iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.51255

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 11 Issue IV Apr 2023- Available at www.ijraset.com

Repository and Retrieval of Data using AES Security in Cloud Computing Environment

Dr. N. Usha Rani[1], Shaik Danish Anjum[2], Kokkula Vishal[3], Narra Hemanth Reddy[4], Shaik Shahid Akram[5]
Department of CSE, SVU College of Engineering

Abstract: ***The use of the internet is continuously expanding. People exchange vast amount of digital data every day. Some information is critical and must be protected from unauthorised access. Encryption methods are critical for preventing unauthorised access to original data. To encrypt data, a variety of algorithms can be utilised. The Advanced Encryption Standard (AES) algorithm, which is extensively supported and used, is one of the most efficient algorithms available. The goal of this work is to demonstrate how to create secure file transfer using AES encryption and decryption techniques in a cloud environment. Hackers can intercept files as they are being sent from the source to the destination. If files are not wrapped, they can be easily exploited. Thus, AES algorithm is used to safeguard file transfer networks. If AES is employed in file sharing systems, it is claimed to dissuade thieves from attempting to steal data when sending files. According to the study's findings, AES offers more protection during data encryption and decryption during file transfers without interruption from hackers attempting to steal data intentionally.***

Keywords: **Security, Data owner, data user, cloud service provider, upload file, generate key.**

I. INTRODUCTION

In today's world, computers are used for various purposes like gaming, designing, web surfing, and transferring information or files. Internet connectivity plays a crucial role in transferring large amounts of data across different sectors. However, the security risks associated with transferring files across a network pose a significant threat. Therefore, encryption using the AES algorithm is a reliable method to secure the content of the file while it's being transferred, ensuring it reaches the intended destination safely.

Data is considered a vital asset for any organization as it forms the foundation of information, knowledge, and wisdom that can help make accurate decisions and achieve goals. As data continues to grow exponentially, organizations face challenges in storing and exploring the data due to limited resources. Cloud computing has emerged as a popular solution due to its many advantages such as scalability, reliability, and cost-effectiveness. Despite its numerous benefits, cloud computing also faces several obstacles, mainly related to security threats such as data privacy and sharing concerns. Users must trust cloud servers to store and manage their data, making it vulnerable to unauthorized access and misuse. Additionally, data sharing among different stakeholders can result in intentional or unintentional disclosure to unauthorized third parties. Therefore, it's crucial to address these issues effectively to ensure the fast growth of cloud computing technology. Many applications of cloud computing include: 1) Hybrid Cloud 2) Testing and Development 3) Recovery 4) Backup 5) Image Editing Applications 6) Antivirus Applications 7) URL Conversion Applications 8) Social Media Applications 9) Accounting Applications 10) Management Application.

II. LITERATURE STUDY

A comparison [1] was made between the encryption and decryption performance of three encryption algorithms: AES, DES, and RSA. The same text file was used in four trials, and it was found that AES took the least amount of time to encrypt and decrypt the file, followed by DES and RSA. The results of the simulation showed that the AES algorithm was faster than DES and RSA in terms of encryption and decryption speed. Kao et al. introduced a key management scheme called Cloud, which was designed to protect the cloud from security threats. In Cloud, users' data is indirectly encrypted through RSA using their public keys. The users' private keys are stored on their mobile devices instead of their PCs or servers. Additionally, two-dimensional barcode images are used to represent the users' private keys, which are then used for the decryption of their sensitive data.

The researchers in work proposed and evaluated two cryptographic algorithms [2] to ensure the confidentiality, integrity, and authenticity of data. The first algorithm uses a hash code and symmetric keys to protect the data's confidentiality and integrity. The second algorithm employs the elliptic curve digital signature algorithm to ensure the authenticity of the data. In addition, they also used the advanced encryption standard-Galois counter mode with the whirlpool hash function to provide both authenticity and confidentiality. Overall, their proposed algorithms aim to provide a secure and efficient solution for protecting sensitive data.

