e-ISSN 2320 –7876 www.ijfans.org
Vol.11, S Iss.1, 2022
 UGC CARE Listed ( Group -I) Journal

# Privacy Protection in Healthcare Information system using Heterogeneous Public Cloud Authorities

**Mohammed Mujahid Hyder [1] Md Ateeq Ur Rahman [2] Syed Shujath Ali [3]**

[1] Research Scholar, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

[2] Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

[3] Assistant Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086.

***Abstract -*** The rapid development of the Internet of Things (IoT) has led to the emergence of more and more novel applications in recent years. One of them is the e-health system, which can provide people with high-quality and convenient health care. Meanwhile, it is a key issue and challenges to protect the privacy and security of the user's personal health record. Some cryptographic methods have been proposed such as encrypt user's data before sharing it. However, it is complicated to share the data with multiple parties (doctors, health departments, etc.), due to the fact that data should be encrypted under each recipient's keys. Although several (t, n) threshold secret sharing schemes can share the data only need one encryption operation, there is a limitation that the decryption private key has to be reconstructed by one party. To offset this shortcoming, in this paper, we propose an efficient identity-based distributed decryption scheme for personal health record sharing system. It is convenient to share their data with multiple parties and does not require reconstructing the decryption private key. We prove that our scheme is secure under chosen-cipher text attack (CCA). Moreover, we implement our scheme by using the Java pairing-based cryptography (JPBC) library on a laptop and an Android phone. The experimental results show that our system is practical in the electronic personal health record system.

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.

***Index Terms*** **—** Distributed decryption, identity-based encryption, security, privacy, e-health system.

## I. 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. 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. 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. 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.

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. 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. 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. 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. 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.

## II. SYSTEM ANALYSIS

**Problem Statement:**

The advancement of modern technologies, such as sensors and cloud computing, has completely changed conventional healthcare systems. Such systems can demonstrate the strong potential of next-generation healthcare services after digitizing paper-based medical records. Individuals' health conditions can be remotely sensed by medical devices, transmitted by medical networks, and processed by the edge, fog, and cloud computing. Innovative healthcare systems that can improve quality of life will become more essential for various smart healthcare services such as remote monitoring, diagnosis, treatment, and prescription based on personal electronic health (e-health) data. However, the modern ehealthcare system is a double-edged sword. While it gives us advanced healthcare services, security concerns have increasingly emerged.

**Objective:**

PHR includes not only health data, but also some important information related to patient care. This data is managed by the patient and usually stored in the cloud server (medical servers) [4]. Unlike the electronic medical record, the PHR is not created and maintained by institutions (such as medical establishments and hospitals). The data collection and uploading are done by the patient. The purpose of PHRs is to store an accurate and complete summary of the individual's medical.

**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:**

E-health system, which can provide people with high-quality and convenient health care. Meanwhile, it is a key issue and challenges to protect the privacy and security of the user's personal health record. 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. Personal health record is been highly secured with an effective cipher-text converted attribute based encryption technique so as to increase the privacy policy standard. 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.
- Fulfilling the security concern even search string data retrieval process is also been well organized with and lower data access timelines.

**Proposed System:**

A medication recommender system is absolutely necessary in order to aid doctors and patients in expanding their knowledge about medications for particular medical conditions. A recommender framework is a common system that makes an item recommendation to the user based on their benefit and needs. These frameworks use consumer surveys to analyze the responses and offer recommendations based on the respondents' precise needs. The drug recommender system uses sentiment analysis and feature engineering to conditionally provide medications based on patient reviews. Sentiment analysis is a succession of approaches, techniques, and instruments for identifying and separating emotional information from language, such as opinions and attitudes. In contrast, the process of "feathering engineering" involves adding new features to the ones that already exist in order to enhance model performance.

The Sequential Model and XGBoost classifier surpass all other models with roughly 95% accuracy, according to the data. We implemented this model in a real-world setting in which users can log in, submit their symptoms, and receive a list of medicines that are recommended for their condition.

