International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

An Efficient Verifiable Attribute-based Keyword Search Technique for Outsourced Encrypted Data in Cloud

[1]A R Balaji & [2]M.Vikram
[1]M.Tech. Student,Department of Computer Science & Engineering, SV College of Engineering,Tirupathi, IndiaE-mail: balu1649@gmail.com
[2]Associate Professor,Department of Computer Science & Engineering, SV College of Engineering, Tirupathi, IndiaE-mail: vikram.m@svcolleges.edu.in

ABSTRACT

It is common nowadays for data owners to outsource their data to the cloud. As the cloud cannot be completely trusted, the outsourced data needs to be encrypted.However this even brings a range of issues, such as: How should a data owner grant search permission to the data users? How can the authorized data users search over a data owner have outsourced encrypted data? How can the data users be assured that the cloud successfully execute the search operations on their side? To solve these questions, we propose a new cryptographic solution, called verifiable attribute-based keyword search (VABKS). The solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) searching over the data owner's outsourced encrypted data, (ii) outsource the complicated search operations to the cloud, and (iii) check whether the cloud has faithfully executed the search operations. We now define the security requirements of VABKS and describe a construction that satisfies them. Performance evaluation shows that the proposed schemes are practical and deployable.

Key words: ABE; ABKS; CP-ABE; KP-ABE; VABK

1. INTRODUCTION

Cloud computing allows data owners to use heavy data storage and vast computation capabilities at a very low minimized cost .Apart to the benefits; data outsourcing to take this away from data owners of direct control over their outsourced data. To alleviate concerns, data owners should encrypt their data before outsourcing to the cloud. However, encryption can delay some useful functions such as searching over the outsourced encrypted data while enforcing an access control policy. Moreover, it is natural to outsource the search operations to the cloud, while keeping the outsourced data private. There is a necessity 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.

2. EXISTING SYSTEM

To the best of our knowledge till now, no existing solution is adequate for what we want to achieve.

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 ciphertext 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 and CP-ABE (ciphertext-policy ABE) where the ciphertext 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 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 getting 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 difference 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 secured 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

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

classified into two categories: searchable encryption in the symmetric-key setting and searchable encryption in the public-key setting. Various variants have been invented to support difficult 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 trusted users. However, all these solutions fully do not solve the problem we study, because

(i) Some of these solutions needs interactions between the data users and the data owners (or a trusted proxy, such as a trapdoor generation entity) to give the search capabilities, and

(ii) All these solutions (except) assume that the server fully executed search operations. In contrast, our solution allows a data user with respective credentials to issue search tokens by which the cloud can do the keyword search operations on behalf of the user, without having 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 verifiability.

Verifiable Keyword Search.

Recently, verifiable keyword search solutions have been proposed in, where each keyword is represented as a root of some polynomial. It is possible to check whether a keyword is present by evaluating the polynomial on the keyword and verifying whether the output is 0 or not. However, these approaches work only when keywords are sent in plaintext to the cloud, and are not suitable for our purpose because the cloud should not learn anything about the keywords. It is worth representing that the secure verifiable keyword search in the symmetric-key setting can be not secure in the public-key setting because the adversary can infer keywords in question via an off-line keyword guessing attack.

3. PROPOSED SYSTEM

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 the access control policy, while allowing the trusted data users to outsource the search operations to the cloud and check whether or not the cloud has faithfully executed the search operations. Or 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 now define the security states of ABKS and present a scheme that provably satisfies them. The scheme is constructed in a novel 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. Experimental evaluation shows that the VABKS solutions are practical.

3.1 verifiable Attribute –Based Keyword Search

In the model of ABKS, the party (e.g., cloud) is considered to prform the search operation faithfully (despite that the party may attempt to infer useful information about the keywords).VABKS achieves the goal of ABKS despite that the party executing the search operation may be malicious.

We consider the system model represented in Fig: 1, which consistsof 4 parties: a data owner, who outsources its encrypted data as well as encrypted keyword-index to the cloud; a cloud, which provides storage of data services and can perform keyword search operations on behalf of the data users; a data user, who is to get the data owner's encrypted data according to some keyword (i.e., keyword search); a trusted authority, which issues credentials to the data owners/users. The credentials are sent over authenticated private channels (which can be achieved through another layer of mechanisms).

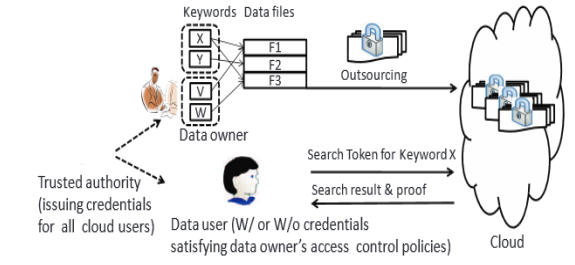

Fig. 1. VABKS system model, where keywords X, Y and V, W may correspond to different access control policies.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

The data owners are generally trusted. Both authorized and unauthorized data users are completely not trusted, meaning that they may try to infer some sensitive information of interest. The cloud is not trusted as it may do the search operations, which already implies that the cloud may manipulate the outsourced encrypted data.

Informally, security of VABKS is defined as the following four requirements, where the cloud is the adversary *A*.

• *Data secrecy:* Given encrypted keywords and search tokens, *A* still cannot learn any information (in a computational sense) about the encrypted data files. This definition can be formalized by the chosen-plaintext security game, where two challengesD0= (KG, MP, FS0), D1= (KG, MP, FS1) correspond to the same KG and MP, and|FS0|=|FS1|.

