Secure key word search and data sharing mechanism for cloud computing

A. Bharathi[1] , SD. Sumiya[2]
[1]Assistant Professor, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.
2PG Scholar, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

Abstract

Temporary 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 (ABKS) schemes, the authorized users can generate some search tokens and send them to the cloud for running the search operation. These search tokens can be used to extract all the ciphertexts which are produced at any time and contain the corresponding keyword. Since this may lead to some information leakage, it is more secure to propose a scheme in which the search tokens can only extract the ciphertexts generated in a specified time interval. To this end, in this paper, we introduce a new cryptographic primitive called key-policy attribute-based temporary keyword search (KPABTKS) which provide 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 (SCKA) both in the random oracle model and under the hardness of Decisional Bilinear Diffie-Hellman (DBDH) assumption. Furthermore, we show that the complexity of the encryption algorithm is linear with respect to the number of the involved attributes. Performance evaluation shows our scheme's practicality.

1. INTRODUCTION

Tdoday, cloud computing plays an important role in our daily life, because it provides efficient, reliable and scalable resources for data storage and computational activities at a very low price. However, the direct access of the cloud to the sensitive information of its users threatens their privacy. A trivial solution to address this problem is encrypting data before outsourcing it to the cloud. However, searching on the encrypted data is very difficult.

Public key encryption with keyword search (PEKS) is a cryptographic primitive which was first introduced by Boneh et al. [1] to facilitate

searching on the encrypted data. In PEKS, each data owner who knows the public key of the intended data user generates a searchable ciphertext by means of his/her public key, and outsources it to the cloud. Then, the data user extracts a search token related to an arbitrary keyword by using his/her secret key, and issues it to the cloud. The cloud service provider (CSP) runs the search operation by using the received search token on behalf of the data user to find the relevant results to the intended keywords.

Zheng et al. [2] introduced the notion of attribute-based keyword search (ABKS) to allow a data owner to control the access of data users for searching on his/her outsourced encrypted data. They used attribute-based encryption (ABE) [3] to construct a searchable cryptographic primitive in the multi-sender/multireceiver model. In their work, the legitimate data users can enlist the cloud to run the search operation on behalf of them without requiring any interaction with the data owner. In a secure ABKS scheme, a data owner cannot obtain any information about the keywords which the data users intend to look for.

However, in all of the PEKS and ABKS schemes, once the cloud receives a valid search token related to a certain keyword, the cloud can investigate the keyword's presence in the past and any future ciphertext. So, if the adversary realizes the corresponding keyword of the target search token, then she will be able to get some information about the next documents which will be outsourced to the cloud. Therefore, it will be more secure to limit the time period in which the search token can be used.

Motivated by this problem, Abdalla et al. [4] introduced the notion of public key encryption with temporary keyword search (PETKS) which restricts the validation of the token to a certain time period. They applied anonymous identity-based encryption [5] in their generic scheme. In addition, Yu et al. [6] proposed another public key searchable encryption in the context of temporary keyword search. Despite the good features of their schemes, these schemes do not provide the facility for data owners to enforce their intended access policy. In this paper, 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 ciphertext 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 ciphertext. 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 ciphertext is positive, if (i) the data user's attributes satisfies the access control policy, (ii) the time interval of the

search token encompasses the time of encrypting, and (iii) the search token and the ciphertext are related to the same keyword. To show that the proposed notion can be realized, we also propose a concrete instantiation for this new cryptographic primitive based on bilinear map.

2. LITERATURE SURVEY

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.

3. PROPOSED SYSTEM

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 ciphertext 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 ciphertext. 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 ciphertext is positive, if the data user's attributes satisfies the access control policy, the time interval of the search token encompasses the time of encrypting, and the search token and the ciphertext are related to the same keyword. To show that the proposed notion can be realized, we also propose a concrete instantiation for this new cryptographic primitive based on bilinear map.

Implementation

The Modules are:

1.Data owner

2.Data User

3.Cloud Server

4. key-policy attribute-based temporary keyword search (KPABTKS)

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 ciphertexts. 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 from documents.

Data User

Is an entity who is looking for documents which contains an intended keyword, and are encrypted in a determined time interval. The time interval is arbitrarily selected by the data user. The data user for searching a keyword in a specific time interval, generates a search token which is valid just for that time interval. The data users can generate the search tokens without interacting with the data owners.