©IJRASET: All Rights are Reserved

In the paper [3], various methods and schemes proposed to ensure secure data transfer and storage in cloud environments. The use of RSA algorithm, numerical conversions, digital encoding, and mathematical series are all important in the encryption and decryption of data. The Ciphertext-Policy Attribute-Based Proxy Re-Encryption Scheme and the file hierarchy attribute-based encryption scheme are also effective in providing access control and preventing attacks such as chosen plaintext attacks. However, it's important to note that some schemes may have increased computation costs, which could be a potential disadvantage. Overall, it's crucial for organizations to implement secure methods for data transfer and storage to prevent unauthorized access and ensure the confidentiality, integrity, and authenticity of their data.

The RSA method [4] may require more storage space and the decryption procedure may take longer due to the longer key bits. However, it is important to note that the RSA [5] method is still widely used for its security and reliability, especially in situations where confidentiality is of utmost importance. Regarding the fair data access control scheme proposed by Liu et al., the use of fake keys for obfuscation is an interesting approach to enhance security. However, the inefficiency of the authentication scheme should be addressed in future studies to improve the overall security of the proposed scheme.

A system [6] proposed a CP-ABE scheme that aimed to reduce the computation cost of heavy decryption by facilitating decryption outsourcing, revocation attributes, and policy updating. However, the scheme lacks in terms of privacy protection. The performance of the proposed scheme was analyzed through rigorous tests, which measured storage overhead and processing power.

III. EXISTING SYSTEM

Data protection is the primary concern in the area of information security and cloud computing. Numerous solutions have been developed to address this challenge. However, there is a lack of comprehensive analysis among the existing solutions and a necessity emerges to explore, classify, and analyze the significant existing work for investigating the applicability of these solutions to meet the requirements.

A. Limitations

1) Potential security issue when the data owner outsources the data to the could as the cloud server usually is provided by an untrusted third party

2) Access policy, generated when the data was encrypted and remains the same afterwards so some users quit the group and their access permission should be revoked.

3) Revocation needs to be executed in ABE-RSA algorithm, cannot ensure the integrity of the corresponding message.

4) It takes more processing time.

5) Less security and privacy

IV. REPOSITORY AND RETRIEVAL USING AES IN CLOUD ENVIRONMENT

A number of models for data protection in the cloud environment have been explored and developed for many applications. Typically, data protection is achieved through leakage prevention and leaker detection and this article concentrates on achieving efficient protection by preventing leakage and detecting 19 the malicious entity responsible for leakage as depicted. The major approaches for preventing data leakage are tailored by utilizing cryptography, access control mechanisms.

The AES [7] is a symmetric key encryption algorithm that is widely used to protect electronic data. It was selected by NIST in 2001 as a replacement for the older Data Encryption Standard (DES) and Triple DES encryption algorithms. AES uses a fixed block size of 128 bits and supports key sizes of 128, 192, or 256 bits. It uses a substitution-permutation network (SPN) structure to perform its encryption and decryption operations. AES is considered to be very secure and has become the de facto standard for encryption in a wide range of applications, including electronic communication, online transactions, and data storage.

While AES is harder to implement than DES and Triple DES, it has proven to be a more secure and efficient encryption algorithm. Its widespread adoption is due in large part to its strength and reliability, as well as its flexibility and ease of integration into existing systems.

Working of the cipher : AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows : 128 bit key – 10 rounds

