A Detailed Survey on Searchable Encryption and Revocation Schemes in the Mobile Cloud storage

U.K.Gopalakrishnan[1], G.Maheswari[2]
Department of Computer Science
[1] M.Phil Research Scholar, Sree Narayana Guru College of Arts and Science Coimbatore, Tamilnadu, India
[2] Assistant Professor, Sree Narayana Guru College of Arts and Science Coimbatore, Tamilnadu, India

Abstract- *On large exploration of mobile networks, mobile terminals is becoming as an important application platform. Due to growing user demand for data storage and processing on the mobile platform makes mobile cloud storage service more important. Utilization of those services will enable the user to outsource their data to the cloud server through mobile network. Despite of more advantageous, there exist some limitation which leads to concern in terms of data privacy and confidentiality to outsourced data. To mitigate those challenges, many state of art approaches has been proposed in terms of privacy preserving schemes to outsourced data. In this paper, a detailed survey has been carried on searchable encryption model and revocation scheme which acts as privacy preserving models.*

The analysed model addresses the privacy and integrity on sensitive data before outsourcing. In addition Attribute based Encryption scheme envisioned as cryptographic primitive to protect the data security and realize fine-grained access control in one-to much communications.ABE mechanism enables the operations like key issue, data encryption and decryption to be performed on the basis of attributes. With the deepening research on ABE, more and more attention has been paid to the revocation mechanism for user's attributes can be changed dynamically in practice. Searchable encryption is a technology that allows a semi-trusted server to provide retrieval service on encrypted data with search trapdoor of keyword provided by a user, while the server knows nothing about the search keyword. These analysis provides an outline to model an efficiently revocable and searchable attribute-based encryption scheme for mobile cloud storage to simultaneously supports efficient attribute revocation, attribute grant and keyword search.

Keywords- Privacy Preserving, Searchable Encryption, User Revocation, Outsourced Data, Attribute Based Encryption

I. INTRODUCTION

Nowadays, Mobile phone is exploring in large extent which leads to on demand network access through mobile networks. In addition, these exploration leads to more data growing which makes storage and processing more challenges. In order to avoid those challenges, mobile cloud platform has becoming solution to alleviate those complexities. The Mobile Cloud Computing provides user to outsource their data and provides effective access from anywhere. Despite of those benefits, security stands major bottleneck of those services[1].

For the protection of data privacy and control, data is usually encrypted before outsourcing, which makes its effective utilization. In particular, indexing and searching the outsourced encrypted data becomes problematic. Searchable encryption (SE) allows searching over encrypted data in the cloud and returns to the user the data that correspond to the given keywords, without having to reveal the keywords. It is thus a critical enabler for securing outsourced data.

Traditional searchable encryption [2] schemes allow a user to securely search over encrypted data through keywords but only support exact keyword matching, which is not a practical requirement for current mobile phone input methods and Boolean search without capturing the relevance of data files. An efficiently revocable and searchable attribute-based encryption scheme for mobile cloud storage which simultaneously supports efficient attribute revocation[3], attribute grant and keyword search[4] in mobile cloud environment has been considered as base model by more researchers.

The rest of the paper is organized as section 2 details the literature along its advantageous of the analysed model in terms of efficient searchable encryption model and revocation scheme in parallel. Section 3 describes the outline of the proposed model to overcome challenges experienced in the literatures and finally section 4 is concluded.

II. REVIEW OF LITERATURES

In this section, security challenges of the outsourcing data from mobile environment to cloud is considered in detail. The detailed analysis is carried out in various sections as analysis of attribute based encryption mechanism of keyword search on encrypted data, automated user revocation models.

2.1 Multi-Authority Attribute-Based Encryption Scheme with Attribute Hierarchy

In this analysis, Attribute based encryption with attribute hierarchy program has been considered with one authority which causes severe impact in the outsourced data by data owner. In order to solve the problem in hierarchical attribute based encryption has been formulated, a multi-authority hierarchical attribute based encryption scheme has been considered. The scheme removes the trusted central authority, and prevents the communication between authorities, thereby ensuring the users' privacy and improving the system performance through generation of access policies and access constraints for each user group [5].

