ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2023-5.384 ResearchBib IF: 8.848 / 2023

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-3, ISSUE-6

EFFICIENT AND SECURE STORAGE OPERATIONS FOR MOBILE CLOUD COMPUTING

Laziz Shirinov

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Email: shirinovlaziz05@gmail.com

Phone: +998 99 876 66 17

Abstract: *This paper presents a holistic security framework for securing data storage in the public cloud, with a focus on lightweight wireless data storage and retrieval devices without exposing the data content to cloud service providers.*

Keywords: *secure, mobile, cloud computing, Privacy Preserving Cipher Policy Attribute-Based Encryption, Attribute Based Data Storage*

ЭФФЕКТИВНЫЕ И БЕЗОПАСНЫЕ ОПЕРАЦИИ ХРАНЕНИЯ ДАННЫХ ДЛЯ МОБИЛЬНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Аннотация: *в данной статье представлена целостная система безопасности для обеспечения безопасности хранения данных в общедоступном облаке с акцентом на легкие беспроводные устройства хранения и извлечения данных без предоставления содержимого данных поставщикам облачных услуг.*

Ключевые слова: *безопасность, мобильные устройства, облачные вычисления, Политика шифрования с сохранением конфиденциальности, Шифрование на основе атрибутов, Хранение данных на основе атрибутов*

MOBIL BULUTLI HISOBLASH UCHUN SAMARALI VA XAVFSIZ MA'LUMOTLARNI SAQLASH OPERATSIYALARI

Annotatsiya: *ushbu maqolada bulutli provayderlarga ma'lumotlar tarkibini taqdim etmasdan, simsiz ma'lumotlarni saqlash va olish qurilmalariga e'tibor qaratgan holda ommaviy bulutda ma'lumotlarni saqlash xavfsizligini ta'minlash uchun yaxlit xavfsizlik tizimi keltirilgan.*

Kalit so'zlar: *xavfsizlik, mobil qurilmalar, bulutli hisoblash, maxfiylikni saqlaydigan shifrlash siyosati, atributlarga asoslangan shifrlash, atributlarga asoslangan ma'lumotlarni saqlash.*

Introduction

To achieve this goal, consider two parameters:

1) Preserve cipher confidentiality, policy based on encryption parameters Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE)

Using PP-CP-ABE, lightweight devices can securely outsource heavy encryption and decoding operations when transmitting data to a cloud service provider without revealing the content of the data and the security keys used.

2) Attribute Based Data Storage (ABDS) system as a cryptographic access control mechanism.

Feature, ABDS minimizes the load of cloud services by reducing communication costs for data management.

Research results

The CP-ABE structure allows multiple access and encryption parameters to be assigned to each user. Multiple users can have common parameters that allow the encrypting device to define data access policy by composing multiple parameters using logical operators such as “AND”, “OR”, etc. To decrypt a message, the user handle parameters must satisfy the access policy. This unique feature of CP-ABE makes it attractive to store data in cloud services that require efficient data access and management for a large number of users.

With the rapid development of wireless communication technologies, the mobile cloud has become the emergence of a cloud service model [1], in which mobile devices and sensors are used as information collection and processing nodes for the cloud infrastructure.

With CP-ABE, the new challenge is how to incorporate wireless mobile devices, especially lightweight devices such as cell phones and sensors, into the cloud system.

This new problem arises because CP-ABE schemes always require, intensive computational resources and decoding and, encryption algorithms.

To solve this problem, an effective solution is to outsource the heavy encryption and decoding computations without exposing sensitive data contents or keys to cloud service providers.

Another research problem is how to share encrypted data with a large number of users, in which the data sharing group may change frequently. For example, when a user revokes access to a file, he/she has no access rights to any future updates to the file, i.e., the local copy (if it exists) will become out of date. To do this, the updated data must be encrypted with a new encryption key.

In addition, the third research task is how to upload/download updated encrypted data stored in the cloud of the system. For example, when some data fields from an encrypted database are changed, the encrypted data must be downloaded from the cloud and then decrypted. Once the update is complete, the files must be re-encrypted and sent to the cloud service. Frequent download/upload operations will cause huge overhead on the limited resources of wireless devices. Thus, it is desirable to design secure and efficient management schemes to balance the transmission and storage operational overhead of managing encrypted data [2].

