# Verifiable Attribute-Based Through Text and Image Search with Fine-Grained Owner-Enforced Search Authorization in the Cloud

**Nirupama Devangaon[1], Dr Suvarna Nandyal[2]**

[1]CSE Department, PDA Engineering College, Kalaburagi, Karnataka, India

[2]H.O.D CSE Department, PDA Engineering College, Kalaburagi, Karnataka, India

**Abstract:** ***Search over encrypted data is a critically important enabling technique in cloud computing, where encryption-before outsourcing is a crucial answer for ensuring user information security in the untrusted cloud server condition. In this work we focus on Role- based authentication is a combination of symmetric key cryptography and public key cryptography where by every encryption process needs Data, Public Key, Group Key, The Policy is a set of rule that can be specified as chain also for e.g., in the context of hospital a policy can be given as {doctor, patient} which means anybody from the doctors group or patient group can simultaneously decrypt the document on the other hand a policy can be specified as chain policy for instance{doctor},{patient} This is known as nested policy .In such cases a patient can decrypt the document only when that is decrypted by doctors first, Policy based encryption is becoming popular in an enterprise context where different authorities require different permission and privacy settings for the access of the records. In this work we have develop a novel CP-ABE(Cryptography-Attributed based Encryption) based technique in an enterprise hospital context deployed in a local cloud with fog computing architecture .Our proposed system provides different level of encryption, decryption, authentication, authorization and privacy setting for doctors in the context of patients, medical image, image feature records. The data used for communication between doctor and patient is images of skin cancer and related symptoms. Both text and image is encrypted and decrypted by AES(Advanced Encryption Standard)during data transfer . Further machine learning Bayesian Classifier approach is used to diagnose abnormality in the skin cancer image. In this work we demonstrate the use of CP-ABE with human entities as well as in the context of machine learning .The overall work demonstrate the entire process of medical scanning in an enterprise hospital application both plain record encryption and image encryption with the help of CP-ABE. In order to demonstrate the efficiency of the system we have developed a simple medical application where doctor encrypt text and image which can visualize only their own patient's data and the usability of machine learning image classification technique which automatically can retrieve the observation of the image as abnormal or normal. This proves machine learning and performance evaluation shows efficiency of our system.***

**Keywords:** Cloud computing, CP-ABE, AES, Text and Image Search, Symmetric key Cryptography

## 1. Introduction

Cloud computing has emerged as a new enterprise IT architecture. Many organizations are moving their databases into the cloud. When sensitive data are outsourced to the cloud, data owners naturally become concerned with the protection of their data in the cloud. Encryption-before-outsourcing has been viewed as a central methods for securing user data [1].Cloud application designers have been effectively creating applications for IaaS infrastructure-as-a-service is described as hardware and software including servers, storage, networks and OS(Amazon AWS, Rack space, and so forth) and PaaS platform-as-a-service is described as a collection of tools and means to facilitate developing and deploying different applications [6] (Azure, Google App Engine, Cloud Foundry) stages. These stages give essential security highlights including support for confirmation, DoS assault Relief, firewall arrangement administration, logging, fundamental client and profile administration yet security concerns keep on being the main obstruction for big business cloud selection. Cloud security concerns run from safely designing virtual machines conveyed on an IaaS stage to overseeing client benefits in a PaaS cloud. Given that the cloud administrations can be conveyed in many flavors i.e. in any blend of administration conveyance models, SaaS, PaaS and IaaS (SPI), and operational models, open, private and half and half, the cloud security concerns and arrangements are setting (design) subordinate.

### 1.1 Cloud Security

Security and privacy of data in the cloud have developed as an area of real concern, particularly when data is sensitive and delicate, such as healthcare and financial data [2]. The key requirements of system are.

1) Secure storage of data on the remote cloud server.
2) Allow authorized user to search and access over the data[2].

and cloud API. The figure beneath highlights the layers, inside a cloud administration, that are secured by the supplier versus Initially, we should discuss the cloud security operational model. By definition, cloud security obligations in an open cloud are shared between the cloud client (your venture) and the cloud specialist co-op where as in a private cloud, the client is dealing with all parts of the cloud stage. Cloud specialist co-ops are in charge of securing the mutual foundation including switches, switches, stack balancers, firewalls, hypervisors, capacity systems, administration supports, DNS, index administrations the client.

