ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

An Efficient Novel Technique for Searching Encrypted Data by Improving Privacy and Security on Mobile Cloud

S. Lavanya[1], C. Madhuri Yashoda[2]

M.Tech Student, Dept. of CSE, BIT Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India[1]

Assistant Professor, Dept. of CSE, BIT Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India[2]

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 cipher texts 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 cipher texts generated in a specified time interval. In this paper, we introducing a new cryptographic primitive called key-policy attribute-based temporary keyword search (KPABTKS) which provide this property.

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. In 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) to construct a searchable cryptographic primitive in the multi-sender/multireceiver model. So, if the adversary realizes the corresponding keyword of the target search token, then it will be able to get some information about the next documents which will be outsourced to the cloud. By using this the documents cannot protected & it will be less secure.

In this paper, introducing 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, shows that the complexity of the encryption algorithm is linear with respect to the number of the involved attributes.

I. INTRODUCTION

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a cloud It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. More likely, users want to control the privileges of data manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the cloud servers or another user, which is out of users control in most cases, privacy risks would rise dramatically because the servers might illegally inspect users‟ data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation. Therefore, not only the access but also the operation should be controlled. Secondly, personal information (defined by each user‟s

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

attributes set) is at risk because one‟s identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client‟s personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers. They are counterparts to each other in the sense that the decision of encryption policy (who can or cannot decrypt the message) is made by different parties.

In the KP-ABE, a cipher text is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user‟s identity (e.g. IIT AND (Ph.D. OR Master)). A user can decrypt the cipher text if and only if the access tree in his private key is satisfied by the attributes in the cipher text. However, the encryption policy is described in the keys, so the encrypted does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when are-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to there-encrypted files, and this process causes considerable problems in implementation. On the other hand, those problems and overhead are all solved in the CP-ABE [. In the CP-ABE, cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users‟ attributes. A user can decrypt the cipher text if and only if his attributes in the private key satisfy the access tree specified in the cipher text. By doing so, the encrypted holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots**.**

II. LITERATURE SURVEY

Yang, X. Jia, K. Ren, and B. Zhang[4] This paper describes Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems.

G. Tzeng [5], This paper describes propose efficient and secure (string) oblivious transfer (OT1n) schemes for any n_ 2. We build our OT1 n scheme from fundamental cryptographic techniques directly. The receiver‟s choice is unconditionally secure and the secrecy of the unchosen secrets is based on the hardness of the decisional Diffie-Hellman problem.

Yu, C. Wang, K. Ren, and W. Lou[5] This paper describes Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

Shamir, [1] This paper introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other 's signatures without exchanging private or public keys, without keeping key directories , and without using the services of a third party. The scheme assumes t h e existence of trusted key generation centers, whose sole purpose is t o give each user a personalized smart card v when he first join st he network.

A. Sahai and B. Waters,[2] This paper introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, $\omega\_$, if and only if the identities ω and ω are close to each other as measured by the “set overlap” distance metric.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

V. Goyal, O. Pandey, A. Sahai, and B. Waters,[3] This paper describes As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level(i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE).

III. EXISTING SYSTEM

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. In 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) to construct a searchable cryptographic primitive in the multi-sender/multireceiver model. 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. By using this we cannot protect our documents.

Disadvantages:-

- Efficiency is less.
- Security is less.

IV. PROPOSED WORK

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.

Advantages:-

- Security is high.
- Efficiency is improved.

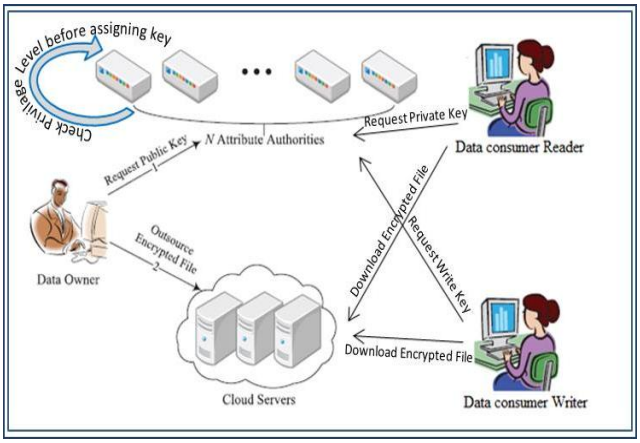

Fig 1.1: architecture of system

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

V. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it‟s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Module description:

Attribute Authorities:
Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

Data Consumers:
Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

Data Owners:
Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

Cloud Server:
Then, the owner sends the encrypted data to the cloud server together with the cipher-texts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

VI. CONCLUSIONS AND FUTURE WORK

This paper proposes a key-policy attribute-based temporary keyword search (KPABTKS), each data user can generate a search token which is valid only for a limited time interval. 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.

REFERENCES

[1] 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.
[2] 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.
[3] 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

[4] 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.
[5] 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.
[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM journal on computing, vol. 32, no. 3, pp. 586–615, 2003.
[7] 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.
[8] 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.
[9] 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.
[10] 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.