IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Keyword Search on Confidential Data in A Cloud Environment

M. Prasanna Lakshmi[1*], V. Esther Jyothi[2], M. Venkata Rao[3]

[1,2]Dept. of Computer Applications, V.R. Siddhartha Engineering College, Vijayawada, India
[3]Department of Mathematics, V.R. Siddhartha Engineering College, Vijayawada India

**Corresponding Author: mundlamuri70@gmail.com, Tel.: +919491753743*

DOI: https://doi.org/10.26438/ijcse/v7i4.336338 | Available online at: www.ijcseonline.org

Accepted: 10/Apr/2019, Published: 30/Apr/2019

Abstract— Keyword search on confidential data in a cloud environment is the main focus of this research. The cloud providers are not fully trusted. So, it is necessary to outsource data in the encrypted form. In the attribute-based keyword search schemes, the authorized users can generate some search tokens and send them to the cloud for running the search operation. A new cryptographic primitive called key-policy attribute-based temporary keyword search provides this property. To evaluate the security of our scheme, we formally prove that our proposed scheme achieves the keyword secrecy property and is secure against selectively chosen keyword attack both in the random oracle model and under the hardness of Decisional Bilinear Diffie-Hellman assumption.

Keywords—*Cipher text, Token, Encrypted form, leakage information, Temporary keyword*

I. Introduction

We propose a novel notion of Key-Policy Attribute-Based Temporary Keyword Search (KP- ABTKS). In KP-ABTKS schemes, the data owner generates a searchable cipher text related to a keyword and the time of encrypting according to an intended access control policy, and outsources it to the cloud. After that, each authorized data user selects an arbitrary time interval and generates a search token for the intended keyword to find the cipher text [1]. Then, he/she sends the generated token to the cloud to run the search operation. By receiving the token, the cloud looks for the documents contain the intended keyword. The search result on a cipher text is positive.

Section I contains the introduction of Keyword Search on Confidential Data in A Cloud Environment, Section II explains the related work of Attribute-Based Encryption (ABE), Section III explains the methodologies of keyword search, Section VI concludes research work.

II. Related Work

To the best of our knowledge, no existing solution is adequate for what we want to achieve. In what follows we briefly review the relevant techniques.

Attribute-Based Encryption (ABE): ABE is a popular method for enforcing access control policies via cryptographic means. Basically, this technique allows entities with proper credentials to decrypt a cipher text that was encrypted according to an access control policy. Depending on how the access control policy is enforced, there are two variants: KP-ABE (key-policy ABE) where the decryption key is associated to the access control policy [2], and CP-ABE (cipher text- policy ABE) where the cipher text is associated to the access control policy [3]. ABE has been enriched with various features In this paper, we use ABE to construct a new primitive called attribute-based keyword search (ABKS), by which keywords are encrypted according to an access control policy and data users with proper cryptographic credentials can generate tokens that can be used to search over the outsourced encrypted data. This effectively prevents a data owner from knowing the keywords a data user is searching for, while requiring no interactions between the data users and the data owners/trusted authorities. This is in contrast to where the data users interact with the data owners/trusted authorities to obtain search tokens.

Keyword Search over Encrypted Data: This technique allows a data owner to generate some tokens that can be used by a data user to search over the data owner’s encrypted data. Existing solutions for keyword search over encrypted data can be classified into two categories: searchable encryption in the symmetric-key setting and searchable encryption in the public-key setting have been proposed to support complex search operations. Moreover, searchable encryption in the multi-users setting has been investigated as well where the data owner can enforce an access control policy by distributing some (stateful) secret keys to the authorized users [4]. However, all these solutions do not solve the problem we study, because (i) some of these solutions require interactions between the data users and the data owners (or a trusted proxy, such as a trapdoor generation entity to grant search capabilities, and (ii) all these solutions assume that the server faithfully executed search operations. In contrast, our solution allows a data user with proper credentials to issue search tokens by which the cloud can perform keyword search operations on behalf of the user, without requiring any interaction with the data owner. Moreover, the data user can verify whether or not the cloud has faithfully executed the keyword search operations. This is true even for the powerful technique called predicate encryption which does not offer the desired variability.

