JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Securing Data in Green Cloud Computing Using Attribute based Encryption

Ms. M.Dharani Jyothi (M.C.A). Rajeev Gandhi Memorial college Of Engineering and Technology, Nandyal

***Mr.M.Vinay Kumar (M-Tech), Assistant professor. Rajeev Gandhi Memorial college Of Engineering and Technology, Nandyal**

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 utilization 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. So, In contrast to the current ABE-OD Thus, our overall cloud server overhead is unaffected by the amount of users who comply with an access policy and utilize the outsourcing decryption service. Finally, we expand our strategy to an ABE-OD scheme that is RCCA secure.

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

1. INTRODUCTION

1.1 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 centers that are accessible to several people online. Functions from central servers are frequently spread across several locations by large clouds, which are common nowadays. It might be referred to as an edge server if the connection to the user is reasonably close. People today have grown accustomed to storing their photos, contacts, and other material on cloud servers as a result of the advent 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. Clouds are one thing, but Users/terminals are merely seen as "devices" of input and output while using cloud services, although they can save money by outsourcing their data storage or computation to the servers. However, because a user cannot control their own data, protecting user privacy is a major concern in both academia 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 others. The attribute-based encryption (ABE) [6], a fine-grained and flexible scheme for access structure, has emerged as one of the most popular ideas to be investigated in cloud computing, despite the fact that a variety of cryptographic techniques and talents have been proposed. Sahai and Waters' proposed ABE [6], was considered an expanded version of the identity-based encryption (IBE) concept. Other than broadcast encryption, the one-to-many encryption paradigm is effective. ABE schemes have recently been divided into two different categories, key policy ABE (KP-ABE) and ciphertexts-policy ABE (CPABE) [7, 8], in accordance with the deployment of access control policies. The decryption cost of various ABE systems is a significant hurdle, though. Because the complexity of the access policy linearly increases with the user's decryption cost and the length of the ciphertexts. It has grown to be a major barrier for many clouds computing applications, including those for wireless sensors and smartphones.

2. Literature Survey

• **[1] Y. Fan, Y. Liao, F. Li, S. Zhou, G. Zhang. "Identity-based auditing for shared cloud data with efficient and secure sensitive information hiding:** The progress of research, particularly in the areas of data analysis, artificial intelligence, etc., is facilitated by the arrival of cloud computing and the flourishing of data sharing. We provide an identity-based auditing method for shared cloud data with a secure way to hide sensitive information in order to handle sensitive information hiding, efficiently auditing shared data, and preventing malicious managers. With the help of this approach, users can communicate plaintext with researchers while simultaneously keeping sensitive data hidden from both the cloud and the researchers.

[2] Y. Liao, Y. He, F. Li, S. Zhou, Analysis of a mobile payment protocol with outsourced verification in cloud server and the improvement: 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 computing power and storage space, this is undesirable. Decryption overhead can 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.Today, using mobile devices like an iPad or a smart phone to make payments is becoming one of the most popular methods utilized by business and financial organizations. 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.

3. OVERVIEW OF THESYSTEM

3.1 Existing System

In contrast to the currently used ABE-OD methods, our cloud server's total overhead is unaffected by the number of users who comply with an access policy and seek the outsourcing decryption service. The fundamental disadvantage of ABE is that it has linearly increasing processing costs as the complexity of the access policy increases. The fairness between the user and the proxy is disregarded by all current ABE techniques with external decryption.

3.1.1 Disadvantages of Existing System

- Less feature compatibility
- Low accuracy.

3.2 Proposed System

We suggested using green cloud computing to reuse resources and use less energy overall, provided that the same activity could be completed with the same level of quality. We suggest 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 cipher text decrypted, our method is significantly more effective for the cloud server than the GHW method.

3.3 Methodology

User: User must first register on the website before logging in. They look for a necessary file after logging in. If the file is available, details about it will be

displayed. A request to view the data in that specific file will be sent to the cloud server after the file has been displayed. A request to open the file and access the data inside it will be supplied to them through email if the server accepts their request.

Owner of Data: Once the cloud server accepts the registration into the website, Owner can register and login here. After logging in, the user can see and upload files to the cloud Delete the files you don't want. Owners have access to the graphical view of the file information.

Cloud Server: After logging in, the cloud server will examine the owner's registrations, offer acceptance or rejection, and also check for registered users. The cloud server may also view the files that the owners have uploaded and the user's requests for approval or denial. Data is sent to Authority to create a key for data decryption after the request is approved.

