International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Attribute-Based Encryption Schemes for Users and Cloud Server in Green Cloud Computing : Cost-Efficient Outsourced Decryption

G. Kalyan Kumar[1], A. Murali Mohan Kumar[2]
MCA Student[1], Assistant. Professor[2]
Mother Theresa Institute of Computer Applications, Palamaner, S. V. University, Andhra Pradesh, India

Article Info

Publication Issue :
Volume 8, Issue 6
November-December-2022

Page Number : 82-89

Article History
Accepted: 01 Nov 2022
Published: 05 Nov 2022

ABSTRACT

The green cloud networks assist in lowering user costs by lowering the cost of decryption and preventing the leak of private information. However, this approach is ineffective for cloud servers in green cloud networks. In order to lower the overall overhead of the cloud server, we have suggested account recyclable usage of resources. This is a novel and secure solution. Another strategy we've suggested in our schemes is outsourcing the attribute-based encryption (ABE) scheme's decryption to a cloud server. However, the cloud server must repeatedly perform the same ciphertext decryption for various users who adhere to the same access policy. Therefore, in contrast to the current ABE-OD methods, our cloud server's overall overhead is unaffected by the number of users that comply with an access policy and request the outsourcing decryption service. Finally, we expand our strategy to an ABE-OD scheme that is RCCA secure.

Keywords : Attribute-Based Encryption, Outsourced Decryption, Bilinear Maps, Green Cloud Computing

I. INTRODUCTION

The on-demand availability of computer system resources, in particular data storage and processing power, without direct active supervision by the user is known as cloud computing. The phrase is typically used to describe data centres that are accessible to several people online. Functions from central servers are frequently spread over several locations by large clouds, which are common nowadays. It could be referred to as an edge server if the connection to the user is somewhat near.

People nowadays have become accustomed to storing their photos, contacts, and other material on cloud servers as a result of the growth of cloud computing. Meanwhile, individuals or businesses use powerful computational power. Numerous cutting-edge applications are being developed for cloud computing to make people's daily lives more convenient. On the one hand, cloud users/terminals are solely seen as "devices" of input and output, but on the other hand, they can save money by outsourcing their data storage or processing to the cloud servers. However, because a user cannot manage their own data, protecting user privacy is a major concern in both

academics and business. Thus, a series of security concerns are taken into account, including keyword searching [5], outsourcing verification [4], outsourcing computation [3], and remotely auditing [1], among othersoutside malicious attack and multi-tenancy. The stored information of integrity is conserved for data integrity in the cloud system. The unauthorized users should not be accessed misappropriate or vary of data. Data integrity and reliability of data are faithful to preserve by the cloud computing provider. . From the user's standpoint, data confidentiality is also essential, therefore they keep their private or confidential data on the cloud. In order to guarantee access control procedures and authentication, data confidentiality is observed. A rise in cloud authentication and data secrecy might advance the faith in cloud computing. Therefore, from the user's perspective, security, integrity, privacy, and confidentiality should be fundamental requirements for data storage in the cloud. Green et al. used the substantial computing capacity of a cloud server or several proxies to lower the calculation cost of the ABE's decryption technique. The GHW approach was the idea of ABE with outsourced decryption (ABE-OD). A user can finish a lot of work in their scheme by paying a little fee to decode ciphertexts using a cloud server. As a result of computing a delegated transformation key and the original ciphertexts, the cloud server first produces altered ciphertexts. The user may then acquire the associated plaintext by computing a "decryption" method. The ABE-OD method used throughout the outsourcing process was unable to divulge any information regarding the plaintext due to security concerns. They didn't address two other problems in their ABE-OD plan, though. One is that there is no system in place to guarantee the accuracy of the altered ciphertexts.

II. Related works

Identity-based auditing with efficient and safe sensitive information concealing for shared cloud data.
The advent of cloud computing arouses the flourish of data sharing, promoting the development of research, especially in the fields of data analysis, artificial intelligence, etc. In order to address sensitive information hiding, auditing shared data efficiently and malicious manager preventing, we propose an identity-based auditing scheme for shared cloud data with a secure mechanism to hide sensitive information. This scheme provides a solution that allows users to share plaintext with researchers and keeps sensitive information invisible to the cloud and researchers at the same time.