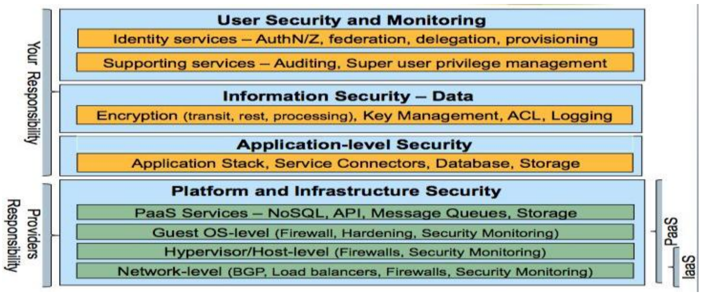

Your Responsibility
Providers Responsibility
User Security and Monitoring
Identity services – AuthN/Z, federation, delegation, provisioning
Supporting services – Auditing, Super user privilege management
Information Security – Data
Encryption (transit, rest, processing), Key Management, ACL, Logging
Application-level Security
Application Stack, Service Connectors, Database, Storage
Platform and Infrastructure Security
PaaS Services – NoSQL, API, Message Queues, Storage
Guest OS-level (Firewall, Hardening, Security Monitoring)
Hypervisor/Host-level (Firewalls, Security Monitoring)
Network-level (BGP, Load balancers, Firewalls, Security Monitoring)
PaaS
IaaS

**Figure 1:** Layers within the Cloud Service

Prior to signing up with a provider, it is critical to play out a crevice examination on the cloud benefit abilities. This activity ought to benchmark the cloud stage's development, straightforwardness, consistence with big business security norms (e.g. ISO 27001) and administrative benchmarks, for example, PCI DSS, HIPAA and SOX. Cloud security development models can help quicken the movement methodology of uses to the cloud.

### 1.2 Cloud Security Architecture

As a first step, architects need to comprehend what security capacities are offered by cloud stages (PaaS, IaaS). The figure beneath delineates the design for building Security offerings and abilities proceed to develop and differ between cloud suppliers. Thus you will regularly find that security components, for example, key administration and information encryption won't be accessible. For instance: the requirement for an AES 128 piece encryption benefit for encoding security antiques and keys escrowed to a key administration benefit. For such basic administrations, one will keep on relying on interior security administrations. A "Crossover cloud" organization engineering example might be the main practical choice for such applications that reliant on interior administrations. Another regular utilize case is Single-Sign(SSO)

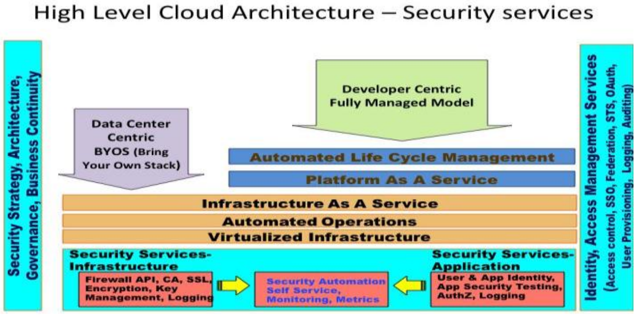

High Level Cloud Architecture – Security services
Security Strategy, Architecture, Governance, Business Continuity
Data Center Centric BYOS (Bring Your Own Stack)
Developer Centric Fully Managed Model
Automated Life Cycle Management
Platform As A Service
Infrastructure As A Service
Automated Operations
Virtualized Infrastructure
Security Services-Infrastructure
Firewall API, CA, SSL, Encryption, Key Management, Logging
Security Automation Self Service, Monitoring, Metrics
Security Services-Application
User & App Identity, App Security Testing, AuthZ, Logging
Identity, Access Management Services
(Access control, SSO, Federation, STS, OAuth, User Provisioning, Logging, Auditing)

**Figure 2:** Cloud Architecture

### 1.3 Cloud Security Principles

Every enterprise has different levels of risk tolerance and the demonstrated by the product development culture, new technology adoption, IT service delivery models, technology strategy, and investments made in the area of security tools and capabilities. Following is a sample of cloud security principles that an enterprise security architect needs to consider and customize.

