iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43570

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 V May 2022- Available at www.ijraset.com

Data Storage Security in Cloud Computing Using AES Algorithm and MD5 Algorithm

Vaibhav Varma[1], Mohit Patil[2], Sonal Patil[3], Madhuri Patil[4], Anilkumar Kadam[5]
[1, 2, 3, 4, 5]*Computer Department, Savitribai Phule Pune University*

Abstract: ***The proposed method uses cryptographic techniques to maintain security as security is a critical issue for the cloud, and keeping secure data is a major concern today. Overload due to data duplication is a new challenge for clouds. This article presents the data a download algorithm based on MD5 and AES. Because MD5 more secure than other hashing algorithms, goal Using MD5 algorithm for duplicating data and bringing data to server after uninstalling duplicate copy server. Purpose of use AES security is encrypting data and storing it securely on a server. Update the hash of a newly uploaded file using AES. Results and provides a comparison of several hashing algorithms, showing that MD5 is much safer and takes less time than others. The basic method, which does not use duplicate testing, uses additional storage space and takes longer. The main goal storing useful data in the cloud.***
Keywords: Cloud Computing, Security, AES Algorithm, MD5 Algorithm

I. INTRODUCTION

Since its beginnings, cloud computing has been used by billions of users all over the world as an innovation and final solution for utility and distributed computing on Web applications. Its use and impact are felt in a variety of industries, disciplines, and businesses all around the world. Nonetheless, cloud computing has encountered some challenges; the purpose of this research is to identify the factors impacting performance and provide some remedies or advice to cloud users who may encounter performance issues:

1) The ability to transform data from a variety of sources into intelligence and deliver it to the appropriate individuals and systems.
2) When several users access the cloud service, load balancing and traffic control are required.
3) Large-scale data, high-performance computing, automation, response speed, rapid prototyping, and rapid time to production are all issues that must be addressed.
4) Using the cloud as a platform to help create a more dynamic business intelligence environment

II. LITERATURE SURVEY

Kui Ren [1] Changing the computer paradigm that is very interesting in today's information technology cloud computing. However, security and privacy are seen as major barriers to widespread adoption. The authors present many safety concerns and encourage further research into security solutions in a public cloud-safe environment.

Sailee Wakhare [2] Protected password stockpiling is an important concept in a dependent framework confidential word verification, which is still widely used authentication system, despite its somewhat security imperfection. In the meantime, suggest a password authentication framework intended for secure passwords stockpiling and can be successfully integrated into existing verification frameworks. In our program, for the first time, it became clear private key from customer using cryptographic hash function. At that time; a quick password is converted into a bad password. Finally, a bad password has been encrypted with an Invalid Password (ENP) using asymmetric key calculation, and too many encryption encryption may be used to improve security. Cryptographic hash function and symmetric encryption make it difficult to distinguish passwords from ENPs.We will use message notification i.e. The MD5 and AES algorithm for this purpose. Moreover, there are a lot of comparisons of ENPs with a clear secret key provided, say make the previous attack impossible.

Sadi Arman [3] Cryptography is an emerging topic that has gained momentum from the explosion of data. With the advent of data it has become increasingly important to protect data from external interference. Various algorithms with a pre-defined data acquisition method have been used of which the Advanced Encryption Standard (AES) is one of them. The paper offers a major overhaul of the Advanced Encryption Standard, with the aim of security and ease of use centered on Symmetric Key Cryptosystem and AES algorithm.

©IJRASET: All Rights are Reserved

Performance is compared using different parameters such as data blocking, block size, encryption / encryption speed, processing time, and integration time. The main reason for this test was to exploit the success of the newly converted AES over real AES using a real-life application. A new key deployment process, a proper switch key method, and a complete Mix-Column process have been introduced. This paper provides statistics based on the AES-128 bit version, but the proposed algorithm may also apply to other versions. The goal was to get faster performance and less memory usage while keeping security difficult to break.

Brent Waters [4] A new way to get Ciphertext-Policy Attribute is introduced. Encryption (CPABE) is achieved in a standard model under tangible and non-cryptographic assumptions. Any encryptor can display access controls through any access system on top of system attributes using our solutions. The amount of ciphertext, encryption time, and encryption duration all measure according to the complexity of the access formula in our most efficient way.. The only previous attempt made to determine these parameters was evidence of a typical group model. Within our framework, we display three structures. The Parallel Bilinear Diffie-Hellman Exponent (PBDHE) decision-making, which is not considered a common BDHE hypothesis, is used to argue that our first system is selectively protected. Our next two solutions suggest compromising performance to gain potential protection under the (weak) Bilinear-Diffie-Hellman decision system.

