International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 1698-1706

EFFICIENT CLOUD STORAGE USING DATA PARTITION AND TIME BASED ACCESS CONTROL WITH SECURE AES ENCRYPTION TECHNIQUE

P.Pandiaraja, K.Aravinthan, R.Lakshmi Narayanan, K.S.Kaaviya, K.Madumithra
Department of Computer Science and Engineering
M.Kumarasamy College of Engineering, Thalavapalayam, Karur-639 113

Abstract

Cloud Computing (CC) links the computing plus storage data's measured by diverse operating systems towards create accessible services for example huge scaled data storage and extraordinary performance computing to users. The info outsourced towards a public cloud that want to be protected. Appropriately, encrypted outsourced documents cannot be deduplicated. The Deduplication system is used to progress storage operation and can moreover functional to network data transmissions to decrease the amount of bytes that need be sent. Uploaded data was divided into lumps and that are related to the stored replica and whenever a match occurs, the redundant chunk is substituted with a minor reference that opinions to the stored chunk. This proposed work achieves Division plus Replication of Data (DROPs) within the Cloud for Optimal Performance and Security that judicially fragments user uploaded documents into dissimilar portions also replicates them at dissimilar places in the cloud server. The separation of a files into manifold fragments is accomplished based on a given consumer criteria such that the discrete fragments do not discloses any significant truths. The node splitting procedure is confirmed by the means of Grid Topology algorithm. To add progress in the retrieval time, replicate the data fragments above the nodes that produce the highest read/write requests. The data encrypted using AES algorithm

Keywords: *File splitting, Replication, AES Encryption, Time based Access Control*

1. Introduction

The term "cloud" has been used to describe the structures for distributed computing. Cloud Computing (CC) is a procedure of remaining chiefly based computing which offers dynamic resources, virtualization, reliability to the customers. [1].The purpose of CC is to decrease the amount and allow customers to take advantage of complete services furnished through the cloud and lets in them to concentrate on their essential company. CC is intently associated with Grid computing however particular from it. CC consists the computing and storage data's controlled by exclusive operating systems to make to be had offerings which comprise large scale data and extreme performance computing to clients [2,3].

Transmission of records is in an exceptionally good manner of CC, relating with the grid computing. Nowadays, organizations and corporations are shifting and spreading their employer through way of accepting the CC to decrease their charge. In the CC environs, customers of cloud offerings do no longer require roughly technique now not going into detail about the implementation and they may access to their info and entire computing responsibilities only by means of the Internet connection[4,5,6]. Throughout the access the records as well as computing, the clients do now not even understand in which the records are located away or the garage location of the record fragments. Therefore, the protection misfortune positions up quickly. Data protection within the CC is extra complex than data security in the conventional statistics systems [7, 8, 9].

The advantages of the cloud garage are bendy with decreased price and in addition they control the information loss risk in cloud and so on. Currently much more cloud approaches focus in the direction of TPA based data auditing and checking the file integrity, allowing the data dynamics. Remote service provider is liable for maintaining the data properly. The current integrity

ISSN: 2005-4238 IJAST

checking protocol of data detects the information modification and misleading server inside the cloud storage [10, 11, 12].

Proposed method, Improving cloud Security by means of the aid of Fragmenting plus replicating records that fragments customer's documents into sets and duplicate them at algorithmically within the cloud. To progress the overall performance blowfish algorithm is to implement. Also the attack on a particular node will not monitor the places of last fragments in record sequence in the cloud [13, 14]. To grip the attacker indefinite about the seats of the record fragments and in addition improve security, choose nodes in one of these technique that they are no longer contiguous and are at certain distance from every single other. Correspondingly practice Graph Topology Grid set of rules for node separation [15].

The objectives of the paper are

1. To buida device which provide better authentication scheme this avoids legal users to enter.
2. To improve the security concerns with usage of blowfish encryption.
3. To offer organized replication to grow the performance.
4. To build the time oriented access permission to control for secure data sharing with users

2. BACKROUND WORK

The primary problem of current technique changed into, that takes extra time and cost parameters to perform the dynamic processing of records encryption and decryption techniques to store facts in cloud with progressed safety. The proposed implementation of Data Partition and Replication Technique overcomes such boundaries additionally attains excessive overall performance, reduced price and restricted data garage area in cloud [16].

