MEDICAL IMAGES SECURITY IN CLOUD COMPUTING USING CP-ABE ALGORITHM

K. Karunasri, Gadiraju Mahesh and R. Shiva Shankar
Department of CSE, SRKR Engineering College, Bhimavaram, Andhrapradesh, India
E-Mail: karunasri.kallepalli369@gmail.com

ABSTRACT

Health care is required to maintain a person's mental and physical well-being. Every day, healthcare facilities generate a large amount of data, which must be stored and processed. As a result, massive storage systems are needed to resolve this problem. Cloud storage is one of the emerging technologies in the health care sector. Cloud as a service offers scalable computational resources. Despite its advantages, storing health data on cloud storage will raise security concerns. For this purpose, a Ciphertext Policy Attribute-Based Encryption Algorithm (CP-ABE) is proposed in a multi-cloud environment to store medical images securely. The implementation results show that the proposed solution enhances data storage effectiveness and security using a novel technique. Consequently, the proposed method provides the healthcare providers security and privacy for efficiently sharing and storing the data.

Keywords: Security, Data Storage, Cloud Computing, ciphertext policy attribute-based encryption algorithm (CP-ABE).

INTRODUCTION

Health care has become one of the largest sectors in terms of revenue as well as employment. Nowadays, Health care professionals mainly depend on medical images to support clinical decisions. Because of new advancements in imaging tools, modern healthcare institutions generate a massive level of healthcare images daily [1]. The main reason for this is the growth in the number of patients requiring medical services. As a result, ample storage space is always in high demand. Unfortunately, healthcare domains rely on local data centres to store medical data and manage business processes. A significant adverse effect on operational expenses like licensing charges and servicing. To resolve these concerns, healthcare organizations are looking into cloud storage instead of on-premise hosted solutions.

Cloud computing is a relatively new technology that helps healthcare professionals to concentrate solely on their primary duties. Furthermore, the provider is responsible for its maintenance and management. So, it is possible to use this technology to access computing resources and services at any time and from any location. Health care organizations are billed according to a pay-per-business model [2]. Cloud services such as Software, Infrastructure, and platforms are provided to consumers. Cloud security is divided into three categories: user information security, network security, and system security. Figure1 shows the absolute division security.

In the proposed paper, the goal is to provide user information security. Cloud technology helps different healthcare providers to collaborate, communicate, and coordinate. It will provide infrastructure and applications that are fast, adaptable, expandable, and cost-effective [3].

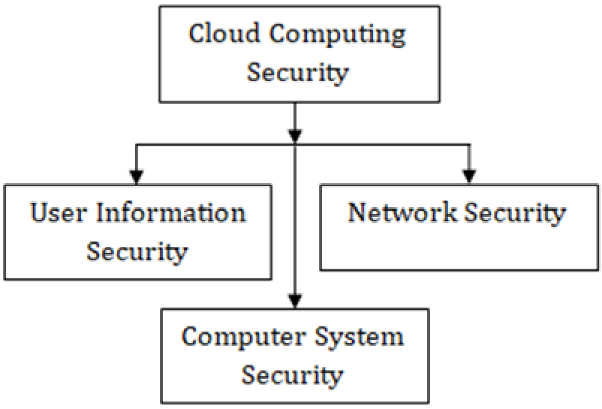


Figure-1. Categorical division of cloud security.

The cloud can assist pharmacy information systems, electronic health records (EHRs), patient records, laboratory information systems protection, management, storage, archiving, and sharing. Patients will receive better overall care due to current health records and ongoing interactions between multiple health care providers.

Despite its advantages, the main obstacles are the absence of standards, restrictions, interoperability issues, safety, privacy, and trust issues, which prevent primary care providers from adopting cloud computing. The current paper discusses a proposed algorithm called CP-ABE to provide data confidentiality and security on the cloud for the medical images by encrypting them and helping the health care providers securely store and retrieve the pictures only by the authorized users.

CLOUD-BASED MEDICAL IMAGES

Medical providers depend on the information provided by patients' medical imaging to detect the disease in the early stages, and they can provide better treatment. Health care providers focus on cloud storage rather than local data centers because they provide huge medical records daily. Cloud offers scalable, cost-efficient resources and three deployment models are suggested as services: Software, platform, and infrastructure [2].

a) Software As A Service

Healthcare institutions use imaging tools and Software for processing medical images. In this Doctor sends medical images to the cloud provider who analyses the digital record, and the final result of a medical image is sent to doctors. Users are charged only for the cloud services they use, as shown in Figure2.