**Advantages**:

- Able to predict drug recommender systems uses sentiment analysis and feature engineering most accurately.
- By receiving a list of medicines that are recommended for their condition Minimize loss and maximize profits.

## III. PROPOSED MODULAR IMPLEMENTATION

Below is the proposed modular implementation of the project. It consists of four modules:

**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.

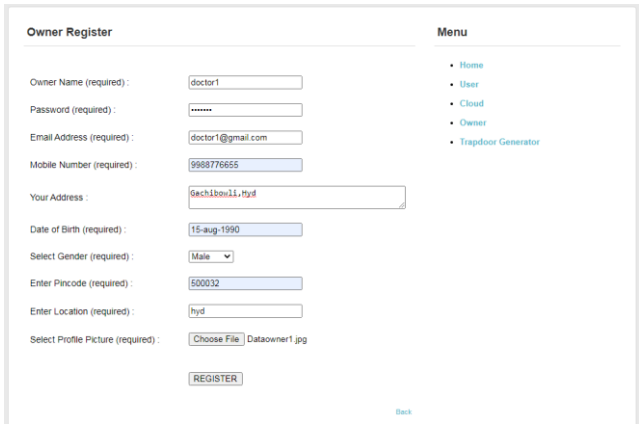
## IV. PROJECT EXECUTION

**Welcome screen:**

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


**Registration page:**

Using this registration page the person could be able to create his cloud owner registration with his personal information which could be reused in logging into his account it with the credentials entered on this page. This is the page where are all owners have to use to create the account in the database and while the service is provided by the cloud server.

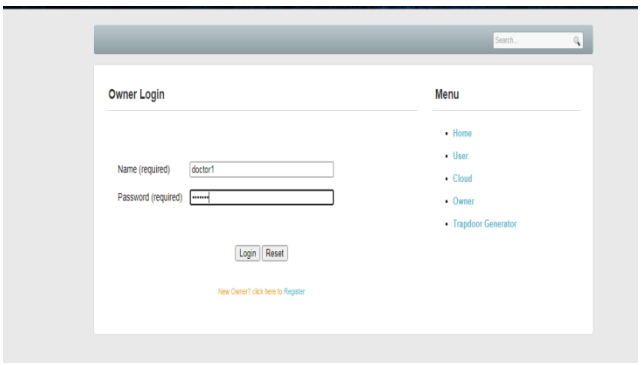



Registered Sucessfully

Back Home

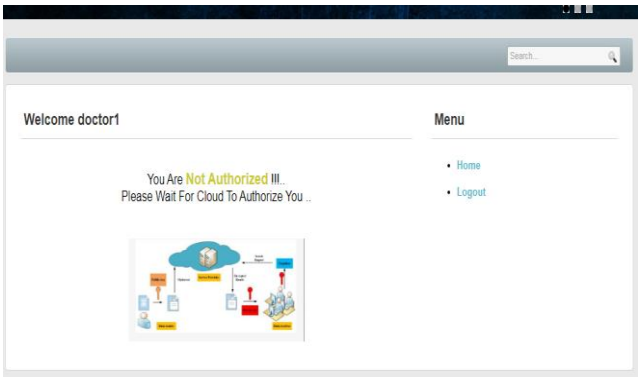
**Owner Login page :**

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




**Owner homepage:**

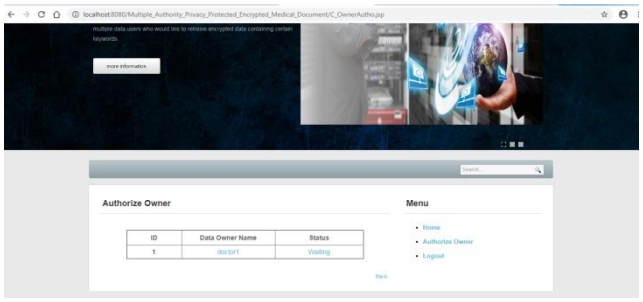
Owner will enter into this page upon successful entry of credentials in the Owner login page. If the data owner is not authorised by the cloud administrator then a warning message will be prompted as below.

