OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

(Multidisciplinary Journal)

PRIVACY PROTECTION OF ENCRYPTED MEDICAL DATA OVER MULTI-AUTHORITY CLOUD SYSTEM

Mariya Ahmed[1] and Dr. T.K.Shaik Shavali[2]

Research Scholar, Dept. Of Computer Science and Engineering, Lords Institute of Engineering and Technology, Hyderabad, Telangana, India[1]
Professor and Head, Dept. of Computer Science and Engineering, Lords Institute of Engineering and Technology, Hyderabad, Telangana, India[2]

Abstract: - In the present-day cloud computing Private sensitive data service utilization of independent and corporate needs enormous computational power and scalability over data storage facilities to encourage big data utility applications power domains like insurance, public Health Care, and Research and Development areas needs to focus on Security attributes. An electronic insurance record or sensitive personal health record or client-specific personal information needs to get safeguarded from another id third party uses of the public cloud which could be done by adopting data transformation schemes. In the domain of cloud computing in which data as a service place a demanding situations over shared data utilization and inter-access facilities. Data access policies that are been empowered over insensitive data are being sufficiently scaled up whereas methodologies to interact sensitive information of data providers are to be enhanced to the present day security requirements. So user specific sensitive information is to get privacy-preserving by adopting effective and efficient encryption methodologies and not encouraging limitations over data utilization strategies which brings a great reliability and trustworthiness of personal sensitive information. Electronic health records or medical information or personal insurance policy reports or preparatory personal employee information to get maintained following high level security strategies so as to bring reliability and usability in a more wider boundaries. In order to facilitate a wide scalability, attribute based encryption is been adopted facilitating authorized methodologies to be performed over integrated security policies in multiple authority architectural platforms. Infocus of improvising security strategies by adopting optimal encryption methodologies main bring a overhead are barrier gates to search techniques of encrypted data formats.

Keywords:- *User data privacy, Encryption, Multi-authority, Forward security, Hashing Functions, Attribute Based Encryption*

INTRODUCTION

The present situation either identical or Enterprise collectively demands a huge quantity of big data applications through which data outsourcing is done effectively and service deployments could be monitored by cloud Service with effective and efficient data management policies as well as effective query processing is on demand[1][3]. When we are dealing with user sensitive data we may need to carefully e and has the privacy policies so that the outsourced data is in the hands of reliable circumstances[2]. In general data owner pushes sensitive data like insurance record, personal health record the, commercial transactions into the public cloud servers with an expectation on reliability and trustability over their personal information without having a profound inside look into the proprietor Re security policies[6]. But it is the duty of Cloud Service Provider or cloud servers who administrate the data users has to empower reliability by adopting typical encryption schemes over the sensitive data which is under sharable nature[4].

This sensitive Data Encryption policy should effectively work on the shareable data volumes in such that uses of trustable access only get privileged utilizing the shared data[5]. So the user-sensitive shareable data which is in plain formats should get converted into unencrypted formats that are ciphertext may be under table form but could battle with the access trails of unauthorized parties.Sensitive information of data provider needs to get privacy preserved in such that reliability of the system will be obtained especially for the data like individual insurance record, personal health record and individual employee information[8]. Sensitive data is been categorized into public and private roles where in public Information will be maintained corporate administration system and doesn't require any individual attention towards it. Where is

private sensitive information of user like personal health record is to be administered by the system in a more reliable and effectively. An additional focus will be maintained by the individual if the data is of private sensitive category so that system should acquire satisfactory trustability of the data provider and not giving any chance of leaks in the data accessible tier of the private sensitive date of the user provider[7]. Describe it sensitive electronic Medical Health record should be kept under availability to an external third party e in such that the local parties needs to get service benefits at appropriate time line with the more effectively and efficiently. So this corporate level of outsourcing the private sensitive electronic personal health record is to get maintained globally answer get accessible in a flexible manner without disturbing any privacy policies like data integrity of the data provided by the data owner.

When we focus and address private sensitive information by increasing the privacy preservation policy levels which could be done by by an effective encryption policy mechanism not only addresses privacy but also needs to address flexible data access control for the proprietary third-party person in order to facilitate services in an effective and efficient manner[9]. So the access policies are been framed in Association with the privacy protection privacy policies so that at a glance data provider private sensitive information secure availability and flexible data accessibility is been driven in a more effective and efficient manner. More or less when we emphasize on security level effective encryption methodology that is been driven when we upload sensitive information on the cloud in the same way at the retrieval third party notes high level security over sensitive information decryption should be driven responsibility[10].

