ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Data Storage Schemes Based on Identity

Mukka Sushanth Kumar
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

Nachu Priyanka
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

B.Ranjitha, M.Tech
Assistant Professor,
Depatment of CSE,
TKR College of Engineering & Technology.

Abstract:

Secure distributed data storage can shift the burden of maintaining a large number of files from the owner to proxy servers. Proxy servers can convert encrypted files for the owner to encrypted files for the receiver without the necessity of knowing the content of the original files. In practice, the original files will be removed by the owner for the sake of space efficiency. Hence, the issues on confidentiality and integrity of the outsourced data must be addressed carefully. In this paper, we propose two identity-based secure distributed data storage (IBSDDS) schemes. Our schemes can capture the following properties:

(1) The file owner can decide the access permission independently without the help of the private key generator (PKG); (2) For one query, a receiver can only access one file, instead of all files of the owner; (3) Our schemes are secure against the collusion attacks, namely even if the receiver can compromise the proxy servers, he cannot obtain the owner's secret key. Although the first scheme is only secure against the chosen plaintext attacks (CPA), the second scheme is secure against the chosen ciphertext attacks (CCA). To the best of our knowledge, it is the first IBSDDS schemes where an access permissions is made by the owner for an exact file and collusion attacks can be protected in the standard model.

Index Terms:

Distributed Data Storage, Identity-based System, Access Control, Security.

INTRODUCTION:

Cloud computing provides users with a convenient mechanism to manage their personal files with the notion called database-as-a-service (DAS) [1], [2], [3].

In DAS schemes, a user can outsource his encrypted files to untrusted proxy servers. Proxy servers can perform some functions on the outsourced ciphertexts without knowing anything about the original files. Unfortunately, this technique has not been employed extensively. The main reason lies in that users are especially concerned on the confidentiality, integrity and query of the outsourced files as cloud computing is a lot more complicated than the local data storage systems, as the cloud is managed by an untrusted third party.

After outsorcing the files to proxy servers, the user will remove them from his local machine. Therefore, how to guarantee the outsoured files are not accessed by the unauthorized users and not modified by proxy servers is an important problem that has been considered in the data storage research community. Furthermore, how to guarantee that an authorized user can query the outsourced files from proxy servers is another concern as the proxy server only maintains the outsourced ciphertexts. Consequently, research around these topics grows significantly.

EXISTING SYSTEM:

Cloud computing provides users with a convenient mechanism to manage their personal files with the notion called database-as-a-service (DAS). In DAS schemes, a user can outsource his encrypted files to untrusted proxy servers. Proxy servers can perform some functions on the outsourced ciphertexts without knowing anything about the original files. Unfortunately, this technique has not been employed extensively. The main reason lies in that users are especially concerned on the confidentiality, integrity and query of the outsourced files as cloud computing is a lot more complicated than the local data storage systems, as the cloud is managed by an untrusted third party. After outsorcing the files to proxy servers, the user will remove them from his local machine.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Therefore, how to guarantee the outsoured files are not accessed by the unauthorized users and not modified by proxy servers is an important problem that has been considered in the data storage research community. Furthermore, how to guarantee that an authorized user can query the outsourced files from proxy servers is another concern as the proxy server only maintains the outsourced ciphertexts. Consequently, research around these topics grows significantly.

DISADVANTAGES OF EXISTING SYSTEM:

Users are especially concerned on the confidentiality, integrity and query of the outsourced files as cloud computing is a lot more complicated than the local data storage systems, as the cloud is managed by an untrusted third party.

- The outsoured files are not accessed by the unauthorized users and not modified by proxy servers is an important problem that has been considered in the data storage research community.

PROPOSED SYSTEM:

In this paper, we propose two identity-based secure distributed data storage (IBSDDS) schemes in standard model where, for one query, the receiver can only access one of the owner's files, instead of all files. In other words, an access permission (re-encryption key) is bound not only to the identity of the receiver but also the file. The access permission can be decided by the owner, instead of the trusted party (PKG). Furthermore, our schemes are secure against the collusion attacks.

ADVANTAGES OF PROPOSED SYSTEM:

It has two schemes of security,the first scheme is CPA secure, the second scheme achieves CCA security.

- To the best of our knowledge, it is the first IBSDDS schemes where an access permission is made by the owner for an exact file and collusion attacks can be protected in the standard model.

- To achieve a stronger security and implement file-based access control, the owner must be online to authenticate requesters and also to generate access permissions for them. Therefore, the owner in our schemes needs do more computations than that in PRE schemes. Although PRE schemes can provide the similar functionalities of our schemes when the owner only has one file, these are not flexible and practical.

MODULES:

- Data Owner
- Private key Generator
- Proxy Server
- The Receiver Module

MODULES DESCRIPTION:

• Data Owner:

In this module, first the new data owner registers and then get a valid login credentials. After logged in, the data owner has the permission to upload their file into the Cloud Server. The data owner encrypts his data and outsources the ciphertexts to the proxy servers.

• Private Key Generator:

In this module, the private key generator (PKG) validates the users' identities and issues secret keys to them. The key is generated and sent to their respective mail id's with the file name and the corresponding key values.

• Proxy Server:

Proxy servers store the encrypted data and transfer the cipher text for the owner to the cipher text for the receiver when they obtain access permission (re-encryption key) from the owner. In these systems, proxy servers are assumed to be trusted. They authenticate receivers and validate access permissions. The interactions between the proxy servers and receivers are executed in a secure channel. Therefore, these systems cannot provide an end-to-end data security, namely they cannot ensure the confidentiality of the data stored at the proxy server. In these schemes, a receiver authenticates himself to the proxy server using his password.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Then, the proxy server passes the authentication result to the file owner. The owner will make access permission according to the received information.

