



## Improving Quality and Correctness of Cloud Data by Implementing AES Algorithm

---

D. Madhavi, M.Sri Manisha Reddy, M. Ramya and G. Sanjana

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

August 28, 2022

# **IMPROVING QUALITY AND CORRECTNESS OF CLOUD DATA BY IMPLEMENTING AES ALGORITHM**

**Dr. D. Madhavi, Associate Professor (dasarimadhavi3@gmail.com) ,Sridevi Women's Engineering College, Computer Science Engineering.**

**M.Sri Manisha Reddy (manishareddy2626@gmail.com), M. Ramya(ramyasri774625@gmail.com), G. Sanjana (sanjana.gangam@gmail.com)**

## **ABSTRACT:**

Cloud computing is a technology which that is based on networks. Cloud computing has its origin in distributed computing, grid computing, and utility computing. The users may pay for what they are using in the cloud. To reduce the infrastructure the users can move the data from their environment to the cloud environment. The users can lose the control over the data. The data moving on infrastructure will face several attacks and also the possibility that the attacker will spoof the data from an authenticated user with ease. It mainly concentrates on improving cloud computing data protection through T clouds and trusted computing. High speed networks and ubiquitous Internet access become available to user to access anywhere at any time. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a cloud. Cloud storage is a model of networked online storage where data is stored in virtualized pools of storage that the third parties generally host. Hosting companies operate large data centers, and people who requires the data to be hosted buy or lease storage capacity from them.

*Keywords: Distributed computing, grid computing, utility computing, T clouds, Ubiquitous.*

## **1.INTRODUCTION**

The data center operators, in the background, virtualizes 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. We construct a secure cloud storage system that supports the function of secure data forwarding by using an AES and Proxy reencryption. In this model initial phase owner will upload the data with AES Encryption. Next phase, inside of cloud again the data has divided into small pieces, for this process we will apply a dividing key. Data will place in different storage locations. The information of data storage will monitor by a unique data distributor. If the valid user accessing the data cloud will retrieve the data as reversible manner. As the technology is growing rapidly, the access to software and data storing also changes accordingly. Cloud is anywhere and everywhere. The resources are provided to the customer as a service like Software, Platform and Infrastructure as services respectively. The cloud providers provide cargo deck in the shape of information centers, where the data is stored in a very centralized location. In cloud there is a Service Level Agreement (SLA) between the service provider and user.

### **1.1 AES (ADVANCED ENCRYPTION STANDARDS):**

AES is based on a design principle known as a Substitution permutation network. It is

fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network. AES has fixed block size and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum. AES operates on a 4x4 column major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have

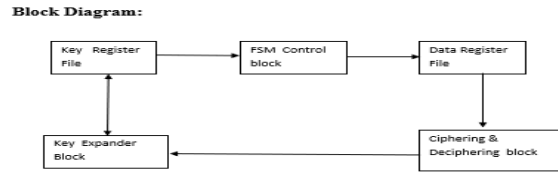


Fig.1.3.1: Block Diagram of AES

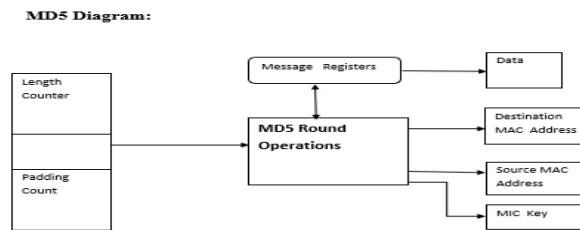


Fig.1.3.2: MD5 Diagram of AES Activate Wi

additional columns in the state). as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

## 2.PURPOSE

Cloud data protection is the practice of securing a company’s data in a cloud environment, wherever that data is located, whether it’s at rest or in motion, and whether it’s managed internally by the company or externally by a third party. This practice has become increasingly important as more companies have switched from building and managing their own data centres to storing their applications and data in the cloud instead. A 2018 survey by IDG, a leading technology media company, stated that 73% of companies had applications or infrastructure in the cloud, with another 17% expected to make the move in the coming year.