- Services running in a cloud should follow the principles of least privileges.
- Isolation between various security zones should be guaranteed using layers of firewalls – Cloud firewall, hypervisor firewall, guest firewall and application container. Firewall policies in the cloud should comply with trust zone isolation standards based on data sensitivity.
- Applications should use end-to-end transport level encryption (SSL, TLS and IPSEC) to secure data in transit between applications deployed in the cloud as well as to the enterprise.
- Applications should externalize authentication and authorization to trusted security services. Single Sign-on should be supported using SAML 2.0.
- Data masking and encryption should be employed based on data sensitivity aligned with enterprise data classification standard.
- Applications in a trusted zone should be deployed on authorized enterprise standard VM images
- Industry standard VPN protocols such as SSH, SSL and IPSEC should be employed when deploying virtual private cloud (VPC).
- Security monitoring in the cloud should be integrated with existing enterprise security monitoring tools using an API.
- Organization of Paper: I. Introduction II. Related Work III. Proposed Work IV. Implementation and Results V.Conclusion And Future Work

## 2. Related Work

There has been a great interest in developing Attribute-Based Encryption due to its fine grained access control property [1]. ABE is a popular method for enforcing access control policies via cryptographic means the methodology which we used is CP-ABE(cipher text-policy ABE) where the cipher text is associated to access control policy .In this paper we use ABE to construct a new primitive called Attribute-Based Keyword Search (ABKS),by which text are encrypted according to access control policy and data users with proper cryptographic credentials can generate tokens that can be used to search over outsourced encrypted data [2]Fine grained access control provides different access rights to different set of users and thus provides flexibility in access rights specification to different set of users[3].We also achieve fine-grained access control on encrypted data using CP-ABE in CP-ABE scheme ,a user’s private key is associated with a set of attributes ,and cipher text are associated with access control policy .If user attributes satisfy then he is able to decrypt cipher text [4].Fine-grained authorization framework in which every user obtain search capabilities under the authorization of local trusted authorities, based on checking for user attributes[5].Fine-grained data access system realize the main challenges for maintaining data confidentiality, enforcing fine-grained data access control, applying efficient user revocation mechanism, preventing collusion between users to access unauthorized digital objects and achieving scalability[6].To ensure confidentiality, the sensitive data like health record, banking etc is encrypted before outsourcing to the cloud[7].we make whole process verifiable for text and image search to ensure authenticity of the returned search results[8].

## 3. Proposed Work

In order to overcome this basic drawback of CP-ABE (Cryptography-Attribute based Encryption) based systems we propose a novel updated CP-ABE system which can be used for both text as well as binary(image records) .The proposed work develop medical application where doctor can register the patient their text record will be encrypted with privacy setting of doctors ,patient personal record such as phone number , email-id and case history will be encrypted with an access to only patient and doctor ,the doctor can upload the skin cancer image with privacy settings of only doctors and patients. A doctor upon viewing the skin cancer image through a machine learning system. The result of machine learning system is a set of feature vector which will again be encrypted with the policy of only machine learning. Feature vector of Image is mean of red, green, blue and standard deviation of red ,green, blue is extracted and saved redis database which can be retrieved by all entities of hospital. The doctor will be able to analysis whether a particular record is abnormal or normal that information is again encrypted with the policy of doctor and that particular patient therefore a patient can view his own record, medical diagnosis observation a doctor will be able to see the patient general information, case history and the medical images and diagnosis. But a doctor will not able to visualize the images of the doctors of the other patients a doctor will not able to visualize the personal information of the patient. The admin on the other hand would be able to see all the information of the patient along with their personal information but will not able to view medical diagnosis reports.

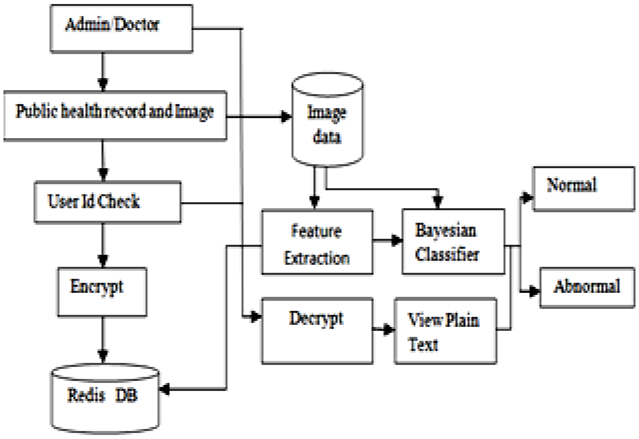
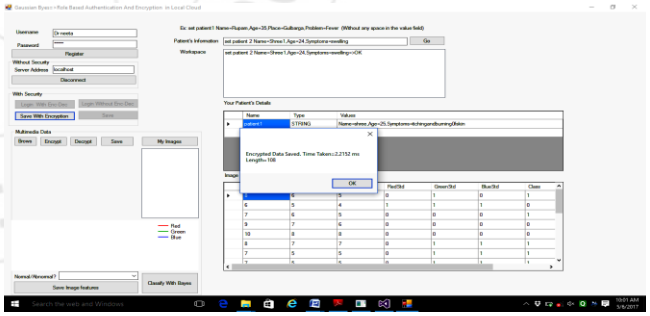