It additionally ensures high resilient in opposition to threads, attacks and deceptive server method division besides repetition of data in CC for best performance plus security (DROPs).

DROPs procedure is a new field of research in information security in cloud environment. This will provide more secure file storage compared to existing encryption system. In DROPs methodology Division and Replication are perform to protect data security and also consider the data retrieval process. Efficient encryption technique applied to encrypt the fragmented files. This proposed approach considers three parts that are Data Owner, Cloud Service Provider and Data User.

Steps involved in file fragmentation

Step 1: Calculate document size.
Step 2: Data Partitioning file:
If File size<=min size or size>=max size Show error
Message.
Else
Divide report as in keeping with the wide variety of servers
With index and extension.
Step 3: Generate private key for encryption.
Step 4: Encrypt respective partition using non- public keys.
Step 5: Save partition sequence, keys and record
Characteristic.
Step 6: Send every partition at respective garage server.
Step 7: Merging file: Get report walls from garage servers.
Step 8: Extract every partition and Merge report otherwise
Statistics is corrupted.

ISSN: 2005-4238 IJAST

Step 9: Decrypt the merged document with key.

3. IMPLEMENTATION

AES Encryption
The Advanced Encryption Standard stands a symmetric encryption algorithm is utmost widely used encryption techniques in cloud besides cipher are denoted to as the block cipher. AES reports no attacks. Some benefits of AES are enforce on eight-bit processors and domain an execution on 32-bit structure processors.

AES encryption perform multiple rounds. Each round has 4 vital phases in conjunction with sub-byte, shift row, mix column and upload round key. Sub-byte is the substitution of bytes the use of lookup-up table. Shift row is the shifting of rows reliable with byte period. Mix column is multiplication over Galois subject matrix. Finally, inside the upload round key step, the output matrix of blend column is XOR ed with the round key. The extensive variability of rounds used for encryption is established upon at the perilous issue size. For a 128-bit key, these 4 phases are applied to 9 rounds, in which the 10th round does not take into account the comprehensive column step. Mean while complete phases are recursive, decryption is the substitute of encryption [17, 18,19].

Algorithm Procedure

The set of regulations initiates with an Add round key diploma perceived via the practice of 9 rounds of 4 degrees and a tenth round of 3 choices. This relates for every encryption, decryption with the exclusion that every degree of spherical the decryption set of strategies is the inverse of its encryption set of rules. The four choices are as follows:

1. Substitutebytes (SB)
2. Shiftrows (SR)
3. MixColumns(MC)
4. Add RoundKey(ARK)

The 10th spherical in reality leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm will have:

1. Inverse SR
2. Inverse SB
3. Inverse ARK
4. Inverse MC

Once more, the tenth round leaves out the Inverse Mix Columns degree. Every of those degrees are taken into consideration in extra element
Procedure

- CloudFramework
- FileFragmentation
- AESEncryption
- Replication
- Time based AccessControl
- FileRetrieval

Cloud Framework

Cloud framework consists of cloud service provider, Data owner and Data user. Cloud service provider provides secure storage for data. CSP take handles of file encryption, fragmentation and replication. When data owner wants store their file on cloud server first the user should register and get cloud access permission. If all credentials are valid then only the user can send file in

ISSN: 2005-4238 IJAST

cloud. Data user makes use of data present the cloud environment. User should also register and get permission to access the data from cloud

File Fragmentation

To increase additional reliability, better performance, stable storage capacity plus security, fragmentation shows exact significant role. Fragmentation is a procedure in which each delicate file will dividing into numerous fragments in such a way that it is incredible to attain entire file in one attempt. When the file is stored in cloud, the file will get encrypted. Then, cloud manager will start fragmentation with the assistance of fragmentation engine.

