JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3952-3956
https://publishoa.com
ISSN: 1309-3452

A Light Weight Secure Data Sharing Scheme for Mobile Cloud Computing

[1]N. Sujata Kumari, [2]K.Divya Charitha Yadav, [3]Devu Asha, [4]M.Deepika.

[1]Assistant Professor, Department of CSE, Sridevi Women's Engineering College, Hyderabad, T.S,. India.

[2,3,4]UG Student, Department of CSE, Sridevi Women's Engineering College, Hyderabad, T.S,. India.

E-mail:[1]nsujata02@gmail.com , [2]charithadivya22@gmail.com , [3]ashadevu2001@gmail.com , [4]deeparamesh369@gmail.com .

Received 2022 March 15; **Revised** 2022 April 20; **Accepted** 2022 May 10.

Abstract

Background: With the rise of cloud computing. mobile devices may now store and access personal data at any time and from any location. As a result, the mobile cloud's data security issue only gets worse, impeding the technology's ability to advance. For the purpose of enhancing cloud security, extensive research has been done. The majority of them, nonetheless, are not appropriate for mobile clouds because of the constrained computational capabilities of mobile devices. Mobile cloud applications have a huge need for solutions with reduced computational overhead. For cloud computing on mobile devices, we suggest a lightweight data sharing scheme (LDSS). It adopts the CP-ABE access control technology, which is utilized in a typical cloud environment but modifies the access control tree's structure to make it appropriate for mobile cloud environments. Through the use of LDSS, a significant chunk of the computationally demanding CP-ABE access control tree transformation is transferred from mobile devices to external proxy servers in order to lower the cost of user revocation. To solve the tricky problem of lazy revocation in program based CP-ABE systems, it includes attribute description fields.

Objective: An approach that re-examines the concept of public key cryptography is attribute-based encryption, which came about somewhat later. The secret key of a person and the cypher text are established based on attributes in attribute-based encryption, also known as ABE. A symmetric key can only decrypt a particular cipher-text using an ABE if the cipher-attributes text's match those of the person's key. Both keys and cipher-texts are labelled with units of descriptive attributes. Because fewer keys are required, the encryption and decryption processes are quicker as a result.

Conclusion: Users can safely share data via the cloud between one other. In order to provide effective access control over cypher text, we build an algorithm called LDSS-CP-ABE based on the Attribute-Based Encryption (ABE) approach. For encryption and decryption processes, we use proxy servers. The computational cost on client-side mobile devices is significantly reduced by our technique, which conducts computationally complex processes in ABE on proxy servers. With the cost down, performance has gone up.

Keywords-Attribute-Based Encryption, LDSS(ABE), Trusted Authority, Cipher Text, Mobile Cloud Computing (MCC) Providers of encryption services and decryption services (DSP).

1. Introduction

When employing traditional hardware for the majority of tasks, cloud computing refers to thestorage and online access of data. Over 50% of IT firms have shifted their operations to the cloud. The next trend that is emerging is data sharing over the cloud Daily life generates an increasing amount of data, and standard hardware's limited storage capacity makes it impossible to store all of that data Therefore, moving the data to the cloud, where the user can have unlimited storage, is necessary. The majority of us are most worried about the security of that data.

Utilization forfeits the ownership of the data after uploading it to the cloud. Due to the sensitivity of personal data files, data owners are given the option of sharing their files with the whole public or only certain data users. So many data owners are really concerned about the protection of their customers' sensitive personal information. When anyone uploads data to the cloud, they are putting that data in a location where they have no control over its monitoring. In

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3952-3956
https://publishoa.com
ISSN: 1309-3452
addition, when someone uploads: data to the cloud, the cloud service provider has the ability to track each user's password in order to access the encrypted data, which is a hassle. Data should be encrypted before being uploaded to the cloud, which can keep it secure from everyone, in order to overcome this problem. The data encryption component now poses some new challenges, such as the need to develop an effective encryption method that makes it difficult for hackers to access or decrypt encrypted data. The second major issue is how long encryption takes. Traditional hardware with extensive configuration can quickly encrypt data, however, limited resource devices struggle with this issue. Their encryption and decryption processes take longer. Therefore, it is necessary to offer an effective cryptosystem that can operate uniformly or differently on every device.