**Figure 3:** Module Diagram

The doctor inserts patient record or patient data, patient data may be personal information of the patient, case history and scanning images of patient is encrypted with a key(Symmetric key) after encoding the plain text is converted into cipher text and stored in local cloud Redis database, if the doctor or patient want to view the data first they should decrypt the data which is in the form of cipher text with a same key(Symmetric key). Once decoding process completed they can view data which is converted into plain text, the image features is extracted and put away in the informational index i.e., data base which can be retrieved by all entities of the hospital. We have taken a Bayesian classifier (Machine Learning System) which helps doctor to detect and classify automatically certain medical images as normal or abnormal. Shown in above diagram Fig 3.

## 4. Implementation and Results


Gaussian Byes:->Role Based Authentication And Encryption in Local Cloud

Username: Dr neeta
Password: *****
Server Address: localhost

Ex: set patient1 Name=Rupam,Age=35,Place=Gulbarga,Problem=Fever (Without any space in the value field)

Patient's Information: set patient 2 Name=Shree1,Age=24,Symptoms=swelling

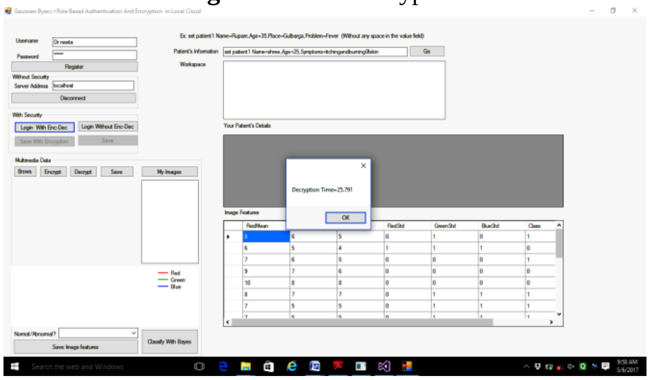
Workspace: set patient 2 Name=Shree1,Age=24,Symptoms=swelling=>OK

Your Patient's Details

| Name | Type | Values |
|---|---|---|
| patient1 | STRING | Name=shree,Age=25,Symptoms=itchingandburning0fskin |

Encrypted Data Saved. Time Taken::2.2152 ms
Length=108

**Figure 4**: Text Encryption


Gaussian Byes:->Role Based Authentication And Encryption in Local Cloud

Username: Dr neeta
Password: *****
Server Address: localhost

Ex: set patient1 Name=Rupam,Age=35,Place=Gulbarga,Problem=Fever (Without any space in the value field)

Patient's Information: set patient1 Name=shree,Age=25,Symptoms=itchingandburning0fskin

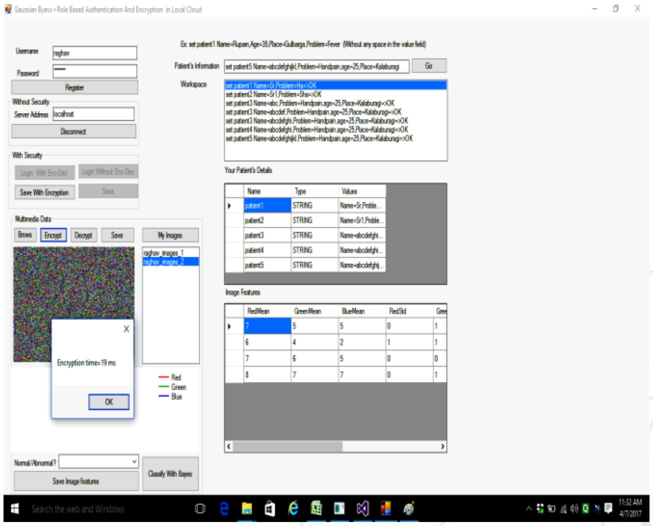
Decryption Time=25.791

Image Features

| RedMean | | | RedStd | GreenStd | BlueStd | Class |
|---|---|---|---|---|---|---|
| 8 | 6 | 5 | 0 | 1 | 0 | 1 |
| 6 | 5 | 4 | 1 | 1 | 1 | 0 |
| 7 | 6 | 5 | 0 | 0 | 0 | 1 |
| 9 | 7 | 6 | 0 | 0 | 0 | 0 |
| 10 | 8 | 8 | 0 | 0 | 0 | 0 |
| 8 | 7 | 7 | 0 | 1 | 1 | 1 |
| 7 | 5 | 5 | 0 | 1 | 1 | 1 |