## 3.LITERATURE SURVEY

### Privacy-preserving and Secure Distributed Storage Codes

Author: Nihar B. Shah, K. V. Rashmi, Kennan Ramchandran, Fellow, IEEE, and P. Vijay Kumar, Fellow, IEEE. 2011.

Storage outsourcing is a rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. However, Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature. The main issue is how to frequently, efficiently and securely verify that a storage server is faithfully storing its client’s (potentially very large) outsourced data. The storage server is assumed to be untrusted in terms of both security and reliability.

(In other words, it might maliciously or accidentally erase hosted data; it might also relegate it to slow or off-line storage.) The problem is exacerbated by the client being a small computing device with

limited resources. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form. In this paper, we construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption.

### **Repair Locality from a Combinatorial Perspective.**

Author: Anyu Wang and Zhifang Zhang  
Key Laboratory of Mathematics Mechanization, IEEE  
Dec.2014.

Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. We have built a prototype of Plutus on OpenAFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

### **Pattern-driven Parallel I/O Tuning cloud storage**

Author: Babak Behzad, Surendra Byna, Prabhat Lawrence  
Berkeley National Laboratory.2011 IEEE.

We introduce HAIL (High-Availability and Integrity Layer), a distributed cryptographic system that allows a set of servers to prove to a client that a stored file is intact and retrievable. HAIL strengthens, formally unifies, and streamlines distinct approaches from the cryptographic and distributed-systems communities. Proofs in HAIL are efficiently computable by servers and highly compact—typically tens or hundreds of bytes, irrespective of file size.

HAIL cryptographically verifies and reactively reallocates file shares. It is robust against an active, mobile adversary, i.e., one that may progressively corrupt the full set of servers. We propose a strong, formal adversarial model for HAIL, and rigorous analysis and parameter choices. We show how HAIL improves on the security and efficiency of existing tools, like Proofs of Retrievability (PORs) deployed on individual servers. We also report on a prototype implementation.

### **3.1 Existing system:**

In Existing System, we use a straightforward integration method. In straightforward integration method Storing data in a third party's cloud system causes serious concern on data confidentiality. 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. When he wants to use a message, he needs to retrieve the Codeword symbols from storage servers, decode them, and then decrypt them by using cryptographic keys.

General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. A decentralized architecture for storage systems offers good scalability, because a storage server can join or leave without control of a central authority.

#### **Disadvantages:**

- The user can perform more computation and communication traffic between the user and storage servers is high.
- The user has to manage his cryptographic keys otherwise this security has to be broken.

- The data storing and retrieving, it is hard for storage servers to directly support other functions.

### 3.2. Proposed system:

we address the problem of forwarding data to another user by storage servers directly under the command of the data owner. We consider 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 that shall perform cryptographic functions on behalf of the user. These key servers are highly protected by security mechanisms. Here Storage system has allocated by different data container. Once owner uploads the data with AES encryption mechanism, system again takes the data and makes Secure Data segregation process. All the data pieces will be saved in different location in cloud storage. Here public distributor monitors all the data and corresponding positions where it is saved.

#### Advantages:

- 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 the partial decryption process.
- More flexible adjustment between the number of storage servers and robustness

## 4. SYSTEM ARCHITECTURE

### System Architecture:

The purpose of system architecture activities is to define a comprehensive solution based on principles, concepts, and properties logically related to and consistent with each other. The solution architecture has features, properties, and characteristics which satisfy, as far as possible the problem or opportunity (traceable mission/business and that the stake holders requirements) and life cycle concepts (e.g., operational, support) and the used technologies (e.g., mechanics, electronics, hydraulics, software, services, procedures, human activity) required by a set of system requirements.

