Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.199

IJCSMC, Vol. 9, Issue. 1, January 2020, pg.121 – 127

A SECURE ERASURE CODE-BASED CLOUD STORAGE SYSTEM WITH SECURED DATA FORWARDING

[1]G.Suganya; [2]S.Hariharan; [2]S.Jeeva; [2]J.Nandhakumar; [2]M.Nirmal

[1]Assistant Professor, Department of CSE, VSBCETC, Coimbatore, India

[2]UG Scholar, Department of CSE, VSBCETC, Coimbatore, India

Abstract: High-speed networks and ubiquitous Internet access become available to users for access anywhere at anytime. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a Cloud storage is a model of networked online storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers, The data center operators, in the background, virtualized the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers. Data robustness is a major requirement for storage systems. There have been many proposals of storing data over storage servers. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. A decentralized erasure code is suitable for use in a distributed storage system.

Index Terms— Cloud computing security, Encryption, Secure storage.

I. Introduction:

Proving secure and performance analysis demonstrates the effectiveness in Cloud Computing environment. EXTRAORDINARY speed network and universal internet access is accessible to consumers for use everywhere and at any time. Cloud storage is a virtual storage system where the information can be stored and retrieved from virtual servers instead of using physical servers and hence saving storage space. Hosting companies own large data centers. People who request to store data in the cloud storage can either purchase or rent the storage space from the cloud providers. The data center operators virtualize the resources in the back end. This is done based on the requests of the clients and given to them in the form of storage pools. The consumers can use these pools to store their documents or data objects Physically, the resources may be spanned across multiple servers. The users who store the information to the cloud do not need to know how the information is stored. This paper focuses on providing a secure cloud storage that supports functionalities also.

The cloud is measured as a large scale distributed storage system that includes many autonomous storage servers. Data robustness is the major requirement for the storage systems. There have been many schemes for keeping data over storage servers. One tactic to deliver data robustness is to duplicate a message such that each storage server provides a copy of the message. Another way is to encode the message by erasure coding. In erasure codes, the replica of the message is kept in every storage server. In both the methods, even if one of the storage server flops, the message can be recovered by any one of the remaining servers.

This method is suitable for use in a distributed environment. In order to provide strong confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages. There are three problems in the above straight forward integration of encryption and encoding. First, the users have the information stored in a single location. So, when many users access the data at the same time the traffic to the system becomes high. Second, the user has to manage his cryptographic keys. If the user's device that is storing the cryptographic keys is lost or compromised, the security is broken. In the existing method, the owner of messages has to retrieve, decode, decrypt and then forward them to another user.

In order to deliver strong confidentiality for message in storage servers, the idea that consists of distributed storage servers and key servers is considered. If the consumer keeps the key, there are risks for the key getting missed. Therefore, the key is kept in the key servers where it is partly encoded. The key servers must be encrypted to guarantee security and they should serve as an autonomous different from the storage servers. With this concern, a novel decentralized erasure code is suggested, appropriate for usage in a distributed storage system. The consumer will upload the files and it will be encrypted with AES Encryption and Proxy re-encryption. The data will be divided into small pieces by using a dividing key inside the cloud storage. The data is stored in different storage locations which will be monitored by the unique data distributors. If the valid user is accessing the data, it is retrieved in reversible manner from the cloud storage