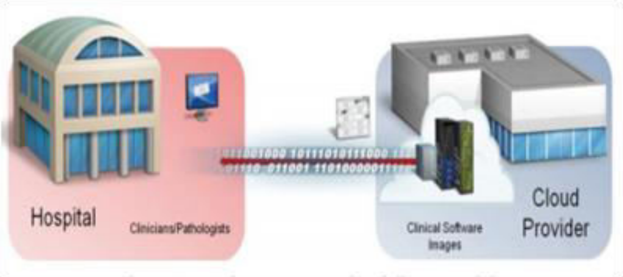


Figure-2. A delivery model for software as a service [2].

b) Platform As A Service

Health care organizations deploy their applications on the provided cloud platform. In these databases, programming languages and deployment tools are offered to clients through the internet. Clients depend on this resource to build and install the image processing tools and can access services from anywhere and anytime. Cloud providers are responsible for maintaining and upgrading the platform, as shown in Figure3.

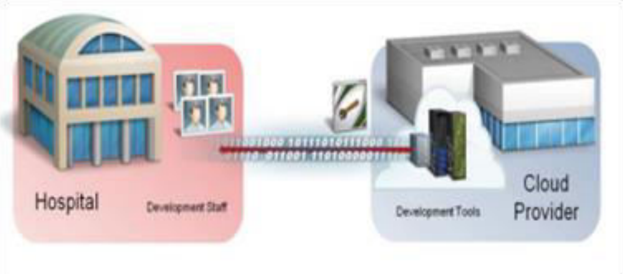


Figure-3. A delivery model for a platform as a service [2].

c) Infrastructure As A Service

Health care suppliers rent storage systems and remote virtual machines. This virtualization uses technology to utilize the same hardware components to minimize operating charges. A cloud service provider is responsible for upgrading and maintenance of cloud infrastructure. Medical providers use cloud facilities to store patients' images of medicine and help perform online backups by cloud services, as shown in Figure-4.

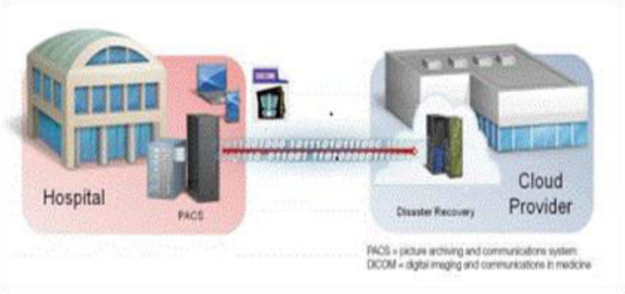

DICOM
Hospital
PACS
Disaster Recovery
Cloud Provider
PACS = picture archiving and communications system
DICOM = digital imaging and communications in medicine

Figure-4. A delivery model for infrastructure as a service [2].

SECURITY CONCERNS IN CLOUD-BASED IMAGE STORAGE

Cloud aimed to provide outsourcing service to an external party. For this reason, cloud computing relies on various technologies like virtualization, Distributed systems, and web technologies. Despite their uses, these technologies are sources of security risks.

a. Virtualization

Virtualization is a technique which it offers cost-efficient savings by creating several virtual versions from the physical hardware resources. It allows several applications and operating systems to execute on the same hardware. It ensures high availability, storage migration, and low latency. Virtual machines bring safety issues like VM image sharing.

b. Data And Storage Issues

Cloud computing architecture depends upon distributed systems for providing scalable computational resources. Data stored in local data centres raises availability, load balancing, and scalability issues. Implementation in cloud storage leads to security issues like improper environment, data backup, and data recovery vulnerability.

c. Web Technologies

Cloud provider highly depends on web technologies to provide IT services accessible through the internet. Standard application programming interfaces (API) are used to manage and connect application layers with the cloud services. Specific security issues such as SQL injection, session management, and cross-site scripting are arising.

CLOUD-BASED IMAGE PRIVACY REQUIREMENTS

The use of the cloud provides high levels of availability, scalability, reliability, and cost-saving. Due to this, health firms are looking to implement cloud storage. Regardless of its benefits, the transitions into the cloud have several obstacles. In this, privacy and security issues must be cleared before shifting into cloud storage. In this, we discussed security requirements and security services.