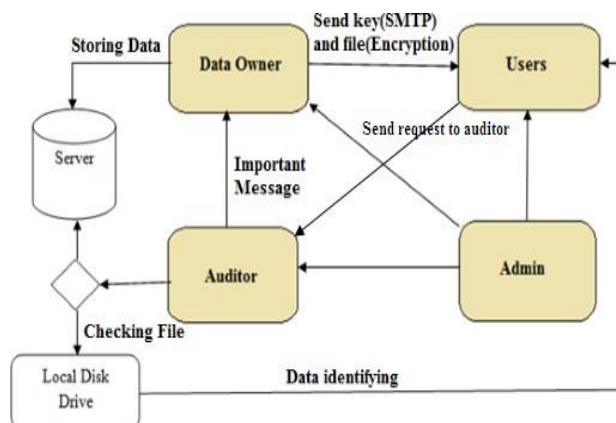
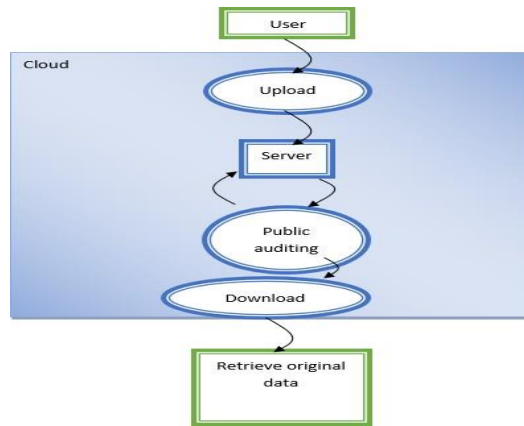


Fig: System Architecture

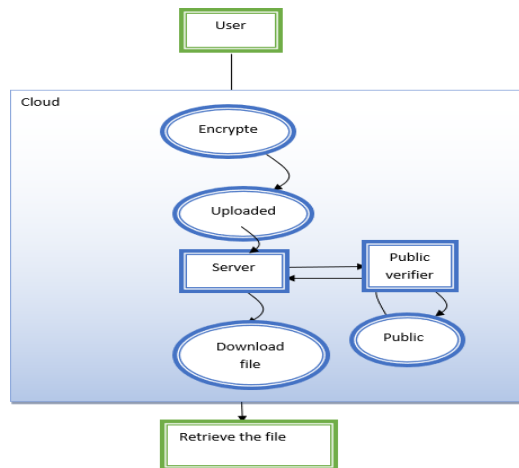
## 5. DATA FLOW DIAGRAM

A data flow diagram shows how processes flow through a system. It also gives you information about things such as the inputs and outputs (where things come from, which route they go through, and where they end up), and the process itself. This includes data stores and the various subprocesses the data moves through.

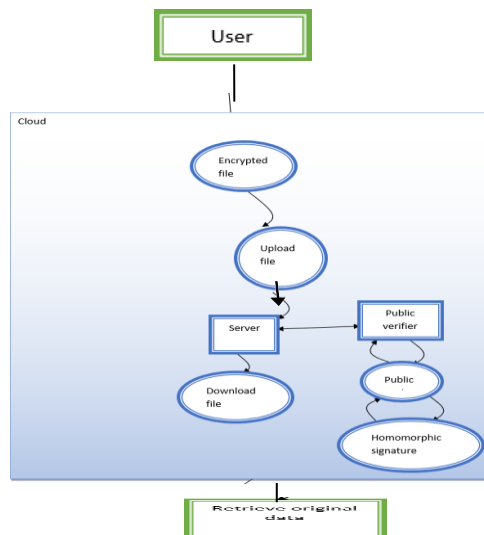
### Level 0: File Uploading



### Level 1: Creating an Encrypted file



### Level 2: Decrypting file and retrieving the original file.

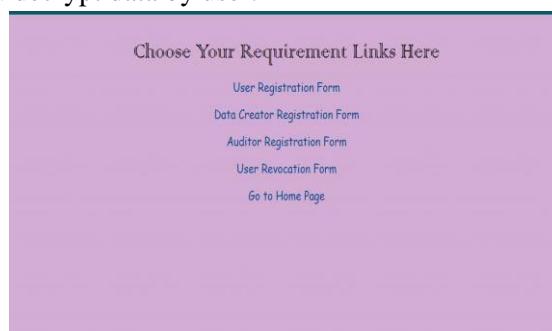


## 6.IMPLEMENTATION OF DATA

**Web Page:** Home Page



**Admin Page:** In admin Requirement links we have to register all the form pages, so we can encrypt data by data creator and decrypt data by user.

