International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Attribute Base Keyword Search Is Confirmable Over the Outsource Encrypted Data

Amruta N. Deshmukh[1], Komal B. Bijwe[2]

[1]M.E. Istyear (CSE), P. R. Pote COE&M, Amravati, India
[2]Assistant Professor, P. R. Pote COE&M, Amravati, India

Abstract: ***In this world all data proprietor can outsource their data to the cloud. But cloud cannot faith on the outsource data that data should be encrypted. Because of that all, the lots of problem can be occur. Such as, how can the authorized data users search over a data owner's outsourced. How can the data users be assured that the capabilities to the data users? Solve these all question we propose the cryptographic solution called as Attribute base keyword search is more realistic over the outsource encrypted data. There is a need to allow the data users to verify whether the cloud faithfully executed the search operations or not. To the best of our knowledge, existing solutions cannot achieve these objectives simultaneously. As for all that problems. We the applicability of our construction to sharing of audit-log information and broadcast encryption. We verify whether the cloud can perform the appropriate search operation or not, and check that data owner's outsources search over the encrypted data.***

Keyword: Attribute-based encryption, Bilinear map, Encryption, keyword search over encrypted data.

1. Introduction

Cloud computing platforms assemble vast Computation all resources and make them available to users as a service. The cloud users can outsource their heavy computation tasks and/or storage to cloud providers while still enjoying promising properties, e.g., low maintenance cost and pervasive accessing. While it is promising, cloud computing also confronts many challenges against data privacy/system vulnerabilities and service quality [2]. There is a need to allow the data users to verify whether the cloud faithfully executed the search operations or not. To the best of our knowledge, existing solutions cannot achieve these objectives simultaneously. [1] To explain the motivation for solving the above questions, we consider the following Motivational application: The data owner, says Alice, encrypted her personal health data that was collected by sensors attached her and outsourced the encrypted data to the cloud. In order to facilitate the examination on health condition, Alice may need to share the encrypted data with professionals, e.g. doctors that work in some specific department, so that the professionals can retrieve qualified Records from the cloud. In order to assure that only certain professionals satisfying some policy can conduct keyword search and retrieve corresponding encrypted data of their interests, Alice needs to delegate keyword search capability by specifying the fine-grained access control policy. One method for alleviating some of these problems is to store data in encrypted form. Thus, if the storage is compromised the amount of information loss will be limited. One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data at a fine-grained level. We introduced the as Attribute base keyword search is more realistic over the outsource encrypted data. This is cryptographic solution for this all problem. This allows a data owner to delegate keyword search capability over his encrypted data to authorized users by while complying with access control policies. We formally define its syntax and rigorously formalize the security definitions.[2]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 [1].

2. Related Work

Attribute base encryption- Attribute-based encryption (ABE) was first introduced by, which is to specify fine-grained access control on encrypted data, such that only data users with proper credentials (i.e., satisfying the access control policy) can decrypt the cipher texts. There are two flavors of ABE depending on the manner of associating access control policy: key-policy ABE (KP-ABE).[2] While ABE allows data owners to achieve fine-grained access control enforcement on encrypted data, unfortunately it cannot support keyword search.[1] 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 . 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 [1].

3. Keyword Search over 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. Several variants 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 user.[1]The concept of attribute-based encryption with keyword search (ABKS) was introduced by and independently. It allows data owner to grant search capability to authorized users by specifying fine-grained access control when encrypting plaintext. However, it does not support the data owner delegating search capability to authorized users when encrypted data were stored in the cloud [2].

Licensed Under Creative Commons Attribution CC BY

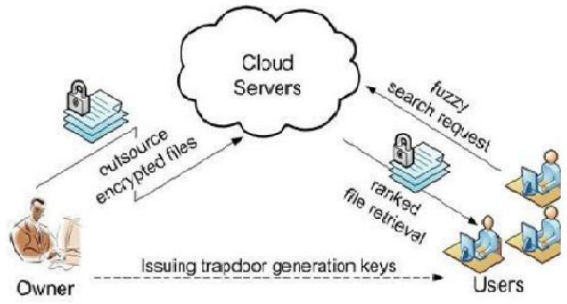

Figure1: Searchable Encryption [4]

4. Bilinear Maps

We present a few facts related to groups with efficiently computable bilinear maps.