III.RESULTS AND DISCUSSION

A. Proposed System

This study includes the technique for duplicate data in a proposed algorithm design, and when users upload a file to the cloud, they should first check which duplicate data comes from which category. Figure 1 shows that on the client side, the first empty file is read by a byte, and the function of MD5 is to create a file hash, and then compare it between files in the duplicate test section. If the hash map file is the same, it receives duplicate data and retrieves data from the server after extracting duplicate copies. If the file hash map does not match, create a private key with AES-256 and save the encrypted data to the server.

Steps For Uploading File To Server

1) User loads a file to server
2) Check De-duplication by hash match.
3) Index of directory maintains hash for hashmap.
4) In Index1 contains the file name, file hash, secret key.
5) The directory contains test sets text files.
6) If hashmap of files matches it detect duplication and does not get uploaded to the server.
7) If hash map of file does not match, then using AES 256 store encrypted file to server.
8) The updated file index contains secret key and encrypt using AES 256 and store encrypted file securely to the server.

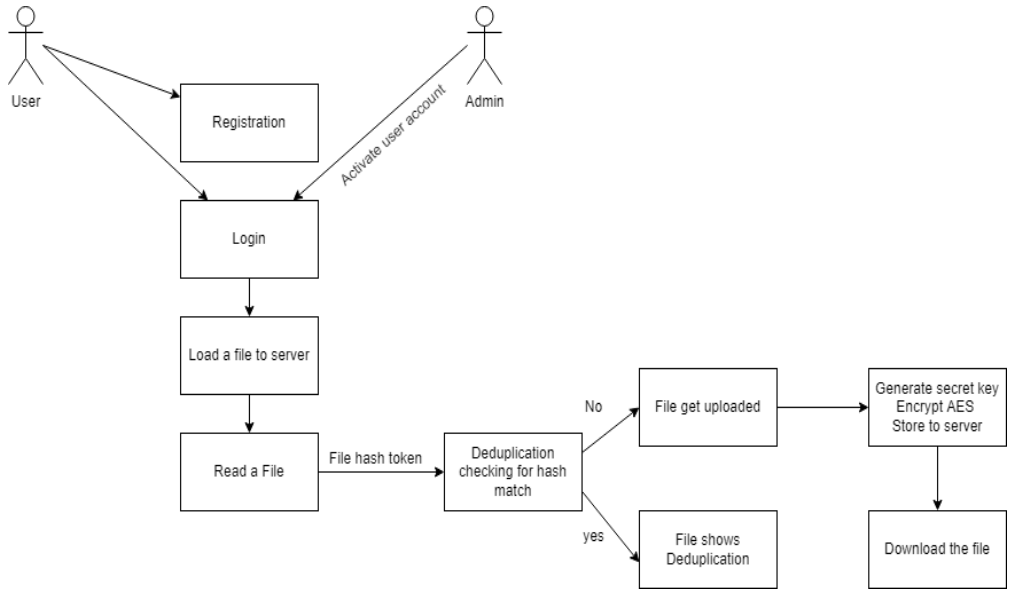


Fig. 1 System Design

B. Methodology

AES Algorithm :- AES is a duplicate of the Feistel cipher. Based totally on 'substitution - permutation network'.. Includes a series of connected functions, some of which include replacing input (modified) inputs and others involving slicing pieces (permissions).AES works with data bytes instead of bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bits) of input data at a time.

The number of cycles depends on the length of the key as follows:
128 bit key – 10 rounds
192 bit key – 12 rounds
256 bit key – 14 rounds
MD5 Algorithm :- The MD5 message-digest hashing algorithm uses 512-bit strings that are separated into 16 words of 32 bits each. Therefore 128 bit hash is generated . Each 512-bit block of data is processed along with the value produced in the previous stage to produce the MD5 digest value. In the first stage, the message-digest values are initialised using sequential hexadecimal numerical integers. Each stage includes four message-digest passes, which change values in the current data block as well as values digested from the previous block. The MD5 digest for that block is calculated using the previous block's final value

C. Results

Step 1:New file successfully uploaded to the server using the AES encryption algorithm after checking the hash function using MD5 algorithm