A. Security Requirements

a. Integrity

Medical providers depend on medical images to diagnose the disease, so any modification in medical images degrades image quality and leads to the wrong diagnosis. So, integrity can be achieved through watermarking and encryption.

b. Confidentiality

Patient's medical data are private, should be protected from unauthorized users, and should be disclosed to only authorized health care professionals. Specific measures must be taken to safeguard Images against cloud providers. So encryption must be done to medical images before transmitting them to the cloud. Techniques that achieve this are CP-ABE, visual cryptography, steganography, etc.

c. Data ownership

It is essential to determine the rightful owner of medical images. Patients should be able to access their medical records and delegate access to authorized healthcare professionals. Techniques like watermarking and steganography have been proposed to identify the owner by embedding the patient's id into the image. The extracted watermark is used for authentication purposes.

B. Security Services

a)Authentication

It refers to the process of identifying a user Authentication system checks if the identification of a user is identical to the stored credentials. Access control policy generally relies on an authentication mechanism to manage permission to access cloud services.

b)Authorization

It permits specific access rights to resources, services, and activities. Based on users' identities, it allows or denies access to detailed medical data. Security policy is deployed within healthcare organizations so that rightful owners access service.

c)Availability

Patients' records should be accessible from anywhere and anytime because they are used for diagnosis and detection. Cloud infrastructure uses a distributed systems approach to enhance reliability. Diverse Technologies are involved in ensuring availability, including load balancing algorithms.

LITERATURE SURVEY

AthishMon, *et.al* [4] proposed digital watermarking and cryptography to protect medical data transfer in an EHR system. In this case, encryption and digital watermarking techniques were used to protect the medical image from unauthorized access. Because telemedicine is becoming more popular, it is critical to safeguard the medical image in medical care.

Al Hamid, *et.al* [5] discussed that this paper's primary goal is to use fog computing to protect healthcare data in the cloud. A key agreement method is proposed that uses bilinear pairing encryption to create session keys for encrypted transmission. Using the decoy approach, healthcare data is processed and securely stored.

Yao, Xin,*et.al* [6] implemented a CB-PHR system in which data owners allow multiple data providers, such as physicians and doctors, to upload encoded medical data in the cloud to enable seamless safety. Still, every data user should also give way to encrypted data indexes to allow questions about the encrypted data. (MOPSE) a scheme that enables the cloud to combine encrypted information indexes from various data sources without knowledge of the index's data.

Doctors most rely on medical images to support clinical decisions Marwan *et.al* [2]proposed a visual cryptography scheme for protecting medical images in the cloud. This visual cryptography is used to encrypt each secret image into shares and is stored in 2 clouds to achieve privacy. During the decryption, overlapping allocations create other interferences, affecting the reconstructed image's quality.

Huaqun Wang [7] proposed the public cloud data exchange system and its application in Electronic-Health records. This thesis presents a new method for secure data transmission to ensure data owner privacy and the security of external providers' cloud data. The proposed model allows for data adaptability while addressing security and privacy concerns about data sharing.

Waleed, *et.al* [8] explained a new technology for user security and privacy in open-source cloud computing applications. This aspect of the research article concentrates on methods to strengthen user privacy and safety in cloud computing. In this, a simulation of a few of the possible threats on consumers' metadata and data stored in Eucalyptus data files are used for the needed details on the risks of compromising cloud users' personal information. Esposito Christian *et.al* [9] used seven stages of key management procedures. A leak detection component was used to read data communicated and archived within cloud computing whenever a manufacturing operation is carried out. The entire infrastructure's proper data stream was checked. Even though all of the firm's preventive measures are taken, a data loss can still happen. The identification of breaches is still a developing field.

Sajid Anam, *et.al* [10] illustrated a few essential details regarding industrial SCADA (Supervisory control and data acquisition) devices, concentrating on attacks, weaknesses, and maintenance. The type of information in that environment requires it to be saved on server/s for backup or the ability to share purposes, so these systems typically rely on a third person. The confidential information on such clouds is protected, and the data may not even be distributed between other customers.

Rachna Jain, *et.al* [11] assured about the encryption protocols that could be used as secure storage that can support cloud computing to a certain point; this also depends on the massive drawback of safe storage, it is that it cannot operate processing on encrypted files; this issue is fixed using homomorphic encryption, even though data is collected as ciphertext as well as processing is done on this encrypted text. As a result, there is no sign of information leakage. The proposed methodology deals with effective data scanning to safeguard it from beginning to finish. A distinct concept of performance monitoring has been taken.

El Makkaoui, *et.al* [12] introduced the processes and classifications of Homomorphic Encryption and briefly explained the difficulties faced during method adoption. Some of the issues that may arise include system efficiency, reliability, processing server lag, etc. To solve the problems, we have to improve performance, and innovative multi-agent structures at Cloud processing services can be used. Garg Prachi, *et.al* [13] discussed the issue of data protection that had been analyzed, and it illustrates existing security strikes on the premise of the Amazon EC2 cloud. Cross-site scripting attacks, SQL injection attacks, man-in-the-middle attacks, network security attacks like Sniffer attacks, DNS attacks, and application security threats like cookie poising, Denial of service attacks, and Backdoor attacks have been mentioned. It presents a methodology that engages two distinct protocols, DES and AES, and compares to address the abovementioned safety problems.

