International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue-09, Dec 2017

Fragmentation & Replication of Data in Cloud Storage with Rights & Security

[1]Mr. R. A. Auti, [2]Mr. D. G. Deshmukh

[1]Asst Professor, [2]P. G. Student,

Department of Computer Science & Engineering, Everest Educational Society's Group of Institutions College of Engineering & Technology, Aurangabad, Maharashtra, India.

Abstract - **Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, we propose Di- vision and Replication of Data in the Cloud with Attribute based encryption (ABE) that collectively approaches the security and performance issues. In this system, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. And also, This kind of computing model brings challenges to the security and privacy of data stored in cloud. Attribute-based encryption (ABE) technology has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting. However, the computation cost and ciphertext size in most ABE schemes grow with the complexity of the access policy. Outsourced ABE (OABE) with fine-grained access control system can largely reduce the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider (CSP).**

Keywords:-attribute-based encryption; cloud computing; outsourced key-issuing; outsourced decryption; Division of Cloud Data.

I. INTRODUCTION

Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing. Cloud security issues may stem due to the core technologies implementation (virtual machine (VM). The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented. The main aim of our project is secure the files store on cloud. The division of a file into fragments is performed based on a given user criteria. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security. This system select the nodes in a manner that they are not adjacent and are at certain distance from each other. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time.

II. LITERATURE SURVRY

In this paper, Author studied the structural robustness of the state-of-the-art data center network[2] (DCN) architectures. Our results revealed that the DCell architecture de- grades gracefully under all of the failure types as compared to the FatTree and ThreeTier architecture. Because of the connectivity pattern, layered architecture, and heterogeneous nature of the network, the results demonstrated that the classical robustness metrics are insufficient to quantify the DCN robustness appropriately. Henceforth, signifying and igniting the need for new robustness metrics for the DCN robustness quantification. Author proposed deterioration metric to quantify the DCN robustness. The deterioration metric evaluates the network robustness based on the percentage change in the graph structure. The results of the deterioration metric illustrated that the DCell is the most robust architecture among all of the considered DCNs[2].

III. SYSTEM DEVELOPMENT

User module

Data Owner (DO): This is a participant who intends to upload and share his data files on the cloud storage system in a secure way. The encrypted cipher texts will be shared with intended receivers whose access structure will be satisfied by attribute set embedded in cipher texts, that is to say the predicate . The responsibility of DO is to generate indexes for some keywords and upload encrypted data with the indexes.

Data User (DU): This is a participant who decrypts the encrypted data stored in S-CSP with the help of D-CSP. If the attribute set for DU satisfies the access structures, DU is able to access the encrypted files and recover the original files from it. DU downloads. Data user is responsible for choosing keywords to create trapdoor, and decrypting data.

1. Key Generation Cloud Service Provider:

Trusted Authority (TA): TA is the attribute authority center, which is responsible for the initialization of system parameters, and the generation of attribute private keys and trap- door.

Key Generation Cloud Service Provider (KG-CSP):It a participant that supplies out- sourcing computing service for TA by completing the costly key generation tasks allocated by TA.

2. Decryption Cloud Service Provider :

Decryption-Cloud Service Provider (D-CSP): It is a participant that supplies outsourcing computing service through accomplishing partial decryption for cipher texts and key- word search service on the partially decrypted cipher texts for data users who want to access the cipher text.

Storage-Cloud Service Provider (S-CSP): It is a participant that supplies out sourcing data storage service for users who want to share file in cloud.

Data Division(Fragmentation)/Replication Module: The file fragmented means to be broken up into small pieces. This is exactly what happens to files when they become fragmented. They are broken down into small individual pieces and stored in random locations. This causes less than optimal processing times because it takes longer to read through and find all of the different locations of the file, instead of being able to look in just one location. In a fragmentation schema file f is split into n fragments, all fragments are signed and distributed to n multiples nodes, one fragment per node. The user can reconstruct file by accessing m fragments arbitrarily chosen**.**

System Architecture:

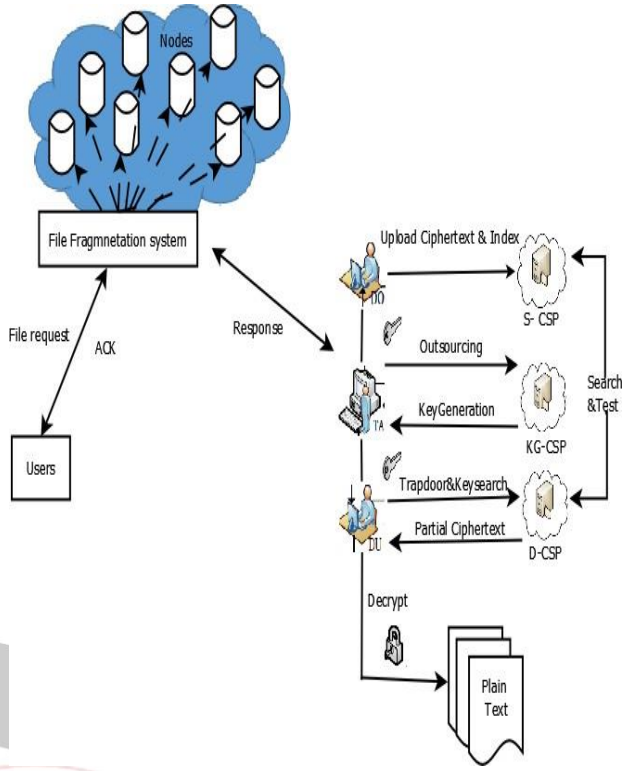

Fig 1. System Architecture

this system develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes. The proposed system, scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. this system do not rely on traditional cryptographic techniques for data security. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement retrieval) on the data. this system ensure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security . The system architecture for KSF-OABE scheme is shown as following figure, which involves the following participants.

Trusted Authority (TA):

TA is the attribute authority center, which is responsible for the initialization of system parameters, and the generation of attribute private keys and trapdoor. Key Generation Cloud Service Provider (KG-CSP). It is a participant that supplies outsourcing computing service for TA by completing the costly key generation tasks allocated by TA. Decryption-Cloud Service Provider (D-CSP). It is a participant that supplies outsourcing computing service through accomplishing partial decryption for ciphertexts and keyword search service on the partially decrypted cipher- texts for data users who want to access the ciphertext. Storage-Cloud Service Provider (S-

CSP). It is a participant that supplies outsourcing data storage service for users who want to share file in cloud.

Data Owner (DO):

This is a participant who intend s to upload and share his data files on the cloud storage sys- tem in a secure way. The encrypted ciphertexts will be shared with intended receivers whose access structure will be satisfied by attribute set embedded in ciphertexts, that is to say the predicate y (w,A) =1. The responsibility of DO is to generate indexes for some keywords and upload encrypted data with the indexes.

Data User (DU):

Data User (DU) This is a participant who decrypts the encrypted data stored in S-CSP with the help of D-CSP. If the attribute set for DU satisfies the access structures, DU is able to access the encrypted files and recover the original files from it. DU downloads intended ciphertexts with the help of trapdoor associated with appointed keyword. Data user is responsible for choosing keywords to create trapdoor, and decrypting data.

IV. SYSTEM PERFORMANCE

4.1 Performance Analysis:

Test case ID	Test case Name	Test case de-scription	Test proce-dure	Input data	Output
1	Registration	To register the new user to the system.	a)Enter unique user name. b) En-ter valid 10 digit mobile number	a)User Name b)Mobile number	a)Unique user name-True b)Already used user name- False
2	Registration	Email address validation	a)Check for @ sign in email address. b) Check for .com at the end of email address.	a)Provide proper email address. b)Email ad-dress ending with .com	a)Proper mail address-True b)Wrong mail address.- False
3	User Login	To check the user name and password of user.	a)Enter the login id b) Enter valid password	User id and password.	a)Proper user name and password-True a)Wrong user name and password-False

Testing Strategy

Test come in several tests such as unit testing, validation of the smallest components of the system, ensuring handling of know input and outputs correctly. Integration testing includes testing of an entire sub system and ensure that a set of components performance efficiently when united. Functional testing verify end-to-end scenarios that user will be absorbed in. The methodology for software testing is defined below.

Unit Testing

A unit is the smallest testable part of the software. It usually has one or a few inputs and usually a single output. This design for validation of the program that it functions properly so that it produces the desired output for the system. It is done on each module of the system. It is applied on each module of the system individually.

GUI Testing

Functional testing (or GUI testing) governs how the user and the application interact with each other and also tests the application performance. This test includes how to display images. The proposed system is tested for user inputs against different modules, validations are done. The interface is tested for appearance of different controls, visibility graphs are tested. The GUI is tested whether each button is working properly or not. A GUI allows the user to interact with the system using the buttons. The test case is:

Purpose of Test : Respective procedure should be called and executed. Driver: each button on the form(type submit, browse, textArea) Stub: Java swing component

Test Procedure : click the specific button

Expected Results : On click of each button the respective procedure should be called and executed.
Actual Results: Functionality of button is executed successfully. Pass/Fail: pass.