II. SYSTEM ARCHITECTURE:

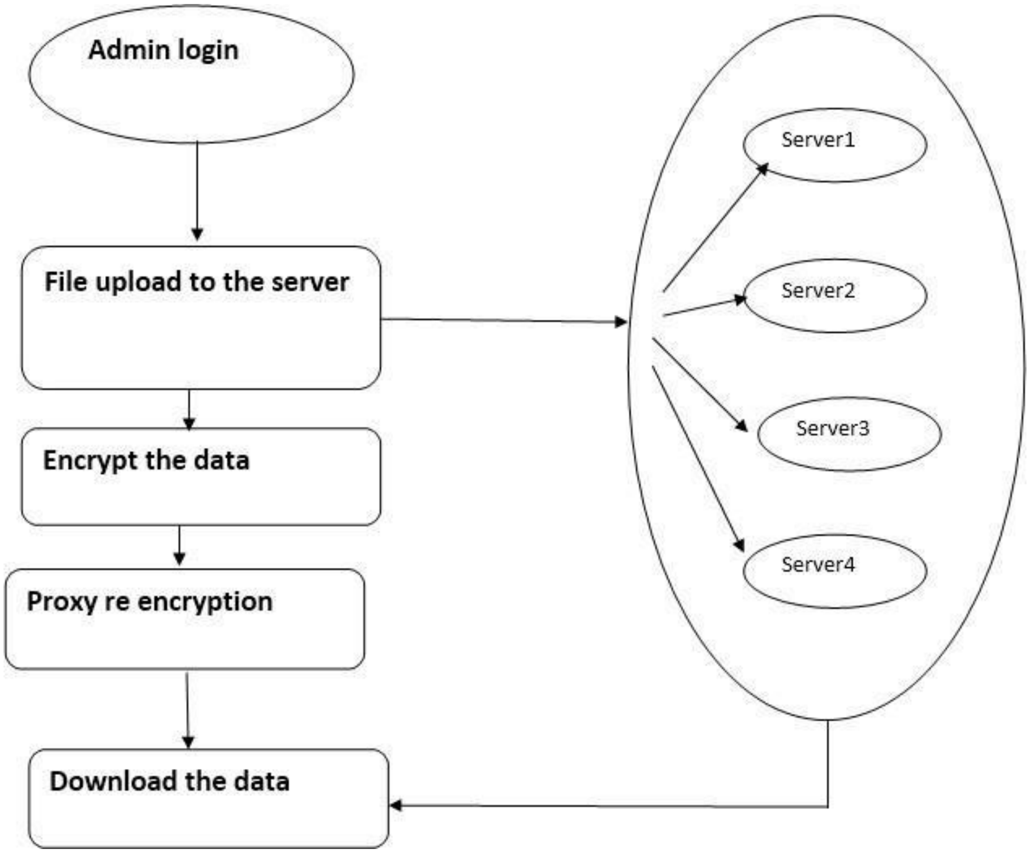

Figure 1 (Block Diagram)

III. PROPOSED WORK:

In our proposed system we address the problem of forwarding data to another user by storage servers directly under the command of the data owner. User considers the system model that consists of distributed storage servers and key servers. Since storing cryptographic keys in a single device is risky, a user distributes his cryptographic key to key servers. The distributed systems require independent servers to perform all operations. We propose a new threshold proxy re-encryption scheme and integrate it with a secure decentralized code to form a secure distributed storage system.

IV.PROPOSED ADVANTAGE:

Tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding. The storage servers independently perform encoding and re- encryption process and the key servers independently perform partial decryption process. More flexible adjustment between the number of storage servers and robustness.