Authority: Authority will log in, check for users, review any files that the cloud server has approved, and generate a secret key that will be emailed to the user.

4 Architecture

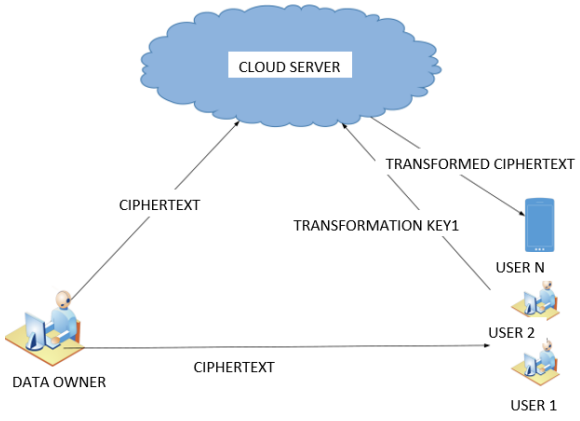


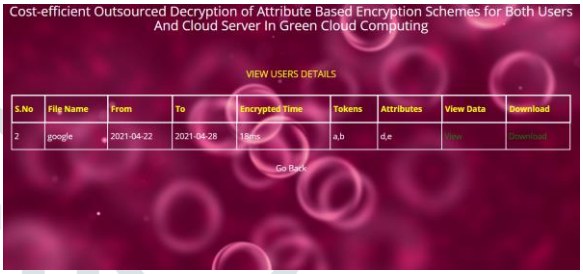
Fig 1: Frame work of proposed method

Above architecture diagram shows three stages of data flow form one module to another module. Data collection, preprocessing, and algorithm training.

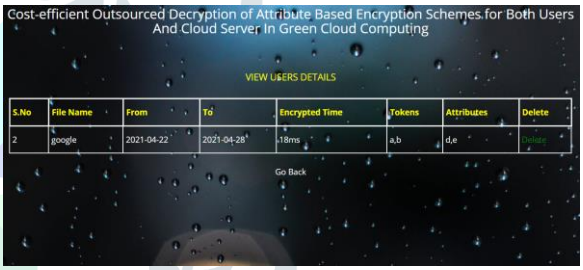
5 RESULTS SCREEN SHOTS

Home Page:

Upload Data:



Data:



Result:

6. CONCLUSION

✓ Key components of green cloud computing are resource reuse and lower overall energy consumption for completing the same work while maintaining service quality. We took into account outsourcing the ABE scheme's decryption in the context of green cloud computing. We propose a new and safe mechanism employed in the ABE-OD schemes to lower the overall overhead of the cloud server when several users satisfying the access policy want their outsourced decryptions for the same ciphertexts. Our strategy can lower both user and cloud server overhead.

Future Enhancement

✓ In addition to lowering the user's computation cost, the cloud server's overhead only requires constant computation cost for all outsourced decryptions of the same ciphertexts. Finally, we expanded our strategy to an ABE-OD scheme with RCCA security.

7. References

[1] C. Yang and J. Ye, "Secure and efficient fine-grained data access control scheme in cloud computing", Journal of High Speed Networks, Vol.21, No.4, pp.259–271, 2015.

[2] X. Chen, J. Li, J. Ma, et al., "New algorithms for secure outsourcing of modular exponentiations", IEEE Transactions on Parallel and Distributed Systems, Vol.25, No.9, pp.2386–2396, 2014.

[3] P. Li, J. Li, Z. Huang, et al., "Privacy-preserving outsourced classification in cloud computing", Cluster Computing, Vol.21, No.1, pp.277–286, 2018.

[4] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions", Future Generation Computer Systems, Vol.79, pp.849–861, 2018.

[5] W. Shen, J. Qin, J. Yu, et al., "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage", IEEE Transactions on Information Forensics and Security, Vol.14, No.2, pp.331–346, 2019.

[6] R. Kaur, I. Chana and J. Bhattacharya J, "Data deduplication techniques for efficient cloud storage management: A systematic review", The Journal of Supercomputing, Vol.74, No.5, pp.2035–2085, 2018.

[7] Cisco, "Cisco global cloud index: Forecast and methodology, 2014–2019",

[8] Cloudsfer, "Migrate & backup your files from any cloud to any cloud",

[9] Y. Liu, S. Xiao, H. Wang, et al., "New provable data transfer from provable data possession and deletion for secure cloud storage", International Journal of Distributed Sensor Networks, Vol.15, No.4, pp.1–12, 2019.

.