Based on the fragmentation threshold value, the file will get fragmented into number of pieces. Then it will be stored in cloud nodes using allocation techniques. After fragmentation, the primary node will be determined and it gets stored initially. Then, all the remaining the fragments will be placed in remaining available nodes. File fragmentation is used to reduces the total data transfer cost. The probabilities of finding each splited document are also very low. Fragmentation is divided based on three type namely horizontal, vertical and mixed fragmentation

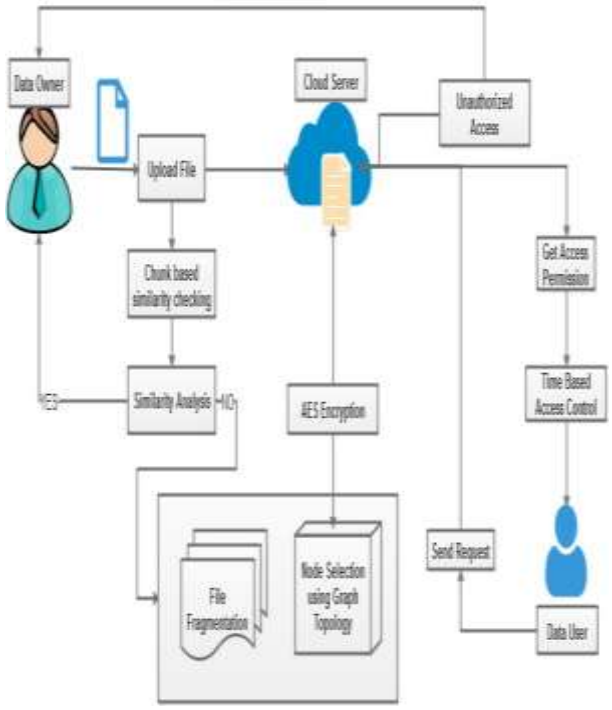

Figure 3. 1 : Data Owner with Cloud User Architecture

AES Encryption

Encryption is a famous technique that performs a data protection role from intruders. AES algorithm makes use of a specific structure to encrypt data to offer the high safety. To do this it is based on number of rounds and inner every round incorporates of 4 sub-systems. The AES encryption is well-defined as a set of rules complete certain conversions which can be to be completed on data set aside in an array. The first step of the encryption process is to place the data into an array; after which the cipher fluctuations are frequently completed over an amount of encryption rounds. The extensive variety of sequences is decided primarily based on diverse key lengths, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256- bit keys

ISSN: 2005-4238 IJAST

Replication

Data replication technique keeping a amount of replicas at the similar server or on mixed servers. In replication procedure fragmented data is copied and dispersed from unique database to certain other. So, it reduces the workload of the authentic server and the statistics on the server where its miles copied are continuously which is not present in mirroring method. Replication decreases the chance of data loss in cloud and improves the performance, availability plus reliability of data. Replications will also growth the variety of record copies in the cloud. Thus, it intensifications the chance of node shielding the file to be a victim of attacks. Replication plus Security must to be stable in order that every single service not drops the opposite.

Time based Access Control

The owner encrypts data for the purpose that intended users can decrypt it after a assigned time. User sends the file request to the corresponding data owner. Data owner set the time for accessing the data. The encrypted cipher text contains the features that only with the corresponding user's secret key and time token. The permitted accessing time, combined with user's attribute set, determines whether the user satisfies the policy or not.

File Retrieval

The user can download files by entering a secret file key, then the entire splits file get merged and can be downloaded. With the access policy present within the cipher text, a consumer can decrypt the cipher text to access the information, only if his/her attribute set satisfies the policy, and the access permission to time is in the fixed predefined releasing time in Fig 3.1.

4.EXPERIMENTAL RESULTS

Experimental result shows the overall performance of the proposed system. Here fragmented file storage was implemented using PHP as front end and MySQL as back end. This will helps to improve file security in Fig 4.1

File Upload

The data owner can view the uploaded files with their details in Fig 4.1 and the uploaded files are encrypted using AES encryption algorithm and then stored on database with securely in Fig 4.2

Figure 4.1. File storage details with file encryption

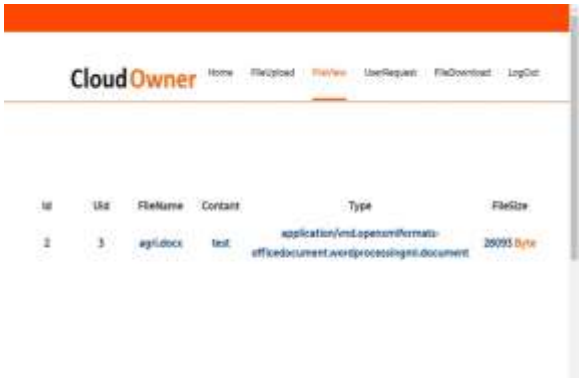

Figure 4.2 : .The process of AES encryption algorithm to encrypted and uploaded files stored on database with securely