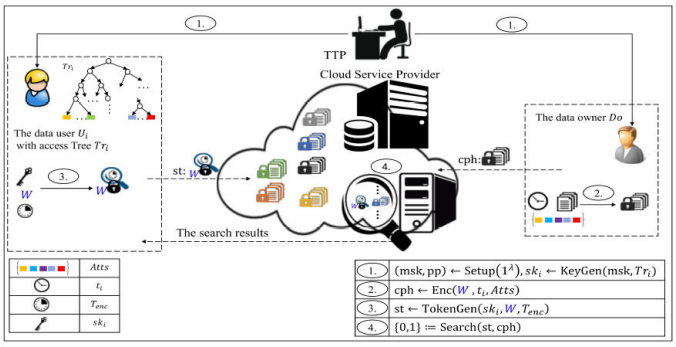
Cloud Server

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.

key-policy attribute-based temporary keyword search (KPABTKS)

KP-ABTKS, 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. The cloud applies the generated search token to find the corresponding ciphertexts which have been encrypted in a time interval specified by the data user.

Architecture



Algorithm

RSA Algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the integers are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

RSA derives its security from the difficulty of factoring large integers that are the product of two large prime numbers. Multiplying these two numbers is easy, but determining the original prime numbers from the total -- factoring -- is considered infeasible due to the time it would take even using today's super computers. The public and the private key-generation algorithm is the most complex part of RSA cryptography. Two large prime numbers, p and q, are generated using the Rabin-Miller primality test algorithm. A modulus n is calculated by multiplying p and q. This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length. The public key consists of the modulus n, and a public exponent, e, which is normally set at 65537, as it's a prime number that is not too large. The e figure doesn't have to be a secretly selected prime number as the public key is shared with everyone. The private key

consists of the modulus n and the private exponent d, which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of n.

4. CONCLUSION

Securing cloud storage is an important problem in cloud computing. We addressed this issue and introduced the notion of key-policy attribute-based temporary keyword search (KPABTKS). According to this notion, each data user can generate a search token which is valid only for a limited time interval. We proposed the first concrete construction for this new cryptographic primitive based on bilinear map. We formally showed that our scheme is provably secure in the random oracle model. The complexity of encryption algorithm of our proposal is linear with respect to the number of the involved attributes. In addition, the number of required pairing in the search algorithms is independent of the number of the intended time units specified in the search token and it is linear with respect to the number of attributes. Performance evaluation of our scheme in term of both computational cost and execution time shows the practical aspects of the proposed scheme.

5. 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-basedkeyword 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 extensions,” in Advances in Cryptology–CRYPTO 2005. Springer, 2005, pp.205–222.

[5] X. Boyen and B. Waters, “Anonymous hierarchical identity-based encryption (without random oracles),” in Annual International CryptologyConference. 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] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.

[8] E.-J. Goh et al., “Secure indexes.” IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[9] 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.

[10] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340– 352, 2016.

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

[12] 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.

[13] A. Awad, A. Matthews, Y. Qiao, and B. Lee, "Chaotic searchable encryption for mobile cloud storage," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2017.

[14] J. Li, D. Lin, A. C. Squicciarini, J. Li, and C. Jia, "Towards privacypreserving storage and retrieval in multiple clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 499–509, July 2017.

[15] J. Li, R. Ma, and H. Guan, "Tees: An efficient search scheme over encrypted data on mobile cloud," IEEE Transactions on Cloud Computing, vol. 5, no. 1, pp. 126–139, Jan 2017.

[16] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM journal on computing, vol. 32, no. 3, pp. 586–615, 2003.

[17] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in International Conference on Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.

[18] D. J. Park, K. Kim, and P. J. Lee, "Public key encryption with conjunctive field keyword search," in International Workshop on Information Security Applications. Springer, 2004, pp. 73–86.

[19] J. Baek, R. Safavi-Naini, and W. Susilo, Public key encryption with keyword search revisited," in Computational Science and Its Applications– ICCSA 2008. Springer, 2008, pp. 1249–1259.

[20] S.-T. Hsu, C. C. Yang, and M.-S. Hwang, "A study of public key encryption with keyword search." IJ Network Security, vol. 15, no. 2, pp. 71–79, 2013.

[21] H. Yin, Z. Qin, J. Zhang, L. Ou, and K. Li, "Achieving secure, universal, and fine-grained query results verification for secure search scheme over encrypted cloud data," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2017.

[22] S. Qiu, J. Liu, Y. Shi, M. Li, and W. Wang, "Identity-based private matching over outsourced encrypted datasets," IEEE Transactions onCloud Computing, vol. PP, no. 99, pp. 1–1, 2017.

AUTHOR'S PROFILE

A. BHARATHI is currently working as Assistant professor in audisankara college of engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupathi(Dt.),Andrapradesh, India.

SD. SUMIYA is pursuing MCA from audisankara college of engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupathi(Dt.),Andrapradesh, India.