Nayak AA *et.al* [14] defined security risks and the defensive measures that could be done to fix those conflicts, and it also goes over the features of cloud computing and its use in the modern world. It discusses potential risks to information or data secrecy. The "Threat Protection System Using Self-Destructive Mechanism" was proposed in this study for cloud access control. It also clarified the theoretical perspectives of all cloud-related hazards and their alternatives. Users had compared the different security protocols and their course of action, which would be used efficiently.

Babitha MP *et.al* [15] explained various data privacy and security concerns in a computing environment and suggested a model for improving security-related services such as authorization, authentication, Confidentiality, and tracking in latency. The Advanced Encryption Standard of 128 bits enhances Confidentiality and security. Then details are AES-encrypted and stored in the cloud SMS notification process to restrict users' access to data.

Chen *et.al* [16] to safeguard an EHR communication and integration mechanism in hybrid health care clouds in routine and contingency cases in this procedure, every medical record has been encoded in private and public cloud environments that used an independent symmetric key. The doctors create an EHR, encrypted with CK and license L. The decryption is possible with the patient private key and splits into two, which are stored in the patient, smart card and the in-hospital server.

Saran Puneet, *et.al* [17] proposed research of medical facilities it is the literature review on how cloud computing is necessary for storing Health care data and concerning the protection of data in cloud servers and networks by analyzing state of the art with infield and security between two hospitals is controlled by a security provider such as AWS, GOOGLE that is not only easily accessible to a client by itself, but it is less vulnerable to attacks which increase the medical record security [18].A revolutionary rough skyline calculation approach was designed to trim poor designs employing all-round command connection to enhance hanging. Multi-feature similarity syntheses utilizing an evolutionary algorithm and relevance feedback systems are used to improve the effectiveness of the image extractor method [19].

RS Shankar, *et.al* [20] did their research on a brain hugely inspired Knowledge-Growing System (KGS) that can significantly increase knowledge via the acquisition of information when time is surpassing. The difficulties of duplicating user-requested material on ideal Cloud sites and allocating sites to users are examined [21]. Many businesses must be able to analyze large quantities of data in a contemporary way [22]. Apache Map Reduce (MR) substantially improved parallel computing for regular users, while Hadoop and cloud-based computing made large-scale parallel and distributed data more accessible than ever [23].

METHODOLOGY

a) Dataset

The data set consists of 1000scans of chest infected images Obtained in mosmed repository. Among these, 100 CT Scan images are considered and applied with the proposed algorithm. The average size of every input image is 200kb. In cloud storage, the size of the medical image can be up to 1000kb. In this work, 3 attributes are considered: image name, image size, and image resolution.

b) Objectives

a. To improve the encryption and decryption, and reduce processing time for faster access.
b. To provide efficient and equal shares of the images that are encrypted.
c. Efficient management of multiple cloud storage.
d. To improve the quality of the image decryption quality is calculated using PSNR for every output image.

SYSTEM ARCHITECTURE

The healthcare provider who wants to store images on the cloud must login to the system. Once login is successful, the image is uploaded, and the image is encrypted before storing on cloud storage, as shown in Figure 5. Security must be provided to pictures because no one should modify the data. So this purpose CP-ABE algorithm was used.

Setup phase

In this process, setup takes implied security parameters, and no inputs are taken. Here it outputs the Master key Mk and public key PK.