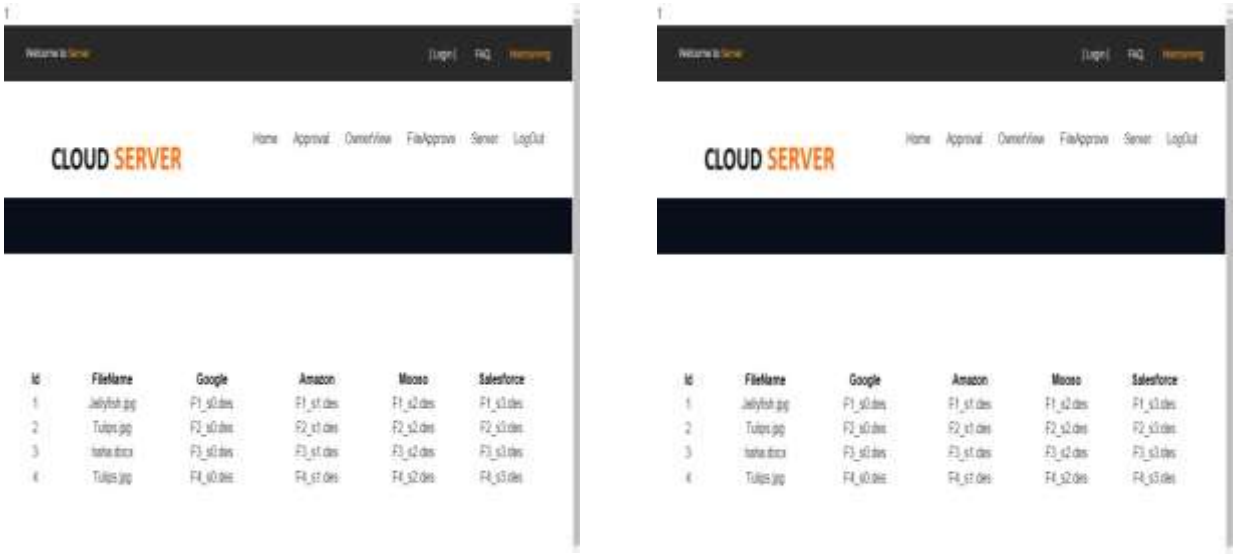

Figure 4.3 The file division and storage process. Uploaded files are fragmented and stored on different location.

File Request

In Figure 4.4 shows the user can search file using file name and send request to the specific file owner for secret key.

Key Sharing with Time Control

ISSN: 2005-4238 IJAST

Figure 4.4.1 The process of file appeal to the user and owner .

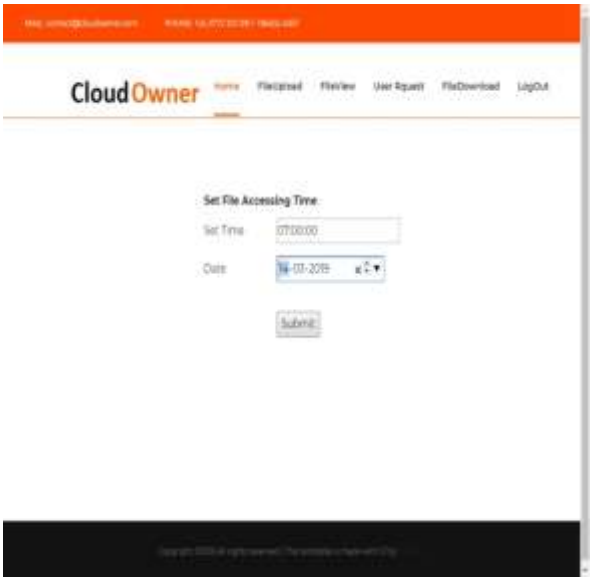

Figure 4.5 Key sharing is the process of share secret key to the requested user to access file. When owner accepts the user request secret key will be send to the owner through email or SMS.

File download

Figure 4.6: This diagram shows the process of file download. After got permission from file access user can download the file decrypt using secret key shared by data owner.