II LITERATURE SURVEY

2.1 Security Challenges for the Public Cloud, IEEE :

Focusing on the upcoming enhancements administrating services over Cloud Computing domain computational operational it is are been entertained in such that area of software as a service is been empowered with the new attribute of security requirements. Based on the operational nature of cloud computing that is a request that could range from a user on towards the cloud server computational resources are being effectively administered with the wide scope in drastic resource

deployment and came to an effective utilization policy. The fundamental operational activities shouldn't get disturbed when we attempt to enhance the computational services that got delivered or outsourced both to an independent body d or a corporate division committed to specific commercial and managerial terms effectively. These logical computational strategies need to get administered by cloud service providers as it involves commercial and managerial statistics of the system as well as needs to randomly adopt resource deployment in rapid timelines. So this recommended Cloud Service Provider infrastructural and managerial capability with sophisticated computational methodologies should play an effective part towards security both within and outside the system limits and should also handle privacy attacks from and malicious users which may reduce the reliability and trustability over the system

2.2 Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption

Maintaining sensitive personal information is a crucial factor intern facilitating patient control on towards access privileges of of their own personal health records without compromising on security e factors makes is to move to adopt typical encryption process model before it is been outsourced on to the Cloud Service. Handling electronic health records has a great demand when we accommodate them in cloud computing environment which could be driven with patient centric model of of medical data exchange aaj is been kept available for outsource to a third party service provider authorized parties.We may need to emphasize on several security risks over the private information of the the data owner provided content needs to get empowered with privacy, scalability, index key management, trustable data access is been contributed in an effective way. In this research we also focus on many data owner count situation and bifurcate the users into a variety of domain based security models which in turn minimizes the complexity in maintaining key Management process.

2.3 Secure sharing of Personal Health Records in cloud computing:

This research paper introduces a new approach related to data access control mechanism in a fine grained manner along with the the data retrieval strategies over shareable data in an encrypted format associated with a signature. Sensitive information of a data owner provided electronic medical data or personal health record could be maintained in a cloud computing platform without compromising on security levels could be in a situation to outsource this personal data to a third party service provider so as to facilitate privileged services to the data uses. In this research we adopted signature oriented attribute-based encryption strategy which converts plain text formats to ciphertext format fulfills the need of security requirements. By associating and digital signature in the process of encryption not only facilitates confidentiality, authenticity, recollect ability, self dependent and collision free are been provided effectively.

III SYSTEM ANALYSIS

Existing system:

As personal health records are a sensitive information we may need to address them with the flexible access policy but restricted to the desired authorized permissible uses so as to avail medical Services inappropriate timeline in a more effective manner. This identity-based first that is been converted from plane formats to unpredictable ciphertext formats doesn't

support wide ability in retrieval process. Electronic medical records been encrypted in order to maintain privacy protection so that the third party could be in a situation to to request for the the personal information which could be delivered and decrypted with an appropriate security key is been administered effectively.

Disadvantages of existing system:

- In Medical field modular element i.e Personal health record after encryption doesn't facilitate data retrieval operations or filtering with the desired parameter couldn't be driven in an effective way.
- Even though third party access control requires only a security key to decrypt the data but needs to get privileged with flexible data filtration for fetching of data with an identification string of plane formats towards encrypted electronic health record data needs to get improvised with the proper search algorithm.

Proposed system:

Private sensitive personal health record is been mapped to security key as well as within machine identity key like secret key is been administered by a service provider which is been facilitated to third party access on demand. Unsophisticated searchable encryption technique is been adopted in order to filter or retrieve electronic health record with specific identity key string query so as to permit privileged service or perform data filling operations by an appropriate authorized users.

Advantages of proposed system:

- This cipher-text converted attribute based encrypted data meets high level security standards so as to bring reliability to data uses for their sensitive information.

1. Fulfilling the security concern even search string data retrieval process is also been well organized with and lower data access timelines.

IV IMPLEMENTATION

Data Owner

In this module, Data owner has to register to cloud and logs in, Encrypts and uploads a file selecting the related domain like java or .net etc... And also uploads the patient details giving the patients credentials. Once uploaded the data owner has the options of deleting the patient details or the file uploaded. And also verifies the file or the details whether attacked by the attacker.

Cloud Server

In this module the cloud will authorize both the owner and the user. Views all the requests from the users and provides the keyword search control. In this module able to view all the uploaded files and the details and also the content attackers who try to attack the files or the patient details. And also will have a track of the top searched keywords and the file rank depicted on the chart.

