CIADS: A Framework for Secured Storage of Patients Medical Data in Cloud

SURESH JAGANATHAN
Department of Computer Science and Engineering
SSN College of Engineering, Anna University
Chennai, Tamilnadu
INDIA
sureshj@ssn.edu.in

DHIVYA VEERAPPAN
Programmer Analyst
Cognizant Technology Solutions
Chennai, Tamilnadu
INDIA
vsdhivya@gmail.com

Abstract: Patient medical details, diagnosis results and recommendations by the doctors considered as medical data. These data are a valuable asset for the hospitals and stored securely. Grid computing provides facility called ImageCare platform provided by DICOMGrid, which allows only authorized doctors to store, search and access medical data. Since the data resides in off-site, these considerations have to be checked, i) storage size, ii) security type, iii) backup and iv) recovery of data. In this paper, a new cloud storage model is proposed *(CIADS[**C**onfidential-**I**ntegrity-**A**uthentication based **D**ata **S**tore])* for patient's medical data, adopting DaaS model. The proposed model addresses the above-said considerations and also based on CDMI set of standards provided by SNIA.

Key–Words: Security, Cloud Computing, Cloud Storage, Encryption, CDMI, Medical Data

1 Introduction

Efficiency is improved by centralizing the resources. Cloud Computing [1] technology does this by interconnecting the remote machines using internet. It allows the user to use the applications without installation and access the personal files at any computer with the help of internet. The cloud model improved availability and composed of five essential characteristics. They are (i) on-demand self-service, (ii) broad network access, (iii) resource pooling, (iv) rapid elasticity and (v) measured service. These features improve the availability of the cloud service to the users.

The health-care [2] industry is the most predominant and fastest growing industries in the world. It consists of diagnostic, preventive, remedial, and prescriptive details by physician, nurses, and hospitals. It also contains medical equipment for treatment, pharmaceutical and health insurance firms. All the documents of health-care industry considered as medical images should retain for future use and analysis of health information. In order to maintain standards of those medical images, Digital Imaging and Communications in Medicine (DICOM) format is used by health-care organizations. Short and long term history about the health information of the country and other health related information can be easily collected using these medical data.

Cloud Computing providers offer a set of software interfaces or APIs that customers use to manage and interact with cloud services [3]. Organizations and third parties often build upon these interfaces to provide value-added services to the customers. All interaction, maintenance and management operations are performed using these interfaces. Authentication and access control to encryption and activity monitoring helps to the interface to protect against both accidental and malicious attempts. There are many ways to compromise the user data. Deletion or alteration of files without a backup of the original content is an obvious example. Loss of an encoding key may result in an active destruction of data. Unauthorized parties must prevent from accessing the sensitive data [4].

Rest of the paper organized as follows, Section 2 explores the related works and current status of security in cloud data store. Section 3 elaborates the algorithmic approach of our proposed work. Section 4 describes proposed framework with the help of use-case diagrams. Section 5 details the proposed system implementation. Section 6 analyzes the experimental results. Section 7 concludes the work.

2 Related Works

Cloud computing security [5] has become an important cause of interfering its development. It has become a hot topic in industry and academic research. Cloud computing has unique attributes that need security assessment in areas such as information credibility, recovery, and privacy, and an assessment of constitutional releases in fields such as e-discovery, regulatory compliance, and auditing. Cloud computing is fraught with security threats and customers going to use it should ask questions and assess the cloud vendor regarding safety measurements provided, before committing.

Customers should demand transparency, bypassing vendors that deny supplying comprehensive data on security programs. Ask inquiries associated to the requirements of policy makers, architects, coders and operators, risk-control methods. Level of testing to verify the functioning as services as proposed, and that vendors can recognise unanticipated vulnerabilities. Noted critical security issues [6] in cloud data store are, i) privileged client access, ii) regulatory compliance, iii data location, iv) data segregation, v) recovery, vi) investigative support and vii) long-term viability.

Since it includes many technologies, there are a number of security issues [7]. The primary security challenge with clouds is that the owner of the data may not have control of where the data retained, because, the data may retrain in some remote locations based on resources available. These resources are scheduled automatically, which is the major advantage of cloud computing. So, to protect the data from the untrusted processes [8], a protection mechanism is needed.

Cloud malware injection [9] attack attempts to inject a malicious service, application into the cloud system depending on the cloud service models. An intruder creates a malicious application, the service instance and add it to the cloud system. Then the attacker modifies the cloud system to treat the malicious software as a valid instance. If it is successful, normal users can request the malicious service instance, and then the malicious code executed; this in-turn affects the security of end-user [10].

Some providers offer free limited trial periods. By using this opportunity malicious code authors and others, inject codes to perform unwanted activities. PaaS providers have suffered most from this kind of attacks; recent evidence shows that hackers have begun to target IaaS vendors as well [11]. While usage scenario is a bit different for different users, there is a core set of evaluation criteria common to all use cases that should consider when choosing a cloud storage provider. Here are eight questions that will help to compare cloud storage services:

1. Does the provider accommodate and support primary use case(s)?
2. Where will data be stored?
3. What kind of security mechanisms are in place?
4. How does the provider ensure data durability, reliability and availability?
5. How easy is it to upload the data, especially when moving large data sets into the cloud?
6. How easy does the provider make it transfer data out of the storage cloud?
7. What kind of access performance does the provider support?
8. Will the provider help to comply with key industry regulations?

2.1 Current Status

Data security[11] involves encrypting the data and also ensuring that appropriate policies adopted for data sharing. Data mining techniques[12] may be applicable to malware detection in clouds. The rapid change to cloud concerns about the critical issues in the environment. Wentao Liu et.al.[14] explained that single security method cannot solve problems. Many traditional and new technologies and strategies should combine for protecting the total cloud computing system.

Dimitrios Zissis et.al. [15] introduced Trusted Third Party, which reduces the security burden to the clients. They assure security characteristics within a distributed information system. The proposed solution uses cryptography, specifically Public Key Infrastructure operation and Lightweight Directory Access Protocol, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution provides trusted cloud service to all the entities [16]. A trusted third party provides low and High level confidentiality, Server and Client Authentication, Creation of Security Domains, Cryptographic Separation of Data, Certificate-Based Authorization.