Let G1 and G2 be two multiplicative cyclic groups of prime order p.
Let g be a generator of G1 and e be a bilinear map, e :G1 × G1 → G2. The bilinear map e has the following properties:
1. Bilinearity: for all u, v ∈G1 and a, b ∈Zp, we have e(ua, vb) = e(u, v)ab
2. Non-degeneracy: e(g, g) = 1.[3]

5. Security Definitions

The security of ABKS requires that the cipher texts and tokens leak nothing about the underlying keywords. Informally, the adversary is allowed to query cipher text of any plaintext and tokens except those corresponding to two keywords in the challenge phase. We expect that the adversary cannot distinguish the challenge cipher text that is generated from one of keywords kw0 and kw1. To formalize aforementioned security notion, we define the selective chosen keyword security game as follows. Note that in our corruption model, the adversary is not allowed to get the re-encryption key from uncorrupted users to corrupted users. Note that in our security model we consider the static corrupted model in the sense that the set of corrupted users has to be selected in the setup phase

6. System Model

A data owner (say Alice) encrypts her data and the keyword index and outsource the encrypted data and the associated encrypted keyword index to the cloud server. Moreover, the data owner can retrieve encrypted data of her interest by issuing a search token with respect to some keyword to the cloud. The data owners are naturally trusted. Both authorized and unauthorized data users are semi-trusted, meaning that they may try to infer some sensitive information of interest. The cloud is not trusted as it may manipulate the search operations, which already implies that the cloud may manipulate the outsourced encrypted data.

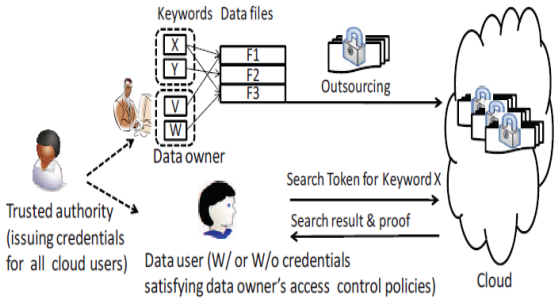

Figure 2: System model, where keywords X, Y and V, W may correspond to different access control policies.[1]

7. Construction

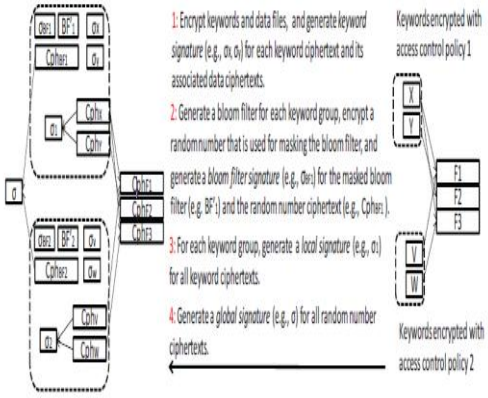

Figure 3: Basic idea for achieving verifiability, where data files F1, F2, F3 were encrypted to cphF1, cphF2, cphF3 , keywords X, Y were encrypted to cphX, cphY with access control policy 1, and keywords V,W were encrypted to cphV, cphW with access control policy 2. Given a search token tk, for keyword group i, the cloud provides (_w, cphBFi) as the proof when it finds keyword cipher textcphw that matches tk, and (cphBFi,BF′i, _BFi) otherwise.[1]

A keyword signature is generated for each keyword cipher text and its associated data cipher texts. It is used for preventing the cloud from returning incorrect data cipher texts as the search result. For each keyword group, one bloom filter is built from its keywords. This allows a data user to check that the searched keyword was indeed not in the keyword group when the cloud returns a null search result, without downloading all keyword cipher texts from the cloud. A random number is selected and encrypted with the same access control policy as keywords. The random number masks the bloom filter for preserving keyword privacy. A bloom filter signature is generated cipher text for assuring their integrity.