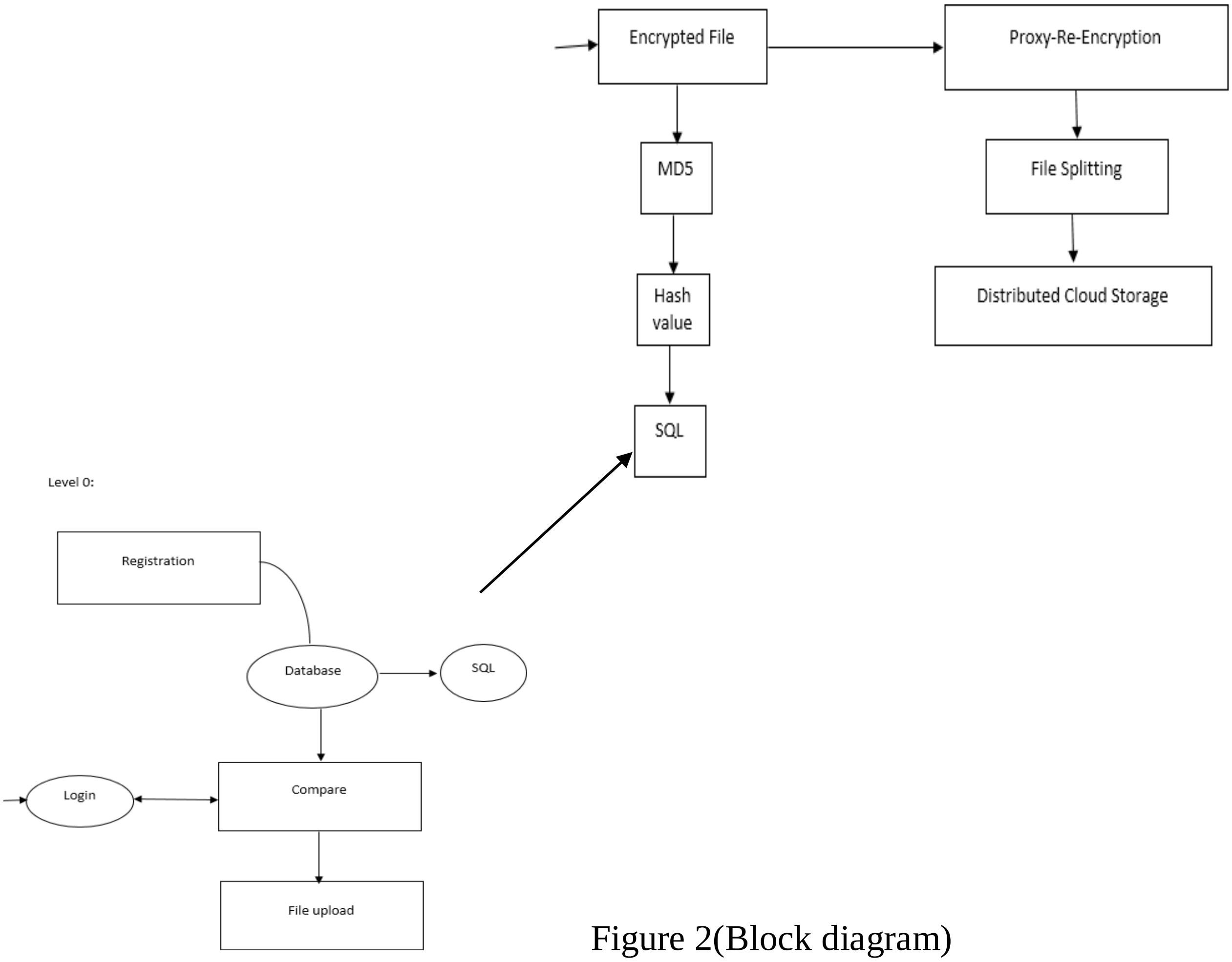

Figure 2(Block diagram)

V. RELATED WORKS:

A. Proxy Re-encryption:

Proxy re-encryption schemes are crypto frameworks that allow intermediaries (proxies) to alter a cipher content which has been encoded for one client, so that it may be unscrambled by another client. By using proxy re-encryption technique the encrypted data (cipher text) in the cloud is again altered by the user. It provides highly secured information stored in the cloud. Every user will have a public key and private key. Public key of each user is well-known to everybody but private key is known only by the particular user. This is achieved using MD5 algorithm.

Keeping in mind the end goal to preserve security, the customers will encode their information when they out- source it to the cloud. In any case, the encrypted type of files significantly impede the usage due to its haphazardness. Numerous researches have been done for the goal of information usage with functionalities without compromising with the information security. Fig. 4 explains the pseudo code of proxy re-encryption.

A.Homomorphism: Given two cipher texts c and d on plaintexts m and n separately, an individual can acquire the cipher text on the original message m + n or m*n by calculating c and d without the necessity to decrypt cipher texts.

B.Proxy re-encryption: Proxy re-encryption is the process where the data that is already encrypted by a certain encrypting algorithm is again encoded using a hashing algorithm. This is done to improve security of the stored files.

C.Threshold decryption: By distributing the private key into numerous fragments of undisclosed portions, all clients can work collectively to obtain the original plain text message which serves as the outcome of the function. Erasure codes are used in the method of threshold proxy re-encryption.

D. Advanced Encryption Standard:

Advanced encryption Standard (AES) is a symmetric encryption algorithm that produces 128 bit key (in this project). This method is efficient for both hardware and software. Fig. 3 explains the algorithm used for AES encryption technique.

E.MD5 Hashing Algorithm:

The Md5 algorithm is a hash function that produces 128-bit hash value that is stored as a 32 bit hexadecimal value. The advantage of MD5 is it produces different hash values for the same plain text.

CONCLUSION:

In this paper, a protected cloud storage framework that supports functionalities is considered. We incorporate a novel proposal which is the proxy re-encryption scheme and erasure codes over encrypted messages. The proxy re-encryption framework supports encoding, forwarding, and decryption functions in a decentralized manner. Proxy re-encryption is used to re-encrypt the data that is already encrypted and this reduces the storage space when it is being stored in a distributed environment. Additionally, each storage server individually implements encoding and re-encryption and every key server autonomously carries out partial decryption. The storage system and freshly proposed file system are highly harmonious and can provide a new level of security.

REFERENCES:

[1]. Xuechen Zhang ECE Department Wayne State Universities Trans. Kei Davison Alamos National Laboratory Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

[2]. Huayu Zhang, Hui Li, Bing Zhu, Jun Chen 2014 IEEE 33rd International Symposium on Reliable Distributed System.

[3]. Weidong Sun, Yijie Wang, Yongquan Fu, Xiaoqiang Pei 2014 IEEE 8th International Symposium on Service Oriented System Engineering.

[4]. Jibin Wang, Lili Yang, Hu Zhang, Zhaogang Xu, Ying Guo 2015 Third International Conference on Advanced Cloud and Big Data**.**

[5]. David Nunez, Isaac Agudo, Javier Lopez 2015 IEEE 28th Computer Security Foundations Symposium.

[6]. Chungsik Song, Younghee Park, Jerry Gao, Sri Kinnera Zegers 2015 IEEE First International Conference on Big Data Computing Service and Applications (Big Data Service) (2015).