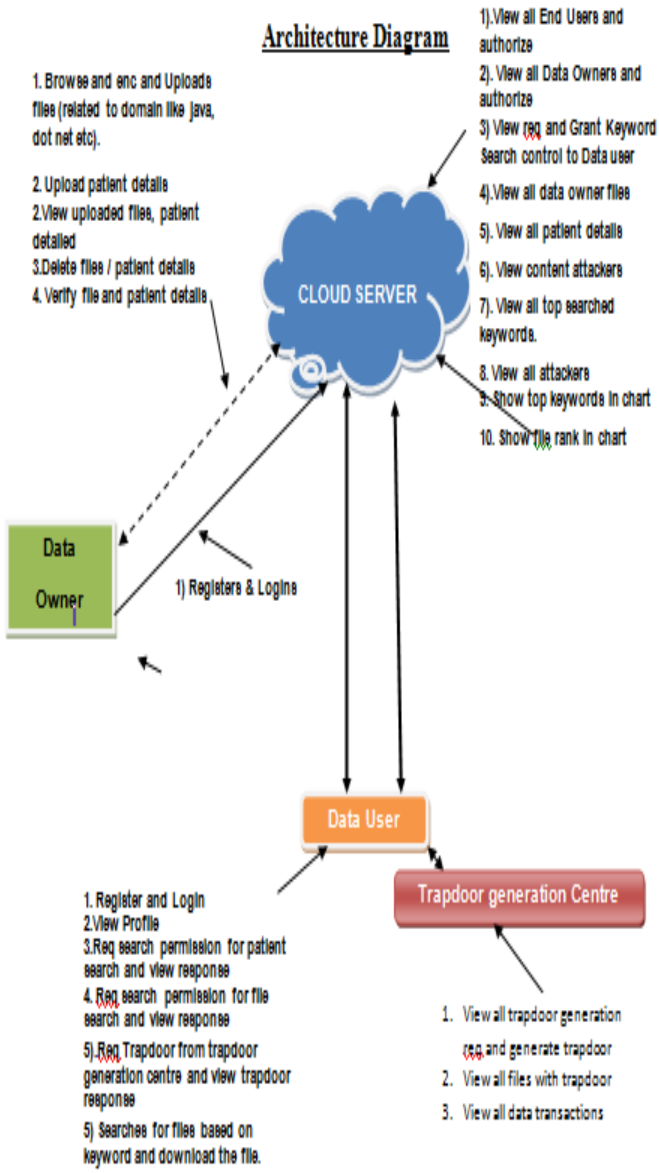
TRAPDOOR GENERATION CENTRE

In this module, the trapdoor generation centre views all the requests processed by the data user and generates the trapdoor, after the generation the files are displayed with the corresponding trapdoor generated for particular files or patient details.

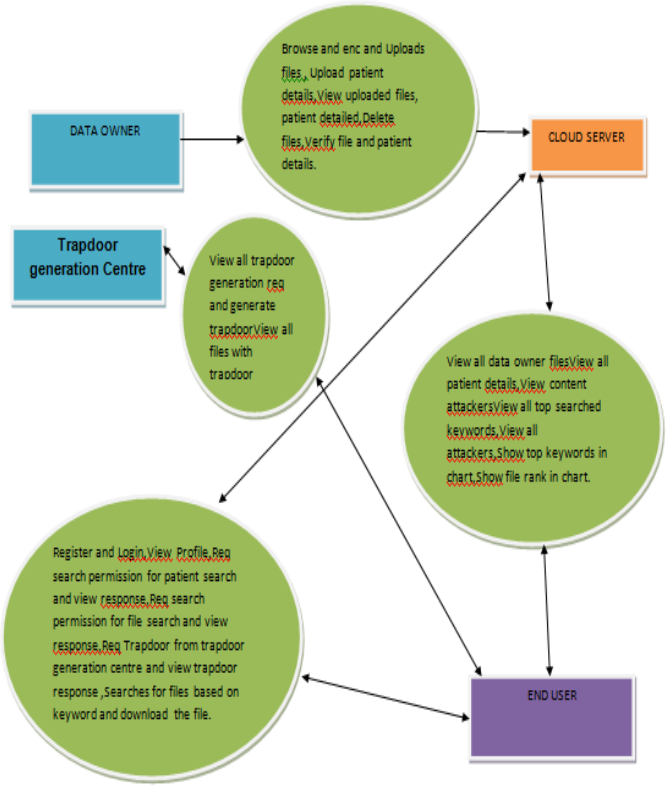
Query User

In this module, the user has to register to cloud and logs in. before the user can search for the files or the patient details the user must request for the serach permission from the cloud only when the user is provided with the serach permission he can view the file and later the user has to request for the trapdoor from the trapdoor generation center if he wants to download the searched file or the patient details.

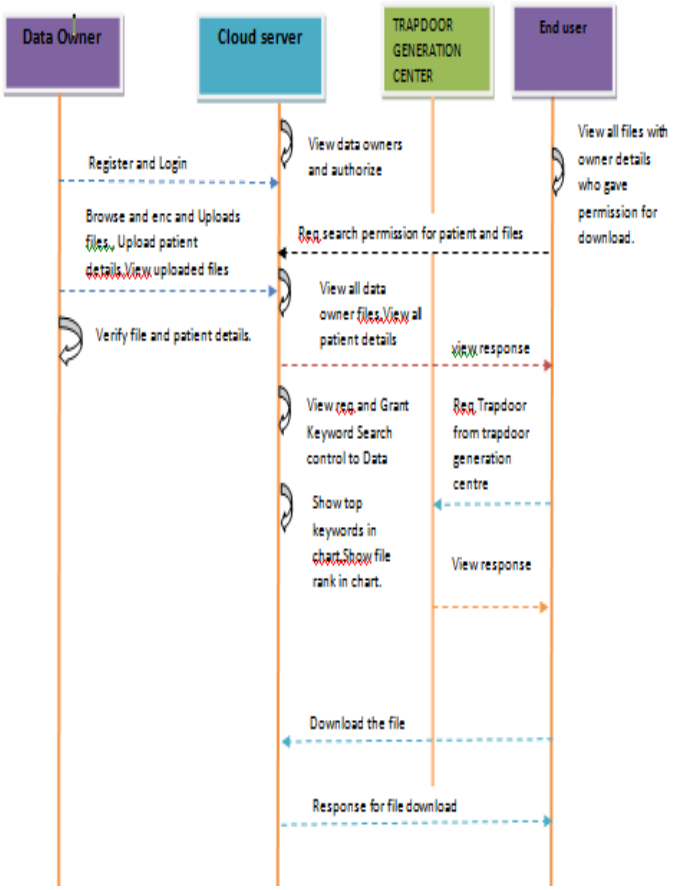
V SYSTEM DESIGN



Data flow diagram:



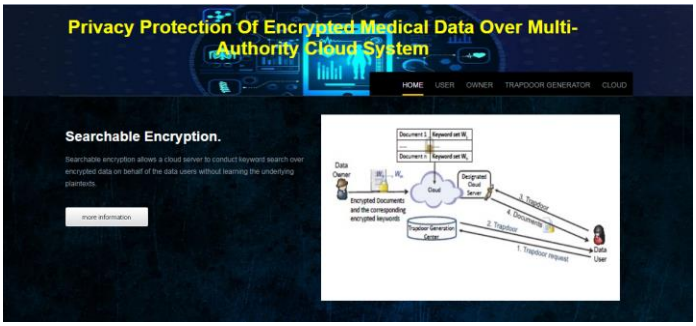
Sequence diagram:



VI PROJECT EXECUTION AND TESTING

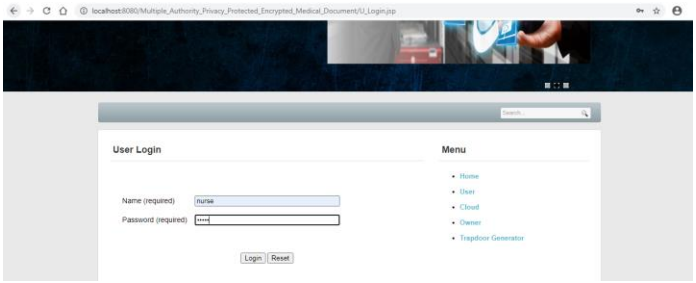
Welcome screen:

This is a welcome page of the project that Privacy Protection of Encrypted Medical Data over Multi-Authority Cloud System.

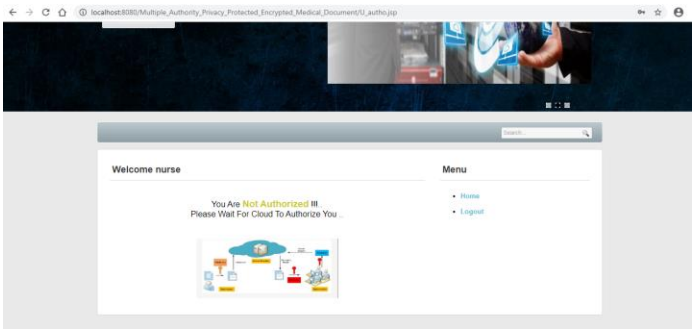


User Login page :

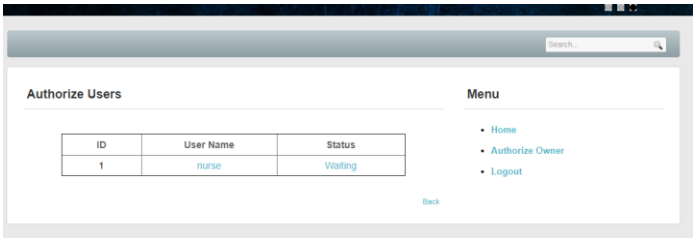
This is a user login page through which users can able to use his services by entering their credentials like user mail ID and password as well there is an option to make a new registration to create a new user account. If the entered credentials are not correct it will be redirected to the very same page. If the user enters the right credentials will get migrated to the user home page successfully and can utilize specified services provided by the server.

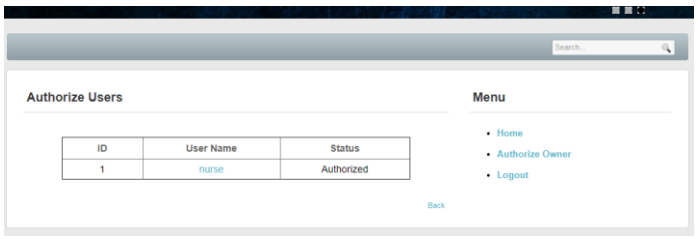


One more User Registration & Authorization Process…



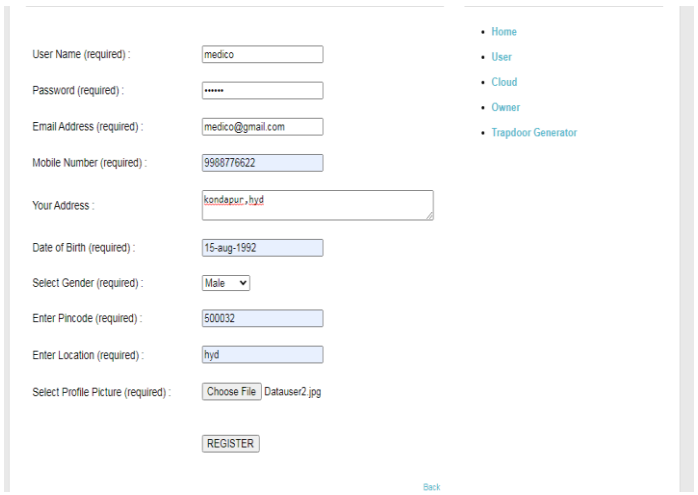
User Authorization page :