**Figure 5:** Text Decryption

The above Fig 4 and 5 shows Text encryption and decryption in role based authentication, once the registration is successful the doctor can enter the patient information and encrypt with a key (symmetric key) by using AES (Advanced Encryption Standard), with the same key the doctor can decrypt the patient information by using AES.



Username: raghav

Server Address: localhost

Ex: set patient1 Name=Rupam,Age=35,Place=Gulbarga,Problem=Fever (Without any space in the value field)

Patient's Information: set patient5 Name=abcdefghijkl,Problem=Handpain,age=25,Place=Kalaburagi

Workspace:

```
set patient1 Name=Sr,Problem=Ha=>OK
set patient2 Name=Sr1,Problem=Sha=>OK
set patient3 Name=abc,Problem=Handpain,age=25,Place=Kalaburagi=>OK
set patient3 Name=abcdef,Problem=Handpain,age=25,Place=Kalaburagi=>OK
set patient3 Name=abcdefghi,Problem=Handpain,age=25,Place=Kalaburagi=>OK
set patient4 Name=abcdefghi,Problem=Handpain,age=25,Place=Kalaburagi=>OK
set patient5 Name=abcdefghijkl,Problem=Handpain,age=25,Place=Kalaburagi=>OK
```

raghav_images_1
raghav_images_2

Encryption time=19 ms

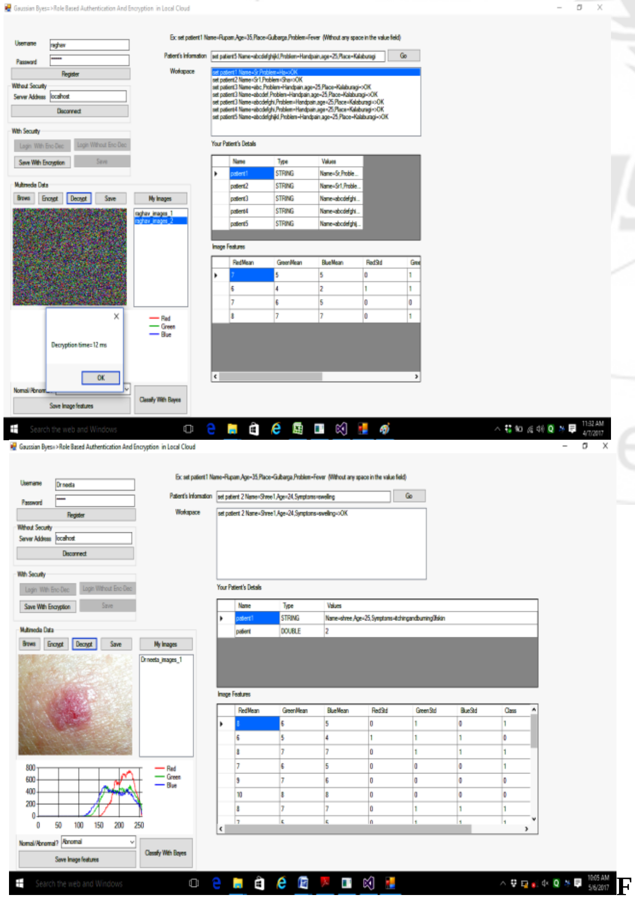
Your Patient's Details

| Name | Type | Values |
|---|---|---|
| patient1 | STRING | Name=Sr,Proble... |
| patient2 | STRING | Name=Sr1,Proble... |
| patient3 | STRING | Name=abcdefghi... |
| patient4 | STRING | Name=abcdefghi... |
| patient5 | STRING | Name=abcdefghij... |

Image Features

| RedMean | GreenMean | BlueMean | RedStd | Gree |
|---|---|---|---|---|
| 7 | 5 | 5 | 0 | 1 |
| 6 | 4 | 2 | 1 | 1 |
| 7 | 6 | 5 | 0 | 0 |
| 8 | 7 | 7 | 0 | 1 |

**Figure 6**: Image Encryption



Username: raghav

Server Address: localhost

Ex: set patient1 Name=Rupam,Age=35,Place=Gulbarga,Problem=Fever (Without any space in the value field)