192 bit key – 12 rounds

256 bit key – 14 rounds

Creation of Round keys : A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

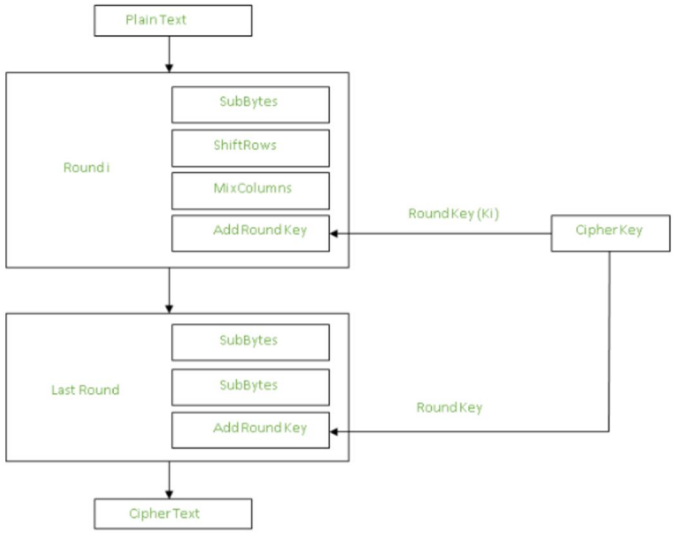


Figure 1: The Advanced Encryption Standard (AES) process

Basic process of AES algorithms is explained in the above Figure 1.

V. SYSTEM ARCHITECTURE

This system has three elemants, those are Cloud environment, Data owner, and Data user. And Figure 2 depicts process of the this work.

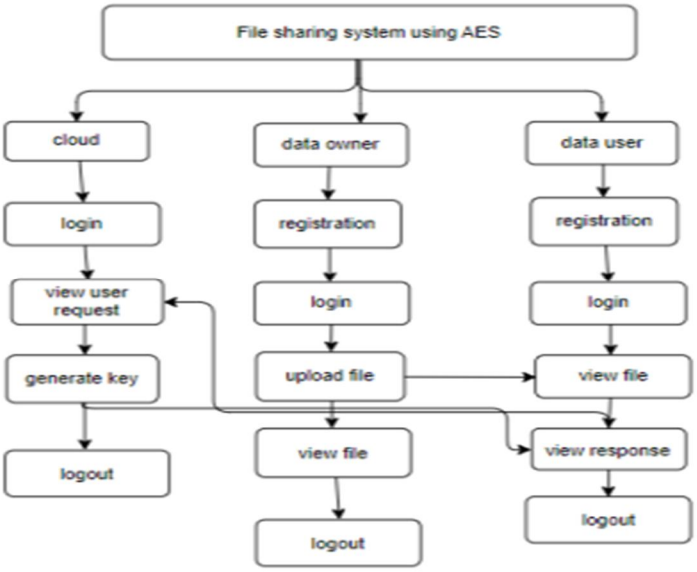


Figure 2: System Architecture

In the cloud environment, data protection is of paramount importance, and preventing data leakage is a critical aspect of it. Leakage prevention and leaker detection are two main strategies for achieving efficient data protection. Leakage prevention involves implementing measures that restrict access to data and ensure that only authorized individuals can access it. This can be achieved through various access control mechanisms such as role-based access control (RBAC), attribute-based access control (ABAC), and mandatory access control (MAC), among others.

Cryptography is another approach to preventing data leakage that involves the use of encryption techniques to protect data from unauthorized access.

Encryption can be used to ensure that data is only accessible to those who have the necessary keys to decrypt it. Additionally, encryption can help to ensure that data is not altered or tampered with during transmission or storage. Modern encryption techniques, such as homomorphic encryption, allow for computations to be performed on encrypted data without the need to decrypt it, making it an efficient way to protect sensitive information.

Leaker detection involves monitoring and identifying individuals or entities that are responsible for data leakage. This can involve the use of data loss prevention (DLP) solutions that analyze network traffic and identify patterns that indicate potential data leakage. Leaker detection can also involve the use of forensic analysis to identify the source of data breaches and track down the individuals responsible. In addition to DLP, machine learning algorithms can be utilized to detect anomalies in user behavior and identify potential leakers.

Overall, preventing data leakage is an essential aspect of data protection in the cloud environment. Access control mechanisms, cryptography, and leaker detection are three critical approaches that can be utilized to achieve efficient data protection. By implementing these strategies, organizations can ensure that their data is protected from unauthorized access, leakage, and misuse. It is important for businesses to understand the significance of data protection in the cloud environment and take proactive measures to secure their data.

VI. IMPLEMENTATION

The process of the work is divided into modules.