Analysis of a cloud server-based outsourced verification mechanism for mobile payments and its advancement
Today, using mobile devices like an iPad or a smart phone to make payments is becoming one of the most popular methods utilised by business and financial organisations. However, due to the mobile devices' constrained capacity, large-scale computing cannot be done on them. Therefore, it is preferable to outsource securely some mobile payment processing to an unreliable cloud server.

attribute-based encryption with constant ciphertext length verified outsourced decryption
An effective cryptographic technique for ensuring the security of user data is attribute-based encryption. The practical use of ABE is constrained by the decryption expense and ciphertext size. For the majority of current ABE schemes, the size of the ciphertexts and the decryption cost increase linearly with the complexity of the access structure. For devices with limited computational power and storage capacity, this is undesirable. Decryption overhead may be reduced by the user by using outsourced decryption, which enables the user to outsource a significant portion of their decryption activities to the cloud service provider.

III. Methodology

Proposed system:

We suggested using green cloud computing to reuse resources and consume less energy overall, provided that the same activity could be completed with the same level of quality. We provide a fresh method for contracting out the decryption of the ABE scheme. In addition to lowering the calculation cost for user decryption when numerous users need the same cypher text decrypted, our technique is significantly more effective for the cloud server than the GHW method.

Advantages: By outsourcing their data storage, cloud users and terminals can reduce their costs.

• Lowers overall energy use.

• Powerful computational ability..

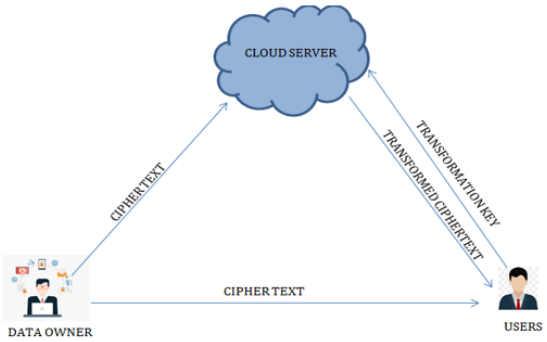


Figure 1 : block diagram

IV. Implementation

This project is implemented by using below mentionedalgorithm called Attribute-Based Encryption

Attribute-Based Encryption

This encryption method used the third side. The third party, the so-called trusted centre, as well as the data owner, the user, get the data. The trusted center's job is to produce encryption and decryption keys for data owners and recipients. A comprehensive set of pre-defined properties is used to produce both public and master keys. The attribute is added to the set and new open and master keys are produced whenever a user with a new attribute is introduced to the system. The data's owner encrypts it using the public key and a few other properties. The person that gets the data can use its own private key to decode it. The user is given a reliable centre via this key.Then it verifies that the characteristics of the user's private key and the characteristics of the encrypted data match. The user can decrypt the data using the private key if the number of matching characteristics reaches a set threshold, d. Data cannot be decrypted otherwise.

Then it checks to see if the encrypted data's attributes match those of the user's private key. If there are enough matching qualities, the user can use the private key to decode the data, d. Otherwise, data cannot be decrypted.

structure descriptions Access

Let P1, P2,..., Dn represent a collection of qualities. If the following conditions hold for a set A 2 P1, P2,..., Pn: B, C: B A, B C C A. A set (a monotone set) A non-empty subsets P1, P2,..., Pn, i.e., A 2P 1, P2,..., Pn, is what is referred to as a "structure access" or "monotone structure access". Users are given access to the data if they possess a certain set of traits that are listed in the A is authorised sets. The sets of characteristics that do not belong to the A are unapproved sets. It is significant to remember that restricted monotone access structure is the employment of encryption techniques based on the characteristics in their original form. In the case of non-monotonic structures, an extension of the technique was presented in 2007.

The algorithm's description

E: G1xG2G2 is a bilinear mapping if G1, G2 are a bilinear group of order p (p - prime), and g is the generating group G1.

creating private keys

The private key generation algorithm receives a collection of user attributes as input, and produces the user's private key as its output. For each user U, the trusted centre creates a private key. User qualities make up AU. A polynomial of degree d-1 is chosen at random such that q(0)=y. D=Di=g(i))/(ti)iAU is the private key.

The threshold value is d.

The overall plan is divided into four sections, each with its own algorithm.

Encryption

The message that has to be encrypted, a set of characteristics whose owner will be able to decrypt the data, and a randomly chosen number are fed into the encryption method, and the result of the algorithm is encrypted data. Using a set of characteristics ACT and a random integer s Zq, owner data encrypt a message M G2: CT=(ACT, E=MYs=e(g,g)ys,Ei=gtisiAU).