Akhil Behl et.al.[17] explored that defining and adopting Service Level Agreement (SLA) with providers helps to improve the trust between providers and the customers.The customers should have a plan to counter the service disruptions, for critical applications or services, by keeping backup repository of applications on-premises.

Cloud moves the application software and databases to the centralized large data centers, which is not trustworthy. Qian Wang et.al.[18] introduced third party auditor (TPA), to verify the integrity of the dynamic data stored in the cloud. Client need not audit the data in data store since it is done by TPA. They identified the difficulties and potential security problems of direct extensions of dynamic data updates. The existing storage model is improved by manipulating the classic Merkle Hash Tree construction for authentication. Signature is extended to multi-user setting, to handle multiple auditing tasks by TPA [19].

Prabavathy et.al. [20] developed a system for efficient storage with duplication and compression in cloud computing. Aim is to reduce storage space and to save bandwidth for file transfer. Deduplication uses metadata structures. Only a copy of the duplicate file kept while others deleted, and metadata determines this. Deduplication method adopted for existing files and incoming files. Bins are created by grouping the files according size. The bins are then segmented, deduplicated, compressed and stored. Compressed segments of the file will be sent through internet with file to segment mapping when user request for the file. These are uncompressed and combined to create a complete file, and it reduces the bandwidth [21]. The user can retrieve any file or data dynamically without any data loss. Due to a reduction of bandwidth for communication user interaction time with a cloud is also reduced. Deduplication resides on the storage space of the cloud controller.

Cloud services will not guarantee about the security of client data in storage infrastructure because the current security approaches reduces the performance of cloud storage. Seny Kamara et.al.[22] designed cloud storage that guarantees confidentiality, integrity and verifiable without affecting the utility of the cloud. They introduced the facility to access the data through interfaces, add and delete the files securely. The system built on new cryptographic primitives and protocols and constructed with searchable symmetric encryption scheme and search authenticates. Unencrypted users sensitive data reside in remote machines, owned and operated by third party service providers accessed by unauthorized persons [23]. The confidentiality of user's data from service providers is achieved by, i)separating SaaS and IaaS providers in cloud computing, ii) encrypting details about owners and iii) data obfuscation.

Cloud computing for healthcare information storage has comprehensive benefits. It provides low-cost ownership, better availability to the clinical users. Since the information is critical, it should be securely stored in the cloud. Christian Neuhaus et.al [24] implemented a data store for medical data that has cryptographic mechanism and information rights management concept. To securely store patient medical data Ming Li et.al. [25] implemented a system with new encryption method.

Table 1 summarizes, the existing cloud security implementation with either of the security mechanisms. They secure the text files or medical images to some extent. Proposed system aims to store the medical images with the highest security in the cloud. In the proposed system, confidentiality, integrity-based authorization and authentication of cloud data store are implemented to achieve the utmost security for patients medical data. In table, **C** refers Confidentiality; **I** refers Integrity; **A** refers Authentication, and **Au** refers Authorization.

2.2 Contributions

Forthcoming section explains the contributions done in proposed cloud data store (CIADS). The proposed security mechanisms deployed in the cloud for secured storage. In proposed framework, CIADS layer provides protection to medical data. User credentials ensure authenticity of users in the system. Authorization service implemented through certificates that are issued by certificate authority. Confidentiality is achieved by implementing a new encrypting algorithm involving confusion and diffusion process. Modified hash algorithm checks integrity of the data. Detailed explanations are available in below subsections.

2.2.1 Certificate Authority

Certificate authority (CA) is a trusted third-party organization or company that issues and verifies user certificate. Certificate contains full details of the owner. CA guarantees that the individual obtains a unique certificate is in fact, who claims to be. It ensures that the person who is using that certificate is a valid person. Authorization provides the access rights over the data to the user.

2.2.2 Confidentiality

Confidentiality prevents disclosure of the information to unauthorized individuals or systems. It ensures that the information is only accessible by authorized persons. It prevents unauthorized access over the data. It maintains the privacy of information in the system. Confidentiality is widely implemented by encryption algorithms. In this proposed system, it is achieved by implementing a new algorithm, which adopts confusion and diffusion process. Confusion is the process of making complex relationship between the encrypted image and the key that is being used. Diffusion is the process of making complex relationship between the original image and the encrypted image as complicated as possible.

Table 1: Comparison of Security Provided Data Store

Paper and Year	Contributions	C	I	A	Au
Qian Wang et.al.(2009)	Introduced TPA	yes	yes	yes	-
Seny Kamara et.al.(2011)	Designed cloud storage that guarantees C & I	yes	yes	-	-
Christian et.al.(2011)	Designed Cloud Storage for Medical Data & guaranteed C & AU	yes	-	-	yes
Akhil Behl et.al (2011)	Implemented SLA for AU	-	-	-	yes
Prabhavathy et. al. (2011)	Initiated design of data store - addressing security (C) in terms of compression	yes	-	-	-
Ming Li et.al. (2012)	New Encryption for Data	yes	-	-	-
Dimitrios Zissis et.al (2012)	Implemented Trusted TPA	yes	yes	yes	-
Wentao Liu et.al. (2012)	Initiated Security in Data Store	yes	-	-	-

2.2.3 Authentication

Authentication is the process of identifying an individual, usually based on the user-name and password. It ensures that the person who is having valid user-name and password is the right person to enter into the system. It confirms the identity of the person, not about the access rights.

2.2.4 Integrity

Integrity maintains and assures the accuracy and consistency of the data. It ensures the trustworthiness of the data and denotes that the data not changed during the transaction. The hash algorithm provides integrity. A hash function takes a variable-length datum as input and produces a fixed length output hash value. One fundamental aspect of the hash algorithm is that it must be injective i.e. any two inputs should not result in same hash values. Since patients, medical data are the primary concern; distortion may lead to wrong diagnosis and even threaten patients life. Traditional methods like MD5, SHA can be used to generate hash values. However, since images do not fit as good candidates for traditional hash algorithms, a new direction has emerged in calculating hash for images [26]. It led to calculating hash-based chaotic theory which deals with dynamic systems. Some chaotic maps like logistic maps are a kind of irreversible map that does not produce original data after getting reversed. This algorithm makes full use of every bit in an image file to generate initial vector and to control the digesting process.

3 Algorithmic Approach

In our proposed data store(CIADS)offers security in-terms of confidentiality and integrity. A detailed explanation of algorithms pertaining to above said issues present in this section.