Patient's Information: set patient5 Name=abcdefghijkl,Problem=Handpain,age=25,Place=Kalaburagi

Workspace:

```
set patient1 Name=Sr,Problem=Ha=>OK
set patient2 Name=Sr1,Problem=Sha=>OK
set patient3 Name=abc,Problem=Handpain,age=25,Place=Kalaburagi=>OK
set patient3 Name=abcdef,Problem=Handpain,age=25,Place=Kalaburagi=>OK
set patient3 Name=abcdefghi,Problem=Handpain,age=25,Place=Kalaburagi=>OK
set patient4 Name=abcdefghi,Problem=Handpain,age=25,Place=Kalaburagi=>OK
set patient5 Name=abcdefghijkl,Problem=Handpain,age=25,Place=Kalaburagi=>OK
```

raghav_images_1
raghav_images_2

Decryption time=12 ms

Your Patient's Details

| Name | Type | Values |
|---|---|---|
| patient1 | STRING | Name=Sr,Proble... |
| patient2 | STRING | Name=Sr1,Proble... |
| patient3 | STRING | Name=abcdefghi... |
| patient4 | STRING | Name=abcdefghi... |
| patient5 | STRING | Name=abcdefghij... |

Image Features

| RedMean | GreenMean | BlueMean | RedStd | Gree |
|---|---|---|---|---|
| 7 | 5 | 5 | 0 | 1 |
| 6 | 4 | 2 | 1 | 1 |
| 7 | 6 | 5 | 0 | 0 |
| 8 | 7 | 7 | 0 | 1 |

Username: Dr neeta

Server Address: localhost

Ex: set patient1 Name=Rupam,Age=35,Place=Gulbarga,Problem=Fever (Without any space in the value field)

Patient's Information: set patient 2 Name=Shree1,Age=24,Symptoms=swelling

Workspace:

```
set patient 2 Name=Shree1,Age=24,Symptoms=swelling=>OK
```

Dr neeta_images_1

Normal/Abnormal? Abnormal

Your Patient's Details

| Name | Type | Values |
|---|---|---|
| patient1 | STRING | Name=shree,Age=25,Symptoms=itchingandburning0fskin |
| patient | DOUBLE | 2 |

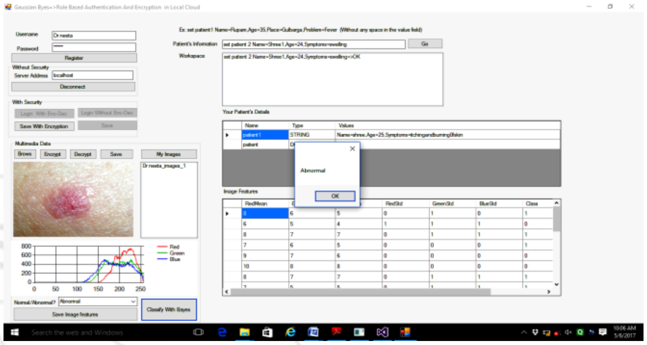
Image Features

| RedMean | GreenMean | BlueMean | RedStd | GreenStd | BlueStd | Class |
|---|---|---|---|---|---|---|
| 8 | 6 | 5 | 0 | 1 | 0 | 1 |
| 6 | 5 | 4 | 1 | 1 | 1 | 0 |
| 8 | 7 | 7 | 0 | 1 | 1 | 1 |
| 7 | 6 | 5 | 0 | 0 | 0 | 1 |
| 9 | 7 | 6 | 0 | 0 | 0 | 0 |
| 10 | 8 | 8 | 0 | 0 | 0 | 0 |
| 8 | 7 | 7 | 0 | 1 | 1 | 1 |
| 7 | 6 | 5 | 0 | 1 | 1 | 1 |

F

**Figure 7**: Image Decryption

The above Fig 6 and 7 shows the image encryption and image decryption, doctor1 upload his patient image ,the image may be abnormal or normal which means red color on the skin is detected as abnormal and the plain skin image is detected as normal which is encrypted with a key(Symmetric key) by using AES (Advance Encryption Standard)and features of the image are saved in dataset which can be retrieved by all entities in the hospital , doctor1 can decrypt the image with the same key by using AES.