• Receiver Module:

The receiver authenticates himself to the owner and decrypts the re-encrypted Ciphertext to obtain the data. In these systems, an end to-end security is provided by cryptographic protocols which are executed by the file owner to prevent proxy servers and unauthorized users from modifying and accessing the sensitive files. These systems can be divided into two types: shared file system and non-shared system.

In shared file systems the owner can share his files with a group of users. Cryptographic techniques deployed in these systems are key sharing, key agreement and key revocation. In non-shared file systems in order to share a file with another user, the owner can compute an access key for the user using his secret key. In these two systems, the integrity of the sensitive files is provided by digital signature schemes and message authentication codes (MAC).

Project Purpose:

Confidentiality is proposed to prevent unauthorized users from accessing the sensitive data as it is subject to unauthorized disclose and access after being outsourced. Since the introduction of DAS, the confidentiality of outsourced data has been the primary focus among the research community. To provide confidentiality to the outsourced data, encryption schemes are deployed Integrity can prevent outsourced data from being replaced and modified.

Some schemes have been proposed to protect the integrity of the outsourced data, such as proof of retrievability and provable data possession . In these schemes, digital signature schemes and message authentication codes (MAC) are deployed. Query in data storage is executed between a receiver and a proxy server. The proxy server can perform some functions on the outsourced ciphertexts and convert them to those for the receiver. As a result, the receiver can obtain the data outsourced by the owner without the proxy server knowing the content of the data.

The main reason lies in that users are especially concerned on the confidentiality, integrity and query of the outsourced files as cloud computing is a lot more complicated than the local data storage systems, as the cloud is managed by an untrusted third party. After outsorcing the files to proxy servers, the user will remove them from his local machine.

Therefore, how to guarantee the outsoured files are not accessed by the unauthorized users and not modified by proxy servers is an important problem that has been considered in the data storage research community. Furthermore, how to guarantee that an authorized user can query the outsourced files from proxy servers is another con**cern as the proxy server only maintains the outsourced ciphertexts. Consequently, research.**

SYSTEM ARCHITECTURE:

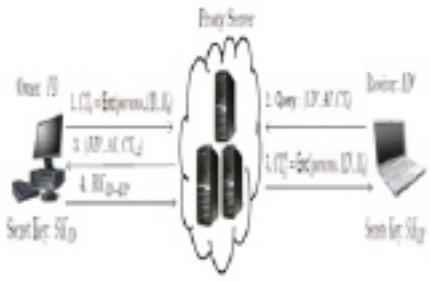

Fig. 1: The Model of Identity-Based Secure Distributed Data Storage Scheme

CONCLUSION:

Distributed data storage schemes provide the users with convenience to outsource their files to untrusted proxy servers. Identity-based secure distributed data storage (IBSDDS) schemes are a special kind of distributed data storage schemes where users are identified by their identities and can communicate without the need of verifying the public key certificates.

In this paper, we proposed two new IBSDDS schemes in standard model where, for one query, the receiver can only access one file, instead of all files. Furthermore, the access permission can be made by the owner, instead of the trusted party. Notably, our schemes are secure against the collusion attacks. The first scheme is CPA secure, while the second one is CCA secure.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES:

[1] H. Hacig¨um¨us, B. R. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model," in Proceedings: SIGMOD Conference - SIGMOD'02 (M. J. Franklin, B. Moon, and A. Ailamaki, eds.), vol. 2002, (Madison, Wisconsin, USA), pp. 216–227, ACM, Jun. 2002.

[2] L. Bouganim and P. Pucheral, "Chip-secured data access: Confidential data on untrusted servers," in Proc. International Conference on Very Large Data Bases - VLDB'02, (Hong Kong, China), pp. 131– 142, Morgan Kaufmann, Aug. 2002.

[3] U. Maheshwari, R. Vingralek, and W. Shapiro, "How to build a trusted database system on untrusted storage," in Proc. Symposium on Operating System Design and Implementation - OSDI'00, (San Diego, California, USA), pp. 135–150, USENIX, Oct. 2000.

[4] A. Ivan and Y. Dodis, "Proxy cryptography revisited," in Proc. Network and Distributed System Security Symposium - NDSS'03, (San Diego, California, USA), pp. 1–20, The Internet Society, Feb. 2003.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Network and Distributed System Security Symposium - NDSS'05, (San Diego, California, USA), pp. 1–15, The Internet Society, Feb. 2005.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Transactions on Information and System Security, vol. 9, no. 1, pp. 1–30, 2006.

[7] S. D. C. di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi, and P. Samarati, "Effficient and private access to outsourced data," in Proc. International Conference on Distributed Computing Systems - ICDCS'11, (Minneapolis, Minnesota, USA), pp. 710–719, IEEE, Jun. 2011.

[8] H.-Y. Lin and W.-G. Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding," IEEE Transactions on Parallel and Distributed Systems, Digital Object Indentifier 10.1109/TPDS.2011.252 2012.

[9] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. Advances in Cryptology - ASIACRYPT'08 (J. Pieprzyk, ed.), vol. 5350 of Lecture Notes in Computer Science, (Melbourne, Australia), pp. 90–107, Springer, Dec. 2008.

[10] A. Juels and B. S. K. Jr., "PORs: Proofs of retrievability for large files," in Proceedings: ACM Conference on Computer and Communications Security - CCS'07 (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria, Virginia, USA), pp. 584–597, ACM, Oct. 2007.