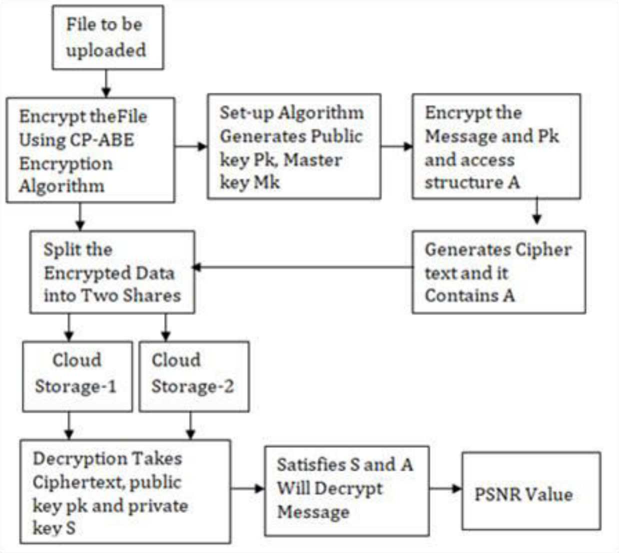

File to be uploaded
Encrypt theFile Using CP-ABE Encryption Algorithm
Set-up Algorithm Generates Public key Pk, Master key Mk
Encrypt the Message and Pk and access structure A
Split the Encrypted Data into Two Shares
Generates Cipher text and it Contains A
Cloud Storage-1
Cloud Storage-2
Decryption Takes Ciphertext, public key pk and private key S
Satisfies S and A Will Decrypt Message
PSNR Value

Figure-5. An operational flow of Architecture.

Encryption

When it comes to encryption, it acquires inputs of public parameter PK generated by the setup algorithm, the input image, and the access structure A, which is nothing but a few attributes of the user from all the set of features. This scheme will encrypt the image and create a ciphertext. So, the person whose features are satisfied with the access policy can decrypt. After the encryption, the encrypted data is divided into shares and stored on virtual clouds. Each share cannot be viewed separately on the cloud; only after decryption, the original image can be viewed.

Multi-cloud

The adoption of the cloud reduces the security threats by CP-ABE methods; the access control policy is usually masked in the header of ciphertext as a decoding variable in plaintext to execute the decryption process effectively. Likewise, the user attributes are stored in unencrypted text in the title of the person's private key. In the CP-ABE technique, decryption operations are commonly done at the operator or even in the cloud, drastically increasing access control effectiveness. When the cloud has been used for decryption, not only the user's features be fully revealed to the cloud, but the malware cloud will also see the confidential data concealed in the access control policy. Analyzing that only one cloud can acquire all attribute series and entire access control structure tends to result in privacy leakage issues, so here we use multi-cloud hereafter encryption. So, in this work, data is split into shares and stored in the multi-cloud after encryption.

Decryption

If the health care users want to get image data stored on the cloud, then the algorithm for decryption uses a public key PK and encipher text CT and a private key SK, a series of attributes. If the characteristics of the user satisfy the access policy, then the requested image is decrypted; otherwise not. After decryption, the PSNR value is used to find the image's pixel resolution.

PROPOSED ALGORITHM

Step 1	Read the file data.
Step 2	Set up: The setup algorithm takes security parameters P and attributes as inputs and generates public key PK and Master key Mk. Setup(p) → (Mk, Pk)
Step 3	Encryption Input: Pk, M, A Output: CT 1. Select random element $s\in Z_{p.}$ 2. Compute Secret shared $\epsilon_{y,}\forall$ T in A. 3. Compute $C_0=L^s$ and $C_1=M.Y^s=M.\ e\ (g.\ g)\ ^{as}$. 4. Compute $C_{y\,=}L^{\in}{}_{y}C_{yp}=H(att(Y))\ \forall\ T\in A$. 5.Return CT = $\{C_{0,}\ C_{1,}\ \forall\ y\ \in Y:\ C_{y,}\ C_{yp}\}$
Step 4	Key generator: It takes Master key Mk and set of attributes S and outputs private key Sk. Keygen (Mk, S) → Sk
Step5	Decryption Input: PK, CT, SK Output: M 1. The decryption algorithm takes public key PK, Ciphertext CT, which contains access policy A and private key SK, which is a private key for set S of attributes. 2. If the Set S of attributes satisfies the access policy A, then the algorithm decrypts the message. $M=\frac{C1\prod_{i=1}^{n} e(\,Cyp,Di,2)}{e(C0\,,D0)\prod_{i=2}^{n} e(Cy,Di,1)}$

a) CP-ABE

In this Ciphertext Policy Attribute-based Encryption method, the data owner specifies the access control policy, consisting of logical pairings of user attributes inserted in encrypted data in cleartext. Variousfact sets discussing the user's features are inserted in the user's private key. If the user has access privileges, then he can decrypt encrypted data as long as the user attributes picked confirms the design of the access control policy.

b) Algorithm

The implementation is built on the JPBC library, a java-based open library that supports cryptographic methods to execute the design setup, key generation, encryption, and decryption algorithms. In decryption, [$D_{0,}$ $D_{i,1,}$ $D_{i,2}$] are the secret key. When the user uploads an image, the setup algorithm takes the user's security parameter and universe of attributes as inputs. It generates public key PK and Master key Mk. The encryption takes, and Pk and access structure as inputs encrypts message M and outputs ciphertext CT.