8. Applications

Our ABKS schemes fit very well for many applications in the cloud computing environment. One of the prominent applications is about Personal Health Records (PHR) for patients: The data owner encrypted his own health records and outsourced these encrypted records to the cloud which hosts the PHR service. The data owner always needs to fetch the related health records upon some keywords since it is too costly to download all encrypted records and decrypt them to

Licensed Under Creative Commons Attribution CC BY

get desired records. In addition, the data owner might need to share these encrypted health records with some professionals, for example, heart doctors in Emergency Room. In order to attain this goal, the data owner has to delegate the search capability.[2].

9. Applications

Our ABKS schemes fit very well for many applications in the cloud computing environment. One of the prominent applications is about Personal Health Records (PHR) for patients: The data owner encrypted his own health records and outsourced these encrypted records to the cloud which hosts the PHR service. The data owner always needs to fetch the related health records upon some keywords since it is too costly to download all encrypted records and decrypt them to get desired records. In addition, the data owner might need to share these encrypted health records with some professionals, for example, heart doctors in Emergency Room. In order to attain this goal, the data owner has to delegate the search capability [2].

10. Conclusion

We introduced the Attribute base keyword search is more realistic over the outsource encrypted data for encrypted for secure cloud computing over outsourced encrypted data.a data owner can delegate the search capability to a group of users by specifying control policies the data owner. Performance evaluation shows that the new primitive is practical. Our study focused on static data. As such, one interesting open problem sfor future research is to accommodate dynamic data.

Reference

[1] Qingji Zheng† Shouhuai Xu† Giuseppe Ateniese University of Texas at San Antonio, USA Sapienza University of Rome, Italy and Johns Hopkins University, USA, VABKS: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data
[2] Yan feng Shi1*, Jiqiang Liu1, Zhen Han1, QingjiZheng3, Rui Zhang2, Shuo Qiu1 1. School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China, 2. The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China, 3. Department of Computer Science, University of Texas at San Antonio, San Antonio, Texas, United States of America*schwannfeng@bjtu. edu.cn, Attribute-Based Proxy Re-Encryption with Keyword Search
[3] Vipul Goyal, Omkant Pandey, Amit Sahai, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data Brent Waters§ SRI International
[4] RANJEETH KUMAR D. VASUMATHI A Novel Implementation of Fuzzy Keyword Search over Encrypted Data in Cloud Computing JNTU CEH Hyderabad A. P. India
[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data, " in Proc. of ACMCCS, pp. 89–98, 2006
[6] J. Bettencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption, " in Proc. of IEEE S&P, pp. 321–334, 2007.
[7] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption, " in Proc. Of CRYPTO, pp. 191–208, 2010.
[8] A. B. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques, " in Proc. of CRYPTO, pp. 180–198, 2012.
[9] M. Chase, "Multi-authority attribute based encryption, " in Proc. of TCC, pp. 515–534, 2007. Proc. of ACM CCS, pp. 121–130, 2009.
[10] Zhang S, Zhang XW, Ou XM (2014) After we knew it: empirical study and modeling of cost-effectiveness of exploiting prevalent known vulnerabilities across iaas cloud. In: 9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '14, Kyoto, Japan - June 03 - 06, 2014. pp. 317–328.
[11] Zhang S, Caragea D, Ou XM (2011) An empirical study on using the national vulnerability database to predict software vulnerabilities. In: Database and Expert Systems Applications - 22nd International Conference, DEXA 2011, Toulouse, France, August 29 - September 2, 2011. Proceedings, Part I. pp. 217–231for the masked bloom filter and the random number

Author Profiles

Amruta N. Deshmukh received her B.E (Computers) from Sandip Foundation Institute of Technology & Research Centre. Nasik. Affiliated to Pune University, Pune, Maharashtra, India in 2013. Currently she is pursuing M.E. in Computer Science and Engineering from P. R. Pote College of Engineering And Technology Amravati, Maharashtra, India.

Komal B. Bijwe completed her M.E. Currently she is working as assistant professor in P. R. Pote College of Engineering and Technology Amravati, Maharashtra, India.

Licensed Under Creative Commons Attribution CC BY