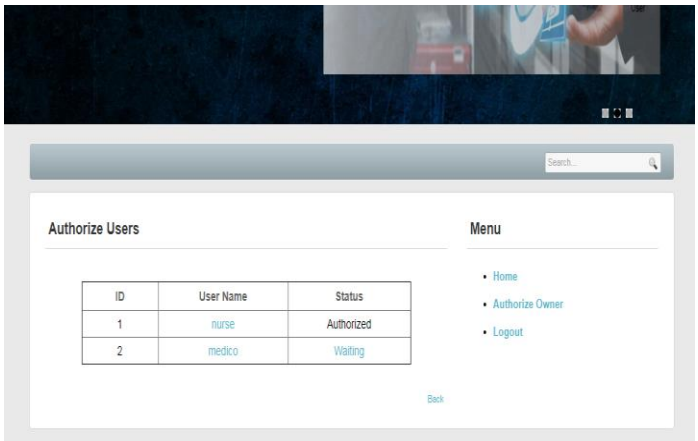


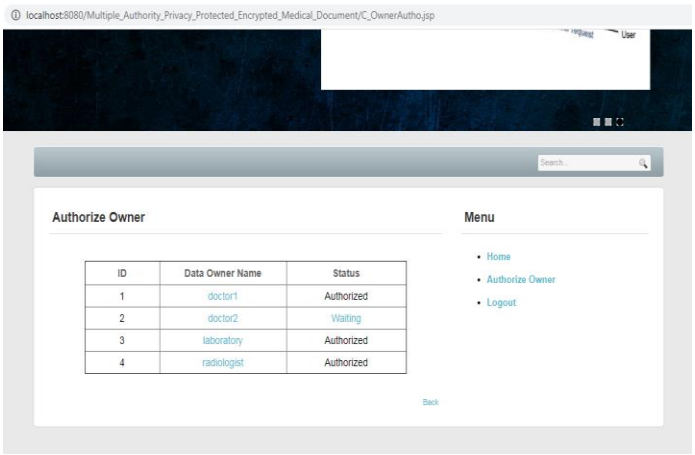


User homepage:

User will enter into this page upon successful entry of credentials in the User login page. This page enables all the services provided by the server like Search, my profile, view files, search permission and trapdoor permission options are facilitated.