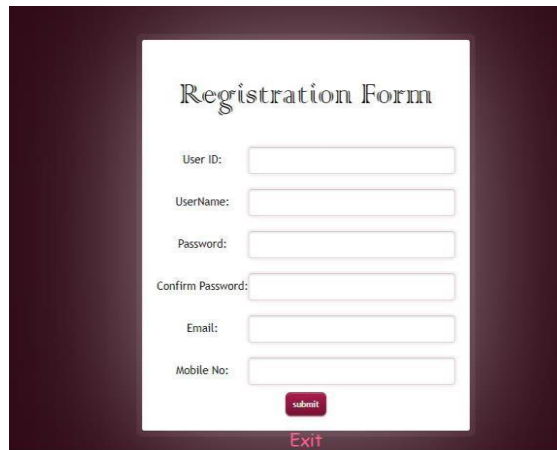


**Data Creator Registration Form:** In this form we have to enter the details of the creator and lock the data by provide a product key (secret key) so the data will be encrypted.

The file should be uploaded now and plaindata is converted into cipher data. File has been unloaded into cloud successfully.

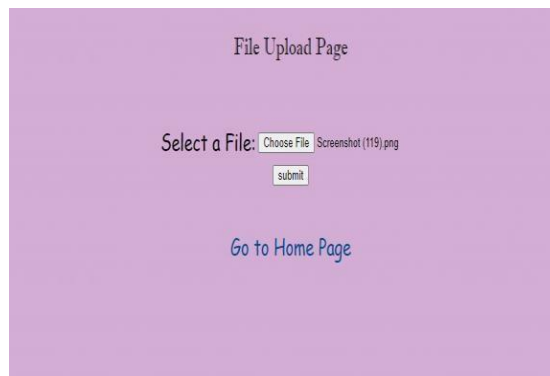


**Auditor Registration Form:** Here the auditor will check whether the plain text is converted into cipher text or not and verifies the data. firstly, he should enter all his details in registration form.



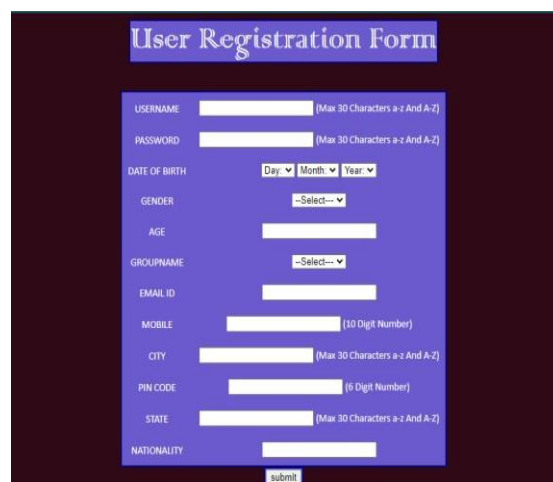
A registration form titled "Registration Form" with the following fields: User ID, UserName, Password, Confirm Password, Email, and Mobile No. There is a "submit" button at the bottom and an "Exit" link below it.

Auditor should apply the same data that is uploaded by the data creator and click on submit button. After clicking on the submit button again it shows the new file upload page



A file upload page titled "File Upload Page" with a "Select a File:" label, a "Choose File" button, and a file name "Screenshot (119).png". There is a "submit" button and a "Go to Home Page" link.

**User Registration form:** In this form we have to enter all the details of the user and he has to select the group name (From where you want to download the data).



A user registration form titled "User Registration Form" with the following fields: USERNAME (Max 30 Characters a-z And A-Z), PASSWORD (Max 30 Characters a-z And A-Z), DATE OF BIRTH (Day, Month, Year dropdowns), GENDER (dropdown), AGE, GROUPNAME (dropdown), EMAIL ID, MOBILE (10 Digit Number), CITY (Max 30 Characters a-z And A-Z), PIN CODE (6 Digit Number), STATE (Max 30 Characters a-z And A-Z), and NATIONALITY. There is a "submit" button at the bottom.

