International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

Enhanced Secure Data Sharing Over Cloud Using ABE Algorithm

Virangni Gaikwad[1], Ekta Bhosale [2], Ankita Istalkar [3], Rajashri Tapkir[4], Prof. Sachin Patil[5]
[1,2,3,4] Student, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegoan, Savitribai Phule Pune University, Pune, Maharashtra, India
[5] Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegoan, Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT

Cloud Computing provides a convenient way of sharing of data, which brings various benefits for both the society and individuals. Security is becoming a wide necessity in day-to-day life. Data security is the most obliged security of all. The data in our system is opened to high potential risks. Due to many security reasons we adopt diverse methods. Now everyone is being dependent on the cloud platform for security and storage but even it is vulnerable to various threats. The data inside cloud is not well-secured as it can be accessed by anyone who would have our credentials. But there exists a resistance for users to directly outsource the shared data to the cloud server as the data often contains valuable information. So we propose an Enhanced Security to the data using encryption- The ciphertext-policy (CP) attribute-based encryption (ABE) (CP-ABE) and Byte Rotation Algorithm emerging as a promising technology for allowing users to conveniently access data in cloud computing, giving security to outsourced information, while thinking that client is not stressed while transferring their classified information. Moreover, the privacy of users are protected in this scheme. The security and performance analysis shows the scheme is secure, efficient and privacy-preserving.

Keywords: Cloud computing, CP, ABE, Encryption, Decryption, Privacy preserving.

I. INTRODUCTION

Cloud computing has introduced the new method for computing and related problems like data privacy, data security in cloud. It offers development environment, allocation and reallocation of assets when needed, storage and interacting facility. The cloud computing is composed of shared computing resources and services that deliver the resources through which users can access the structures, hardware, applications, and services on request which are independent of locations. It contents the on-demand requests of the user. It simplifies the sharable resources "as-a-service" ideal. For the association, the cloud offers data access to move their data totally. Here comes the assistance of the Cloud Computing i.e. It condenses the total of hardware that could have been used at user completion. As there is no essential for the collection of data at user's end because it is already at some other situation. So as an alternative of buying the complete infrastructure required to run the processes and save bulk of data which you are just renting the assets according to your requirements.

CLOUD computing is rapidly emerging technology and on-demand storage and computing services for customers

Security Issues Within The Cloud:

Organizations which are having low budget can now utilize high computing and storage services without

investing in the infrastructure and maintenance. However, the loss of control over data and computation raises many security concerns for organizations, the wide adaptability of the public cloud. The loss of control over data and the storage platform also motivates cloud customers to maintain and have control over data (individual data and the data shared among a group of users through the public cloud) Moreover, the privacy and confidentiality of the data is also recommended to be cared for by the customers. The confidentiality management by a customer ensures that the cloud does not have any information about the customer data. The data encryption is done before storing to the cloud. The access control, key management, encryption, and decryption processes are handled by the customers to ensure data security. However, when the data is shared among a group, the cryptography services need to be flexible enough to handle different users, exercise the access control, and manage the keys in an effective manner to safeguard data confidentiality. A separate key for every user is a cumbersome solution.The changes in the data require the decryption of all of the copies of the users and encryption again with the modified contents. The existing and legitimate group members might show illegitimate behaviour to manipulate the data. The data can be decrypted, modified, and re-encrypted by a malicious insider within a group. Consequently, a legitimate user in the group may have the access to certain unauthorized files within the group. On the other hand, it is necessary for a user to possess a key to conduct various operations on the data. The possession of the key also implicitly proves the legitimacy of a user to operate on the data. Nevertheless, simultaneously dealing with both the issues related to the key is an important issue that needs to be addressed effectively.

II. Related Work

Literature Review

These are various surveys which we are studied

A. Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

A lightweight information sharing plot (LDSS) for portable distributed computing. It receives CP-ABE, an entrance control innovation utilized as a part of typical cloud condition, be that as it may, changes the structure of access control tree to make it reasonable for versatile cloud situations. LDSS moves a vast segment of the computational serious access control tree change in CP-ABE from cell phones to outer intermediary servers. Moreover, to lessen the client renouncement cost, it acquaints property depiction ends with execute apathetic disavowal, which is a prickly issue in pro-gram-based CP-ABE frameworks. The trial comes about demonstrate that LDSS can successfully lessen the overhead on the cell phone side when clients are sharing information in portable cloud situations.

B. Low Latency for File Encryption and Decryption Using BRA Algorithm in Network Security.

Data security is significant deterrent in various zones like military, bank application, educational organization. Document is forward starting with one area then onto the next area in the organize. Numerous programmers are unlawfully get to the data. To give answer for this issue many creators has presented diverse calculations and strategies. The distinctive calculations like DES, triple DES and AES accomplish greater security however it sets aside more opportunity for encryption and decoding records. This algorithm gives greater security and takes littlest measure of time for record encryption and decoding. This encryption can apply on various sorts of records like content, picture, sound, video records. In the Byte Rotation Encryption Algorithm include two procedures. One is irregular key era procedure is utilized. What's more, second is parallel encryption and decoding is process utilizing multithreading procedure.