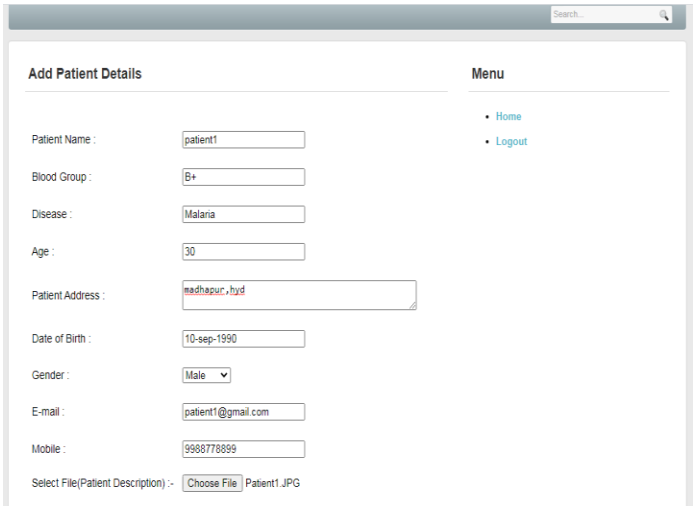


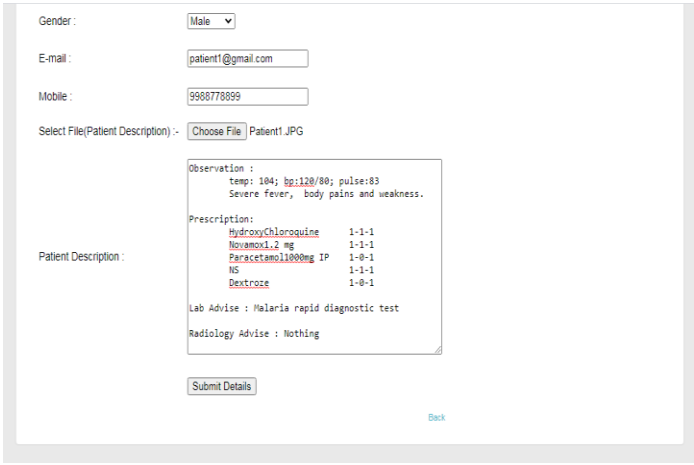


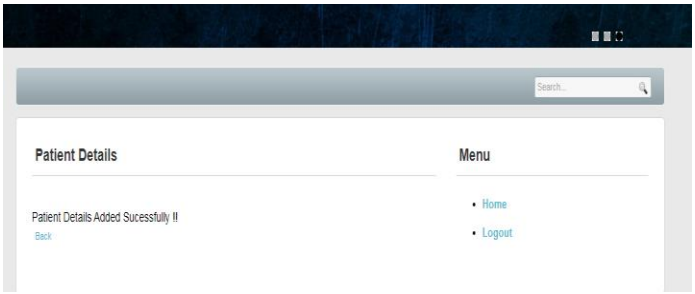


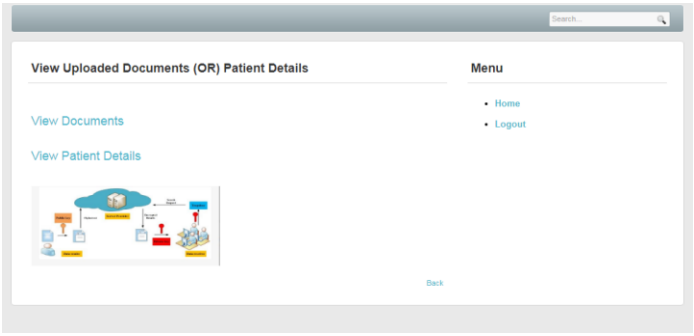
Add Patient details page:

The content of the specific Patient get added by data owner



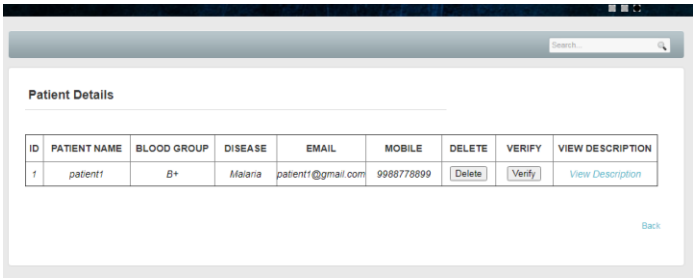


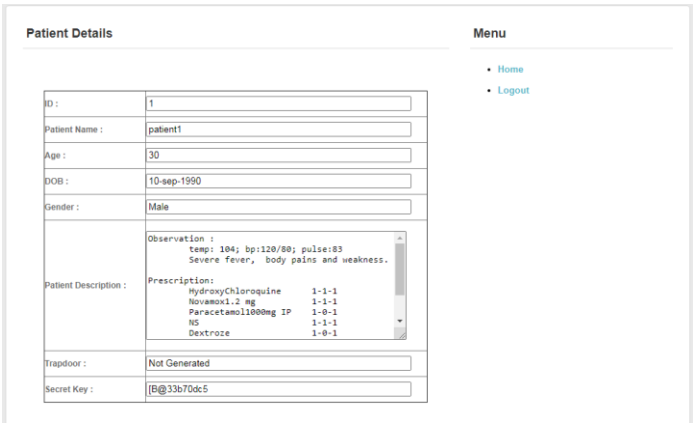


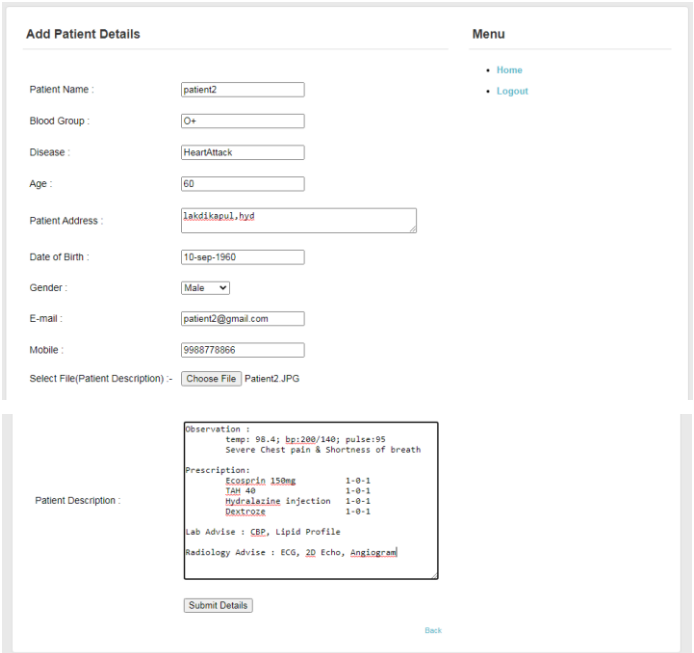


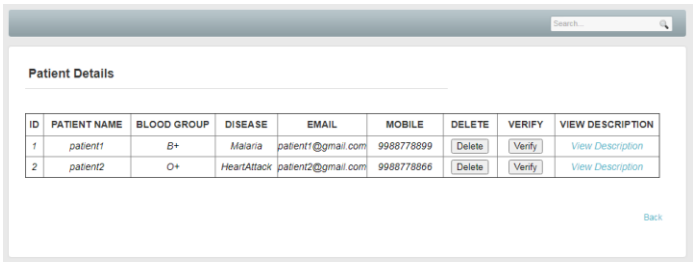
View Patient details page:

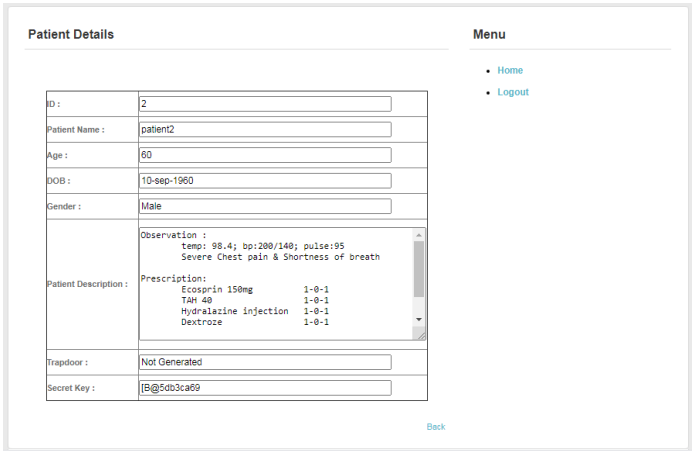
The content of the specific Patient that got selected is been visualized here.

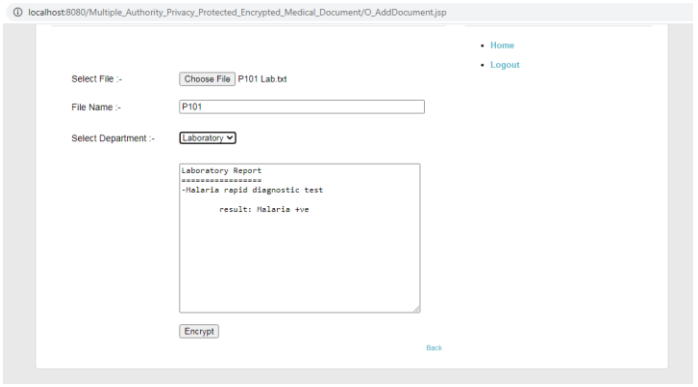


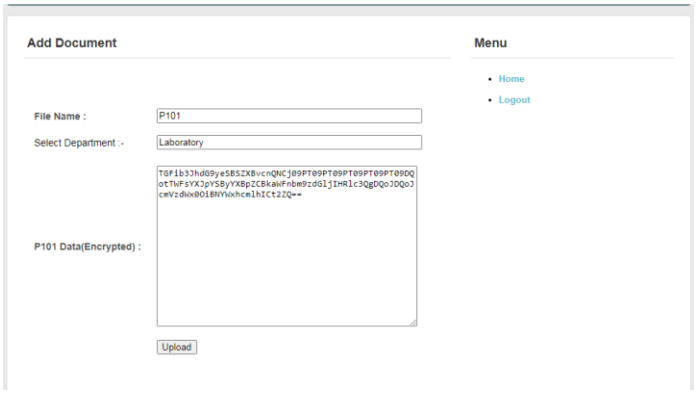


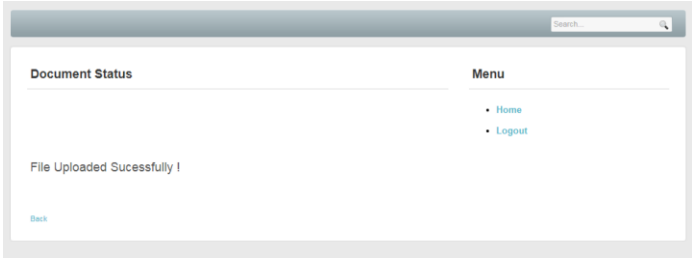




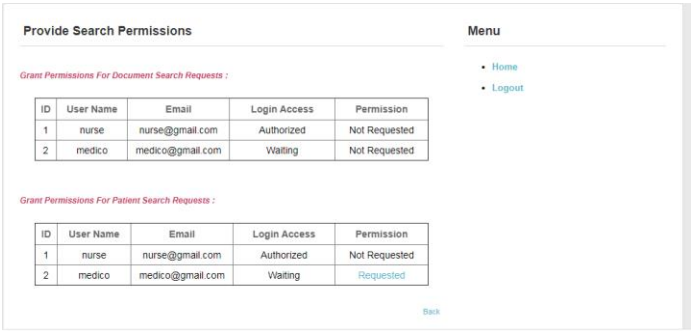


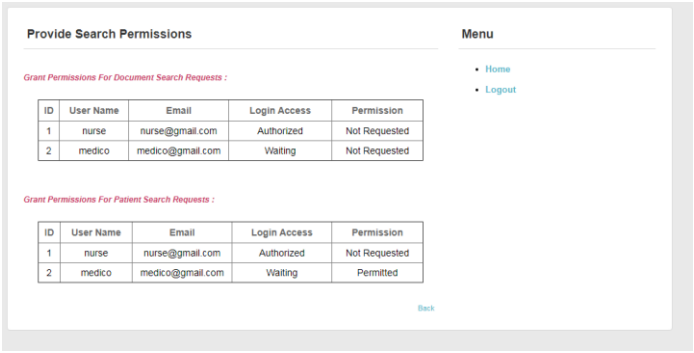






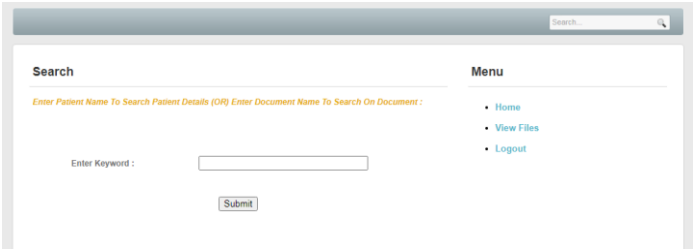
In cloud

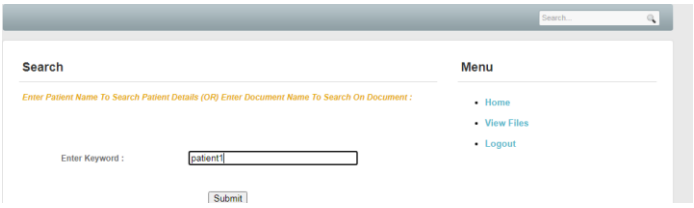


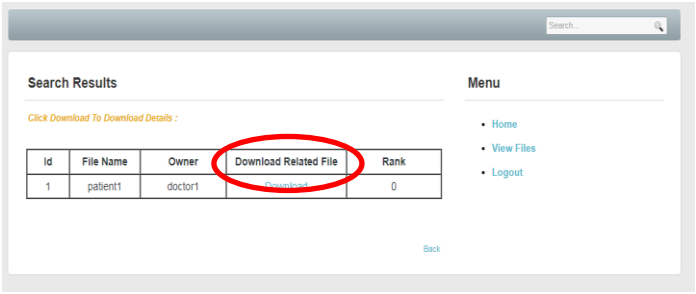


Patient search page:

Hindi action search page we could enter keyboard so that we can filter a specific patient detail and the result will get visualised as well it will provide download facility.







VII CONCLUSION

In this project we recommended and implemented secure and flexible fine grained sensitive encrypted user data in public clouds over multi authority platforms. With the sufficient Research and Analysis that is been made to design probable practical data access retrieval strategies in such that we could facilitate enhanced searchable encryption query handling mechanism are been effectively driven. Sensitive data access policies over optimized and liberalized achieving trustability and reliability over both data owners and data users is been empowered successfully. Electronic health records or medical information or personal insurance policy reports or preparatory personal employee information to get maintained following high level security strategies so as to bring reliability and usability in a more wider boundaries. Thus we facilitated a wide scalability, attribute based encryption is been adopted facilitating authorized methodologies to be performed over integrated security policies in multiple authority architectural platforms. We focus of improvising security strategies by adopting optimal encryption methodologies main bring a overhead are barrier gates to search techniques of encrypted data formats is been achieved successfully.