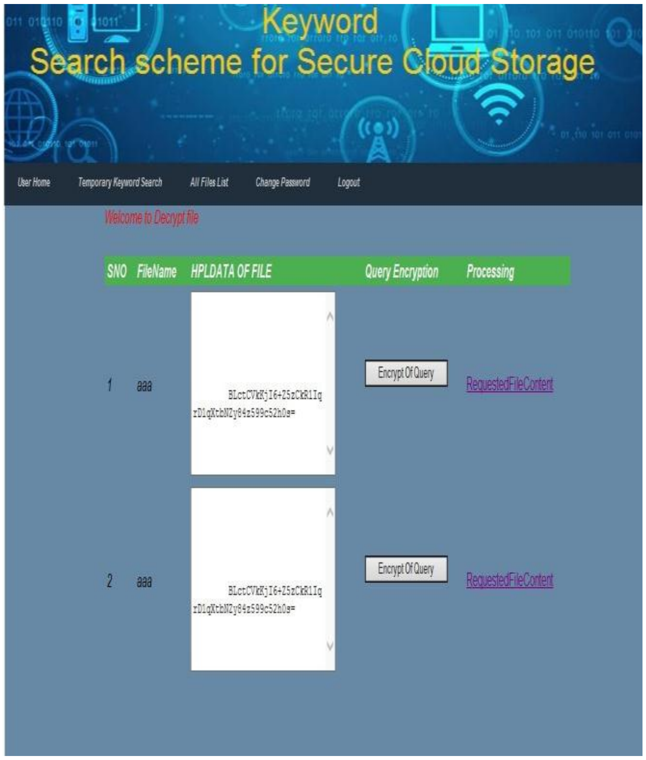
III. Methodology

Verifiable Keyword Search Over Out Sourced Encrypted Data: We propose a novel cryptographic primitive, called verifiable attribute-based keyword search (VABKS). This primitive allows a data owner to control the search, and use of, its outsourced encrypted data according to an access control policy, while allowing the legitimate data users to outsource the (often costly) search operations to the cloud and verify whether or not the cloud has faithfully executed the search operations [5]. In other words, a data user with proper credentials (corresponding to a data owner's access control policy) can (i) search over the data owner's outsourced encrypted data, (ii) outsource the search operations to the cloud, and (iii) verify whether or not the cloud has faithfully executed the search operations. We formally define the security properties of VABKS and present a scheme that provably satisfies them. The scheme is constructed in a modular fashion, by using attribute-based encryption, bloom filter, digital signature, and a new building-block we call attribute-based keyword search (ABKS) that may be of independent value.

Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extension: Limited PEKS schemes. Boneh et. al. also present a couple of PEKS schemes that are what they call limited [6][7]. In the first scheme, the public key has size polynomial in the number of keywords that can be used. In the second scheme, the key and ciphertext have size polynomial in the number of trapdoors that can be securely issued to the gateway. Although these schemes are not very interesting due to their limited nature, one could ask about their consistency. We extend our definitions of consistency to this limited setting and then show that the first scheme is statistically consistent while the second scheme is computationally consistent and statistically consistent under some conditions. Goh and Golle, Staddon, and Waters define consistency conditions analogous to BDOP's "perfect consistency" condition, but none of the constructions in satisfy their respective perfect consistency condition.

Each user is identified with an access control policy. The data owner selects an attribute set, and runs the encryption algorithm with regard to it. If a data user's attributes set satisfies the access tree of the data owner, then he/she can generate a valid search token[8][9]. The cloud applies the generated search token to find the corresponding cipher texts which have been encrypted in a time interval specified by the data user.

Data owner: Is an entity who encrypts its documents under an arbitrary access control policy and outsources them to the cloud. He/She considers the time of encrypting in generating the cipher texts. We should highlight that the data owner also encrypts his/her documents under his/her arbitrary access control policy. However, in this paper we concentrate on the encryption of the extracted keywords (file names) from documents.