The key generator takes a master key, user ID, and name and generates a private key. For decryption, it accepts three inputs PK, ciphertext CT, and a secret key SK with several attributes S. If the Sequence of S attributes meets the requirements of access policy A, the model decrypts the image. The split Image function is used to divide encrypted images into shares. The processing time is calculated from encryption to the uploading of data on clouds.

RESULTS

The experimental results were conducted on 100 CT scans of chest infected images that are collected from https://mosmed.ai/en/datasets/ were shown in Figure-6. Java and JDK 1.8 with Net Beans 8.1 as an IDE are used to implement the algorithm. Parameters such as Encryption time, decryption time, and PSNR (peak signal Noise Ratio) to calculate the quality of the decrypted image. Figure6 shows the chest images dataset.

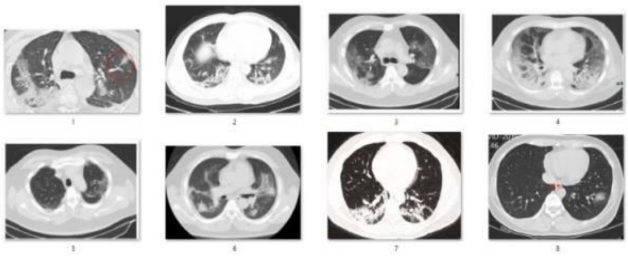
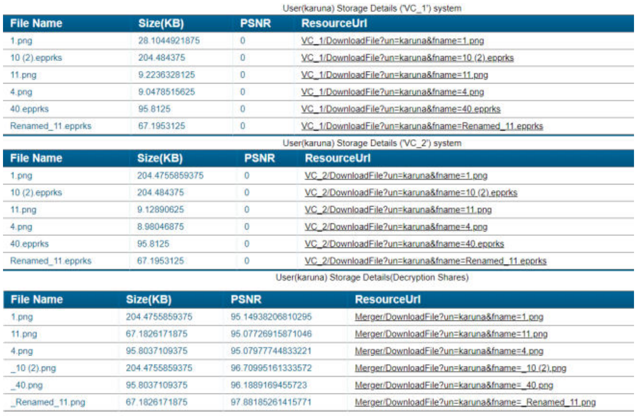


Figure-6. Chest images dataset.

Figure-7 shows image share stored on two clouds, VC1 and VC2, after encryption, and we can decrypt an encrypted image.



User(karuna) Storage Details ('VC_1') system

File Name	Size(KB)	PSNR	ResourceUrl
1.png	28.1044921875	0	VC_1/DownloadFile?un=karuna&fname=1.png
10 (2).epprks	204.484375	0	VC_1/DownloadFile?un=karuna&fname=10 (2).epprks
11.png	9.2236328125	0	VC_1/DownloadFile?un=karuna&fname=11.png
4.png	9.0478515625	0	VC_1/DownloadFile?un=karuna&fname=4.png
40.epprks	95.8125	0	VC_1/DownloadFile?un=karuna&fname=40.epprks
Renamed_11.epprks	67.1953125	0	VC_1/DownloadFile?un=karuna&fname=Renamed_11.epprks

User(karuna) Storage Details ('VC_2') system

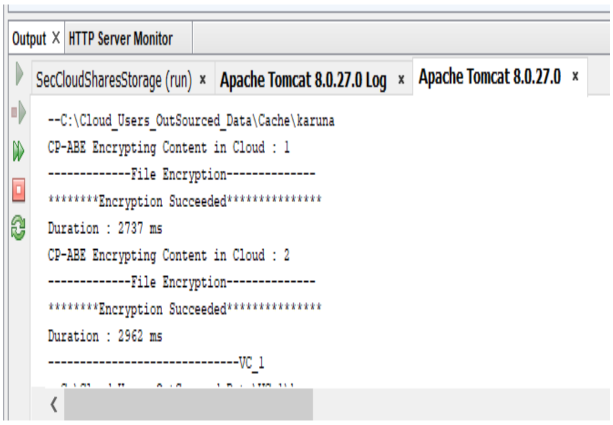
File Name	Size(KB)	PSNR	ResourceUrl
1.png	204.4755859375	0	VC_2/DownloadFile?un=karuna&fname=1.png
10 (2).epprks	204.484375	0	VC_2/DownloadFile?un=karuna&fname=10 (2).epprks
11.png	9.12890625	0	VC_2/DownloadFile?un=karuna&fname=11.png
4.png	8.98046875	0	VC_2/DownloadFile?un=karuna&fname=4.png
40.epprks	95.8125	0	VC_2/DownloadFile?un=karuna&fname=40.epprks
Renamed_11.epprks	67.1953125	0	VC_2/DownloadFile?un=karuna&fname=Renamed_11.epprks

