ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 6, June 2018

An Efficient Search Scheme Over Attribute-Based Encryption Data Access Control

[1]Mrs.S.Poonkodi, [2] Mrs.R.Arul
1-Associate professor, 2-PG Student
Department of Computer science and Engineering
Karpaga Vinayaga College of Engineering & Technology, Chennai, Tamil Nadu, India
rkpoonkodi@gmail.com,mailarulmozhi@gmail.com

Abstract: Cloud storage provides a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloud trustingly. One way of enhancing privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a complicated communication between the data user and cloud..In order to provide safe and secure operation, a hierarchical access control method using modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure is proposed in this paper. In a specific mobile cloud computing model, enormous data which may be from all kinds of mobile devices, such as smart phones, functioned phones and PDAs and so on can be controlled and monitored by the system, and the data can be sensitive to unauthorized third party and constraint to legal users as well.To increase efficient file search scheme, we propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture offloads the computation from mobile devices to the cloud, and we further optimize the communication between the mobile clients and the cloud. It is demonstrated that the data privacy does not degrade when the performance enhancement methods are applied.

Keywords: M-HABE, Cloud, TEES, Hierarchical, Access Control

I. Introduction

Cloud storage provides a convenient, massive, and scalable storage at low cost, The data privacy from storing files on the cloud. Enhancing privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them, encrypt files by using blowfish algorithm. The cloud based hierarchical multi-user data-shared environment. With integrating into cloud computing, security issues such as data confidentiality and user authority may arise in the mobile cloud computing system, and it is concerned as the main constraints to the developments of mobile cloud computing. We propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud.TEES achieves the efficiencies through employing and modifying the ranked keyword search as the encrypted search platform basis, which has been widely employed in cloud storage systems. Traditionally, two categories of encrypted search methods exit that can enable the cloud server to perform the search over the encrypted data: ranked keyword search and Boolean keyword search. It is demonstrated that the data privacy does not degrade when the performance enhancement methods are applied.

Overview

Recently, the cloud computing paradigm is revolutionizing the organizations' way of operating their data particularly in the way they store, access and process data. As an emerging computing paradigm, cloud computing attracts many organizations to consider seriously regarding cloud potential in terms of its cost efficiency, flexibility, and offload of administrative overhead. Most often, organizations delegate their computational operations in addition to their data to the cloud. Despite tremendous advantages that the cloud offers, privacy and security issues in the cloud are preventing companies to utilize those advantages. When data are highly sensitive, the data need to be encrypted before outsourcing to the cloud. However, when data are encrypted, irrespective of the underlying encryption scheme, performing any data mining tasks becomes very challenging without ever decrypting the data. There are other privacy concerns, demonstrated by the following example.

Suppose an insurance company outsourced its encrypted customers database and relevant data mining tasks to a cloud. When an agent from the company wants to determine the risk level of a potential new customer, the agent can use a classification method to determine the risk level of the customer. First, the agent needs to generate a data record q for the customer containing certain personal information of the customer, e.g., credit score, age, marital status, etc. Then this record can be sent to the cloud, and the cloud will compute the class label for q. Nevertheless, since q contains sensitive information, to protect the customer's privacy, q should be encrypted before sending it to the cloud.

About domain

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.

Forrester defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption.

II. System Analaysis

EXISTING SYSTEM:

In the proposed scenario, users with different privilege levels have different rights to access the part of sensing data coming from the mobile devices. Therefore, one same data has to be encrypted into ciphertext once, which ought to be able to be decrypted multiple times by different authorized users. So a secure and hierarchical access control method should be proposed to apply in the mobile cloud computing system. A modified hierarchical attribute-based encryption (MHABE) access control method applied in mobile cloud computing is proposed in this paper, which changes a proposed scheme called hierarchical attribute-based encryption HABE , M-HABE combines the hierarchical identity-based encryption and the ciphertext-policy attribute-based encryption (CP-ABE)

DISADVANTAGE:

- Boolean keyword search and ranked keyword search. In Boolean keyword search the server sends back files only based on the existence or absence of the keywords, without looking at their relevance.
- A one round trip search scheme which could search the encrypted data. It worths noticing that multi-keyword ranked search may incur more serious Keywords-files Association Leak problem.
- The proposed paper can be described as that the modified three-layer structure is designed for solving the security issues but facing file searching issues problem in (M-HABE).