Welcome to Decrypt file

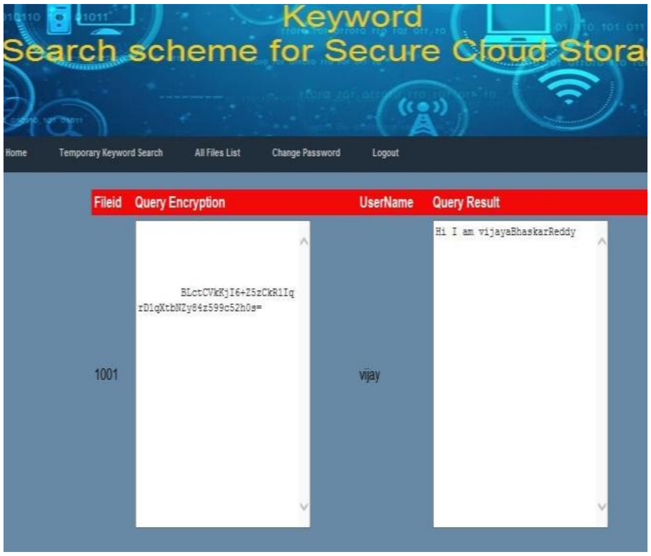
SNO	FileName	HPLDATA OF FILE	Query Encryption	Processing
1	aaa	BLctCVkKjI6+Z5zCkR1Iq rD1qXtbNZy84z599c52h0s=	Encrypt Of Query	RequestedFileContent
2	aaa	BLctCVkKjI6+Z5zCkR1Iq rD1qXtbNZy84z599c52h0s=	Encrypt Of Query	RequestedFileContent

Figure 1.Decrypting a file.

Data user: Is an entity that is looking for documents which contains an intended keyword, and is encrypted in a determined time interval. The time interval is arbitrarily selected by the data user.

Cloud Server (CS): Is an entity with powerful computation and storage resources. CS stores a massive amount of encrypted data, and receives the search tokens to look for the required documents on behalf of the data user. The cloud finds the relevant documents, and sends them back to the data user.

Trusted Third Party (TTP): Is a fully trusted entity that receives each user's access tree, and generates their secret keys corresponding to his/her attributes set presented in his/her access tree. Then, the TTP sends back the users' credentials through a secure and authenticated channel.



Fileid	Query Encryption	UserName	Query Result
1001	BLctCVkKjI6+Z5zCkR1Iq rD1qXtbNZy84z599c52h0s=	vijay	Hi I am vijayaBhaskarReddy

Figure 2.Ecrypting a file.

IV. CONCLUSION AND FUTURE SCOPE

Today's IT world is showing interest towards the Cloud Technology due to their huge Advantages when compared with other technologies and the only drawback of cloud technology is security. Our Web Application Overcomes that drawback by securing the information which is stored on cloud through Encryption and Decryption Process using the mentioned methodologies.

REFERENCES

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.

[2] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: Verifiable attribute-based keyword search over outsourced encrypted data," in INFOCOM, 2014 Proceedings IEEE. IEEE, 2014, pp. 522–530.

[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology– EUROCRYPT 2005. Springer, 2005, pp. 457–473.

[4] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and exten- sions," in Advances in Cryptology– CRYPTO 2005. Springer, 2005, pp. 205–222.

[5] X. Boyen and B. Waters, "Anonymous hierarchical identity-based en- cryption (without random oracles)," in Annual International Cryptology Conference. Springer, 2006, pp. 290–307.

[6] Y. Yu, J. Ni, H. Yang, Y. Mu, and W. Susilo, "Efficient public key encryption with revocable keyword search," Security and Communication Networks, vol. 7, no. 2, pp. 466–472, 2014.

[7] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2706–2716, 2016.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi- keyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, pp. 222–233, 2014.

[9] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, 2016.