This testing involves following actions,

1.Check all elements for size, position, width, length and acceptance of characters or numbers. For instance, you must be able to provide input to the input fields.
Overall functionality related to performance of user graphical interface is checked.

1.Check error messages are displayed correctly.

2. Check the all result display accurately or not.

Integration Testing

Integration testing is the software testing process where individual units are combined and tested as a group. The purpose of this testing is to expose faults in the interaction

between integrated units. Each individual components after unit testing are integrated and tested. Each time a new component is added to the system an integration test is performed. The entire system is tested as characterized by the extent of the advancement project or product. It may incorporate tests based on risks and/or requirement specifications, business procedure, use cases and other abnormal state of system behaviour, connections with the working frameworks and system resources. The final test is used to verify that the system to be delivered meets the specification and its purpose.

Acceptance Testing

It is performed with realistic and various image data for training to demonstrate that the software is working satisfactorily in testing phase. User acceptance is a critical phase of any project and requires significant participation by the end user. It ensures that system meets the functional requirements. Acceptance of end users is done by proper images output.

Validation Testing

Validation testing will be done to ensure validation of the clients requirements given to the software team for the system compared to the performance and results from the software system. Given that the system has passed all the previous unit and integration testing, validating the system will measure an aspect of an implementations behaviour against an expectation and check whether the software complies with that expectation.

Performance Testing

Performance testing is the testing, which is performed, to ascertain how the components of a system are performing, given a particular situation. In proposed system it is mainly focused on increasing the performance of system to increase the accuracy of the output and analysis of result is done by using ac

V. CONCLUSION

The proposed System, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. This system propose a CP-ABE scheme that provides out- sourcing key-issuing, decryption and keyword search function. This proposed system will be efficient since this system only need to download the partial decryption ciphertext corresponding to a specific keyword. The time-consuming pairing operation can be outsourced to the cloud service provider, while the slight operations can be done by users. Thus, the computation cost at both users and trusted authority sides will be minimized. The Division and replication of data in cloud with Attribute Based Encryption. With help of trapdoor provider work isreduces.

ACKNOWLEDGEMENT

The authors are thankful to Head of Dept. Prof. R. A. Auti for providing me various resources and infrastructure facilities. I also offer my most sincere thanks to Principal **Dr. M. V. Kulkarni** Everest College of Engineering, Aurangabad, my colleagues and staff members of computer science department, Everest college of Engineering, Aurangabad for cooperation provided by them in many ways.

REFERENCES

[1]K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.

[2] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, “On the characterization of the structural robustness of data center networks,” IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.

[3] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, “Energy-efficient data replication in cloud computing datacenters,” In IEEE Globecom Workshops, 2013, pp. 446-451. .

[4] L. M. Kaufman, “Data security in the world of cloud computing,” IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[5] S. Pearson, Y. Shen and M. Mowbray, “A Privacy Manager for Cloud Computing,” Proc.First International ConferenceCloud Computing(CloudCom09), M. Gilje-Jaatun, G. Zhao and C. Rong, eds., LNCS 5931, Berlin: Springer-Verlag, pp. 90-106, 2009.

[6] W. K. Hale, “Frequency assignment: Theory and applications,” Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.

[7] S. Pearson, Y. Shen and M. Mowbray, “A Privacy Manager for Cloud Computing,”Proc.First International Conference Cloud Computing(CloudCom’09), M. Gilje- Jaatun, G. Zhao and C. Rong, eds., LNCS 5931, Berlin: Springer-Verlag, pp. 90-106, 2009.

[8] A. Sahai and B. Waters,“Fuzzy Identity Based Encryption,”EUROCRYPT05, LNCS, vol. 3494, pp. 457-473,2005.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine- Grained Access Control of Encrypted Data,”Proc.13th ACM Conference on Computer and Communications Security(CCS ’06), pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[10]A. Lewko, T. Okamoto, A. Sahai, K. Takashimaand B. Waters, “Attribute-Based Encryp- tion and (Hierarchical) Inner Product Encryption,”EUROCRYPT10, H. Gilbert, ed., LNCS 6110, Berlin: Springer-Verlag, pp. 62-91, 2010.

