CLOUD COMPUTING SENSITIVE DATA PROTECTION

using multilayered approach

Gayathri S Nair
S4 MCA

1.Relevance

- Security is one of the main challenges for the implementation of computing for many service based companies.
- It is possible that a file with sensitive information can get corrupted or damaged.
- Once we upload a file in public domains, we should check whether the file is corrupted or not.
- So it is important to consider the need for protection of sensitive data in cloud computing environment.

2.Description

- This model consists of mainly 3 levels of authorization :

1. Authorization Level
2. Encryption
3. Auditor.

The model uses encryption to secure the files present in our system. A cloud user can verify their account using username and password. The auditor can check whether a file is corrupted or not.

In this system the data in files are encrypted. This method leads to protect our data from penetration or exposure to viruses. The data is not exposed to theft or breach, and messages exchanged in the system environment will be protected.

3.Objectives

- To ensure security and privacy for storing sensitive information in cloud
- To enable users to know whether the data is corrupted or not through auditor.
- Auditing the file and replace the corrupted ones thus implementing more security.

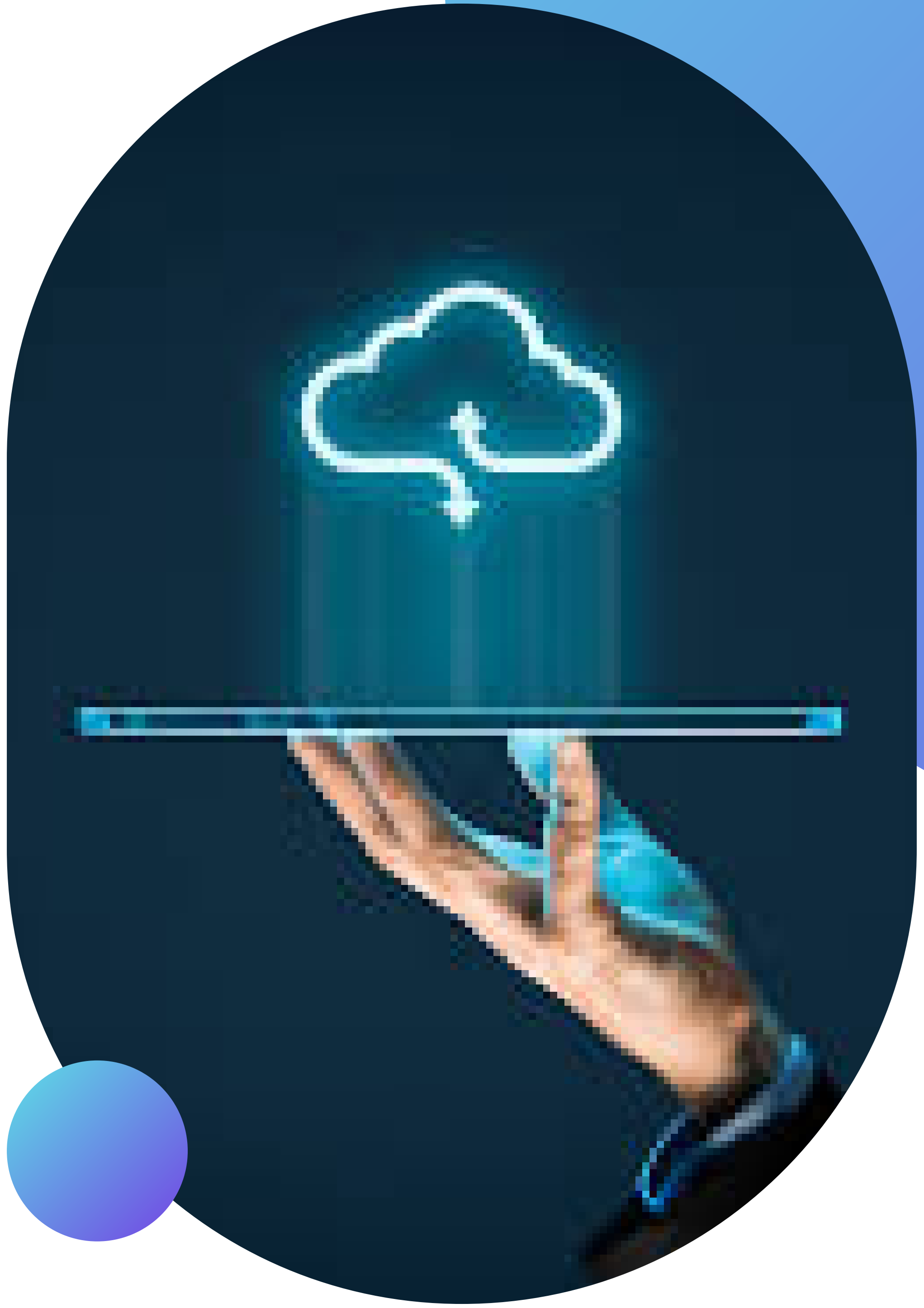
4.Existing System

- The existing system implements a cloud environment for storing data and records.
- It doesn't guarantee the protection of data and content within.
- If a file is stored long back say 2020, the user cannot know whether it is damaged or not unless he/she goes and check the file in the system which is a tedious task.
- Data is prone to malicious attacks and threats.

