to outsource the files. That is, there is no acceptance of small types and format inconsistencies which, on the other hand, are distinctive user searching concept and happen very frequently. This conditional drawback makes unfit in Cloud Computing as it greatly affects system usability, representation user searching experiences very annoying and system efficiency very small. Fuzzy keyword search [11] pattern improves system usage by returning the relationship of matching files. when users searching request exactly match the unknown keywords or the closest possible matching documents based on keyword similarity semantics, when similarity match deviates the keyword similarity during the document search.

F. Multi Keyword Ranked Search over Encryption

Multi-keyword ranked search(MRSE) [3] is applied for searchable encryption techniques in order to retrieve the data stored in the cloud server. The effective data retrieval of data need the large amount of documents in the cloud server to perform search on relevance score based ranking. Such ranked search system enables data users to find the most relevant information quickly, rather than large amount of sorting through every match in the content collection. Ranked search can also methodologically eliminate unnecessary network traffic by sending back only the most relevant data, which is highly desirable in the "pay-as-you-use" cloud service. For security protection, this kind of ranking operation should not leak any keyword related information. On the other hand, to improve the retrieval of search result accuracy as well as to improve the user searching experience, it is necessary for ranking system to support multiple keywords search results. The security system demonstrates the data confidentiality and concealing the patterns of the each search user.

Each keyword in the search request is able to help narrow down the search for Coordinate matching, as many as possible, is an efficient dependent measure among such multi-keyword semantics to provide the result relevance, and has been widely used in the plaintext information retrieval (IR) community. It improves the efficiency in access patterns [7] [10].

Boolean keyword search as an attempt to improve the search flexibility, they are still not adequate to provide users with acceptable result ranking functionality.

G. Privacy Preserved Semantic Search

Privacy preserved semantic search [10] is for protecting sensitive information. It has to be encrypted before outsourcing to the cloud. This search finds the exact match between the encrypted document during search and retrieval. Thus the effective data consumption becomes a very useful challenge which strengthens the data stored in the cloud server. Searchable encryption scheme has been developed to control retrieval over encrypted data. However, these schemes only support exact keyword search. In this scheme building up of semantic tree will choose similar keywords for data retrieval having some data qualifications with satisfactions. Thus the keyword based semantic search scheme supports the verification of correctness and completeness of data in the result. Hence it is a difficult search for ordinary consumers.

Privacy preserved semantic search [8] focuses on realizing secure semantic search through query keyword semantic extension to retrieve the encrypted. Based on the co-occurrence probability of terms, the semantic relationship library is constructed to record the semantic similarity between keywords.

H. Identity Based Encryption

Identity-based encryption (IBE), is an alternative public key encryption which is used for key simplification. It is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user [5].

Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys . It can be operated with human intelligible identities. One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. It can directly encrypts and decrypts the documents with both sender and receiver identity correspondingly. If a Private Key Generator (PKG) is compromised, all messages protected over the complete lifetime of the public-private key pair used by that server are also compromised. Accordingly it corresponds to private key associated with the private key generator(PKG) for the distribution of cipher text. This makes the PKG a high value target to adversaries. To limit the exposure due to a compromised server, the master private-public key pair could be updated with a new independent key pair. However, this introduces a key-management problem where all users must have the most recent public key for the server.

SCHEME	APPROACH	STRENGTH	LIMITATIONS
Order Preserving Encryption(OPE)	It is a symmetric encryption scheme whose encryption	Allow efficient range of query processing over outsourced	The security in case of symmetric encryption cannot