Using PP-CP-ABE, users can securely outsource computation, CP-ABE intensive encryption, and decryption operations to the cloud without exposing data contents and secret keys. In this way, lightweight devices with limited computing resources can access and manage data stored in the cloud data storage. Moreover, ABDS is suitable for mobile computing to balance communication and storage, and thus reduces the cost of data management operations (such as downloads, updates, etc.) for both mobile cloud nodes and storage service providers.

Systems And Models

Table 1. Designations

Acronym	Descriptions
DO	Data Owner
ESP	Encryption Service Provider
DSP	Decryption Service Provider
SSP	Storage Service Provide
T.A.	Trust Authority
T	Access Policy Tree

System model:

1) Data must be encrypted before being sent to the Storage Service Provider (SSP);

2) The Encryption Service Provider (ESP) provides encryption to the data owner without knowing the actual data encryption key (DEK);

3) The decryption service provider (DSP) provides decryption of user data without knowing the content of the data;

4) Even the collusion of ESP, DSP and SSP would not allow access to the user's data content.

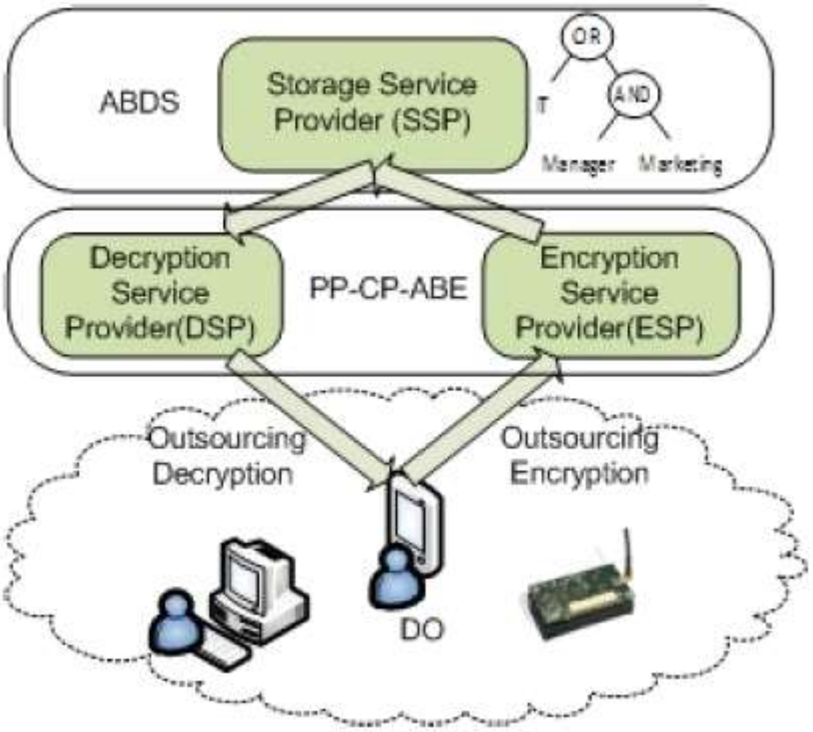
ABDS
Storage Service Provider (SSP)
OR
T
AND
Manager
Marketing
Decryption Service Provider(DSP)
PP-CP-ABE
Encryption Service Provider(ESP)
Outsourcing Decryption
Outsourcing Encryption
DO

Fig.1. SSP, ESP, and DSP form the main components of the proposed system

As shown in Figure 1, SSP, ESP, and DSP form the main components of the proposed system. ESP and DSP provide PP-CP-ABE services and SSP, such as Amazon S3, provides storage services. In particular, more powerful PCs and mobile phones can act as a proxy for communication between sensors that collect information.