3.1 Encryption

Encryption consists of confusion and diffusion process. Algorithm 1 and 2 are the pseudo code, which explains the operations done for encryption of patient's medical data. Let Image I_0 of size MxN is the input of the algorithm. Encrypted image of the same size will be the output. I be the pixel matrix of the image. Confusion creates scrambled image from the input image. In this algorithm $rowsum$ is calculated by adding all the elements of a row. Then $modulo2$ is calculated for $rowsum$. If the result of $modulo$ is zero then right circular shift with K_R applied, else left circular shift applied. This activity carried out for all the rows of the matrix. Once the row confusion completed, then the column confusion is done with the key K_C. In a column confusion $colsum$ is calculated by adding all the elements of a column, use it for the and up or downshift is done according to the $colmod$ value. Apply for all the columns, resulting scrambled image. Scrambled image taken as input for diffusion and carried for rows and columns. Row diffusion is done by XORing the row pixel values with the corresponding K_C value. Column diffusion by ing the column pixel values with the corresponding K_R value and applied to all the rows and columns respectively, producing encrypted image.

Algorithm 1 Confusion operation

```
Input: Images
Output: Confused Image
  for each row 'i' in the matrix 'I' do
      Generate random vector $K_R$
      for each column 'j' in the matrix 'I' do
          rowsum=rowsum + I [i] [j]
      end for
      rowmod=rowsum % 2
      if $rowmod == 0$ then
          for each $K_R$ do
              I=right circular shift(I)
          end for
      else
          for each $K_R$ do
              I=left circular shift(I)
          end for
      end if
  end for
  for each column 'j' in the matrix 'I' do
      Generate random vector $K_C$
      for each row 'i' in the matrix 'I' do
          colsum=colsum + I [i] [j]
      end for
      colmod=colsum % 2
      if $colmod == 0$ then
          for each $K_C$ do
              $I_{scr}$=up circular shift(I)
          end for
      else
          for each $K_C$ do
              $I_{scr}$=down circular shift(I)
          end for
      end if
  end for
```

3.2 Decryption

Decryption adopts inverse diffusion and confusion. Algorithm 3 and 4 details the pseudo-code for above said operations. Inverse diffusion applied for encrypted image. First the column elements are XORed with the corresponding K_R value. Then the row elements are XORed with the corresponding K_C value. This process retains the scrambled image from encrypted image, inverse confusion obtains scrambled image. The column elements are added to get $colsum$. $Modulo2$ is applied to calculate $colsum$. Depending on the modulo value, up or down shift is done and performed for all the columns. Then $rowsum$ is calculated for the elements in a row. Then $Modulo2$ is applied for $rowsum$ to get $rowmod$. Depending on the $rowmod$ value, right or left shift is used and done for all the columns producing original image.

3.3 Hash Method

Hash value calculated the output of confusion process. Since the diffusion leads to the collision, hash cannot apply for output of diffusion that is an encrypted image. 128 byte message digest of the confused image is calculated by using *SHA-512* algorithm. Dividing the output eight 16 bytes and performing XOR operation with neighbouring value. Logistic map operation performed for the XORed output. Use *MD5* for concatenating the result of the previous operation. When applying *MD5*, a 32 digit hexadecimal number is got as output for given image. The resultant hash value verifies the integrity of user's data. Algorithm 5 reveals the pseudo-code for hash calculation.

Algorithm 2 Diffusion operation

```
Input: Confused Image
Output: Encrypted Image
  for each row 'i' in the matrix '$I_{scr}$' do
      for each column 'j' in the matrix '$I_{scr}$' do
          $I_1$=$I_{scr}$ [i] [j] XOR $K_C$ [i]
      end for
  end for
  for each column 'j' in the matrix '$I_1$' do
      for each row 'i' in the matrix '$I_1$' do
          $I_{enc}$=$I_1$ [i] [j] XOR $K_R$ [j]
      end for
  end for
```

Algorithm 3 Inverse Diffusion operation

```
Input: Encrypted Image
Output: Confused Image
  for each column 'j' in the matrix '$I_{enc}$' do
      for each row 'i' in the matrix '$I_{enc}$' do
          $I_1$=$I_{enc}$ [i] [j] XOR $K_R$ [j]
      end for
  end for
  for each row 'i' in the matrix '$I_1$' do
      for each column 'j' in the matrix '$I_1$' do
          $I_{scr}$=$I_1$ [i] [j] XOR $K_C$ [i]
      end for
  end for
```

4 Proposed Framework [CIADS]

Figure 1 illustrates the proposed framework. It has (i) User layer (ii) Interface layer (iii) CIADS layer (iv) Cloud storage.

User layer consists of hospital, scan centres and systems used by doctors and lab technicians. Users will access the system to store securely and retrieve the patient medical data in the cloud. Registration process helps the user to enter into the system and stores the user details in the database in CIADS layer. Login process allows the user to enter into the system. It verifies the user details with the database during the login process. After login, the user will upload the certificate, after verifying it by a certificate authority

Algorithm 4 Inverse confusion operation

```
Input: Confused Image
Output: Original Image
  for each column 'j' in the matrix '$I_{scr}$' do
      for each row 'i' in the matrix '$I_{scr}$' do
          colsum=colsum + I [i] [j]
      end for
      colmod=colsum % 2
      if $colmod == 0$ then
          for each Kc do
              $A_{scr}$=up circular shift($I_{scr}$)
          end for
      else
          for each $K_C$ do
              $A_{scr}$=down circular shift($I_{scr}$)
          end for
      end if
  end for
  for each row 'i' in the matrix '$A_{scr}$' do
      for each column 'j' in the matrix '$A_{scr}$' do
          rowsum=rowsum + $A_{scr}$ [i] [j]
      end for
      rowmod=rowsum % 2
      if $rowmod == 0$ then
          for each $K_R$ do
              I=right circular shift($A_{scr}$)
          end for
      else
          for each $K_R$ do
              I=left circular shift($A_{scr}$)
          end for
      end if
  end for
```

user can access the data. User can either upload or download the medical data. If the user wants to store the data, can select upload service. Upload process will transfer the data from the client to data store. In data store, confidentiality is applied by encryption method and integrity is implemented using hash algorithms. When the user wants to download the data from the cloud, the encrypted data and the hash value will be transferred to data store from the cloud, original data is retrieved after decrypting it. Hash value is calculated for the retrieved data to check the integrity of the data. Then the original data is moved to the client machine.