	algorithm produces cipher text that preserves the numerical ordering.	encrypted data without giving encryption to decryption keys for preserving natural order plain text.	be able to identify the exact difference in high priority.
Privacy Preserve Index (PPI)	Privacy Preserved Index (PPI) model based multi keyword search system is used to fetch documents in distributed environment.	It protects the privacy data through indexing towards data privacy against vulnerabilities.	Attack based semantic search model with indexing are not handle while data outsourcing.
Searchable Encryption (SE)	It is used to store encrypted data on the server and to encrypt and decrypt the document only by the client machines.	Searchable encryption, relevance score and *k-nearest* neighbor techniques integrated to perform privacy preserved ranked search process.	Data authendication and access control cannot maintained with security and privacy in rank search process.
Identity Based Encryption (IBE)	Secure cloud data services are composed with Identity Based Encryption (IBE) schemes. It is an important primitive of ID-based cryptography.	Revocable IBE scheme with outsourced revocation mechanism is used to secure shared data under clouds.	IBE solution may relay on cryptographic techniques that are insecure against code breaking quantum computing attacks.
Multi-keyword Ranked Search over Encryption (MRSE)	Encrypted cloud data search service supports privacy ensured multi keyword based document search.	Inner product similarity based multi-keyword ranked search over encrypted data in cloud computing (MRSE) scheme is used for the search process. It establish set of privacy requirements for secure cloud data utilization.	Attacks are not controlled in any of change point analysis methods over encryption.
Searchabe Attribute Based Encryption (SABE)	The system enables data owners to efficiently share their data to a specified group of users with a sharing policy.	Searchable attribute based proxy re-encryption scheme is used to perform keyword based data search with privacy and security.	Encrypted data index process is not supported while retrieving data during outsource.
Fuzzy Keyword Search	Fuzzy Keyword Search is used for the protection of privacy data have to be encrypted before retrival. Search pattern is done with the keywords.	Synonym based multi-keyword ranked search scheme is applied to share and search encrypted documents in traditional search patterns. Semantic relationship is established only for retrieving plain text.	Data leakages are not controlled while outsourcing a document in high range of transmission.
Privacy Preserved semantic search	The system supports product and service search using keyword based semantic search model. It verifies the keywords before using it for data retrieval.	The Verifiable Keyword-based Semantic Search Scheme improves the search results reordering process.	System supports only exact keyword search which greatly affects data usability. Semantic relationship analysis is not optimized.

Table 1: Comparative Analysis.

III. CONCLUSION

This paper consist of several cloud data search encryption technique for secure allocation of data in cloud server. From this survey we understand that some amount of work has been done in the field of cloud computing for several security issues. It can be applied to achieve scalable, flexible, security, privacy, and improved relavency of data in cloud computing. The study concludes that the order preserving encryption(OPE) is the advanced encryption technique for data in the cloud server. On the other hand the techniques and strategies of encryption in cloud computing have to be improved with its distinct characteristics in mind. In order to achieve ra There is more span for future research in the field of secure encryption based data sharing in the cloud.

REFERENCE

[1] Ke Li, Weiming Zhang, Ce Yang and Nenghai Yu, "Security Analysis on One-to-Many Order Preserving Encryption-Based Cloud Data Search", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 9, September 2015.
[2] Yuzhe Tang and Ling Liu, "Privacy-Preserving Multi Keyword Search in Information Networks", IEEE Transactions On Knowledge And Data Engineering, Vol. 27, No. 9, September 2015.
[3] Hongwei Li, Dongxiao Liu ,Yuanshun Dai , Tom H. Luan and Xuemin Shen,"Enabling Efficient Multi Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", IEEE Transactions On Computers 6 March, 2015.

[4] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu and Jianying Zhou , "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", IEEE Transactions On Computers, Vol. 64, No. 4, April 2015.
[5] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing", IEEE Transactions On Computers, Vol. 64, No. 2, February 2015.
[6] Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 9, September 2015.
[7] Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, January 2014.
[8] Zhangjie Fu, Jiangang Shu, Xingming Sun and Nigel Linge , "Smart Cloud Search Services: Verifiable Keyword-based Semantic Search over Encrypted Cloud Data", IEEE Transactions on Consumer Electronics, Vol. 60, No. 4, November 2014.
[9] Qiang Tang, "Nothing is for Free: Security in Searching Shared and Encrypted Data", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 11, November 2014.
[10] Bing Wang,Ning Cao,Ming Li, Wenjing Lou, Y. Thomas Hou and Hui Li, "Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 11, November 2014
[11] Zhangjie Fu, Xingming Sun, Nigel Linge, Lu Zhou, "Achieving Effective Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query", IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, February 2014.