PROPOSED SYSTEM:

Currently, many researches focus on improving the encrypted search accuracy with multi-keywords ranking. Proposed a one round trip search scheme which could search the encrypted data. It worth's noticing that multi-keyword ranked search may incur more serious Keywords-files Association Leak problem , if attackers observed the keywords and the return files to learn some relationships between keywords and files, especially through wireless communication channels for mobile cloud. They proposed privacy preserving method for multi-keyword encrypted search with a way to control the 'double key leak". The ranked keyword search adopts the relevance scores to represent the relevance of a file to the searched keyword and sends the top-k relevant files to the client. It is more suitable for cloud storage than the boolean keyword search approaches since boolean keyword search approaches need to send all the matching files to the clients.

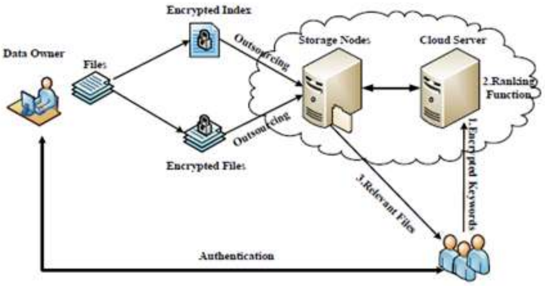
ADVANTAGE PROPOSED SYSTEM:

- Multi-keyword search scheme to perform encrypted data search over mobile cloud in future. As our OPE algorithm is a simple one, another extension is to find a powerful algorithm which will not harm the efficiency.
- The proposed paper can be described as that the modified three-layer structure is designed for solving the security issues.
- The network traffics during file retrival are also significantly reduced

- Confidentiality has been a huge barrier for cloud providers to popularize cloud to consumers since it comes out. It is understandable that consumers cannot trust the cloud services, after all, nobody knows what will happen to the files, especially important confidential ones, once they are placed in cloud vendors' hosts
- A cross-tenant trust model and its RBAC extension was proposed in improving the encrypted search accuracy with multi-keywords ranking. proposed a one round trip search scheme which could search the encrypted data. It worths noticing that multi-keyword ranked search may incur more serious Keywords-files Association Leak problem.

III. SYSTEM ARCHITECTURE

A hierarchical access control method using a modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure is proposed. Differing from the existing paradigms such as the HABE algorithm and the original three-layer structure, the novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the application users with legal access authorities to get corresponding sensing data and to restrict illegal users and unauthorized legal users get access to the data, the proposed promising paradigm makes it extremely suitable for the mobile cloud computing based paradigm. What should be emphasized is that the most important highlight of all in the proposed paper can be described as that the Modified three-layer structure is designed for solving the security issues illustrated above.



Authority of data users: Different authority-level system to get access to sensing data for application users should be established since the paradigm is applied in the hierarchical multi-user shared environment, which also means that the users with higher authority level should get all the data that the users with lower privilege level could get access to, while the lower privilege users cant get the data beyond his/her authority.

Confidentiality of data: Although the cloud services utilized in the scenario are provided by private cloud which is supposed to be secure, it is still necessary to ensure the sensing data protected from malicious third parties that do not belong to the mobile cloud system. Therefore it is important for the system to bring in a secure and efficient encryption scheme.