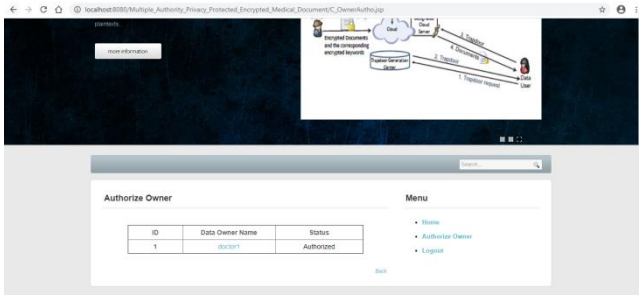



**Owner Authorization page:**

In cloud module there is a facility to organise data owners so that data owners could have while their services after clearing their authentication process in owner login page.

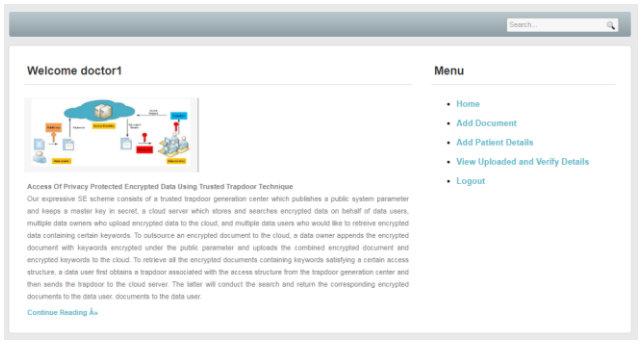
e-ISSN 2320 –7876 www.ijfans.org
Vol.11, S Iss.1, 2022
  **UGC CARE Listed ( Group -I) Journal**



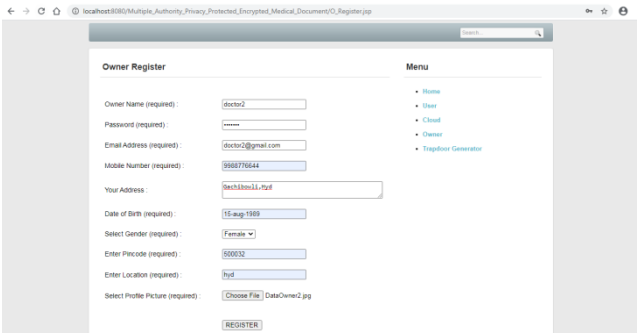

**Owner homepage:**

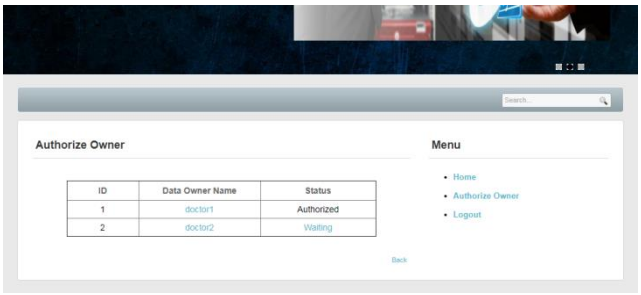
Owner will enter into this page upon successful entry of credentials in the Owner login page. This page enables all the services provided by the server like Add document, at patient details, view uploaded and verify details options are facilitated.