User Interface layer provides the facility for the user to interact with the system. In the case of new user, after registration, login is allowed to access the system. Login checks the user credentials and allows to communicate with CIADS layer. These operations help the user to upload and/or download the medical data to/from the secured data store in the cloud.

Proposed framework consists and implements Confidentiality, Integrity and Authorization for patients medical data in the CIADS layer.

Algorithm 5 Hash algorithm

```
Input: Frames
Output: Hash Value for each frame
  for each frames do
      128 byte message digest = SHA-512 of the image
      divide 128 bytes into eight 16 bytes
      calculate XOR for the nearest pair, that produces four output
      for each XOR output do
          $X_{n+1}$ = $Y_{n+1}$ (1 - Xn)
      end for
      concatenate $X_{n+1}$ values
      Apply MD5 to obtain 32 digit hexadecimal number
  end for
```

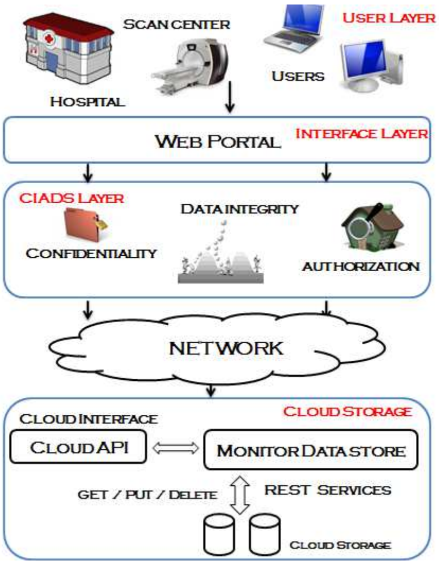


Figure 1: Overall Framework

Confidentiality is employed to maintain the secrecy of client data. Integrity ensures the security of the data. Authorization verifies the organization or a person who enters into the system for access. It allows only the authorized persons to use the system. These services are combined to get the highest security to the data store. The medical data from the repository is sent to the CIADS layer. While uploading data to cloud storage, confidentiality and integrity is adopted. During the retrieval, the data is securely retrieved and checked for integrity. After the successful completion of registration, the user will apply for a certificate with the user details from the certificate authority who is a third party. Certificate authority gets the user details and generates a certificate. The authority will send the certificate to the user. User can download it from the mail and save the certificate. To enter into the system the user need to be authenticated and authorized. Login operation does authentication. Once the login process completes, user provides a certificate, and a certificate authority verifies it. If the certificate authority provides that the user certificate is valid then, the user is considered as an authorized person and is allowed to access the data.

By giving the medical image as input, this input file converted into a number of frames(images) by preprocessing. Applying confidentiality to the frames by using new encryption algorithm and converting the image into scrambled image by confusion and encrypted image by diffusion process. Consider encrypted image as input for decryption. Inverse diffusion is used to produce scrambled image and inverse confusion for reproducing the original image.

Hash value is calculated for the data to ensure the integrity during retrieval from the cloud, and calculated for the scrambled images with the hash algorithm. Upload hash value for all the images in the cloud along with the encrypted data. During download operation hash value will be calculated for the retrieved data and the hash values will be compared for integrity check.

Cloud Store provides off-site virtual storage area for storing patients medical data. It helps the user to store large volume of medical data with low cost in on-demand manner. It provides the facility to take backup, archive and maintain user data remotely through internet and implemented with Restful API in the proposed system.

During upload process, secured data is sent to cloud store. OpenStack offers infrastructure as a service (IaaS) to the consumers. It is an initiative for creating and managing large groups of virtual private servers in the cloud computing environment. It provides five services, i) Nova - Compute Service, ii) Swift - Storage Service, iii) Glance - Imaging Service, iv) Keystone - Identity Service and v) Horizon - UI Service. Proposed system uses OpenStack Swift component to store the secured data. Swift which is the storage component, stores the data in object format in the container. Container allows the user to store, retrieve, delete and update the objects, and this enables the user to upload, download or modify the data in the cloud store. While uploading data, it is stored as object format in the created container and replicas will be generated in the swift, avoiding loss in the cloud.

4.1 Use-Cases

Use-Case diagram represents a simplest way of user's interaction with the system. In this section, use-cases available in our proposed system are explained.

4.1.1 Use-Case 1: User Interface

Actors: Hospital, Doctor, Client machine
Usecase: Registration

Figure 2 explains about the interaction between users and the system. A user who wants to store the data in the cloud has to register in the system, and the details stored in the CIADS layer.

4.1.2 Use-Case 2: Certificate Authority Usage

Actors: Hospital, Doctor, Patient, Client Machine, Third Party
Usecases: Login, Apply for Certificate, Get the Certificate, Get data, Doctor's choice

Figure 3 explains the certificate usage for authorization. The user can enter into the system if the credentials are correct. The system allows the user to apply for a certificate to a third party. The third party will issue a certificate to the user via email. This certificate will ensure that the users are an authorized person; this enables the user to access the medical data storage which is the repository for patient details. The doctor can select the option either to upload the data to the cloud or download to get the data from the cloud storage.

4.1.3 Use-Case 3: Uploading Medical Data

Actors: Doctor, Client Machine, Cloud Data Store
Usecases: Pre-processing of Medical Data, Hash Calculations,Securing(Encryption) the data, Uploading in Cloud

Figure 4 explains the process of uploading the medical data. The data should be pre-processed to upload in the cloud storage, and encrypting the uploaded data. Before calculating the hash value and encrypted data, are sent to the cloud for storing.

4.1.4 Use-Case 4: Downloading Medical Data

Actors: Doctor, Front End, Cloud Data Store
Usecases: Download & Retrieve from Data Store, Decrypt the Data, Hash Calculation & Comparison, Access the Medical Data

Figure 5 explains the operations during download the data from the cloud storage. Apply decryption algorithm over the data, calculate the hash value for the decrypted data and compared with the stored hash value, ensures the data integrity.