Username: Dr neeta

Server Address: localhost

Ex: set patient1 Name=Rupam,Age=35,Place=Gulbarga,Problem=Fever (Without any space in the value field)

Patient's Information: set patient 2 Name=Shree1,Age=24,Symptoms=swelling

Workspace:

```
set patient 2 Name=Shree1,Age=24,Symptoms=swelling=>OK
```

Dr neeta_images_1

Normal/Abnormal? Abnormal

Abnormal

Your Patient's Details

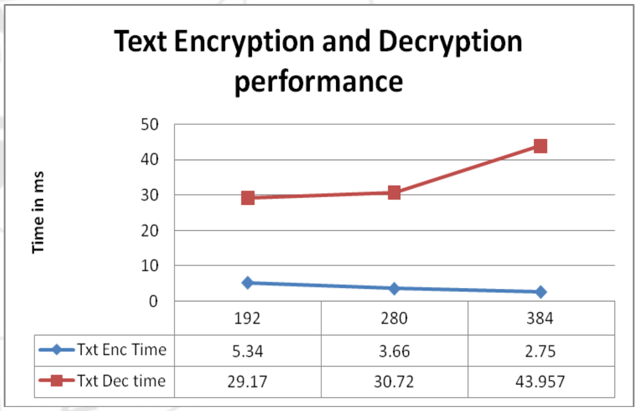
| Name | Type | Values |
|---|---|---|
| patient1 | STRING | Name=shree,Age=25,Symptoms=itchingandburning0fskin |
| patient | D | |

Image Features

| RedMean | | | RedStd | GreenStd | BlueStd | Class |
|---|---|---|---|---|---|---|
| 8 | 6 | 5 | 0 | 1 | 0 | 1 |
| 6 | 5 | 4 | 1 | 1 | 1 | 0 |
| 8 | 7 | 7 | 0 | 1 | 1 | 1 |
| 7 | 6 | 5 | 0 | 0 | 0 | 1 |
| 9 | 7 | 6 | 0 | 0 | 0 | 0 |
| 10 | 8 | 8 | 0 | 0 | 0 | 0 |
| 8 | 7 | 7 | 0 | 1 | 1 | 1 |

**Figure 8:** Machine Learning

Bayesian Classifier by means of which doctors can automatically classify certain medical image as normal or abnormal based on statistical features. Shown in Fig 8



| | 192 | 280 | 384 |
|---|---|---|---|
| Txt Enc Time | 5.34 | 3.66 | 2.75 |
| Txt Dec time | 29.17 | 30.72 | 43.957 |

**Figure 9:** Performance Evaluation of Text

The above Fig 9 shows Text encryption and Decryption Performance where the encryption and decryption time is measured in millisecond. As the length of the text is increasing the encryption time of text decreases and decryption time of text is increasing.

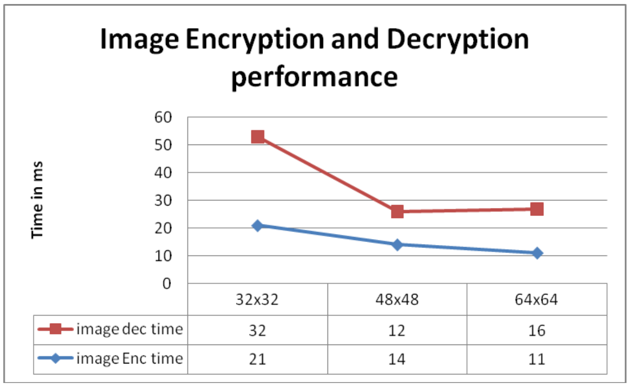


**Figure 10:** Performance Evaluation of image

The above Fig 10 shows the image Encryption and decryption Performance where the image Encryption and Decryption time is measured in millisecond.As the Pixel of the image increases the image Encryption and Decryption time deacreases **.**

## 5. Conclusion and Future Work

In this work, we design the first verifiable attribute-based through text and image search with fine-grained owner-enforced search authorization in cloud. In Cloud Environment search over encrypted data (Text and Image) is experiencing rapid development. The Proposed CP-ABE based technique which reduces the complexity of public key cryptography by adopting symmetric key cryptography and extending it in the model of CP-ABE such that different user group can be given different attributes to access the data. In order to demonstrate the efficiency of the system we have developed a simple medical application where doctor can visualize only their own patient's data. However the observation of doctor associated with image diagnosis which can access by all entities of the hospital. In order to demonstrate the usability of a system in the context of autonomous diagnosis we used cloud based image classification technique which automatically can retrieve the observation of the image to build machine learning model. This proves machine learning and performance evaluation shows efficiency of our system.