Proposed System

The proposed system adds an extra layer of security .

- Files are stored in an encrypted format.
- We can upload any type of file;text,image etc.
- More secure compared with the existing system.
- Auditing helps to restore damaged files and records.



6.Input/Output and Modules identified

The input into the system is any type of file and the output defnes whether the input file is corrupted or not.

01 ADMIN

02 USER

03 AUDITOR

04 STORAGE/SHARING

05 ENCRYPTION

Methodology and algorithms

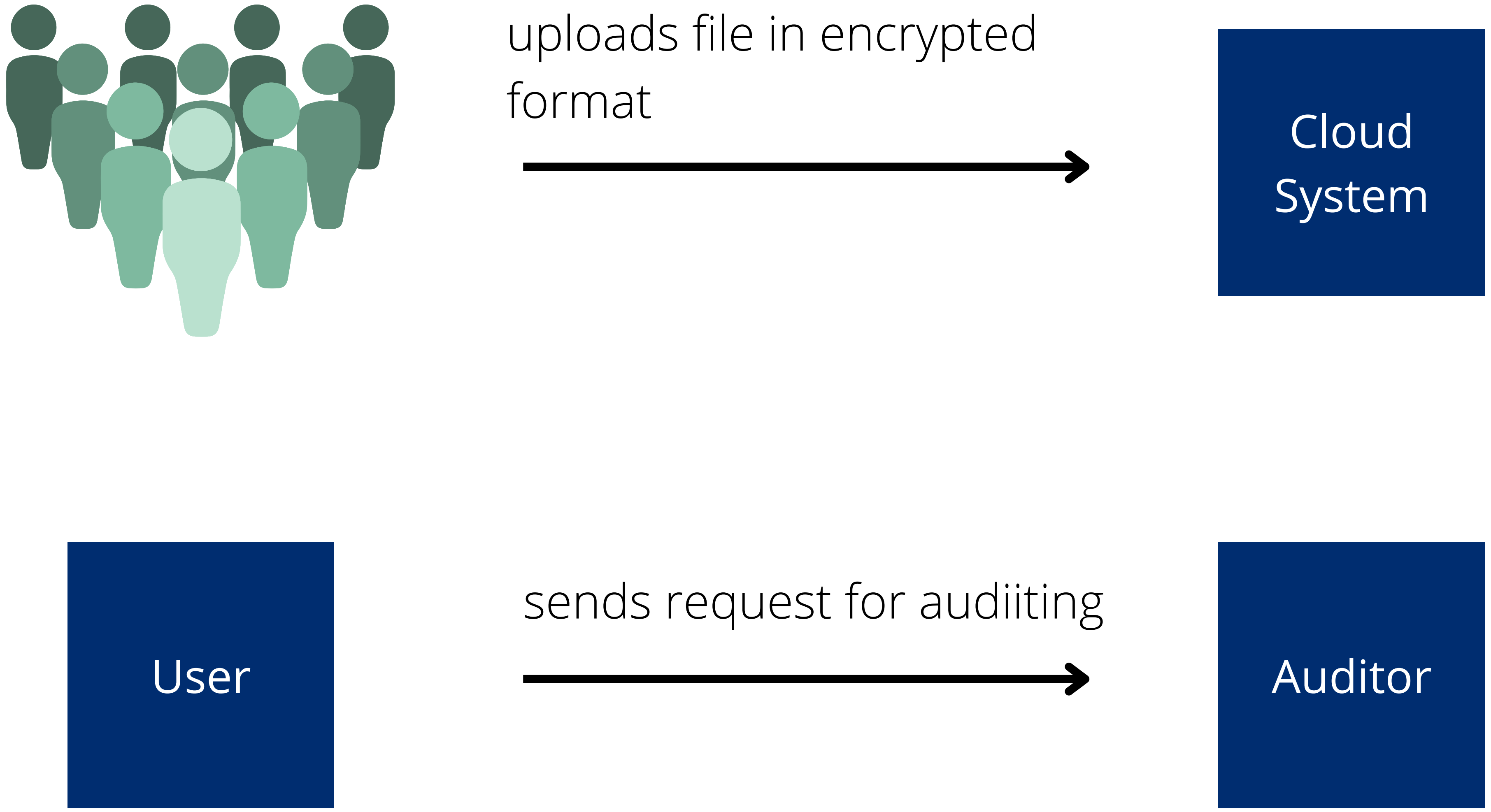
There are mainly 3 types of users namely **ADMIN,USER and AUDITOR.**

USER:

- The User here denotes a typical cloud user.He/She can upload a file from their system.
- The file uploaded will be in an encrypted format.
- It is encrypted using **AES encryption algorithm.**
- Advanced Encryption Standard (AES) is a block cipher.
- Once the file is uploaded, the user can sent request for auditing the file.