Attack model

We assume that the symmetric encryption algorithm and one-way hash function used in this work are secure and the discrete logarithm (DL) problem on both groups $G_0 G_0$ and $G_1 G_1$ complex. In addition, the TA is responsible for distributing cryptographic keys in a highly secure and reliable manner. Consider cloud service providers who are honest but curious. In other words, service providers will work according to the proposed protocols and return correct computational results. However, service providers will try to find out as much important information as possible (for example, personal data, keys, etc.) and may possibly collude with attackers. The attackers' goal is to identify data in the cloud without the permission of DOs. Multiple attackers may join forces to carry out an attack, they may attempt to decrypt the ciphertext and compromise decryption keys that they do not have access to. An example of such an attack would be collusion [3].

In particular, attackers can break Forward Secrecy, which is defined as follows: after a user revokes access to a file, he/she can have a local copy of the file, however, if access is revoked the user should not receive any future updates for it file. While data integrity and findability in the cloud are also important security requirements, these points are not addressed in this paper.

Access Policy Tree

This section briefly describes the Access Policy Tree model used in PP-CP-ABE. This tree consists of leaf nodes and internal nodes. Each leaf node represents an attribute, and each internal node represents a logical element, such as “AND”, “OR”, etc.

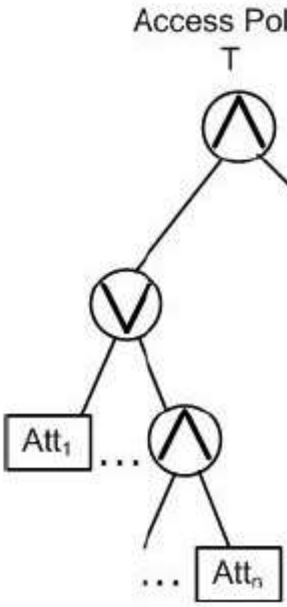

Fig. 2. Access Policy

Several functions and conditions are defined as follows to make it easier to present our solutions:

- *parent(x):* returns the parent node of node *x*;
- *att(x)* denotes the parameter associated with leaf node x in the data access tree;
- *T* consists of a set of leaf nodes (i.e. parameters) and internal nodes (logical gates) and defines a data access policy, that is, if the user owns a set of parameters that satisfy the logical operations of the tree up to the root, he can access the data secured by *T*. The user has private keys corresponding to a set of characteristics (parameters). AND and OR are the most commonly used logic gates.
- *numx* is the number of child nodes. The child node of node *x* is identified by integer *index(y)* from 1 to *numx*
- Threshold value *kx=numx-1* where *x* is AND and *kx = 0* where *x* is OR node. *kx* is used as the degree polynomial of node x using a threshold division scheme.

Conclusion

Finally, a holistic security framework for cloud storage services is proposed to enable data governance in the public cloud. Specifically, our solution allows lightweight wireless devices to securely store and recover their data in the public cloud at minimal cost. To this end, the Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) scheme was proposed to protect users' encrypted data. Using PP-CP-ABE, lightweight devices can securely outsource intensive encryption and decryption operations to cloud service providers without revealing the data content and security keys used. In addition, Attribute Based Data Storage (ABDS) has been proposed as a cryptographic access control mechanism. ABDS is optimal in terms of minimizing computation, storage, and communication overheads. Feature, ABDS minimizes the costs of cloud service providers, as well as communication costs for data management. Performance evaluations demonstrate the security and efficiency of the solution in terms of computation, transmission, and storage.

Currently, PP-CP-ABE is based on the BSW CP-ABE scheme, the disadvantage of which is the linear increase in the size of the ciphertext. The CP-ABE scheme, which has a constant ciphertext size, was considered and privacy-preserving outsourcing of the new CP-ABE scheme was proposed.

List of used literature

1. G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur., 9(1):1-30, 2006

2. J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute - based encryption. In SP ’07: Proceedings of the 2007 IEEE Symposium on Security and Privacy, pages 321-334, Washington, DC, USA, 2007. IEEE Computer Society.

3. D. Boneh, X. Boyen, and E.J. Goh. Hierarchical identity-based encryption with constant size ciphertext. Advances in Cryptology- EUROCRYPT 2005, pages 440-456, 2005.