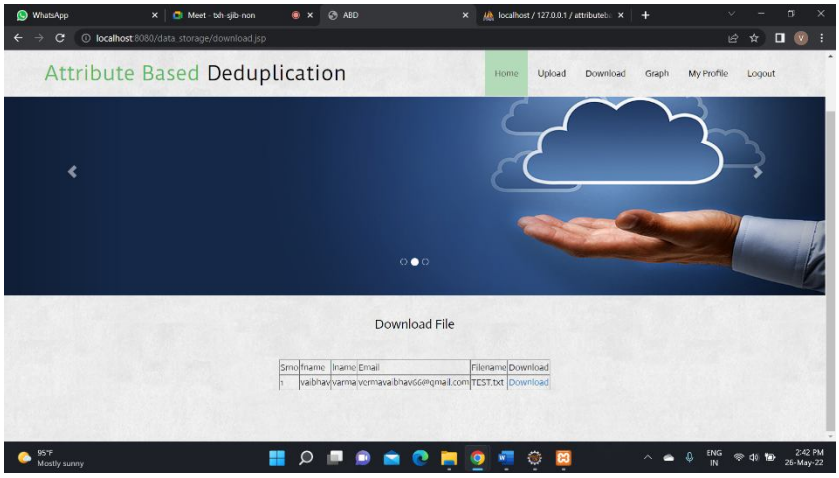


Fig. 2 New File Uploaded

Step 2:When again trying to upload the same file ,the file does not get uploaded as the MD5 algorithm finds the same hash value