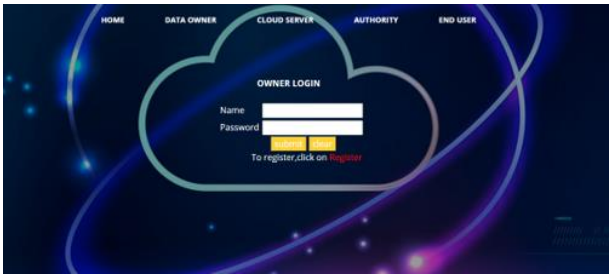
Dencryption

The decryption algorithm receives a collection of user characteristics AU and the encrypted data as inputs, and the decrypted message is the algorithm's output. If |AUACT|d, then e(Ei,Di)=e(g,g)q(i)s,Ys=e(g,g)q(0)s=e(g,g)ys are computed using the values of the iAUACT chosen d attributes. M=E/Ys is the original message. The strategy for the secret sharing principle generates private keys. In order to avoid attacks caused by users working together, the new private key cannot be created by combining several existing private keys.

V. Results and Discussion

The following images will visually depict the process of our project.

Home page: In this home page we can see the logo designing of our website.

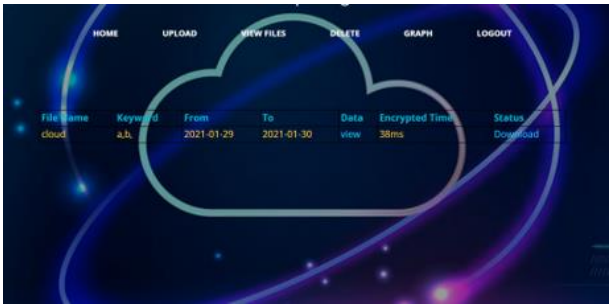


Data Owner Login:

Date Owner Registration: Date owner can register here..

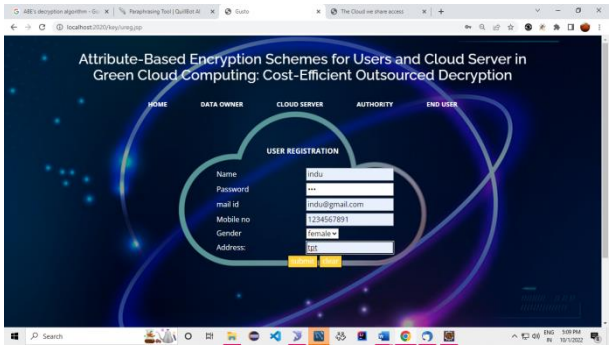
DataOwner home: Data owner Home page

Upload files:data owner can upload files here.