AUDITOR

- Once the auditor receives the request,he/she should send access permission request to the user for accessing the file.
- The user needs to send the original file and the auditor compares the original file with the file present with the auditor.
- The Auditor compares the files and analyze the files using the signature and batch comparison.
- The signature is generated using **SHA algorithm.**
- Secure Hashing Algorithm is a cryptographic hash function which takes an input and produces a 160-bit hash value.
- If the signature and the data of the both files matches the files are secure oitherwise the auditor can replace the file.



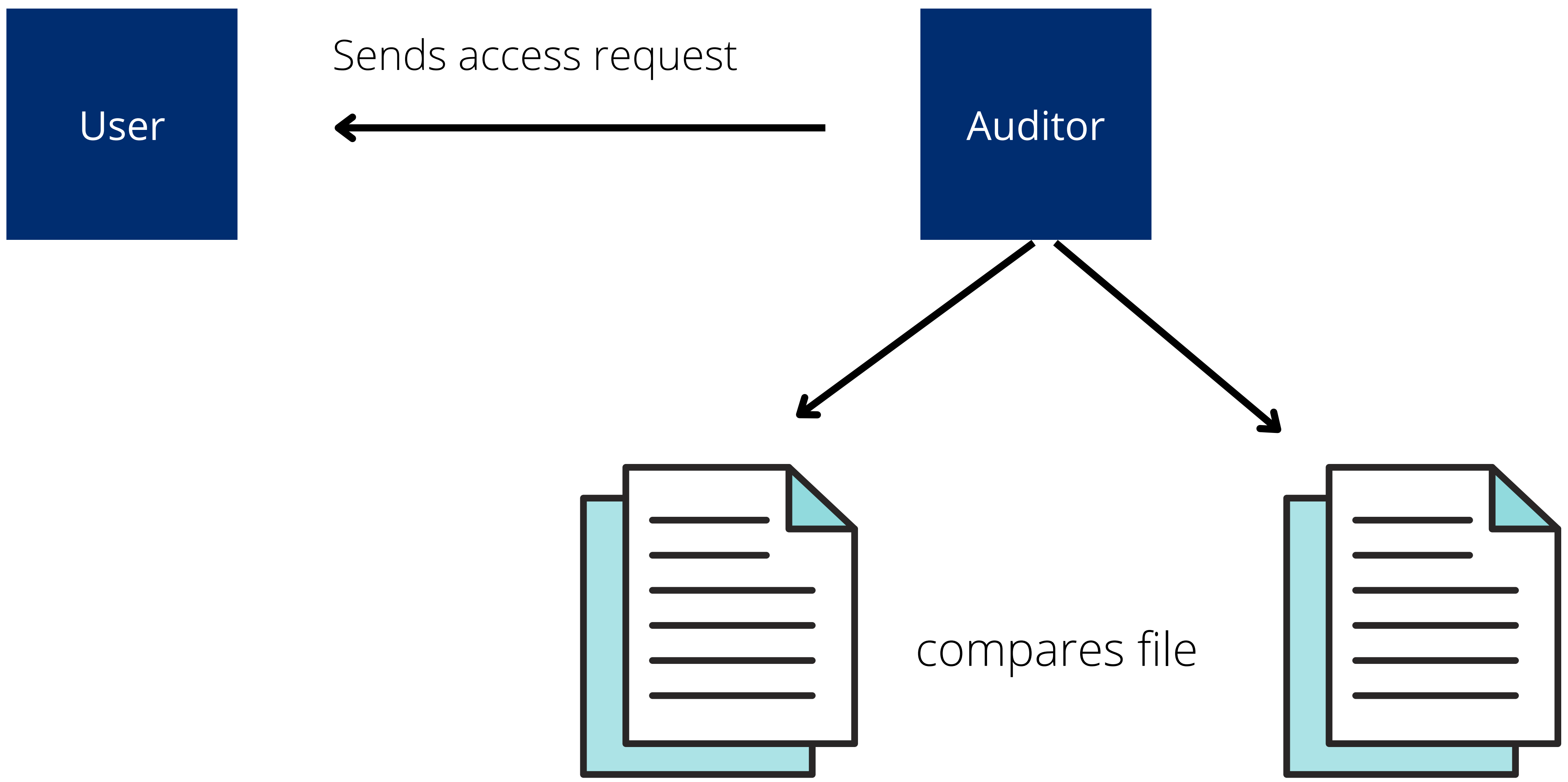
uploads file in encrypted format

Cloud System

User

sends request for audiiting

Auditor


User
Sends access request
Auditor
compares file

Packages

- **pyAesCrypt**
  pyAesCrypt is a Python 3 file-encryption module and script that uses AES256-CBC to encrypt/decrypt files and binary streams.
- **hashlib**
  The Python hashlib module is an interface for hashing messages easily.
  This contains numerous methods which will handle hashing any raw message in an encrypted format.
  The core purpose of this module is to use a hash function on a string,
  and encrypt it so that it is very difficult to decrypt it.

THANK YOU