C. Analysis of multi-threading time metric on single and multi-core CPUs with Matrix multiplication.

With the landing of multi-centre CPUs, to accelerate execution of frame-works utilizing parallelism is prompting new approaches. Prior techniques to actualize parallelism in applications were constrained to either utilization of excess equipment assets or direction level parallelism (ILP). This requested the need of part the undertaking or process into little sections that can keep running in parallel in the errand's unique circumstance, and strings have been presented. It is normal that the quantity of centres per processor would duplicate with increment in silicon do- main on chip. Keeping in mind the end goal to achieve most extreme centre usage of equipment, programming needs to nourish. Multi-threading is prevalent approach to enhance application execution speeds through parallelism. As each string has its possess autonomous asset for assignment execution, various procedures can be executed parallel by expanding number of strings. Parallelism is the running of strings in the meantime on centres of a similar CPU. Multi-threading is famous approach to enhance application execution speeds through parallelism. As each string has its claim free asset for assignment execution, various procedures can be executed parallel by expanding number of strings. Parallelism is the running of strings in the meantime on centres of a similar CPU.

Algorithms Used:

1. Attribute Based Encryption Algorithm:

Step 1: Start

Step 2: Generating the symmetric key for the register users.

Step 3: A set of user attributes is supplied to the input of the private key generation, and the output of the algorithm turns user's private key.

Step 4: The input is fed to the encryption function which it is necessary to encrypt, a set of attributes, decryption of data will be done by owner, and randomly selected number, and the output will be obtained encrypted data.

Step 5: A set of user attributes AU and the encrypted data are supplied to the input of the decryption function, and the output will be obtained decrypted message.

Step 6: Safe data retrieval.

Step 7: End

2. Byte Rotation Algorithm:

Step 1: Start

Step 2: The Data is partitioned into fixed length of blocks. These blocks are represented by matrix Mp.

Step 3: The numerical values is assigned to the data in sequence.

Step 4: The value of Key matrix is randomly selected from the given range.

Step 5: Calculate the Transpose matrix of data block matrix Mp which is denoted by Mt.

Step 6: Calculate the encrypted key matrix Kc .

Step 7: Add both matrix Mt and Kc. The resultant matrix is denoted by Cpk.

Step 8: Rotate the first 3 row horizontally of Cpk matrix. The resultant matrix will be matrix Chr.

Step 9: Rotate the first 3 column of Chr matrix. The resultant matrix is denoted by Cvr.

Step 10: Replace the numerical values of Cvr matrix by the corresponding blocks.

III. RESULTS AND DISCUSSION

In several distributed systems a user should only access data, If a user possess a certain set of credentials or attributes. Currently, the only method is to employ a trusted server to store the data and mediate access control. However, if any server which is storing the data is compromised, then the confidentiality of the data will be compromised. In this survey paper we are presenting a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. The encrypted data

can be kept confidential even if the storage server is untrusted; moreover, our methods get secure against collusion attacks. In previous attributes where used to describe the encrypted data and built policies into user's keys in attribute-based encryption systems while in our new system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

IV. CONCLUSION

Data which is available in the cloud can be at risk if not handled or protected in a rightful manner. This paper discusses various risks and security threats to data in the cloud and given an overview of three types of security concerns. The major concerns of this paper was data security and its malicious threats and solutions in cloud computing. Data has been discussed along with the techniques which are efficient for encrypting the data in the cloud. To build a cost effective and secure data sharing system in cloud computing, we proposed the notation called ABE-Attribute-based encryption is a type of public-key encryption, and ciphertext policy.

V. REFERENCES

[1]. Auditing and Resisting Key Exposure on Cloud Storage Akshata M. Bhand, D. A. Meshram Student, ME (IT) , RMD Sinhgad School of Engineering,Pune, Assistant Professor, ME (IT), RMD Sinhgad School of Engineering, Pune,2017

[2]. Strong Key-Exposure Resilient Auditing for Secure Cloud Storage Jia Yu, and Huaqun Wang - IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. , NO., 2016

[3]. Enabling Cloud Storage Auditing with Key-Exposure Resistance Jia Yu, Kui Ren, Senior Member, IEEE, Cong Wang, Member, IEEE and Vijay Varadharajan, Senior Member, IEEE , IEEE.

[4]. Analysis of multi-threading time metric on single and multi-core CPUs with Matrix multiplication Dhruva R. Rinku, Dr. M Asha Rani 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB17)

[5]. V. Maitri, Dattatray S. Waghole, Vivek S. Deshpande, IEEE Senior Member, \Low latency for _le encryption and decryption using BRA algorithm in network security", 2015 International Conference on Pervasive computing.

Cite this article as :

Virangni Gaikwad, Ekta Bhosale, Ankita Istalkar, Rajashri Tapkir, Prof. Sachin Patil, "Enhanced Secure Data Sharing Over Cloud Using ABE Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 8, pp. 125-128, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194829