User(karuna) Storage Details(Decryption Shares)

File Name	Size(KB)	PSNR	ResourceUrl
1.png	204.4755859375	95.14938206810295	Merger/DownloadFile?un=karuna&fname=1.png
11.png	67.1826171875	95.07726915871046	Merger/DownloadFile?un=karuna&fname=11.png
4.png	95.8037109375	95.07977744833221	Merger/DownloadFile?un=karuna&fname=4.png
_10 (2).png	204.4755859375	96.70995161333572	Merger/DownloadFile?un=karuna&fname=_10 (2).png
_40.png	95.8037109375	96.1889169455723	Merger/DownloadFile?un=karuna&fname=_40.png
_Renamed_11.png	67.1826171875	97.88185261415771	Merger/DownloadFile?un=karuna&fname=_Renamed_11.png

Figure-7. The implementation of CP-ABE encryption and decryption.

The duration of time taken from encryption to the shares of an image stored on the cloud using the CP-ABE algorithm is shown in Figure8.



```
--C:\Cloud_Users_OutSourced_Data\Cache\karuna
CP-ABE Encrypting Content in Cloud : 1
-------------File Encryption--------------
********Encryption Succeeded**************
Duration : 2737 ms
CP-ABE Encrypting Content in Cloud : 2
-------------File Encryption--------------
********Encryption Succeeded**************
Duration : 2962 ms
------------------------------VC_1
```

Figure-8. Processing time from encryption to data stored on cloud.

Table-1. PSNR values comparison B/W VC and CP-ABE.

	PSNR Values	
	Visual Cryptography	CP-ABE
Image1	95	96
Image2	93	95
Image3	95	97
Image4	94	95
Image5	95	97

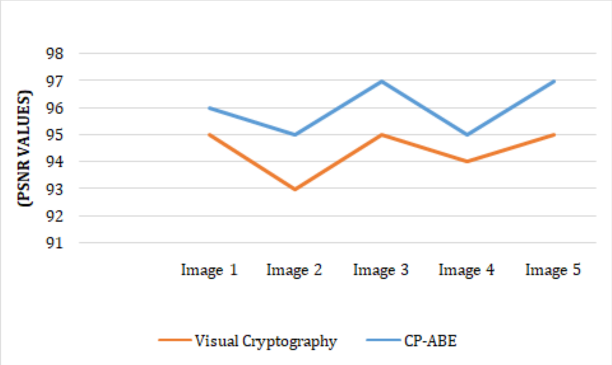


Figure-9. Image resolution comparison between visual cryptography and CP-ABE.

Table-1.Represents the PSNR values compared in b.w CC and CP-ABE for the shared images. Using Table1, a resolution graph was drawn by comparing b/w VC and CP-ABE, as shown in Figure9.

Table-2. Represents the processing time comparison between VC and CP-ABE.

	VISUAL CRYPTOGRAPHY		CP-ABE	
	CLOUD 1	CLOUD 2	CLOUD 1	CLOUD 2
Image 1	3585	3857	2310	2850
Image 2	3957	3910	2838	2392
Image 3	3229	3853	2500	2900
Image 4	3244	3417	2508	2872
Image 5	3486	3138	2351	2655

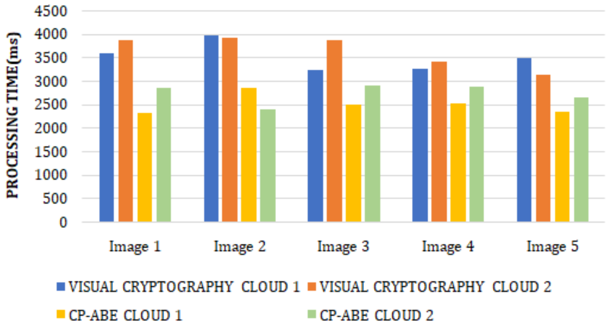


Figure-10. Processing time comparison between visual cryptography and CP-ABE.

From Table2, a graph was shown to represent the Processing time Comparison between Visual Cryptography and CP-ABE in Figure10.

CONCLUSIONS

In General, cloud computing offers cost-efficient storage systems, and it is also advantageous in the growth of the health industry due to its availability, scalability, and low energy consumption. The main concerns in the cloud are privacy and security. The proposed system provides security mechanisms with the help of the CP-ABE algorithm. The proposed algorithm offers Confidentiality by encrypting images with the user attributes and storing encrypted data on the multi-cloud after dividing it into shares. Authorized users could access appropriate data securely after decryption. The results show that the CP-ABE works better by improving the quality of the decryption image, which is calculated using PSNR and reducing the processing time of encryption.