REFERENCES

1. Weizhi Meng, Wenjuan Li, and Lam Kwok, “Towards EffectiveTrust-Based Packet Filtering in Collaborative Network Environments,” IEEE Transactions on Network and Service Management, vol. 14, No.1, 2017

2. W. Meng, Kim-Kwang Raymond Choo, Steven F, Athanasios V.Vasilakos, and Christian W., “Towards Bayesian-based TrustManagement for Insider Attacks in Healthcare Software-DefinedNetworks, “Future Generation Computer Systems, vols. 4344, pp.99-109, 2015.

3. A. Engelmann and A. Jukan, W. zu Braunschweig, “Towards All-Optical Layered Encryption: A Feasibility Analysis of Optical Stream Cipher,” IEEE Transactions on Information Forensics and Security, vol. 24, no. 1, pp. 131–143, 2019.

4. M. Tang, Haichang Gao, Yang Z, Yi Liu, Ping Zhang and P. Wang, “Research on Deep Learning Techniques in Breaking Text-based Captchas and Designing Image-based Captcha,” IEEE Transactions on Information Forensics and Security, Vol.14, No.8, 2016.

5. Jose Fonseca, Marco Vieira, and Henrique Madeira, “Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection,” IEEE Transactions on Dependable and Secure Computing, Vol. 11, No. 5, 2014.

6. Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 1–17, Jul. 2012.

7. R. Wu, G.-J. Ahn, and H. Hu, “Secure sharing of electronic health records in clouds,” In 8th IEEE International Conference

on Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom), 2012, pp. 711-718

8. M. Shucheng Yu, Yao Zheng, Kui R., W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using

Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems. Vol. 24, No. 1, 2013.

9. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9

10. DaeHun Nyang, Aziz Mohaisen, Jeonil Kang, "Keylogging-resistant Visual Authentication Protocols," IEEE Transactions on Mobile Computing, vol. 1, no. 8, August 2014.