International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Revocable Data Access Control for Secure Data Sharing In Cloud

R. Gayathri, M. Ganthimathi

Muthayammal Engineering College, Rasipuram, Rasipuram, Tamil Nadu, India

ABSTRACT

Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising crypto graphical primitive to build a practical data sharing system. However, access control isn't static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, present a concrete construction of RS-IBE, and prove its security in the defined security model. Furthermore have introduced AES algorithm because the more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES. Some features of AES algorithm is Symmetric key symmetric block cipher, 128-bit data, 128/192/256-bit keys, Stronger and faster than Triple-DES, Provide full specification and design details, Software implementable in C and Java. The performance comparisons indicate that the proposers-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

Keywords : Cloud Computing, AES, DES, ABE, KDC, KDC, OPE, TRSE, OPE

I. INTRODUCTION

Cloud storage provides user ease and convenience to handle the data backup and retrieval. Here user need not have to keep pen drive or carry harddisk along with him on travel. But, this will often add to the cost of the users to utilize the cloud storage services for large amount of data storage. Moreover cloud storage is much slower compare to local storage backup for the huge amount of data.

II. LITERATURE REVIEW

Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds

Propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the ser without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches. Existing work on access control in cloud are centralized in nature. Except and, all other schemes use attribute based encryption (ABE). The scheme in uses a symmetric key approach and does not support authentication. The schemes do not support authentication as well. Earlier work by Zhao *et al.* provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to

all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world.

A single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, Ruj *et al.* proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. In the preliminary version of this paper, extend our previous work with added features which enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. In this version also address user revocation. Use attribute based signature scheme to achieve authenticity and privacy. Extend our previous work with added features which enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud.

Towards Secure Multi-Keyword Top-k Retrieval over Encrypted Cloud Data

Cloud computing has emerging as a promising pattern for data outsourcing and high quality data services. However, concerns of sensitive information on cloud potentially cause privacy problems. Data encryption protects data security to some extent, but at the cost of compromised efficiency. Searchable symmetric encryption (SSE) allows retrieval of encrypted data over cloud. In this paper, focus on addressing data privacy issues using searchable symmetric encryption (SSE). For the first time, formulate the privacy issue from the aspect of similarity relevance and scheme robustness. Observe that server-side ranking based on order-preserving encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose a two-round searchable encryption (TRSE) scheme that supports top-k multi-keyword retrieval. In TRSE, employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on cipher text. As a result, information leakage can be eliminated and data security is ensured. Thorough security and performance analysis show that the proposed scheme guarantees high security and practical efficiency. Besides, in order to improve feasibility and save on the expense in the cloud paradigm, it is preferred to get the retrieval result with the most relevant files that match users' interest instead of all the files, which indicates that the files should be ranked in the order of relevance by users' interest and only the files with the highest relevance's are sent back to users. A series of searchable symmetric encryption schemes have been proposed to enable search on cipher text. Traditional SSE schemes enable users to securely retrieve the ciphertext, but these schemes support only Boolean keyword search, i.e., whether a keyword exists in a file or not, without considering the difference of relevance with the queried keyword of these files in the result. Preventing the cloud from involving in ranking and entrusting all the work to the user is a natural way to avoid information leakage. However, the limited computational power on the user side and the high computational overhead precludes information security.

- To improve security without sacrificing efficiency, schemes presented in show that they support top-k single keyword retrieval under various scenarios.
- Authors of made attempts to solve the problem of top-k multi-keyword over encrypted cloud data.
- These schemes, however, suffer from two problems – Boolean representation and how to strike a balance between security and efficiency.
- In the former, files are ranked only by the number of retrieved keywords, which impairs search accuracy. In the latter, security is implicitly compromised to tradeoff for efficiency, which is particularly undesirable in security-oriented applications.

In this paper, introduce the concepts of similarity relevance and scheme robustness to formulate the privacy issue in searchable encryption schemes, and then solve the insecurity problem by proposing a two-

round searchable encryption (TRSE) scheme. Novel technologies in the cryptography community and information retrieval community are employed, including homomorphic encryption and vector space model. In the proposed scheme, the majority of computing work is done on the cloud while the user takes part in ranking, which guarantees top k multi-keyword retrieval over encrypted cloud data with high security and practical efficiency. Propose the concepts of similarity relevance and scheme robustness. Thus perform the first attempt to formulate the privacy issue in searchable encryption, and show server side ranking based on order-preserving encryption (OPE) inevitably violates data privacy. Propose a two-round searchable encryption (TRSE) scheme, which fulfills the secure multi-keyword top-k retrieval over encrypted cloud data. Specifically, for the first time employ relevance score to support multi-keyword top-k retrieval. Thorough analysis on security demonstrates the proposed scheme guarantees high data privacy. Furthermore, performance analysis and experimental results show that our scheme is efficient for practical utilization.