REFERENCES

[1] Hussein N. H. 2019, March. Cloud-Based Efficient and Secure Scheme for Medical Images Storage and Sharing using ECC and SHA-3. In 2019 2nd Scientific Conference of Computer Sciences (SCCS) (pp. 109-115). IEEE.

[2] Marwan M., Kartit A.&Ouahmane H. 2017, October. Protecting medical images in the cloud using a visual cryptography scheme. In 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech) (pp. 1-6). IEEE.

[3] Al-Issa Y., Ottom M. A.&Tamrawi A. 2019. eHealth cloud security challenges: a survey. Journal of healthcare engineering.

[4] AthishMon F. &Suthendran K. 2018. Combined cryptography and digital watermarking for the secure transmission of medical images in EHR systems. International Journal of Pure and Applied Mathematics. 118(8): 265-269.

[5] H. A., Rahman, S. M. M., Hossain, M. S., Almogren A.&Alamri A. 2017. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access. 5, 22313-22328.

[6] Yao X., Lin Y., Liu Q. & Zhang, J. 2018. Privacy-preserving search over encrypted personal health record in multi-source cloud. IEEE Access. 6, 3809-3823.

[7] Wang H. 2018. Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record. IEEE Access. 6, 27818-27826.

[8] Waleed A. M. &Chunlin L. 2016. User privacy and security in cloud computing. International Journal of Security and Its Applications. 10(2): 341-352.

[9] Esposito C., Castiglione A., Martini B.& Choo K. K. R. 2016. Cloud manufacturing: security, privacy, and forensic concerns. IEEE Cloud Computing. 3(4): 16-22.

[10] Sajid A., Abbas H. & Saleem K. 2016. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. IEEE Access. 4, 1375-1384.

[11] Jain R., Madan S. & Garg B. 2016, February. Homomorphic framework to ensure data security in cloud environment. In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH) (pp. 177-181). IEEE.

[12] El Makkaoui K.,Ezzati A. &Hssane A. B. 2015, June. Challenges of using homomorphic encryption to secure cloud computing. In 2015 International Conference on Cloud Technologies and Applications (CloudTech) (pp. 1-7). IEEE.

[13] Garg P., Goel S. & Sharma A. 2017, May. Security techniques for cloud computing environment. In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 771-776). IEEE.

[14] Nayak A. A., Sridhar N. K. & Poornima G. R. 2017, May. Security issues in cloud computing and its counter measure. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT) (pp. 35-41). IEEE.

[15] Babitha M. P. and K. R. Remesh Babu Secure cloud storage using AES encryption. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), pp. 859-864. IEEE.

[16] Chenthara S., Ahmed K., Wang H. & Whittaker F. 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access. 7, 74361-74382.

[17] Saran P., Rajesh D., Pamnani H., Kumar S., Sai T. H. &Shridevi S. 2020, February. A Survey on Health Care facilities by Cloud Computing. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-5). IEEE.

[18] Shankar R. S., Sravani K., Srinivas L. V., Babu D. R. An approach for retrieving an image using Genetic Algorithm. International Journal of Latest Trends in Engineering and Technology. 2017;9(8):057-64.

[19] J Rajanikanth, M. Sai Padmini , R. Shiva Shankar. An Innovative Skyline computation strategy to share unskilled Policies Using MapReduce. Journal of Advanced Research in Dynamical & Control Systems.2018; 10 (9) Special Issue, 637-645.

[20] Shankar R. S., Deshai N., Murthy K. S., Gupta V. M. The Source of Growing Knowledge by Cognitive Artificial Intelligence. In2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN) 2019 Mar 29 (pp. 1-6). IEEE.

[21] Mahesh G., Rao V. M., Shankar R. S., Sirisha G. V. Primal-dual parallel algorithm for optimal content delivery in cloud CDNs. In2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) 2017 Dec 14 (pp. 1-6). IEEE.

[22] Deshai N., Shankar R. S., Sravani K., Ravibabu D. A Developed Task Allotments Policy for Apache Hadoop Executing in the Public Clouds. In2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN) 2019 Mar 29 (pp. 1-4). IEEE.

[23] Li C., He J., Lei C., Guo C.& Zhou K. 2018, December. Achieving privacy-preserving CP-ABE access control with multi-cloud. In 2018 IEEE, Sustainable Computing & Communications (pp. 801-808). IEEE.