1) Data Owner request for login to TPA (Third Party Authority).
2) Data User request for login to TPA.
3) Third Party Authority (TPA) validates login access to both data owners and users.
4) Data Owner upload files.
5) Data User request for files.
6) Admin approves user's request

A. Cloud Service Provider

1) *Login:* CSP will login into the system using default credentials.
2) *View Request:* Csp views the user request for particular file .If he accepts then the file key will be transferred to that user.
3) *Generate Key:* The Csp will be generate the key and he will send to the user.
4) *Logout:* Finally logout from the system.

B. Data Owner

1) *Registrations:* The data owner will register with his/her details like (name, email, password, conform password, contact, address).
2) *Login:* Data owner will login into the system when the CSP accepts the request.
3) *Upload Files:* Data owner will upload files.
4) *View Files:* Data owner will view all files which are uploaded by him in cipher text format.
5) *Logout:* Finally, logout from the system.

C. Data User

1) *Registrations:* The data user will register with his/her details like (name, email, password, conform password, contact, address).
2) *Login:* Data user will login into the system with the valid creditionals.
3) View Files: Data user will view all files which are uploaded by him in cipher text format. Data user will send request to the CSP.
4) *View Response:* Csp will accept the request and key will be sent to that requested user through mail.
5) *Logout:* Finally logout from the system.

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

D. Data Owner Request For Login To Csp (Cloud Service Provider)

The data Owner registers for an account, if the data owner wants to go to the homepage they need to login, when trying to login it will be sent as a request to Cloud Service Provider.

E. Data User Request For Login To CSP

Data User also registers for an account, if the data user wants to go to their homepage first they need to login, when user trying to login it will be sent as request to the Cloud Service Provider.

F. Cloud Service Provider (CSP) Validates Login Access To Both Data Owners And Users

Cloud Service Provider receives the login requests from the both Data Owners and Data Users. CSP only able to validate their accounts. Then the OTP will be sent to that specific persons registered email.

G. Data Owner Upload Files

After enter the key from mail, Data owner can make login. And then data owner will upload the file or data. It will also be stored in cloud.

H. Data User Request For Files

Data users will also make login by entering the OTP key sent by the CSP. Then data user will request for the data owner's file to an Admin.

I. Admin Approves User's Request

Admin will receive the request sent by the data user. Admin can approve or reject the request. If the admin accepts the request, the key will be sent to the particular member.

J. Data User Download Files Using Key

Data user will receive the key, after admin accepts the file request. With the secret key, data users now able to download the file or able to view the file safely.