5. CONCLUSION

In proposed approach, secure data storage was executed by means of division and replication system. The user has to register in cloud, for every registered user, access authorization send from service provider. The user when needs to upload the file, it gets separations into small chunks and for every single upload of file a secret file key is also produced when data user wants

to download and access a file, they should enter a secret file key of their file, then splits chunks get merged and can download the file. This delivers security in both client levels as well as in network level. Proposed work concentrates on secure file access with drops procedure. A time primarily based access mechanism could be impressive to offer data access control to the person. The proposed work will store the time in the efficient manner in downloading, updating, and importing the record again

REFERENCES

1. Pandiaraja. P, Vijayakumar. P, Vijayakumar. V &Seshadhri, R, "Computation Efficient Attribute Based Broadcast Group Key Management for Secure Document Access in Public Cloud" Journal of Information Science and Engineering, 33, No. 3, pp. 695-712,2017.
2. Vijayakumar. P, Pandiaraja. P, Karuppiah. M & Deborah, LJ, "An Efficient Secure Communication for Healthcare System using Wearable Devices" Journal of Computers and Electrical Engineering, Elsevier, Vol 63,Page 232-245, 2017.
3. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, "Energy-efficient data replication in CCdatacenters," In IEEE Globecom Workshops, 2013, pp. 446-451,2013.
4. Vijayakumar,P, Pandiaraja, P, Balamurugan, B &Karuppiah, M , 'A Novel Performance enhancing Task Scheduling Algorithm for Cloud based E-Health Environment', International Journal of E-Health and Medical Communications ,Volume 10, Issue 2,Page102- 117,2019.
5. T.Walloschek, B. Grobauer, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57,2011.
6. Pandiaraja, P & S Parasuraman, 'Applying secure authentication scheme to protect DNS from rebinding attack using proxy", IEEE International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015],pp 1-6, 2015.
7. Pandiaraja, P &Vijayakumar, P , 'Efficient multi-keyword search over encrypted Data in untrusted cloud environment", Proceedings of the 2nd International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM '17), Pages:251-256,2017.
8. A.Sokol, and J. Tong, M. Hogan, F. Liu, "NIST CCstandards roadmap," NIST Special Publication, July 2011.
9. W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference on System Sciences (HICSS), pp. 1-10,2011.
10. P Pandiaraja, N Deepa," A Novel Data Privacy-Preserving Protocol for Multi-data Users by using genetic algorithm",Soft ComputingSpringer Berlin Heidelberg , Vol23,Issue18,pp 8539-8553,2019.
11. S Chitra, B Madhusudhanan, GR Sakthidharan, P Saravanan," Local minima jump PSO for workflow scheduling in CCenvironments", Advances in computer science and its applications, Springer, Berlin, Heidelberg, pp 1225-1234, 2014.
12. N Deepa, P Pandiaraja," Hybrid Context Aware Recommendation System for E-Health Care by merkle hash tree from cloud using evolutionary algorithm", Soft Computing Springer Berlin Heidelberg ,Volume 24,Issue 10,pp 7149-7161.
13. P.Rajesh Kanna, and P.Pandiaraja "An Efficient Sentiment Analysis Approach for Product Review using TurneyAlgorithm",Journal of Procedia Computer Science Elsevier ,Volume 165 ,Issue 2019 ,PP 356-362
14. Pandiaraja, P and JManikandan, "Web proxy based detection and protection mechanisms against client based HTTP attacks", IEEE International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], pp 1-6, 2015.
15. S. Saravanan, T. Abirami, P. Pandiaraja,"Improve Efficient Keywords Searching Data Retrieval Process in Cloud Server", 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW),IEEE Explorer ,PP 219-223

ISSN: 2005-4238 IJAST

16. K Sumathi, P Pandiaraja," Dynamic alternate buffer switching and congestion control in wireless multimedia sensor networks",Peer-to-Peer Networking and Applications, Springer US, 2019.
17. S. Thilagamani,"A survey on Preference Based Resource Allocation Model for Cloud" International Journal of Engineering Development and Research, Vol 5,Issue 1,2017.
18. Deepa, N., Pandiaraja, P. E health care data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption Journal of Ambient Intelligence and Humanized Computing (2020). https://doi.org/10.1007/s12652-020-01911-5
19. P. Santhi, S.Thilagamani," A Survey on Audit Free Cloud Storage via Deniable Attribute Based Encryption", IRA-International Journal of Technology Engineering,Vol.5,No.1,PP.1-5,2016.

ISSN: 2005-4238 IJAST