IV. MODULES

- System modules
- Authority of data users
- Confidentiality of data
- Controlling data
- Top-k relevant
- Keywords-files Control

System modules:

Authentication center login and activate Sub authentication after get approval by Authentication center, Allow login and file storage permission. Authentication center gave approval for user and Owner. Sub Authentication allows file storage permission and generate public and private key. Owner Encrypt and Upload files .Before the file storage to cloud, each file Access permission by Authentication center and Sub authentication. User search File, retrieval Top K files on ranking based. After send Key request to Authentication center. After the key Verification of each file can decrypt and download. Cloud will maintain Key generation, cloud storage and download details.

Authority of data users:

Different authority-level system to get access to sensing data for application users should be established since the paradigm is applied in the hierarchical multi-user shared environment, which also means that the users with higher authority level should get all the data that the users with lower privilege level could get access to, while the lower privilege users can't get the data beyond his/her authority.

Confidentiality of data:

Although the cloud services utilized in the scenario are provided by private cloud which is supposed to be secure, it is still necessary to ensure the sensing data protected from malicious third parties that do not belong to the mobile cloud system. Therefore it is important for the system to bring in a secure and efficient encryption scheme. Confidentiality has been a huge barrier for cloud providers to popularize cloud to consumers since it comes out. It is understandable that consumers cannot trust the cloud services, after all, nobody knows what will happen to the files, especially important and confidential ones, once they are placed in cloud vendors' hosts.

Controlling data:

In order to own a secure control system, cloud vendors may need a specialized operating system. Virtualization based cloud services make it difficult to overcome defects in security control because of the insufficient control mechanisms that virtualized networks offer. And poor key management procedures of virtualized based cloud services make it worse because virtual machines don't have a fixed hardware infrastructure and cloud-based content is often geographically distributed, it is a very tough task to ensure a secure control in cloud. A secure control system distributes appropriate resources to be utilized in

Different occasions

Top-k relevant

The data privacy issue is paramount in cloud storage system, so the sensitive data is encrypted by the owner before outsourcing onto the cloud, and data users retrieve the interested data by encrypted search scheme. The data user stems the keyword to be queried and encrypts it using the keys. After calculating the relevance scores, the position of the files corresponding to the keyword is picked and the top k relevant files. It directly sends the top-k relevant files back to the data user after it receives the retrieval request, which can also reduce the traffic amount for file retrievals at the same time.

Keywords-files Control

When an authorized user searches files from a mobile client, he gets a hash value corresponding to the keyword w to be queried. Then this hash value is embedded into a tuple (h1; h2) and sent to the server. Even if the attacker knows the content to be queried, he does not know anything about the keywords to be queried because of the noise, so he is also unable to determine the terms. The tuple (h1; h2) corresponding to the word "Bund" of our data retrievals is distributed as displayed files.

V. Algorithm

Ranking Function:

Cloud server calculates the relevance scores and return top-k relevant files according to the searching query from data user. The calculation scheme in is used in our scheme. Note that due to the order preserving index, any other relevance scores calculation method can also be employed. In order to get top-k relevant files, we implement a ranking function to calculate the relevant score on the cloud (Section 4.2). Given a keyword in ORS, the cloud server is in charge of calculating the relevance scores for the data user to get the corresponding top-k relevant files. Therefore, we implement both the unwrap and rank functions in the cloud server module

Wrap Function

The wrap function of the keywords is implemented to solve the keywords-files association leak. In the wrap function, the stem, the encryption and the hash operation are exactly the same as in the index building algorithm. The function decrypting the files corresponds to the encryption done by the data owner. The authentication function is used for authentication. We now detail the wrap function of this module. When an authorized data\ user wants to retrieve files, he needs to encrypt the corresponding query keyword w, and get the hash value h from the hash table. This hash value is then sent to the cloud server and used to compute the relevance scores. In order to render this hash value indistinguishable for an attacker, the cloud client should wrap it, adding some noise before sending it to the cloud server