5 Implementation

Figure 6 depicts the work-flow of proposed framework. Web page acts as an interface between the

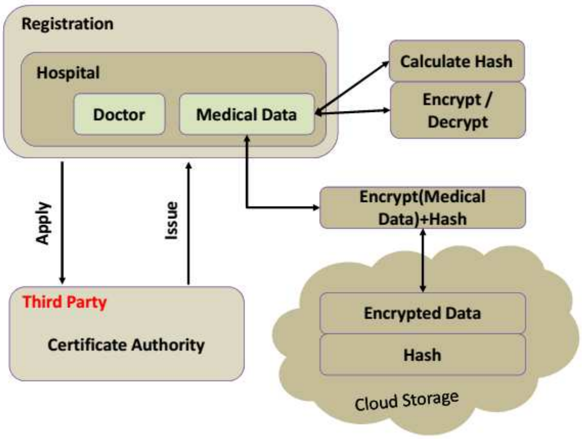


Figure 6: Work-Flow

user and context. The user can enter into the system by registration. Registration gives the user-name, password and other details to the user. Once the registration is completed user needs to contact third-party authority to get a certificate. Third party will get user details and issue a certificate and mail it to the user. Once the user receives the certificate can access the system with login credentials and the certificate. The certificate ensures that the users are the authorized person to access the cloud store.

The user is allowed to enter into the system when the login verification is successful. After user login, certificate verification is done by third party. The user with a valid certificate is allowed to access the medical data from the patient database.

The authorized doctor of the verified hospital can upload or download the medical data into/from the cloud storage. To upload the data, doctor will get the medical data from the patient database and data sent for pre-processing operation, is encrypted, and calculate the hash value. The encrypted data and corresponding hash value is combined and sent to the cloud store. The doctor needs to select download option to download the data from cloud store. It contains a hash value and encrypted data. Decryption is used over encrypted data to retrieve the original data and to calculate the hash value. The hash value from the cloud store and the calculated hash value is compared to ensure the data integrity, which ensures the originality of data.

Figure 7 explains about the encryption process while uploading the data. Data will be pre-processed and converted into frames, and acts as an input for the encryption process. Two keys K_R and K_c are generated, and that must not be constant values. Then the number of iterations is determined. Initializing the counter for iteration and is incremented. Confusion process is carried over for each and every row and column, resulting a scrambled image. Apply diffusion over the scrambled image, the encrypted frame produced as output.

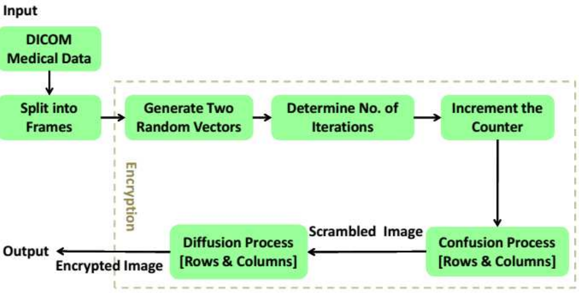

Input
DICOM Medical Data
Split into Frames
Generate Two Random Vectors
Determine No. of Iterations
Increment the Counter
Encryption
Confusion Process [Rows & Columns]
Scrambled Image
Diffusion Process [Rows & Columns]
Output
Encrypted Image

Figure 7: Encryption Process

Figure 8 depicts the decryption process during download operation. Encrypted image, key and number of iterations are input to the decryption process. First applying diffusion over the encrypted frames, producing scrambled image. Then applying confusion on the scrambled image. After each iteration, the counter will be incremented. These operations will retrieve the original frames. After the decryption process, the frames are combined and converted into original data.

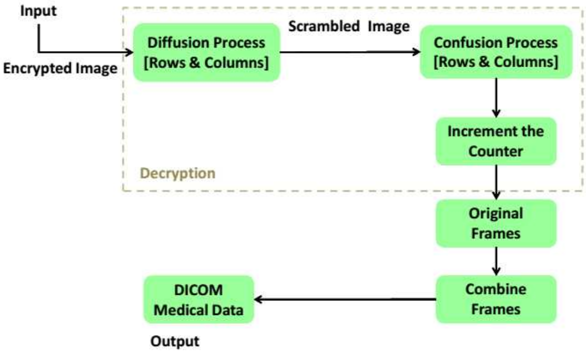
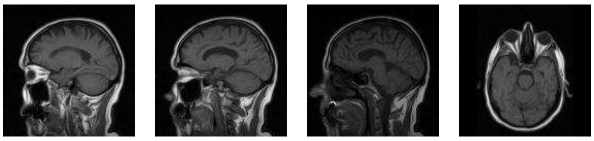


Figure 8: Decryption Process

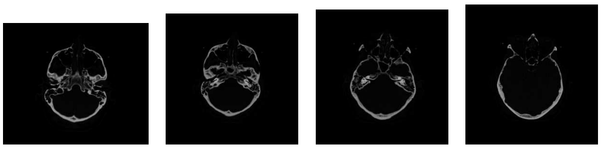
6 Experimental Results

Medical image database contains diagnostic, preventive, re-medical and prescriptive details by physician, nurses and hospitals maintained in DICOM format. Figure 9 & 10 list the sample sequence of images. This preprocessed data given as input to proposed method for encryption. Sample test images of Ferovix CT scan images e.g. Lungs as input. These test images are encrypted using the proposed method, and results shown in Figure 11.



(a) (b) (c) (d)

Figure 9: Infarct Scans(CT Scan) images - Head



(a) (b) (c) (d)

Figure 10: MRI Images - Female Head

6.1 Advantages of Proposed Method

In the Figure 12, *Column1* denotes original frame; *Column2* denotes confused image and *Column3* denotes encrypted image. In the existing algorithm (Figure 12a), the diffusion process is done by the plain image with confused image but in proposed algorithm (Figure 12b) diffusion process does not depend on the original image. XORing confused image with the keys, this makes the encrypted image differ from the original image.

6.2 PSNR Analysis

The proposed new encryption algorithm is applied to various DICOM format medical images, and taking the outputs. Verify the results with PSNR values for QoS analysis. Quality parameter of the reconstructed compression images or videos are measured by Peak Signal to Noise Ratio (PSNR) value. In this analysis, original DICOM data is considered as a signal and the compressed data is considered as noise. PSNR value is calculated by using the Equations 1, 2 and 3 and used to analyse the quality of reconstructed health-care data during download operation from the cloud storage.