2.2 A Multi-User Searchable Encryption Scheme with File-Centric Multi-Key Aggregate Keyword

It provides Secure and searchable encryption scheme with provable security strength and efficiency. Multi-User Searchable Encryption Scheme with File-Centric Multi-Key Aggregate Keyword provides securely searching on multiple indexes and sharing encrypted data between multiple users[6]. A token-adjustment search scheme to preserve the search functionality among multi-indexes, and a key sharing scheme which combines identity-based encryption and public-key encryption is also been included.

2.3 Energy-Efficient Fault-Tolerant Data Storage and Processing in Mobile Cloud

Despite the advances in hardware for hand-held mobile devices, resource-intensive applications still remain off bounds since they require large computation and storage capabilities for processing in mobile environment. However, challenges of reliability and energy efficiency remain largely unaddressed in this context. It has been addressed in an integrated manner for both data storage and processing in mobile cloud as an approach named as k-out-of-n computing. In this solution, mobile devices successfully retrieve or process data in the cloud in the most energy-efficient way, as long as k out of n remote servers is accessible. Through system implementation the feasibility of approach has been proved [7].

2.4 Chaotic Searchable Encryption for Mobile Cloud Storage

The security problem of outsourcing storage from user devices to the cloud is been enabled through secure searchable encryption scheme which is presented for searching of encrypted user data in the cloud. The scheme simultaneously supports fuzzy keyword searching and matched results ranking, which are two important factors in facilitating practical searchable encryption. A chaotic fuzzy transformation method is proposed to support secure fuzzy keyword indexing, storage and query. A secure posting list is also created to rank the matched results while maintaining the privacy and confidentiality of the user data, and saving the resources of the user mobile devices [8].

III. OUTLINE OF THE PROPOSED MODEL

The secure sharing of the data and encrypted search on the encrypted outsourced data is a formidable task. Hence novel model entitled as Data Centric Revocation Constrainst and Searchable encryption for outsourced data using proxy reencryption has been outlined as proposed model to provide automated attribute revocation on the delegating the update of secret key and ciphertext and keyword search on encrypted data is carried out with support of keywords index and search trapdoor respectively without relying on trusted authority.

IV. CONCLUSION

A detailed analysis on Searchable Encryption and Revocation Schemes in the Mobile Cloud storage has been carried. It provides the Security and confidentiality solution for mobile cloud computing. The privacy and integrity on sensitive data is carried out on Attribute based Encryption scheme which acts cryptographic primitive to protect the data security and realize fine-grained access control. In addition, Searchable encryption and revocation mechanism has been formulated as single model named as Data Centric Revocation Constrainst and Searchable encryption for outsourced data using proxy reencryption to provide flexibility and reliability on the outsourced data in the cloud.

REFERENCES

[1] N. Fernando, S. W. Loke, and W. Rahayu, “Mobile cloud computing: A survey,” Future eneration Computer Systems, vol. 29, no. 1, pp. 84–106, 2013.

[2] J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, July 2011.

[3] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187–1198, April 2016.

[4] X. Xie, H. Ma, J. Li, and X. Chen, “New ciphertext-policy attribute-based access control with efficient revocation,” in Information and Communication Technology, K. Mustofa,

E. J. Neuhold, A. M. Tjoa, E. Weippl, and I. You, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 373–382.

[5] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 785–796, Sept 2017.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan 2014.

[7] J. Bringer, H. Chabanne, "Embedding edit distance to enable private keyword search," Secure and Trust Computing, Data Management and Applications, Communications in Computer and Information Science, vol. 186, no. 1, pp. 105-113, 2011

[8] R. Li, Z. Xu, W. Kang, K. Choong Yow, C. Z. Xu, "Efficient multikeyword ranked query over encrypted data in cloud computing," Elsevier, Future Generation Computer Systems, vol. 30, pp. 179– 190, 2014.