To alleviate the computational burden on user side, computing work should be at the server side, so need an encryption scheme to guarantee the operability and security at the same time on server side. Homomorphic encryption allows specific types of computations to be carried out on the corresponding cipher text. The result is the cipher text of the result of the same operations performed on the plaintext. That is, homomorphic encryption allows computation of cipher text without knowing anything about the plaintext to get the correct encrypted result. Although it has such a fine property, original fully homomorphic encryption scheme, which employs ideal lattices over a polynomial ring , is too complicated and inefficient for practical utilization. Fortunately, as a result of employing the vector space model to top-k retrieval, only addition and multiplication operations over integers are needed to compute the relevance scores from the encrypted searchable index. Therefore, can reduce the original homomorphism in a full form to a simplified form that only supports integer operations, which allows more efficiency than the full form does.
In this paper, motivate and solve the problem of secure multi-keyword top-k retrieval over encrypted cloud data. Define similarity relevance and scheme robustness. Based on order preserving encryption invisibly leak sensitive information, devise a server-side ranking SSE scheme. Then propose a two-round searchable encryption (TRSE) scheme employing the fully homomorphic encryption, which fulfills the security requirements of multi-keyword topk retrieval over the encrypted cloud data. By security analysis, Show that the proposed scheme guarantees data privacy. According to the efficiency evaluation of the proposed scheme over real dataset, extensive experimental results demonstrate that our scheme ensures practical efficiency.

III. EXISTING SYSTEM

Cloud computing is a paradigm that provides massive computation capacity and huge memory space at a low cost .It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's Cloud. Cloud computing have stored the valuable information and sensitive data's. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising crypto graphical primitive to build a practical data sharing system. However, access control is not static after to use stored data's anytime and anywhere. Some days back unfortunately user's authorization key is missing there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data.

3.1.1 DRAWBACKS

- Can't access your system for authentication key is missing
- Security wise is very low in the security model
- Efficiency and functionality is low.

IV. PROPOSED SYSTEM

In this system have stored the data's in securely is the main motive of this Paper, so have introduce a concept

like revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, present a concrete construction of RS-IBE, and prove its security in the defined security model. Furthermore have introduced AES algorithm because the more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES. Some features of AES algorithm is Symmetric key symmetric block cipher, 128-bit data, 128/192/256-bit keys, Stronger and faster than Triple-DES, Provide full specification and design details, Software implementable in C and Java. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

V. SYSTEM METHODOLOGY

ARCHITECTURE

RIBE features a mechanism that enables a sender to append the current time period to the cipher text such that the receiver can decrypt the cipher text only under the condition that he/she is not revoked at that time period. As indicated in Figure 1, a RIBE-based data sharing system works as follows: Step 1: The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the cipher text of the shared data to the cloud server. Step 2: When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding cipher text. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available. Step 3: In some cases, e.g., Alice's authorization gets expired, David can download the cipher text of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

Obviously, such a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the cipher text periodically by using secret key. Another challenge comes from efficiency. To update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-re encrypt-upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage. One method to avoid this problem is to require the cloud server to directly re-encrypt the cipher text of the shared data. However, this may introduce cipher text extension; namely, the size of the cipher text of the shared data is linear in the number of times the shared data have been updated. In addition, the technique of proxy re-encryption can also be used to conquer the aforementioned problem of efficiency. Unfortunately, it also requires users to interact with the cloud server in order to update the cipher text of the shared data.

MODULES

- User Registration and Authentication
- Upload Data's from Cloud Server
- Data Provider
- Key Management.

VI. MODULE DESCRIPTION

User Registration and Authentication:
Users can create an account in the website by providing various details such as username, password, name, age, gender, date of birth, income status.

VII. CONCLUSION

Finally I conclude propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, present a concrete construction of RS-IBE, and prove its security in the defined security model. Furthermore have introduced AES algorithm because the more

popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES. Some features of AES algorithm is Symmetric key symmetric block cipher, 128-bit data, 128/192/256-bit keys, Stronger and faster than Triple-DES, Provide full specification and design details, Software implementable in C and Java. The performance comparisons indicate that the proposers-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

VIII. REFERENCES

[1]. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2]. iCloud. (2014) Apple storage service. Online]. Available:https://www.icloud.com/

[3]. Azure. (2014) Azure storage service. Online]. Available: http://www.windowsazure.com/

[4]. Amazon. (2014) Amazon simple storage service (amazon s3). Online]. Available: http://aws.amazon.com/s3/

[5]. K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[6]. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7]. G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

[8]. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[9]. B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[10]. S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[11]. X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

[12]. C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.