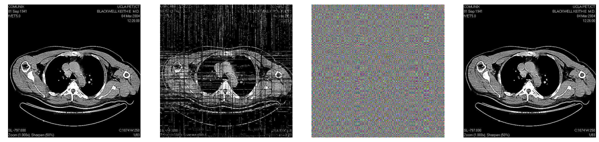
The equations to calculate PSNR values as follows,

Calculate Mean Square Error [MSE]

$$d(f(x,y), f'(x,y)) = ||(f(x,y) - f'(x,y)||^2 \quad (1)$$

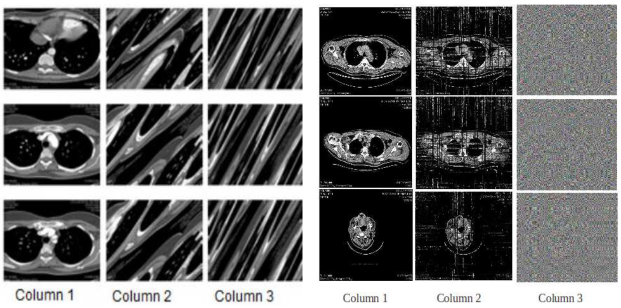
$$= 1/mn \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} ((f(i,j) - f'(i,j)^2) \quad (2)$$

where $f(x,y)$ original image and $f'(x,y)$ reconstructed image, m and n are size of the image.



(a) Original image (b) Confused image (c) Encrypted image (d) Decrypted image

Figure 11: Output of new Encryption Method



(a) Chaotic Cat Map Approach (b) Proposed Method

Figure 12: Comparison of algorithms

PSNR calculation

$$PSNR = 10log_{10}1/MSE \quad (3)$$

Table 2 and Figure 13 shows the comparison of PSNR values between Proposed method and Chaotic Cat Map method. Proposed method has high PSNR value than existing method.

6.3 Histogram Analysis

Figure 14 illustrates the histogram result of the input image, encrypted image and decrypted image. This result shows that the encrypted image entirely differs from the original images. Due to this, middle way attacks are not possible, implies statistical attacks; differential attacks are avoided due to variation

Table 2: PSNR Value Comparison

Bit Rate $[kB]$	Proposed Algorithm $[dB]$	Chaotic Cat Map Algorithm $[dB]$
550	35.578	34.565
750	39.099	38.348
1000	41.141	40.762
1250	39.679	38.935
1500	39.679	38.817

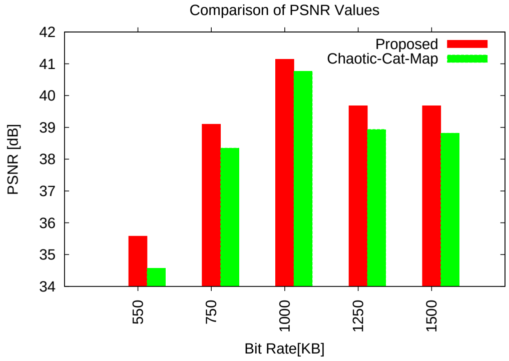
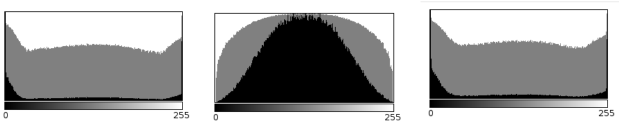


Figure 13: Comparing PSNR Values - Chaotic Cat Map Vs Proposed

Table 3: Difference in Hash value

Images	SHA-512 Algorithm	MD5 Algorithm	Proposed Algorithm
1	30	30	31
2	29	31	31
3	30	30	31
4	29	30	32
5	30	28	29

between original and encrypted image. This analysis reveals that the quality of the retrieved data is much similar to the original data.



(a) Original image (b) Encrypted image (c) Decrypted image

Figure 14: Histogram of images

6.4 Hash Algorithm Analysis

Table 3 shows the number of bits changed in the *SHA-512, MD5* and proposed hash value when replacing one pixel in the confused image. Table 4 shows the average change of bits in the hash value for *SHA-512, MD5* and proposed hash algorithms of test images when replacing one pixel value in the confused image.

The graph (Figure 15) shows the comparison of changes in confused image hash values of *SHA-512, MD5* and an algorithm (proposed) when changing the pixel. Red block denotes *SHA-512* values, green block denotes MD5 values, and blue block denotes the hash value changes of proposed algorithm. It denotes that the proposed algorithm has higher efficiency than the existing hash algorithms.

Table 4: Average changes in Hash value

Images	SHA-512 Algorithm	MD5 Algorithm	Proposed Algorithm
1	94.53	93.75	96.88
2	92.19	96.88	96.88
3	93.75	93.75	96.88
4	90.63	93.75	100
5	92.97	87.5	90.63

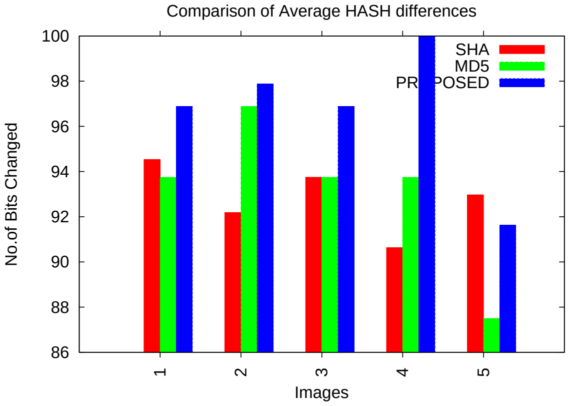


Figure 15: Average Changes in Hash value - Comparison

7 Conclusion

The proposed CIADS data store framework provides three-fold securities for maintaining the confidentiality, integrity and authorization of patients medical data. Confidentiality is achieved by our proposed method. It improves the QoS of the retrieved data than the existing methods. Ensures the integrity by means of combining traditional hash algorithms. Authorization is achieved by implementing JavaCA certificate authority. The secured data is stored in the cloud store, implemented using OpenStack Swift component. As all systems have limitations, our system is developed securely to store DICOM medical images which are in *.avi format. In the future, this will be extended to store all medical data. Also, it can be implemented for all data not only images, but also for documents and other files. Data growth of the medical industry is in an explosive state. Apart from cloud storage, this needs ”Big Data” repositories to store the information securely. In addition, new regulations are mandating longer data retention, and the job of protecting these ever-growing data repositories is becoming even more daunting. In future, these challenges can be countered by implementing ”Big Data” repositories.