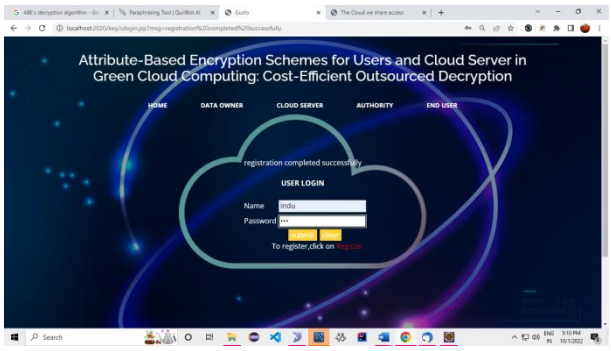


View Files:data owner can view the uploaded files

View:CS can view the uploaded files by the data owner



End User:end user registration



Css login: CSS login page

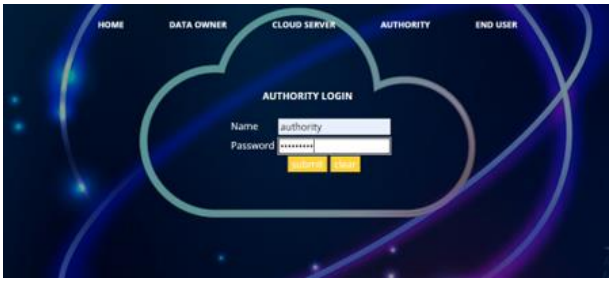
CSS **Home:**Css home page

Data owners: View Data owners

View Files:Owner can view the files

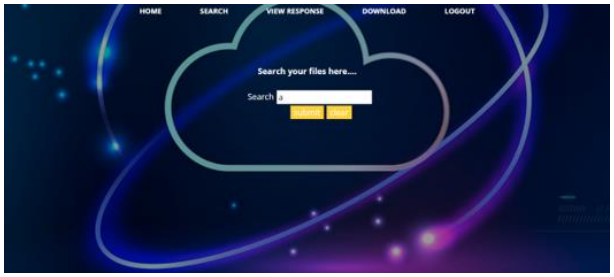
View users:users list

View users req: Data owner can view the req

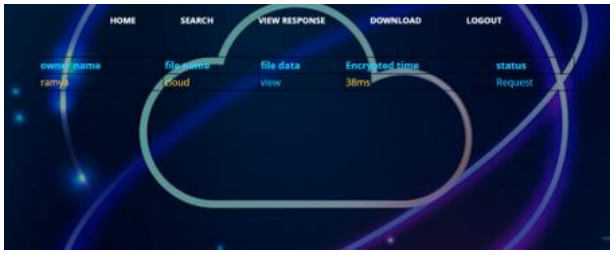


Authority login: Authority login page

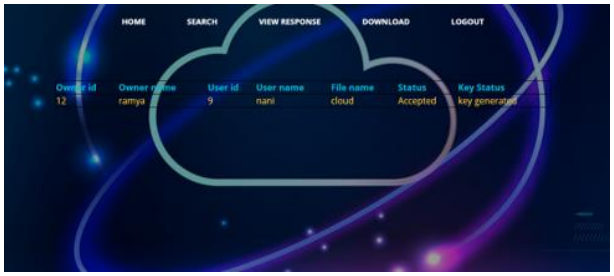
Authority Home : Authority home page



Search files: Search files here



View Response:view response



Download: Downloading the files

Enter the key

Download: Download the file

Data owner login page: This the login page for data owners with their own credentials.

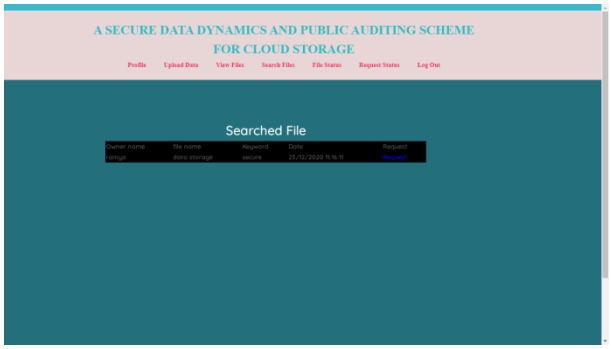
Registration page: This is a registration page.

Owner home page: This is home page of data owners, after login is completed data owners can view this page.

Upload data: Here the data owners can upload the data into cloud.

View files: This is the page contains all files, the data owners can view all the files here.

Search files: With the help of this page we can search the data.



File status: Here we can see the status of files.

Request status: This is the page where we can see the status of requests.

Download: Here we can download the files and we can see the data.

VI. Conclusion

A secure auditing method is to store the data on the cloud in a secure manner. The prospective take the AES-256 algorithm, RSA-15360, and SHA-512 algorithm to assure that TPA cannot knowledge about data toward the robustness auditing scheme. We propose a data dynamics operation with mostly deal insertion, deletion and, modification.

VII. REFERENCES

[1]. The global cloud computing market report 2019.

[2]. J Agarkhed, R Ashalatha-"An efficient auditing scheme for data storage security in cloud".2017[ICCPCT].

[3]. SK Saroj, G Noida, SKChauhan, AK Sharma "Threshold cryptography based data security in cloud computing".S Vats-2015. [4] C. C. Aggarwal, "Opinion mining and sentiment analysis," in Machine Learning for Text. Springer, 2018, pp. 413–434.

[4]. Mell, Peter, and Tim Grance.The NIST definition of cloud computing (2011).

[5]. SwapnaliMorea, SangitaChaudhari,"Third Party Public Auditing Scheme for Cloud Storage ",International Journal of Prpcedia Computer Science ,Volume 79,pp.69-76,2016.

[6]. Zissis, Dimitrios, and DimitriosLekkas. Addressing cloud computing security issues. Future Generation computer systems 28.3(2012):583-592.

[7]. B.L Adokshaja, and S.J.Saritha,"Third Party Public Auditing on Cloud Storage using the Cryptographic Algorithm"ICECDS-2017.

[8]. Cong Wang, Sherman SM Chow, Qian Wang, KuiRen, and WenjingLou."Privacy Preserving Public Auditing for Secure Cloud Storage.http://eprint.iacr.org/2009/579.pdf.

[9]. Cong Wong, Sherman S M Chow, Qian Wang, KuiRen, and Wen jing Lou."Privacy Preserving Public Auditing for Secure Cloud Storage". IEEE Transactions on Computers, Volume 62, ISSUE 2, February 2013.

[10]. AbhishekMohta, Ravi Kant Sahu, Lalit Kumar. "Robust Data Security for Cloud while using Third Party Auditor". International journal of advanced research in CSE (IJARCSE), Volume 2, Issue 2, February 2012.

Cite this article as :

G. Kalyan Kumar, A. Murali Mohan Kumar, "Attribute-Based Encryption Schemes for Users and Cloud Server in Green Cloud Computing : Cost-Efficient Outsourced Decryption", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 82-89, November-December 2022.

Journal URL : https://ijsrcseit.com/CSEIT22864