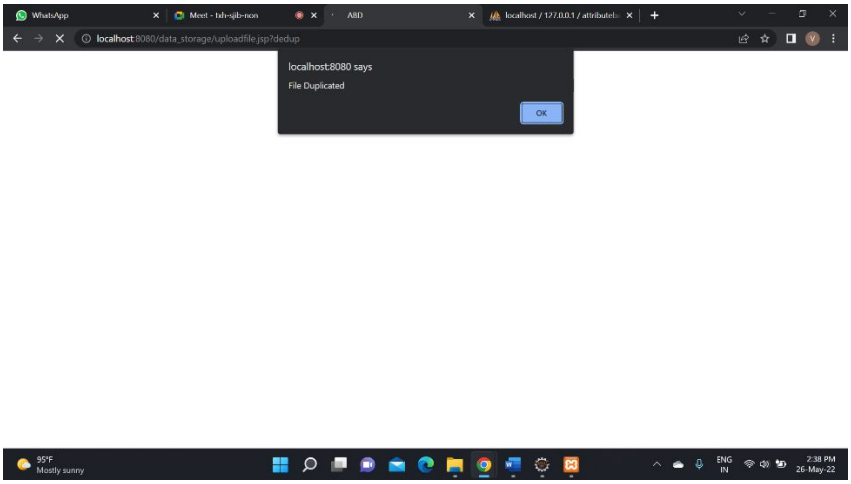


Fig. 3 Example of an image with acceptable resolution

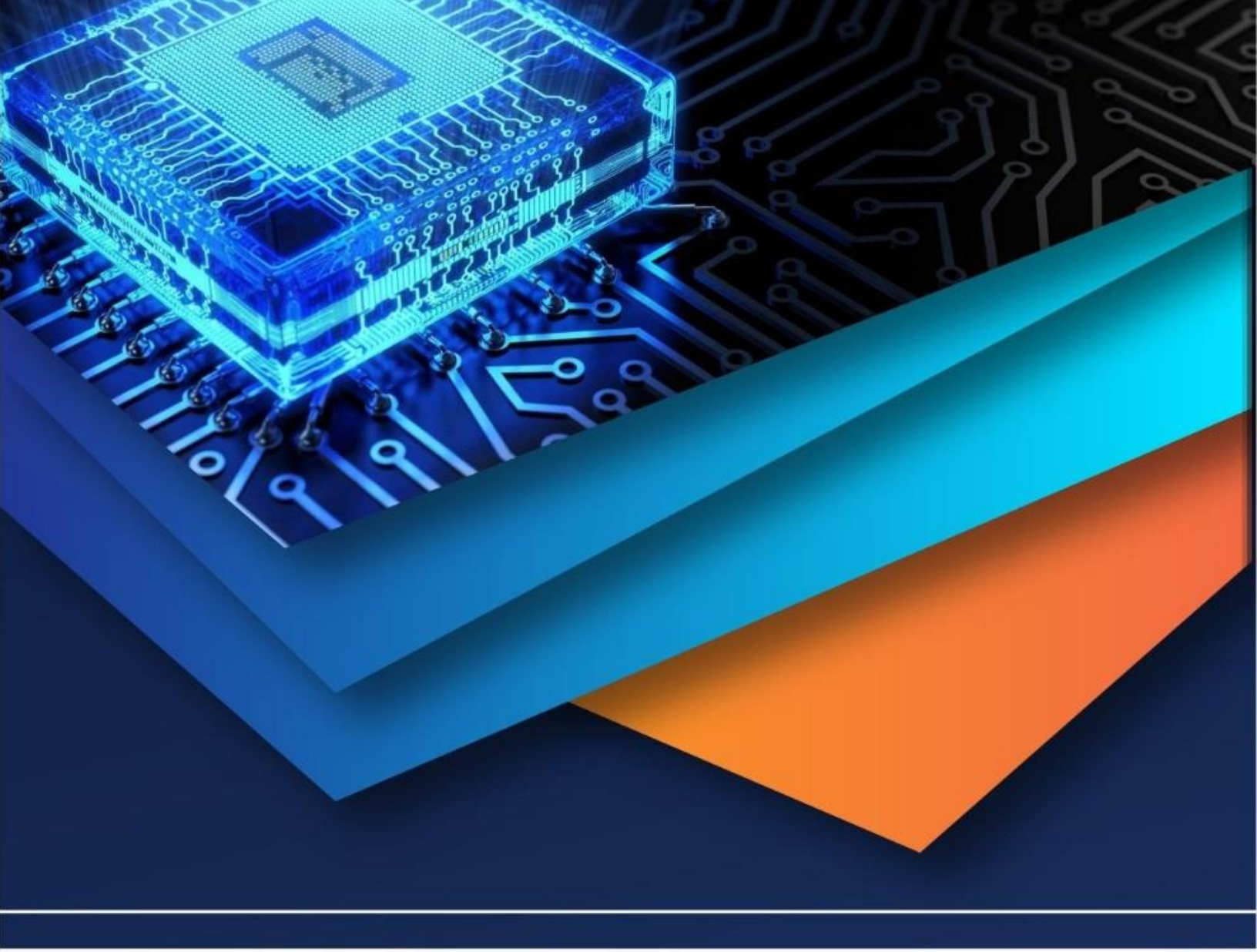
IV. CONCLUSIONS

In the proposed system, with all data stored on the cloud and the internet, it is critical to maintain data security as a top priority. To encrypt confidential data, we utilised the most secure algorithm we've ever used. To guarantee the highest level of security, we used the AES, and MD5 algorithms in the suggested system. However, there are still numerous holes that can be addressed by improving the effectiveness of these strategies .To make the computer accessible to cloud service users, more effort is needed in this field. This project is about data security and privacy, with a focus on data storage and cloud computing. It aims to improve trust between cloud service providers and consumers by protecting data in cloud computing environments.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.
[2] Sailee Wakhare, Priya Pise, Rutuja Khalate, Shivani Birajdar, Sonali Survase, "Secure Login System using MD5 and AES Attribute Based Encryption Algorithm", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075 (Online), Volume-9 Issue-8, June 2020
[3] Sadi Arman; Tanjila Rehnuma; Mahfuzur Rahman ," Design and Implementation of a Modified AES Cryptography with Fast Key Generation Technique", 2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Electronic ISBN:978-1-6654-1917-8 ,Print on Demand(PoD) ISBN:978-1-6654-3027-2
[4] Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization: Brent Waters
[5] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.
[6] Mohamed Ismail, Badamasi Yusuf " ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING WITH ADVANCED ENCRYPTION STANDARD (AES) AND AUTHENTICATION SCHEME (AS)" International Journal of Information System and Engineering Vol. 4 (No.1), ISSN: 2289-7615.
[7] Khalid, U., Ghafoor, A., Irum, M. &, Shibl, M. A., 2013." Cloud Based Secure and Privacy Enhanced Authentication and Authorization Protoco. Procedia", Volume 22, pp. 680-688..
[8] Kokane, M., Jain, P. & Sarangdhar, P., 2013."Data Storage Security in Cloud Computing". International Journal of Advanced Research in Computer and Communication Engineering , 2(3), pp. 1388- 1389.
[9] Wang, G., Q. Liu, J. W. & Guo, M., 2011. "Hierarchical Attribute Based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers. Computers and Security", 30(5), pp. 320-331.
[10] Tidke, P. M. P. a. P. B., 2014. "Improving Data Integrity for Data Storage Security in Cloud Computing". International Journal of Computer Science and Information Technologies (IJCSIT), 5(5), pp. 6680-6684.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)