References:

[1] Kamal Srivastava, Atul Kumar, ”A New Approach of CLOUD: Computing Infrastructure on Demand”, *Trends in Information and Management*, volume 7, No 2, ISSN:0973-4163, 2011.

[2] Jui-Hung Kao, Chien-Yeh Hsu, Yu-Ping Sung, Wei-Pan Liao, ”DICOM-Based Multi-Center Electronic Medical Records Management System”, *International Journal of Bio-Science and Bio-Technology*, No Vol 2, No. 2, 2010.

[3] Joel-Ahmed M. Mondol, ”Cloud security solutions using FPGA Communications”, *IEEE Computers and Signal Processing (PacRim) Conference*,Victoria, BC, pp: 747 - 752 , doi: 10.1109/PACRIM.2011.6032987, 2011.

[4] Farzad Sabahi, ”Cloud Computing Security Threats and Responses”, *IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, pp: 245 - 249 , doi: 10.1109/ICCSN.2011.6014715, 2011.

[5] Hyun-Suk Yu, Yvette E Gelogo, Kyung Jung Kim, ”Securing Data Storage in Cloud Computing”, *Journal of Security Engineering*, pp:251-260, ISSN: 1738-7531, 2012.

[6] Andreas Kronabeter, Stefan Fenz, ”Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation”, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Volume 112, 2013, pp 114-123, doi: 10.1007/978-3-319-03874-2-12.

[7] Xiang Tan and Bo Ai, ”The Issues of Cloud Computing Security in High-speed Railway”, *International Conference on Electric and Mechanical Engineering and Information Technology*, Harbin, Heilongjiang, vol: 8, pp: 4358-4363,doi: 10.1109/EMEIT.2011.6023923., 2011.

[8] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, ”Security Issues for Cloud Computing”, *International Journal of Information Security and Privacy*,4(2), pp:39-51, 2010.

[9] Danish Jamil et al., ”Security issues in cloud computing and countermeasures”, *International Journal of Engineering Science and Technology*, vol: 3, No.4,pp: 2672,2676,ISSN: 0975-5462, 2011.

[10] Jerry Archer, ”Top Threats to Cloud Computing V1”, A Report, *Cloud Security Alliance*, 2010.

[11] Mohammed Almorsy, John Grundy and Amani S. Ibrahim, ”Collaboration-Based Cloud Computing Security Management Framework”, *Proceedings of IEEE 4th International Conference on Cloud Computing*, Washington, DC, pp: 364 - 371 , doi: 10.1109/CLOUD.2011.9, 2011.

[12] B. Shwetha Bindu, B. Yadaiah, ”Secure Data Storage In Cloud Computing”, *International Journal of Research in Computer Science*, Volume 1 Issue 1 pp. 63-73, 2011.

[13] Bhagyashree Ambulkar and Vaishali Borkar, ”Data Mining in Cloud Computing”, *IJCA Proceedings on National Conference on Recent Trends in Computing NCRTC*, (6):23-26, May, Published by Foundation of Computer Science, New York, USA, 2012.

[14] Wentao Liu, ”Research on Cloud Computing Security Problem and Strategy”, *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, pp: 1216 - 1219, doi: 10.1109/CECNet.2012.6202020, 2012.

[15] Dimitrios Zissis , Dimitrios Lekkas, ”Addressing cloud computing security issues”, *Future Generation Computer Systems*, Volume 28, Issue 3, pp: 583592, doi:10.1016/j.future.2010.12.006, 2012.

[16] Farhan Bashir Shaikh, Sajjad Haider, ”Security Threats in Cloud Computing”, *6th International Conference on Internet Technology and Secured Transactions(ICITST)*, Abu Dhabi, pp: 214 - 219, ISBN: 978-1-4577-0884-8, 2011.

[17] Akhil Behl, ”Emerging Security Challenges in Cloud Computing, An insight to Cloud security challenges and their mitigation”, *Information and Communication Technologies (WICT)*, 2011 World Congress, Mumbai, pp: 217 - 222 , doi: 10.1109/WICT.2011.6141247, 2011.

[18] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, ”Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, *IEEE Transactions on Parallel and Distributed Systems*, vol: 22, issue: 5, pp: 847 - 859, doi: 10.1109/TPDS.2010.183, 2010.

[19] Anil Kurmus, Moitrayee Gupta, Roman Pletka, Christian Cachin, and Robert Haas, ”A Comparison of Secure Multi-tenancy Architectures for Filesystem Storage Clouds”, *IBM Research*, 2011.

[20] B Prabavathy, Y V Lokeshwari, and Chitra Babu, ”Optimized Cloud Storage with High Throughput Deduplication Approach”, *IJCA Proceedings on International Conference on Emerging Technology Trends (ICETT)* (1):32-37, 2011. Published by Foundation of Computer Science, New York, USA.

[21] Amrita Upadhyay, Pratibha R Balihalli, Shashibhushan Ivaturi and Shrisha Rao, ”Deduplication and Compression Techniques in Cloud Design”, *IEEE International Systems Conference (SysCon)*, 2012, Vancouver, BC, pp:1-6, doi: 10.1109/SysCon.2012.6189472, 2012.

[22] Seny Kamara, Charalampos Papamanthou, Tom Roeder, ”CS2-A Searchable Cryptographic Cloud Storage System”, *Microsoft Research*, 2011.

[23] Tripathi, A., & Mishra, A, ”Cloud computing security considerations”, *In Proceedings of IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, pp. 1-5. IEEE, 2011.

[24] Christian Neuhaus, Robert Wierschke, Martin von L and Andreas Polze, ”Secure Cloud-based Medical Data Exchange”, *Lecture Notes in Informatics, INFORMATIK*, ISBN: 978-3-88579-286-4, 2011.

[25] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, ”Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption”, *IEEE Transactions on Parallel and Distributed Systems*, 24(1), 131-143, 2012.

[26] Suresh Jaganathan, Arun Fera M, ”An Integrated Algorithm Supporting Confidentiality and Integrity for Secured Access and Storage of DICOM Images”, *International Journal of Biometrics and Bioinformatics, (IJBB) CSC Journals*, vol: (6),ISSN:1985-2347, 2012.

