iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43735

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Inspecting Cloud Storage System for Secure Data Forwarding Using Advanced Encryption Standard

Mr. Ram Prashath R M.C.A., M.Phil.[1], Srineeladevi K [2]
[1]*Assistant Professor,* [2] *Scholar, Department of MCA, Karpagam College of Engineering, Coimbatore, India*

Abstract: ***Data storage and sharing services within the cloud, users can easily modify and share data as a bunch. to make sure share data integrity are often verified publicly, users within the group must compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users thanks to data modifications performed by different users. Encryption schemes available for data privacy but it limits the number of functions exhausted storage system. Building a secure storage system that supports multiple functions is hard when the storage system is distributed and has no central authority. a brand-new idea is proposed proxy re-encryption scheme for decentralizes erasure code for defending the distributed system. The easy method, which allows an existing user to download the corresponding a part of shared data, is inefficient because of the big size of shared data within the cloud. We propose a unique public auditing mechanism. Moreover, our mechanism is in a position to support batch auditing by verifying multiple auditing tasks simultaneously.***
Key Words: Cloud computing, Cloud storage, AES, Cryptography Upload, Auditing

I. INTRODUCTION

Cloud services have three main characteristics that set them apart from traditional hosting. The first is sold on demand, usually by the minute or hour; elasticity, in which a user can have as much or as little of a service as they desire at any one time; and service management, which is handled by the provider (the consumer's only requirement is a computer and Internet connectivity). Cloud computing brings substantial advances in virtualization and distributed computing, as well as increased access to high-speed Internet and heightened interest in a struggling economy. The different service-oriented cloud computing paradigms are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Private or public clouds exist. Anyone on the Internet can purchase cloud services in the open market. (At the moment, Amazon Web Services is the most popular public cloud.) In the private sector, the cloud serves as a private network or data center that provides hosted services to a small number of users. Cloud computing's ultimate purpose is to enable easy, scalable access to computer resources and IT services, whether it's private or public. In a service-oriented cloud computing approach, the following security needs must be met:

A. Data Protection

The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the consumer must ensure that the provider has taken the necessary security precautions to safeguard their data.

B. Security

The providers should ensure that all sensitive data is hidden and that only authorized users have full access to the data. Furthermore, any data that the provider gathers or produces regarding client behavior in the cloud, as well as digital identities and credentials, must be protected.

C. Confidentiality of Data

Cloud users want to ensure that their data is kept private from third parties, such as the cloud provider and possible competitors.

D. Access control with Finer Granularity

The supplier should make it easy to grant varied access privileges to different users and give users the option to select their own access rights. There are several methods for creating fine-grained access control.
Encrypting data using particular encryption algorithms, which offers flexibility in establishing differential access privileges of various users in a viable way, would be an appropriate approach for the aforementioned security challenges.

II. LITERATURE SURVEY

We researched the AES algorithm in the paper 'A Secure Way for Data Storage and Forwarding in the Cloud,' and we are employing it for encryption in this study. The AES algorithm is based on the substitution permutation network design principle. It is both quick and flexible in terms of hardware and software. In 'A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding,' we looked at the Proxy re-encryption technique. In this work, the messages are first encrypted by the owner and then stored in a storage server. When a user wants to share his communications, he sends the storage server a re-encryption key. For the authorized user, the storage server re encrypts the encrypted communications, ensuring data confidentiality and supporting the data forwarding function.

The idea of data partitioning came from the book 'Privacy Issues in Knowledge Discovery. Partitioned data is stored at random on different storage servers, and encryption and encoding on partitioned data is performed to establish high privacy while maintaining the system's robustness in this study.

III. METHODOLOGY

The goal of the proposed system is to provide cloud users with privacy and security while reducing computing costs and time. First and foremost, the administrator will transmit a file that has been encrypted using the AES technique. After encryption, the file will be split into four to five sub-parts and sent to the server, which will then merge the sub-parts into a single file and transmit it to the user, along with the secret key . The original file will only be downloaded after inputting that key; else, a phony file will be downloaded. The notification will be delivered if the file is leaked or hacked by intruders.

A. Data Encryption

The user can log in using his or her own credentials in the cloud login module. If the user does not have an account for that cloud system, the user must first register his information in order to access and enter the cloud system. Username, e-mail, password, and confirm password are fields in the registration procedure.