Blowfish Algorithm

Bruce Schneier, one of the world's leading cryptologists, designed the Blowfish algorithm [10] and made it available in the public domain. Blowfish is a variable length key, 64-bit block cipher. The algorithm was first introduce in 1993, and has not been cracked yet. It can be optimized in hardware applications due to its compactness. The algorithm is shown in Fig.2. It consists of two parts: a key-expansion part and a data- encryption part. Keyexpansion converts a key of at most 448 bits into several sub-key arrays totaling 4168 bytes. Data encryption occurs via a 16-round (commonly) network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

VI. Conclusion

The paper proposed a modified HABE scheme by taking advantages of attributes based encryption (ABE) and hierarchical identity based encryption (HIBE) access control processing. The proposed access control method using MHABE is designed to be utilized within a hierarchical multiuser data-shared environment, to improve efficient search then we developed an efficient implementation to achieve an encrypted search in a mobile cloud. We have proposed a single keyword search scheme to make encrypted data search efficient. However, there are still some possible extensions of our current work remaining. We would like to propose a multi-keyword search scheme to perform encrypted data search over mobile cloud.

REFERENCES

[1]. N. Fernando, S. W. Loke, and W. Rahayu, “Mobile cloud computing: A survey,” Future Generation Computer Systems, vol. 29, no. 1, pp. 84–106, 2013.

[2]. S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, “Cloudbased augmentation for mobile devices: motivation, taxonomies, and open challenges,” Communications Surveys & Tutorials, IEEE, vol. 16, no. 1, pp. 337–368, 2014.

[3]. R. Kumar and S. Rajalakshmi, “Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems,” in Computer Sciences and Applications (CSA), 2013 International Conference on. IEEE, 2013, pp. 663–669.

[4]. J. Carolan, S. Gaede, J. Baty, G. Brunette, A. Licht, J. Remmell, L. Tucker, and J. Weise, “Introduction to cloud computing architecture,” White Paper, 1st edn. Sun Micro Systems Inc, 2009.

[5]. E. E. Marinelli, “Hyrax: cloud computing on mobile devices using mapreduce,” DTIC Document, Tech. Rep., 2009.

[6]. Q. Han, S. Liang, and H. Zhang, “Mobile cloud sensing, big data, and 5g networks make an intelligent and smart world,” Network, IEEE, vol. 29, no. 2, pp. 40–45, 2015.

[7]. I. Stojmenovic, “Access control in distributed systems: Merging theory with practice,” in Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on. IEEE, 2011, pp. 1–2.

[8]. G. Wang, Q. Liu, and J. Wu, “Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,” in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 735–737.

[9]. C. Gentry and A. Silverberg, “Hierarchical id-based cryptography,” in Advances in cryptologyASIACRYPT 2002. Springer, 2002, pp. 548–566.

[10]. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Security and Privacy, 2007. SP’07. IEEE Symposium on. IEEE, 2007, pp. 321–334.

[11]. A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in cryptology. Springer, 1985, pp. 47–53.

[12]. M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, “Security and privacy in cloud computing: A survey,” in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on. IEEE, 2010, pp. 105–112.

[13]. B. Grobauer, T. Walloschek, and E. St¨ocker, “Understanding cloud computing vulnerabilities,” Security & privacy, IEEE, vol. 9, no. 2, pp. 50–57, 2011.

[14]. S. Ghemawat, H. Gobioff, and S.-T. Leung, “The google file system,”in ACM SIGOPS operating systems review, vol. 37, no. 5. ACM, 2003, pp. 29–43.

[15]. M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, “Security and privacy in cloud computing: A survey,” in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on. IEEE, 2010, pp. 105–112.

[16]. D. Huang, “Mobile cloud computing,” IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[17]. O. Mazhelis, G. Fazekas, and P. Tyrvainen, “Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage,” in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[18]. J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian,

[19]. “Virtualized in-cloud security services for mobile devices,” in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[20]. J. Oberheide and F. Jahanian, “When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments,” in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

[21]. A. A. Moffat, T. C. Bell et al., Managing gigabytes: compressing and indexing documents and images. Morgan Kaufmann Pub, 1999.