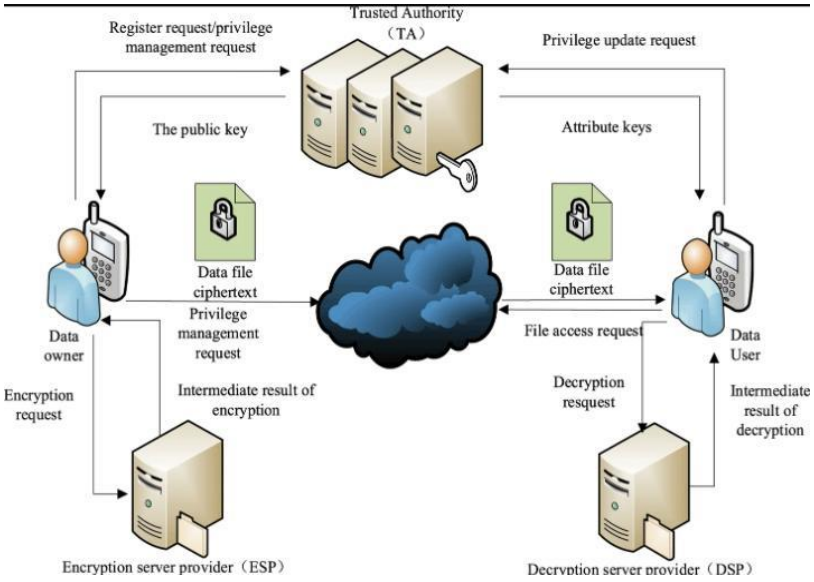
In mobile cloud computing, applications are delivered to mobile devices using the cloud. With the use of development tools, these mobile apps can be remotely delivered. Cloud services enable speedy development or revision of mobile cloud applications. They can be sent to a wide range of gadgets with various operating systems, computer capabilities, and data storage. Users can now use programs that might otherwise be inaccessible. The ultimate objective of MCC is to make it possible for rich mobile apps to be executed on a variety of mobile devices while providing a rich user experience offers business prospects to both cloud service providers and mobile network operators. MCC is more fully described as "a rich mobile computing technology that leverages unified elastic resources of various clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as you-use principle" (MCC).

2. RELATED WORK

Sahai and Waters suggest attribute-based encryption (ABE) Attribute-based encryption (ABE), which was very recently invented, re-examines the idea of public key cryptography. ABE, or attribute-based encryption, is a form of public-key encryption in which attributes are used to establish the connection between a user's private key and the cypher text. A symmetric key can only use an ABE to decrypt a certain cipher-text if the text's cipher-attributes match those of the key's owner. Keys and cipher-texts both have units of descriptive qualities labelled on them. Because fewer keys are required, encryption and decryption are completed more quickly.

3. SYSTEM ARCHITECTURE

An Easy-to-Use Secure Data Sharing Protocol for Mobile Cloud Computing. It adopts the CP ABE access control technology, which is utilized in a typical cloud environment, but modifies the access control tree's structure to make it appropriate for mobile cloud environments.



LDSS architecture mainly has six components:

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3952-3956
https://publishoa.com
ISSN: 1309-3452

Data owner: DO establishes the access control policies and uploads data to the mobile Cloud and shares it with their pals. Its duties include creating and encrypting shared data, defining access mechanisms, and breaking down encrypted data into blocks

Data user: The data owner uploads the data files, which the data user then retrieves from the mobile cloud Only users with access rights to the relevant data files are able to access the files.

Trusted authority: The creation of public and private keys, as well as providing attribute keys to users, is the responsibility of TA. Users can share and access data via this approach without being aware of the encryption and decryption processes. Only at minimal quantity of keys are securely transferred between users by trusted authority.

Encryption service provider: The data encryption procedure provided by ESP for DO is to encrypt the data files that the data owner uploads. Because encryption requires a lot of computation, it places a heavy burden on mobile users. To reduce client-side overheating, encryption service providers are used on mobile devices.

Decryption service provider: Data decryption activities are provided by DSP for DU, and it also decrypts the data files that the data user downloads. Due to the computationally demanding nature of decryption, severe burdens are placed on mobile users in order to reduce the load on client-side mobile devices.

Cloud service provider: Data for DO is kept by Cloud service Provider. Although it may sneak a peek at data that DO has saved in the cloud, it faithfully carries out the activities that DO requests. With the growth of cloud computing and the popularity ofsmart mobile devices, people are progressively adjusting to a new era of data sharing model in which the data is stored on the cloud and the storing and retrieving from the cloud is done by mobile devices.

4. PROPOSED WORK

Mobile devices in a cloud environment with security in a minimally invasive way. They should have an easy-to-understand revocation policy Using a secret key should ensure the security of both encrypted and decrypted data. The approved users with access privileges should be the only ones who share the file. The typical cryptographic algorithm's overhead should be reduced, and research into low overhead security solutions should be possible.