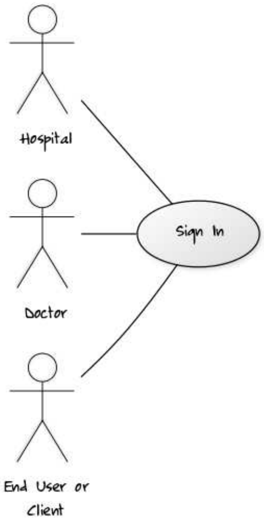


Figure 2: User Interface

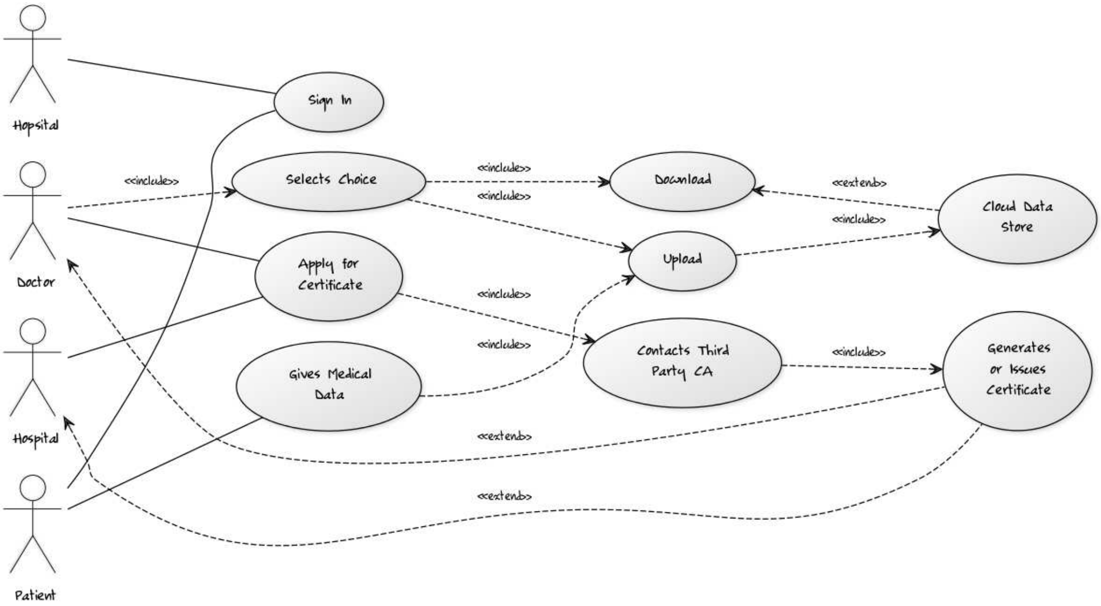


Figure 3: Authorization

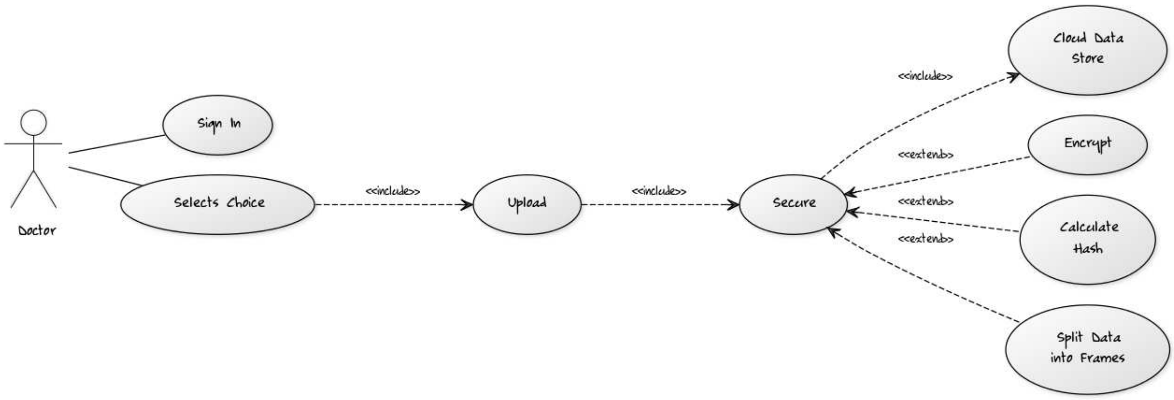


Figure 4: Uploading Medical Data

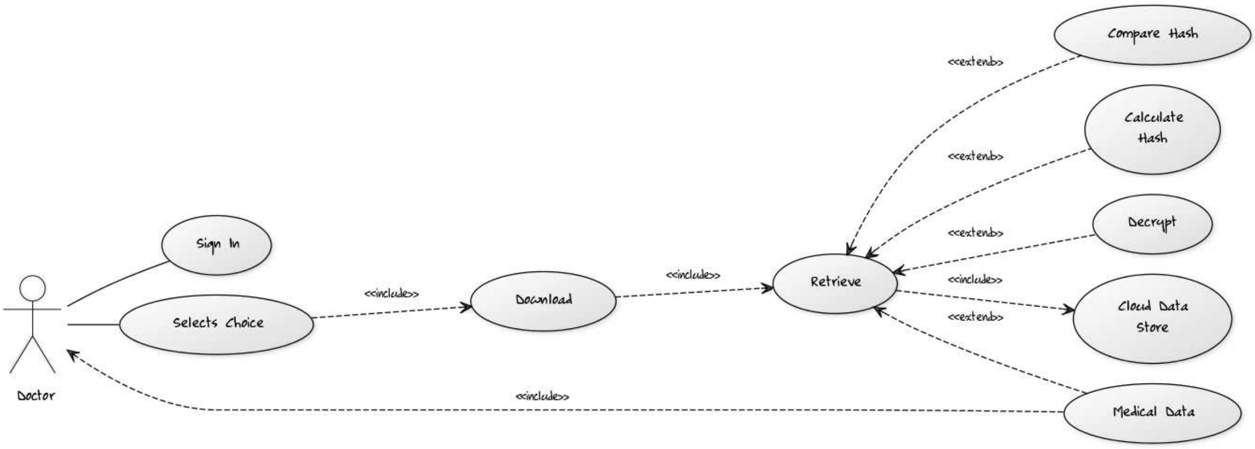


Figure 5: Downloading Medical Data