• *Selective security against chosen-keyword attack:* Without checking respective search tokens, *A* cannot show any information about the keyword from the keyword cipher-text. This property is extended from the selective security against chosen-keyword attack of ABKS.

• *Keyword secrecy:* Given encrypted data files, the probability that *A* learn the plaintext keyword from the keyword ciphertext as well as the search tokens is no more than that of a guess. This property is extended from the keyword secrecy of ABKS.

• *Verifiability:* If *A* returns an not relative search result, it can be found by the user with an overwhelming probability. We formalize this security property via the following verifiability game.

4. CONSTRUCTION OF VABKS

A simple solution for reaching the verifiability is that a data user downloads the keyword cipher texts and conducts the search operations locally. This solution incurs prohibitive communication and computational overhead. As specially shown in Fig 2, we instead let a data user outsource the keyword search operation to the cloud, and then check that the cloud faithfully performed the keyword search operation.Additionally, the data owner uses the signatures and bloom filters as follows:

• A keyword signature is generated for each keyword ciphertext and its respective data ciphertexts. It is used for preventing the cloud from returning incorrect data ciphertexts as the search result.

• For each keyword group, one bloom filter is constructed from its keywords. This makes 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 ciphertexts 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 for the masked bloom filter and the random number ciphertext for assuring their integrity.

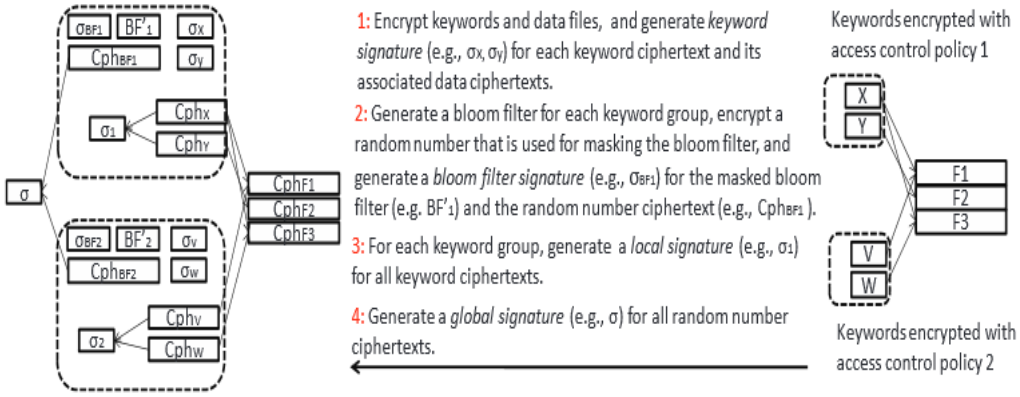

Fig. 2. Basic idea for achieving verifiability, where data files F_1, F_2, F_3 were encrypted to $\text{cph}_{F_1}, \text{cph}_{F_2}, \text{cph}_{F_3}$, keywords X, Y were encrypted to $\text{cph}_X, \text{cph}_Y$ with access control policy 1, and keywords V, W were encrypted to $\text{cph}_V, \text{cph}_W$ with access control policy 2. Given a search token tk, for keyword group i, the cloud provides $(\sigma_w, \text{cph}_{BF_i})$ as the proof when it finds keyword ciphertext cph_w that matches tk, and $(\text{cph}_{BF_i}, BF'_i, \sigma_{BF_i})$ otherwise.

• A global signature is obtained by signing random number ciphertexts of all groups. It allows a data user to verify the integrity of the random number ciphertexts.

• A local signature is generated for all keyword ciphertexts within the same keyword group KG_j. This signature allows the user to validate the integrity of keyword ciphertexts within the keyword group.

5. CONCLUSION

We have introduced a novel cryptographic solution called verifiable attribute-based keyword search for secure cloud computing over outsourced encrypted data. This solution allows a data owner to control the search of its outsourced encrypted data according to an access control policy, while the authorized data users can outsource the search operations to the cloud and force the cloud to faithfully execute the search (as a cheating cloud can be held accountable). Performance evaluation shows that the new primitive is practical. Our study focused on static data. As such, one interesting open problem for future research is to accommodate dynamic data.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Of EUROCRYPT, pp. 457–473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. of ACM CCS , pp. 89–98, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. of IEEE S&P , pp. 321–334, 2007.

[4] 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.

[5] 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.

[6] M. Chase, "Multi-authority attribute based encryption," in Proc. of TCC, pp. 515–534, 2007.

[7] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. of ACM CCS , pp. 121–130, 2009.

[8] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in Proc. of PKC, pp. 196–214, 2009.

[9] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE S&P, pp. 44–, 2000.

[10] E.-J. Goh, "Secure indexes." Cryptology ePrint Archive, Report 2003/216, 2003. http://eprint.iacr.org/2003/216/.

[11] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS , pp. 442–455,2005.

[12] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," In Proc. Of , pp. 79–88, 2006.

[13] M. Chase and S. Kamara, "Structured encryption and controlled disclosure," in Proc. of ASIACRYPT , pp. 577–594, 2010.

[14] K. Kurosawa and Y. Ohtaki, "Uc-secure searchable symmetric encryption," in Proc. of FC , pp. 285–298, Springer Berlin / Heidelberg.

[15] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Of FC, pp. 136–149, 2010ddd

Author1: A R BALAJI,studying M.Tech(computer science) in SV College of Engineering.

Author2: M. Vikram,Working as Assoc. Professor in CSE Dept. of SV College Engeneering. He has more eleven years of experience in teaching. He guided more 6 PG projects and 20 B.Tech projects. His interest areas are data mining and big data.