In order to provide effective access control over ciphertext, we build an algorithm called LDSS-CP ABE based on the Attribute-Based Encryption (ABE) approach. For encryption and decryption activities, a proxy server is used. Our method considerably reduces the computational burden on client-side mobile devices by performing computationally complex ABE procedures on proxy servers. A version attribute is also introduced to the access structure in LDSS, CP-ABE, to guarantee data privacy. It is possible to send the decryption key to the proxy servers securely thanks to a modified format for it. To reduce the revocation overhead for addressing the user revocation problem, we introduce lazy re-encryption and description fields of attributes. In the end, we put an LDSS-based prototype data-sharing architecture into use.

Proposed system algorithm

Step1: Start

Step2: Accept the user's data.

Step 3: The user's formats are used to acquire the attributes of the data by attribute-based encryption.

Step 4: A Random Key is constructed with the aid of these Attributes, and the sort of data needed for encryption is then acquired.

Steps 5: The data is divided into an equal number of blocks and an N x N matrix is created based on these BRE algorithmic building components.

Step 6: A pool of threads will be generated based on the number of blocks.

Step 7: Use a multi-core system to run the threads to quickly produce encrypted data length of time.

Step 8: To open the encrypted file that is kept in the cloud, a secret key is created.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3952-3956
https://publishoa.com
ISSN: 1309-3452
Step 9: The user receives the secret key via email or a mobile device from the authorized user. The encrypted file will be decrypted using this key.

Step 10: Using the key, the selected file will be decrypted in its original format.

Step 11: Stop

5. MODULE DESCRIPTION

Data Owner: The algorithm Setup O is executed by TA after the data owner (DO) registers to generate a master key MK and a public key PK. MK is kept on TA while PK is assigned to DO. DO creates its own attribute set and gives its contact attributes. All of these details will TA and the cloud are sent. The data is received and stored by TA and the cloud. FILE UPLOAD shares it with friends by uploading data to the mobile cloud. The access control is determined by DO, policies, Data is sent by DO to the cloud. Data must be encrypted before uploading since the cloud is unreliable.

Data User: DU logs into the system and requests permission from TA. Attribute keys (SK) in the authorization request are ones that DU already possesses. The authorization request is accepted by TA, who also validates it and generates attribute keys (SK) for DU. DU submits an inquiry to the cloud for data. After receiving the request, Cloud determines whether the DU complies with the access requirements. Required. DU is provided with the cypher text, which also includes the cypher text of data files. The symmetric key's text. With the aid of DSP, DU decrypts the symmetric key's cypher text. The encrypted text of data files is decrypted by DU using the symmetric key.

Trusted Authority: The task of creating public and private keys as well as distributing attribute keys to users falls under the purview of the Trusted Authority (TA). Users can share and access data via this approach without being aware of the encryption and decryption processes. Only transfers are made viaTA. Keys are securely shared (in limited amounts) between users.

Additionally, as data users may access data at any time and require TA to update attribute keys, it is required that TA be available online at all times.

Cloud Server Provider: The data for DO are kept in CSP. While it might sneak a peek at data that DO has saved in the cloud, it faithfully carries out the activities that DO requests. The cloud receives a request for data from DU. After receiving the request, Cloud determines whether the DU satisfies the access criteria. DU cannot if the request does not fulfil the condition, it rejects it, if it does, it sends the cypher text to DU.

6. CONCLUSION

Numerous studies on cloud access control in recent years have relied on an attribute-based encryption. technique (ABE). Traditional ABE, however, is not appropriate for mobile cloud since it requires a lot of computing, and mobile devices only have a few resources. That is paper, we suggest LDSS deal with this problem. It unveils a brand-new LDSS-CP-ABE algorithm. to shift the majority of the processing load from mobile devices to proxy servers, enabling the issue of mobile cloud data sharing in a secure manner. The experimental findings demonstrate that LDSS can protect data privacy in mobile cloud environments while lowering user overhead. There is potential to develop novel strategies in the future to guarantee data integrity. There can also be research. done on how to retrieve cipher text in order to maximize the possibilities of mobile clouds over current data-sharing plans.

References

1. Gentry C, Halevi S. Implementing gentry's fully homomorphic encryption scheme. in Advances in Cryptology-EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129 148, 2011...
2. Braker ski Z. Vaikuntanathan V. Efficient fully homomorphic encryption from standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science California, USA: IEEE press, pp. 97-106, Oct. 2011.
3. Qihua Wang Hongxialin. "Data leakage mitigation for access control in collaborationclouds" the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp. 103-122. Jun. 2011.
4. Adam Skillen and Mohanumad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices, the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3952-3956
https://publishoa.com
ISSN: 1309-3452

5. Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA:ACM pp. 55-66, 2009.
6. Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage.in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation Volume 4. USENIX Association, pp. 10-12, 2000.
7. Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523 528, 2013.
8. Crampton J. Martin K. Wild P. On key assignment for hierarchical access control.in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.
9. Shi E, Bethen court J. Chan T HH, et al. Multi dimensional range query over encrypted data in Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350-364.