Our system can be modified by adopting it in the context of a much complex health care system with different identities and different parties and roles, such as different set of roles for doctors, nurses, pharmacist and patients and so on. By enabling remote data access by the patients and remote message exchanging, this system can be turned into a real time enterprise system.

## References

[1] W.Sun, S.Yu, W.Lou ,T.Hou, H.Li,"Verifiable Attribute-Based,keyword search with fine-grained owner-enforced search authorization in the cloud,"IEEE Transaction Parallel and Dist Syst Vol 27,April 2016.

[2] Q.Zheng, S.Xu, G.Ateniese,"Verifiable Attribute-Based Keyword Search over Outsourced Encrypted Data,"IEEE Conference on Computer Communication,2014.

[3] K.Kaushik, V.Vardharajan, R Nallusamy,"Multi-user Attribute Based Searchable Encryption,"IEEE 14th Int,Conference,2013.

[4] Q.Wang, Y.Zhu, X.Luo,"Multi-user Searchable Encryption with Fine-Grained Access Control without key Sharing,"Int conference on advance science applications and technologies",2014.

[5] M.Li, S.Yu, Y.Zheng, N.Cao and W.Lou,"Authorized keyword search over aencrypted data in cloud computing,"international conference on distributed computing systems,2011.

[6] IM.Ibrahim,S.Nour,El-Din,R.Elgoharyu,H.Faheem,"A Genrianf Fine-Grained Data Access System for Sharing Digital objects in Honest but Curious Cloud Environment," International conference on cloud computing,2013.

[7] Miao Zhou,Yi Mu,Willy Susilo,Man Ho Au,"Privacy-Enhanced Keyword Search in Clouds",2013 12th IEEE International Conference on Trust,Security and Privacy in Computing and Communications.

[8] W.Sun, B.Wang ,N.Cao, M.Lou, Y.T.Hou, and H.li," Verifiable privacy preserving multi-keyword text search in the cloud supporting similarity-based ranking,"IEEETrans.ParallelDistrib.Syst,Vol.25,no.11,pp. 30253035,Nov.2014.

[9] S.YU, C.Wang, K.Ren, and W.Lou," Achieving secure, scalable, and fine-grained data access control in cloud computing,"inProc.IEEEConf.Comput.Commun.,1010,pp. 19.

[10] N.Cao, C.Wang, W.Lou,"Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," IEEE Trans.ParallelDistrib.Syst,Vol.25,no.1,Jan.2014.

[11] Q.Dong, Z.Guan,Z.Chen,"Attribute-based keyword search Efficiency Enhancement Via Online/Offline Approach,"IEEE 21st Int Conference.Parallel Distrib.Syst.2015.

[12] Q.Zheng, S.Xu, G.Ateniese,"Verifiable Attribute-Based Keyword Search over Outsourced Encrypted Data,"IEEE Conference on Computer Communication,2014.

[13] K.Kaushik, V.Vardharajan, R Nallusamy,"Multi-user Attribute Based Searchable Encryption,"IEEE 14th Int,Conference,2013.

[14] IM.Ibrahim,S.Nour,El-Din,R.Elgoharyu,H.Faheem,"A Genric anf Fine-Grained Data Access System for Sharing Digital objects in Honest but Curious Cloud Environment," International conference on cloud computing ,2013.

[15] M.Li, S.Yu, Y.Zheng, K.Ren and W.Lou,"Scalable and Secure sharing of personal health records in cloud computing Usingattribute-based Encryption,"IEEE Trans.Parallel Distrib.Syst,Vol.24,No.1,pp.131-143,Jan.2013.

## Author Profile

**Nirupama Devangaon** is a PG student in Computer Network and Engineering Department at PDA College of Engineering ,Kalaburgi, Karnataka, India. She has graduated from PDA College of Engineering with BE degree in computer science and Engineering Department in the year 2015.Her research interest in the area of Cloud Computing, Internet of Things and Computer Networks.

**Dr.Suvarna Nandyal** born in Kalaburgi,Karnataka,India in 1972.She received her BE degree in Computer Science and Engineering from Gulbarga University in 1993, M.Tech(Computer Science and Engineering) from VTU Belgaum in 2003 and Ph.D in the year 2013. She is presently working as professor and HOD of Computer Science and Engineering Department at PDA College of Engineering Kalaburgi, Karnataka, India. She has published number of papers in international journals and conferences. Her research interest include Image Processing, Machine Learning, Design and Development of mobile based applications, Computer Networks, Multimedia Communication.