User should enter the product key that is sent by the data creator for decrypting the data and click submit now, your data will be downloaded and you can see it.



## 7.RESULTS

Now, you can see the final decrypted data.



Private key sends to the data creator so, he can send to anyone.

public key:Private key Inbox x



manishareddy2626@gmail.com

to manishareddy2626 ▾

public key is1234567891234567

After verified by the auditor send message tothe user.

**\*\*Important Message From Auditor\*\*** Inbox x

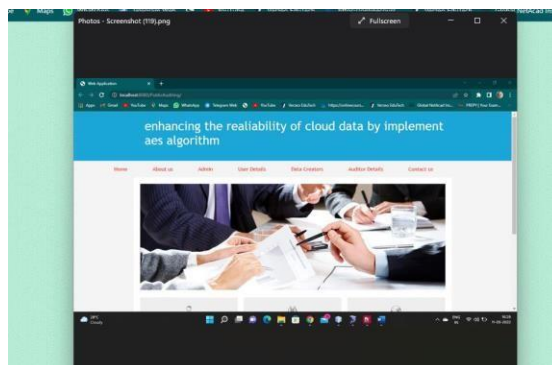


manishareddy2626@gmail.com

to jan ▾

Your Data in Server is Corrupted or Modified

Final output when user enters the private keyand downloads the data.



After process completion. it navigates to home page.

## 8.CONCLUSION

Employment scam detection will guide jobseekers to get only legitimate offers from companies. For tackling employment scam detection, several machine learning algorithms are proposed as countermeasures inthis paper. Supervised mechanism is used to exemplify the use of

several classifiers for employment scam detection. Experimental results indicate that Random Forest classifier outperforms over its peer classification tool. Employment scam detection will guide jobseekers to get only legitimate offers from companies. For tackling employment scam detection, several machine learning algorithms are proposed as countermeasures in this paper. Supervised mechanism is used to exemplify the use of several classifiers for employment scam detection. Experimental results indicate that Random Forest classifier outperforms over its peer classification tool. The proposed approach achieved accuracy 98.27% which is much higher than the existing methods.

## **9.FUTURE SCOPE**

We believe that data security in cloud computing, a section stuffed with challenges is in infancy now, and a lot of research problems are yet to be identified. If the users have strict security policies, their data will be confidential.

To protect the confidentiality of the data, a client-side strategy must be incorporated in the cloud. Encryption and decryption processes have a vital role in preventing threats to data. There are a lot of security problems even when the encryption is implemented.

## **10.REFERENCES**

- [1] Akhil Bhel and Kanika Bhel (2012) "An Analysis of Cloud Computing security issues" World Congress on Information and Communication Technologies.
- [2] Mathisen E. Security challenges and solutions in cloud computing. In 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011) 2011 May 31 (pp. 208-212). IEEE.
- [3] Mohit E, Prem A. To enhance the data security of cloud in cloud computing using RSA algorithm. International Journal of Software Engineering. 2012;1(1).
- [4] Gul I, U.R. Rehman A, Islam MH. Cloud computing security auditing. In The 2nd International Conference on Next Generation Information Technology 2011 Jun 21 (pp. 143-148). IEEE.
- [5] Deng M, Petkovic M, Nalin M, Baroni I. A Home Healthcare System in the Cloud Addressing Security and Privacy Challenges.
- [6] Zhang X, Wu W, Li H, Zhang X. Information security risk management framework for the cloud computing environments. In 2010 10th IEEE international conference on computer and information technology 2010 Jun 29 (pp. 1328-1334). IEEE.
- [7] Mewada S, Singh UK, Sharma P. Security Based Model for Cloud Computing. IRACST-International Journal of Computer Networks and Wireless Communications (IJCNC). 2011;1(1):13-9.
- [8] Liu W. Research on cloud computing security problem and strategy. In 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) 2012 Apr 21 (pp. 1216-1219). IEEE.