**Owner Registration page :**

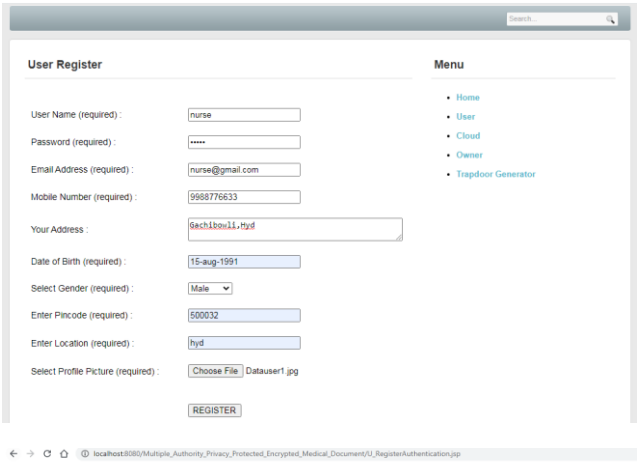
Using this registration page the person could be able to create his cloud owner registration with his personal information which could be reused in logging into his account it with the credentials entered on this page. This is the page where are all owners have to use to create the account in the database and while the service is provided by the cloud server.

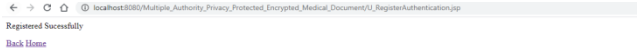



**User Registration page :**

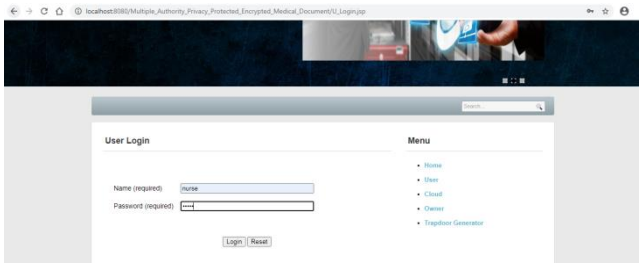
Using this registration page the person could be able to create his cloud owner registration with his personal information which could be reused in logging into his account it with the credentials entered on this page. This is the page where are all owners have to use to create the account in the database and while the service is provided by the cloud server.




**User Login page :**

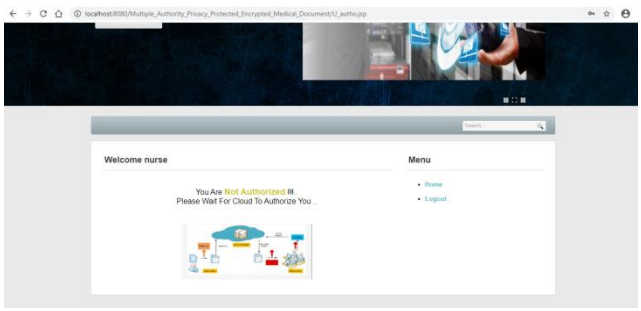
This is a user login page through which users can able to use his services by entering their credentials like user mail ID and password as well there is an option to make a new registration to create a new user account. If the entered credentials are not correct it will be redirected to the very same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

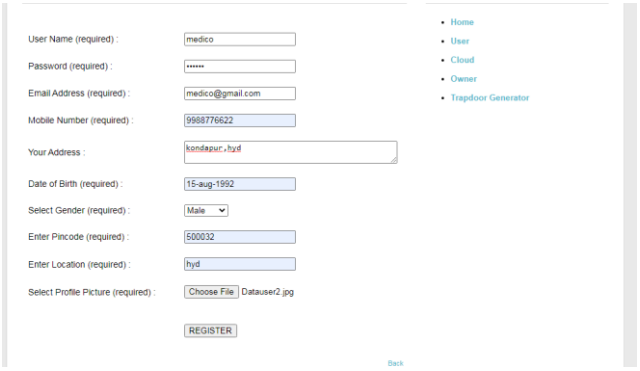



**User homepage:**

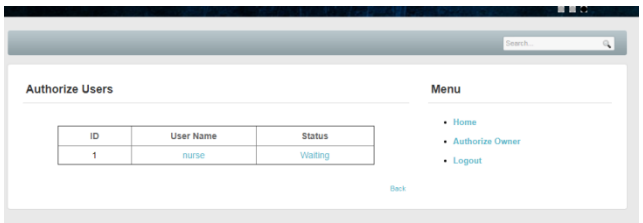
User will enter into this page upon successful entry of credentials in the User login page. This page enables all the services provided by the server like Search, my profile, view files, search permission and trapdoor permission options are facilitated.