After completing the registration process, the information can be stored in the cloud system's database. The user must then log in using his username and password, and the secret key must be sent to his or her email address. The user will then go into his account and view the private key generated by the cloud system. The user must choose one file from the system and then select the upload option. The server can then provide the encrypted form of the uploading file from the cloud.

Secure forensic analysis is one of KP-most ABE's important applications. An audit log offering a full description of all activity on the system or network to be secured is one of the most critical requirements for electronic forensic investigation. However, such audit records create serious security concerns, such as the possibility that a full audit log might become a desired target for enemy capture. The KP-ABE system offers an appealing solution to the audit log issue.

The name of the user, the date and time of the user activity, and the type of data modified or accessed by the user action are all elements that could be included to audit log entries. Then, a forensic analyst assigned to a case would be given a secret key connected with a certain access structure that corresponded to the key allowing for a specific type of encrypted search; this key would only open audit log entries whose attributes met specified criteria. The disadvantage of this technique is that the encryptor has no control over who gets access to the material she encrypts other than through the descriptive attributes she chooses for it.

B. Data Forwarding

We can see the storage details for the uploaded files in the forward module. The file name and forwarded E-mail are visible when we select the storage details option. The selected file name, the forwarder's email address, and the secret key to the forwarder are all included in this process.Another user can now access his account and examine the secret key that was forwarded by the prior user. The current user must then log into the cloud system to review the information received. If the forwarded file is available in the received details, the user will proceed to the download procedure.

C. Data Retrieval

Details such as username and file name are stored in the Download module. First, the server process can be started, which allows the server to connect to its specific client. To download the file, the client must first view the secret key. The fields username, filename, and secret key are used in the file downloading procedure. The client can now access the Enter the Secret Key message box by selecting the download option. The client can then access the file and use it appropriately after inputting that key.

IV. SYSTEM ARCHITECTURE

The Advanced Encryption Standard (AES) is an encryption algorithm securing sensitive the knowledge Encryption Standard (DES) and to a lesser degree Triple DES. It absolutely was to be easy to implement in hardware and software, additionally as in limited environments (for sample, during a wise card) and offer good defenses against various attack techniques. the entire selection process

was Fully hospitable public scrutiny and comment, it being decided that full visibility would confirm absolutely the best analysis of the designs. AES relies on a design principle remarked as a Substitution permutation network. it's fast in together software and hardware. Distinct its predecessor, DES, AES doesn't use a Feistel networkers features a set block size of 128 bits and a key size of 128, 192, or 256 bits, are often specified with block and key sizes in any several of 32 bits, with a minimum of 128 bits. The block size includes a maximum of 256 bits, but the key size has not within the slightest degree theoretic maximum. Maximum AES calculations are drained a special finite field. The AES cipher is stated as sort of repetitions of transformation rounds that convert the input plaintext into the final word output of cipher text. a bunch of opposite rounds are applied to transform cipher text into the primary plaintext using the identical encryption key.