VII. RESULTS

Below results are screenshots of Cloud computing using AES



Figure 3: Home page of Cloud computing using AES



Figure 4: File uploading to transmit



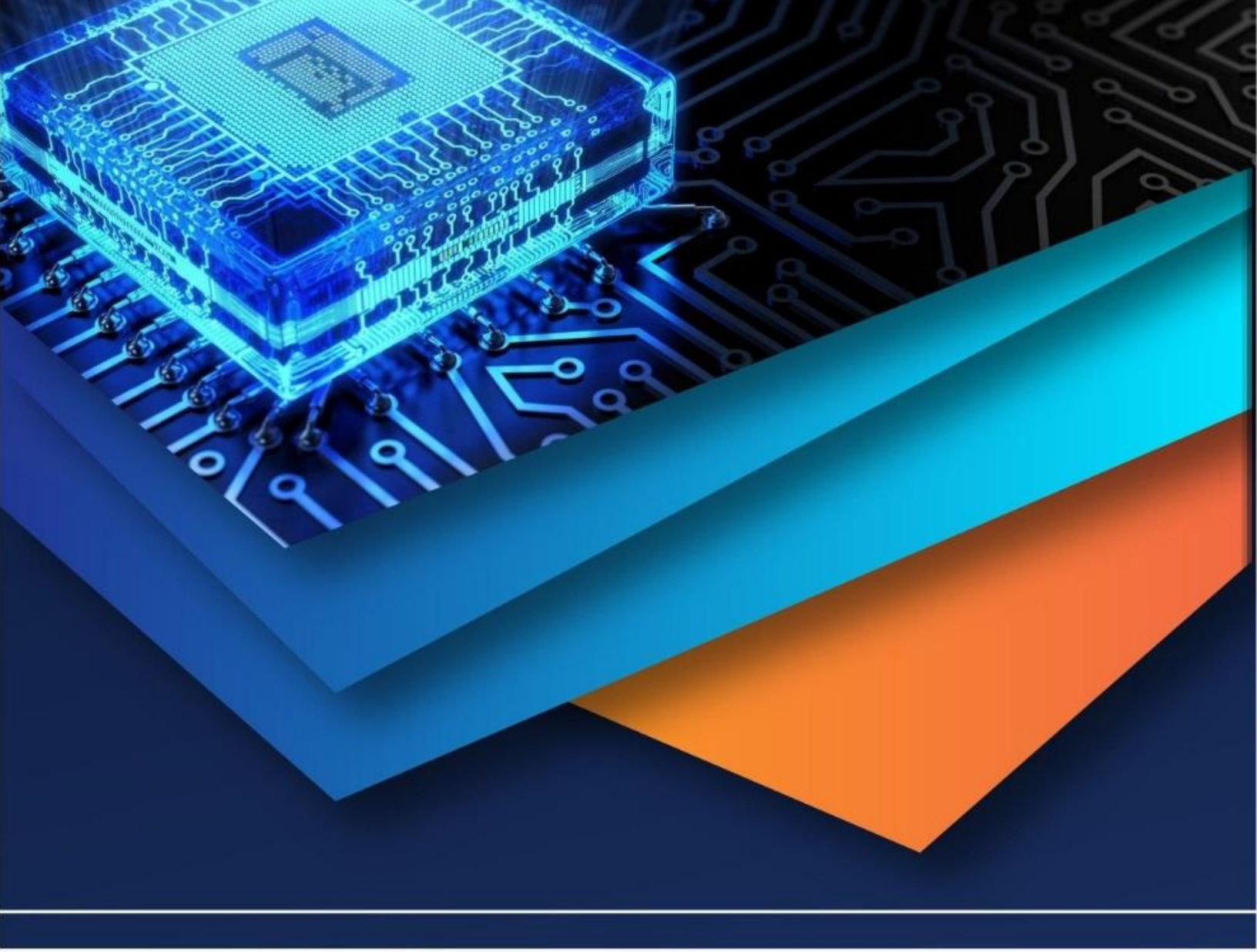
Figure 5: Final output of the file

VIII. CONCLUSION

The use of encryption technologies such as the AES algorithm is crucial to ensure the security of digital data transfers. With the rapid increase in internet usage and the exchange of massive amounts of data, it is essential to protect vital information from unauthorized access. The AES algorithm, which is widely endorsed and implemented, is considered one of the best encryption algorithms in terms of efficiency. Overall, encryption technologies such as the AES algorithm play a critical role in ensuring the security of digital data transfers. As technology advances, it is crucial to continue developing robust solutions to keep up with evolving threats and ensure the safety of vital information.

REFERENCES

[1] Mohammad Ausaf Anwar, Durgaprasad Gangodkar, “Design and Implementation of Mobile Phones based Attendance Marking System”, Department of Computer Science Engineering, Graphic Era University, Dehradun, Uttarakhand, India, 2015.
[2] Jun Lio, “Attendance Management System using a Mobile Device and a Web Application”, Department of Socio-informatics, Faculty of Letters Chuo University
[3] Mahesh G, Jayahari KR, Kamal Bijlani, “A Smart Phone Integrated Smart Classroom”, Amrita e-Learning Research Lab (AERL) Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham, Amrita University, India, 2016.
[4] Ekta Chhatar, Heeral Chauhan, Shubham Gokhale, Sompurna Mukherjee, Prof. Nikhil Jha, “Survey on Student Attendance Management System”, S.B. Jain Institute of Technology, Management and Research, Nagpur, 2016.
[5] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).
[6] Md. Milon Islam, Md. Kamrul Hasan, Md Masum Billah, Md. Manik Uddin, “Development of Smartphone-based Student Attendance System”, Department of Computer Science and Engineering Khulna University of Engineering & Technology, Khulna-9203, Bangladesh, 2017.
[7] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.



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)