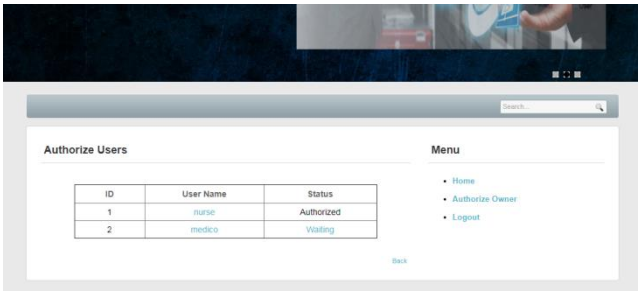

**One more User Registration & Authorization Process…**

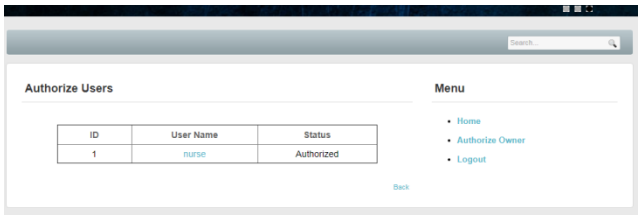


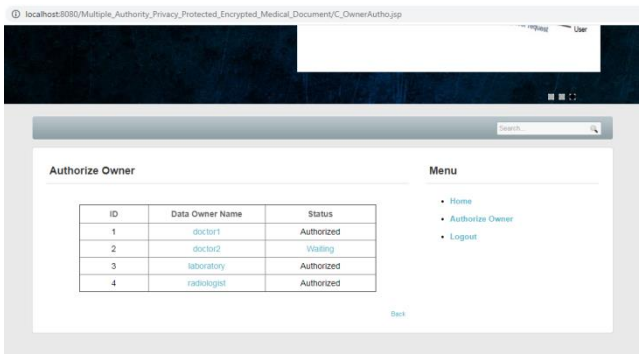

User Authorization page :



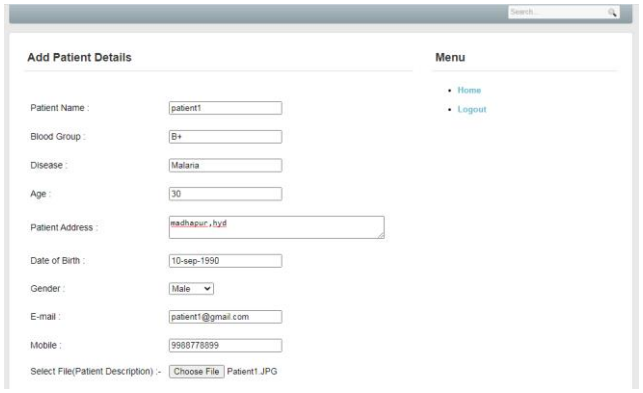
e-ISSN 2320 –7876 www.ijfans.org
Vol.11, S Iss.1, 2022
  **UGC CARE Listed ( Group -I) Journal**

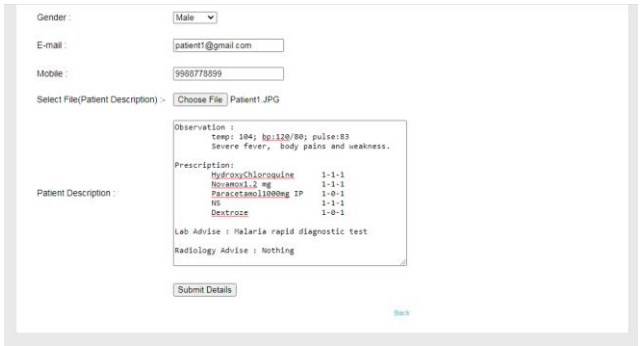


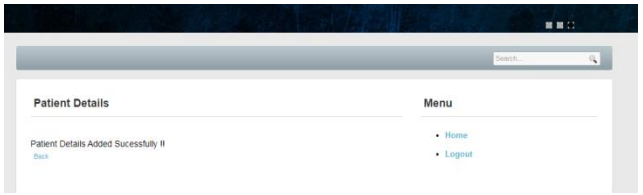


## Add Patient details page:

The content of the specific Patient get added by data owner

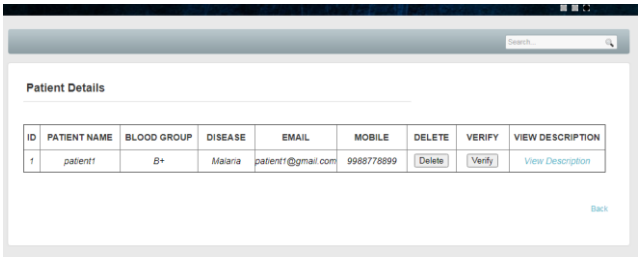


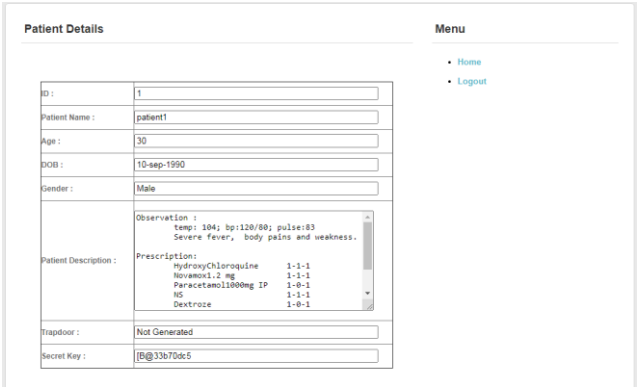



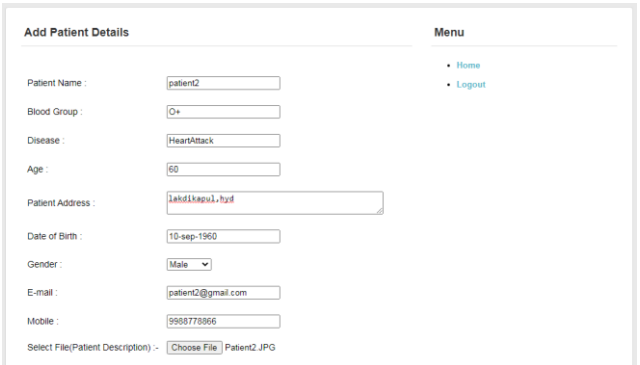




## View Patient details page:

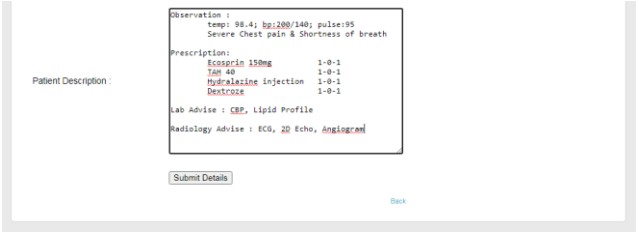
The content of the specific Patient that got selected is been visualized here.

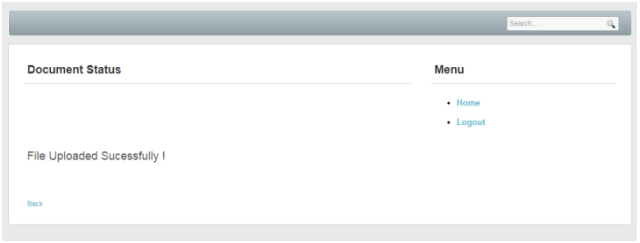


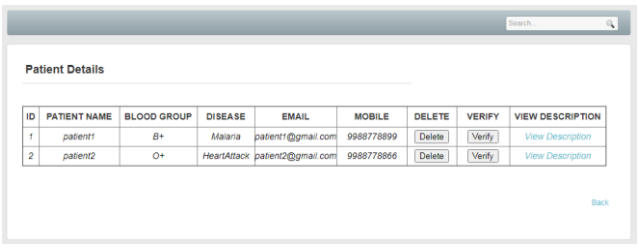



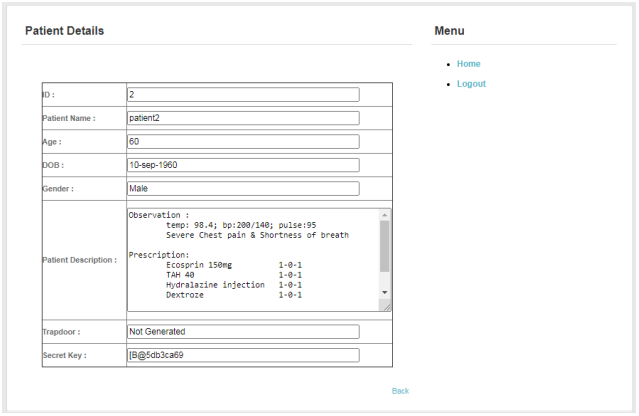



e-ISSN 2320 –7876 www.ijfans.org
Vol.11, S Iss.1, 2022
  **UGC CARE Listed ( Group -I) Journal**

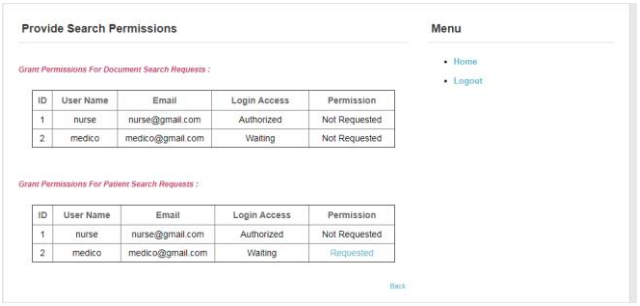


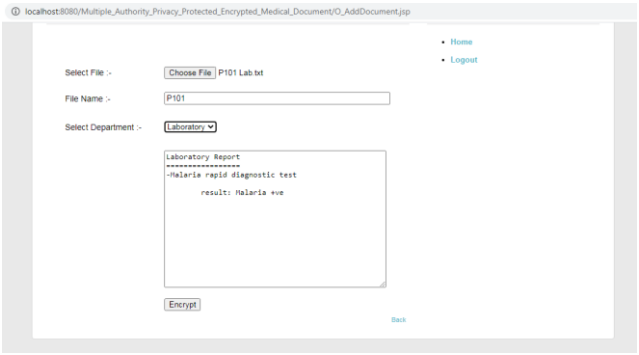



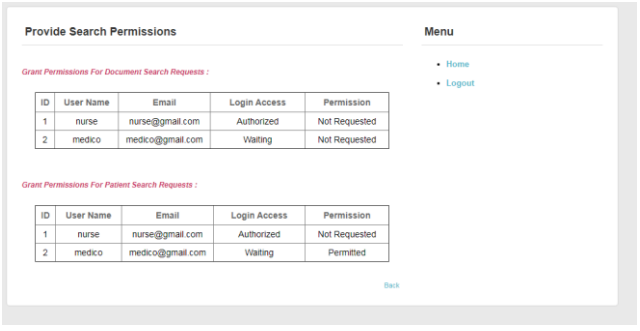



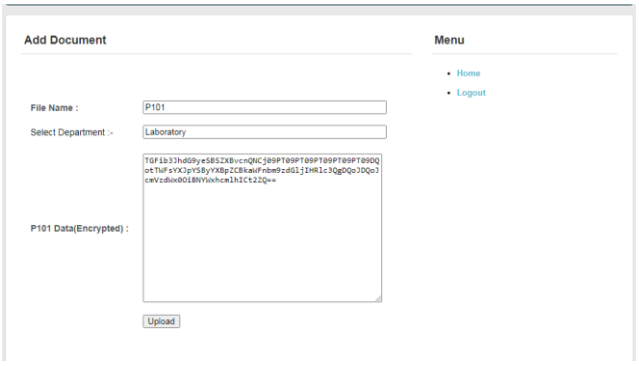




**In cloud**



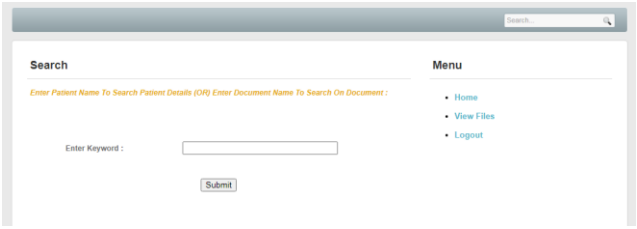



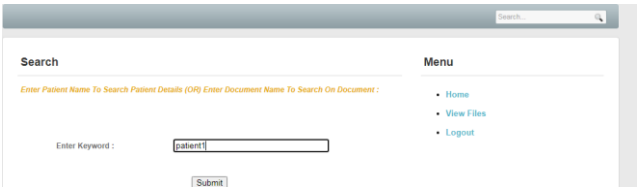



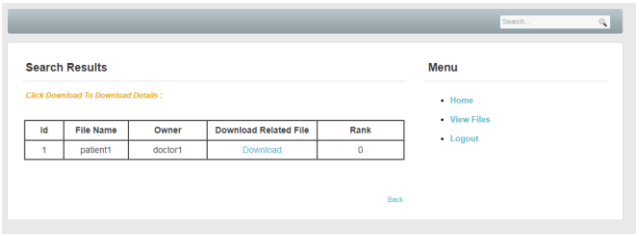




**Patient search page:**

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.




## V. 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.

**Future Scope:** the current project could enhance by new scheme using block-chain to manage keys in the scheme. The new proposed scheme stores the hash values of encrypted personal health records in block-chain, and the related index set is stored in smart contract, which can further improve the efficiency of data integrity verification.

## REFERENCES

[1] G. Eysenbach, “What is e-health?” Journal of medical Internet research,
vol. 3, no. 2, p. e20, 2001.
[2] V. Chang, Y.-H. Kuo, and M. Ramachandran, “Cloud computing adoption
framework: A security framework for business clouds,” Future
Generation Computer Systems, vol. 57, pp. 24–41, 2016.
[3] M. Obaidat and N. Boudriga, Security of E-systems and Computer
Networks. Cambridge University Press, 2007.
[4] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z.
Sands, “Personal health records: definitions, benefits, and strategies for
overcoming barriers to adoption,” Journal of the American Medical
Informatics Association, vol. 13, no. 2, pp. 121–126, 2006.
[5] R. Pifer, “Patient use of digital health tools lags behind hype,

poll finds,"
https://www.healthcaredive.com/news/patient-use-of-digitalhealth-tools-lags-behind-hype-poll-finds/562778/,
accessed Sept 12,
2019.
[6] Protenus, "32 million breached patient records in first half of 2019 double total for all of 2018,"
https://www.prnewswire.com/newsreleases/32-million-breached-patient-records-in-first-half-of-2019-double-total-for-all-of-2018-300894237.html,
accessed Jul 31, 2019.
[7] J. L. Ferna´ndez-Alema´n, I. C. Sen˜or, P. A´ . O. Lozoya, and A. Toval,
"Security and privacy in electronic health records: A systematic literature review," Journal of biomedical informatics, vol. 46, no. 3, pp. 541–562,
2013.
[8] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou,
"Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE transactions on parallel and distributed systems,
vol. 24, no. 1, pp. 131–143, 2012.
[9] H. Qian, J. Li, Y. Zhang, and J. Han,
"Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation,"
International Journal of Information Security,
vol. 14, no. 6, pp. 487–497, 2015.
[10] X. Liu, Y. Xia, W. Yang, and F. Yang,
"Secure and efficient querying over personal health records in cloud computing," Neurocomputing, vol. 274, pp. 99–105, 2018.