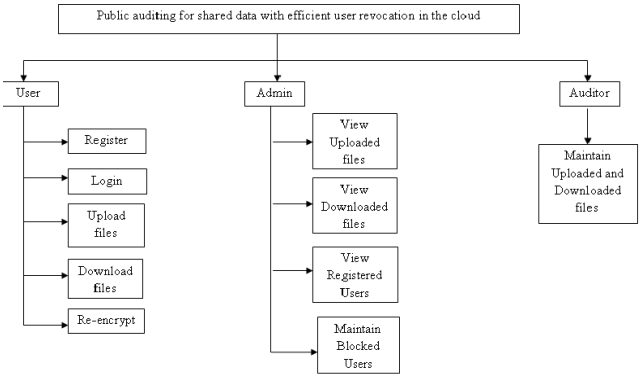


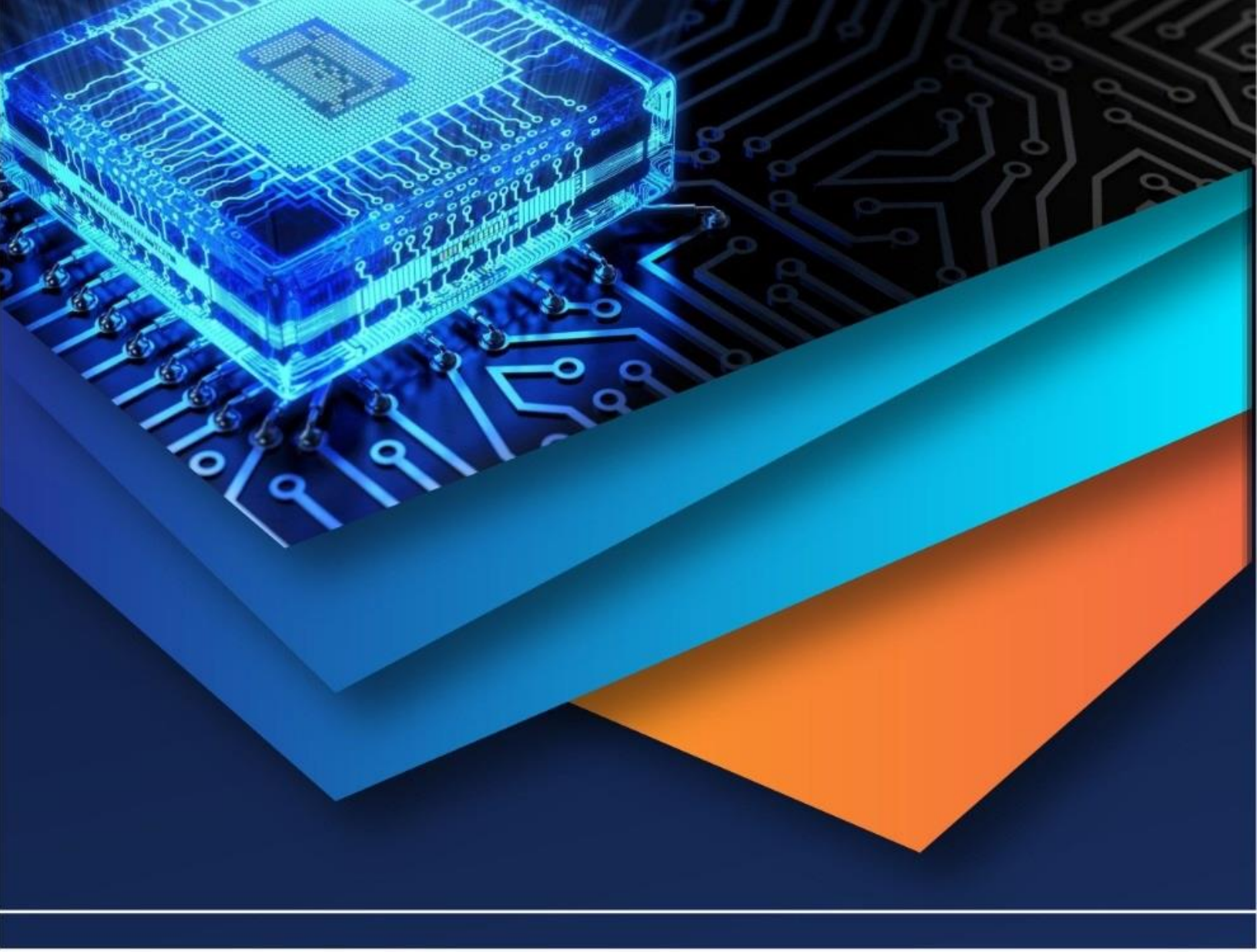
Fig -1 System Architecture

V. CONCLUSION

In today's world, data security is a big concern in cloud computing. We designed a secure cloud storage solution for data storage and forwarding to address this issue. Functionality. We divide and store the encrypted data. They are stored on a storage server. During the process, it will keep the data safe. Data in transit and data at rest It will assist the user in transmit the data to the cloud without fear of it being lost. It will be stored on various servers in the future.

REFERENCES

[1] Guillermo Indalecio, Fernando Gomez-Folgar, and Antonio J. GarciaLoureiro, "GWMEP: Task Manager-as-a-Service in Apache Cloud Stack", IEEE Internet Computing, vol. 20, no. 2, pp. 42-49, March/April 2016.
[2] Lo, ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari, "A Secure Cloud Computing Model Based on Data Classification", Elsevier Procedia Computer Science, vol. 52, pp. 1153-1158, 2015.
[3] Jean Bacon, David Eyers, Thomas F. J. M. Pasquier, Jatinder Singh, Ioannis Papagiannis and Peter Pietzuch, "Information Flow Control for Secure Cloud Computing", IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 76-89, March 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY