|| Volume 5 || Issue 11 || November 2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

ENABLING AND SECURING MULTI-WORD SEARCH IN PRIVACY PRESERVED EHR OVER MULTI-AUTHORITY MEDICAL DATABASES

Manzoor ul Hasan[1] , Dr K.Nagi Reddy[2]

Research Scholar, Dept. of Computer Science & Engineering, LIET, Hyderabad[1]
Professor, Dept. of Computer Science & Engineering, LIET, Hyderabad[2]
hasanmanzoorul5@gmail.com[1]
k.nagireddy@lords.ac.in[2]

Abstract:- In the domain of cloud computing in which data as a service has demanding situations over shared data utilization and inter-access facilities, especially when we emphasize on data service activities and focus to think on insensitive and sensitive categories of information related to data provider concern. Data access policies that are being empowered over insensitive data are being sufficiently scaled up whereas methodologies to interact with sensitive information of data providers are to be enhanced to the present-day security requirements. So the privacy of user-specific sensitive information is to be preserved by adopting effective and efficient encryption methodologies and not encouraging limitations of data utilization strategies. This brings great reliability and trustworthiness to personal and 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 to bring reliability and usability in wider domains. To facilitate scalability, attribute-based encryption is being adopted, facilitating authorized methodologies to be performed over integrated security policies in multiple authority architectural platforms. With the focus on improvising security strategies by adopting optimal encryption methodologies, there might be an overhead and are barricades to the search techniques of encrypted data formats.

Keywords:- *Multi-authority, encrypted data search, e-medical system, cloud storage, forward security.*

I INTRODUCTION

Sensitive information of data providers needs to get privacy preserved in such that reliability of the system will be obtained especially for the data like individual insurance records, personal health records, and individual employee information[1]. Sensitive data is been categorized into public and private roles where the public Information will be maintained by the corporate administration system and doesn't require any individual attention towards it[2]. Whereas the private and sensitive information of the user like personal health record is to be administered by the system more reliably and effectively[4]. 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 access tier of the private sensitive date of the user provider. Describe it sensitive electronic Medical Health record[3] should be kept under availability to an external third party e in such that the local parties need to get service benefits at appropriate time line with the more effectively and efficiently[5]. 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[6].

When we focus and address private sensitive information by increasing the privacy preservation policy levels which could be done 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 to facilitate services effectively[9] and efficiently. 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 more effectively and

efficiently[7][8]. More or less when we emphasize the 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.

Along with the security policies as we need to focus on accessibility parameter secure searchable keyword mechanism has to be performed on all entities of electronic medical records so that filtration or retrieval of an appropriate specific phr needs to get performed in a more optimal timeline. This could be done by adopting the recent research computational methodologies into the present system m that reduces data access time effectively and communication cost pushes down to the line[10]. All these points that we discussed here could be addressed by a single authority more efficiently than multi-authority access control to the remote third party nodes. Access control operations of private sensitive information always are restricted by the client level security policies but giving a chance to some authorized typical personalities like hospital management, doctors, diagnosis department and so on is not a violation of targeted policy standard but in turn, facilitate the resource feeling by appropriate authorized people to avoid the liability towards third party services for the desired uses. The above statement doesn't let all the personalities of the users be in a situation to fill or modify private sensitive information entity but to selected authorized characters could fill technical requirements that are being pushed into the private sensitive electronic health record with appropriate information.

II LITERATURE SURVEY

Secure sharing of Personal Health Records in cloud computing:

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 to facilitate privileged services to the data uses.

This research paper introduces a new approach related to the data access control mechanism in a fine-grained manner along with the data retrieval strategies over shareable data in an encrypted format associated with a signature.

In this research we adopted signature oriented attribute-based encryption strategy which converts plain text formats to ciphertext format fulfills the need for 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.

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

Handling electronic health records has great demand when we accommodate them in a cloud computing environment which could be driven with a patient-centric model of medical data exchange is kept available to outsource to a third-party service provider authorized parties.

Maintaining sensitive personal information is a crucial factor intern facilitating patient control towards access privileges of their health records without compromising on security factors makes is to move to adopt a typical encryption process model before it is been outsourced on to the Cloud Service.

We may need to emphasize several security risks over the private information of the data owner provided content needs to get empowered with privacy, scalability, index key management, trustable data access is been contributed effectively.

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.

All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption

In this research paper research is been aimed towards scalable searchable encryption strategies that provide query string execution searches over personal information of the user which is in encrypted files formats the God associated with data clients.

In cloud computing platforms there is a focusable parameter of the untrustable nature of cloud data service that accommodates private or personal user-specific information in such that we adopt secure encryption strategies on that data.

In this paper, we primarily emphasize file injection collisions that are when data server outsources data towards the data usage so that he could encrypt and deposit that into the storage back ok providing query-based privacy of monarchy word and injection search engine themes are been effectively adopted.

So this file injection collision operations can expose data clients string queries over a few injected files along with improvising search engine methodologies that effectively reduce data leakages.

III SYSTEM ANALYSIS

Existing system :

Electronic medical records have been encrypted to maintain privacy protection so that the third party could be in a situation to request for the personal information which could be delivered and decrypted with an appropriate security key is been administered effectively. As personal health records are sensitive information we may need to address them with the flexible access policy but restricted to the desired authorized permissible uses to avail medical Services inappropriate timeline more effectively. This identity-based first that is been converted from plane formats to unpredictable ciphertext formats don't support wide ability in the retrieval process.

Disadvantages of the existing system:

Personal health record after encryption doesn't facilitate data retrieval operations or filtering with the desired parameter couldn't be driven effectively.

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:

A personal health record is been highly secured with an effective cipher-text converted attribute based encryption technique to increase the privacy policy standard. A private sensitive personal health record is been mapped to security key as well as within a machine identity key like MAC key is been administered by a service provider which is been facilitated to third-party access on demand. Unsophisticated searchable encryption techniques is been adopted to filter retrieve electronic health records with specific identity key string queries to permit privileged service or perform data filling operations by appropriately authorized users.

Advantages of the proposed system:

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

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

IV IMPLEMENTATION

Modules:

In this project, we made four segments based on the operational nature of domain expectations considering their roles and responsibilities as a deciding factor.

1. Data server
2. Cloud owner
3. Data user
4. Data encryption

1. Cloud server:

The cloud server module is a base platform architectural model that provides infrastructural data storage capabilities enabling data access permissions remotely to a wide number of authorized users. Along with that reliability, a parameter has to be facilitated to the data owner who outsources valuable information into the cloud server. Operationally the Data Server login by using valid credentials logins in successfully and been facilitated with operations such as View Owners & Authorize, View Users & Authorize, View User Request, View Cloud Server Files, View Transactions, View Attackers, View Time Delay Results, and View Throughput Results

2. Data Owner:

The data owner is a module about the authority that facilitates shareable data from Cloud user private sensitive data to the cloud server with an appropriate cipher-text conversion policy to increase security standards. Data owner outsources the crucial data i.e PHR permitted to remote third-party person from cloud computing remote servers.

In this module, Operationally there are n numbers of Data Owners are present. Data Owner should register before doing any operations. Once the Owner registers, their details will be stored in the database. After

registration successful, he has to login by using an authorized user name and password. Once Login is successful Owner will do some operations like Upload, View My Files, View My Profile, Verify, Delete File

3. Data user:

The data user module is used to interact with the shareable data the public clouds without disturbing the Data integrity policies framed by the cloud administrator. An authorized or trustable request that got erased from this data user module will be addressed by a remote server and facilitates appropriate data that meets the data access requirements.

In this module, Operationally there are n numbers of users are present. Users should register before doing any operations. Once user registers, their details will be stored in the database. After registration successful, he has to login by using an authorized user name and password. Once Login is successful, the user will do some operations like View My Profile, Search String, View Cloud Files, Request Sk, View File Response, Download

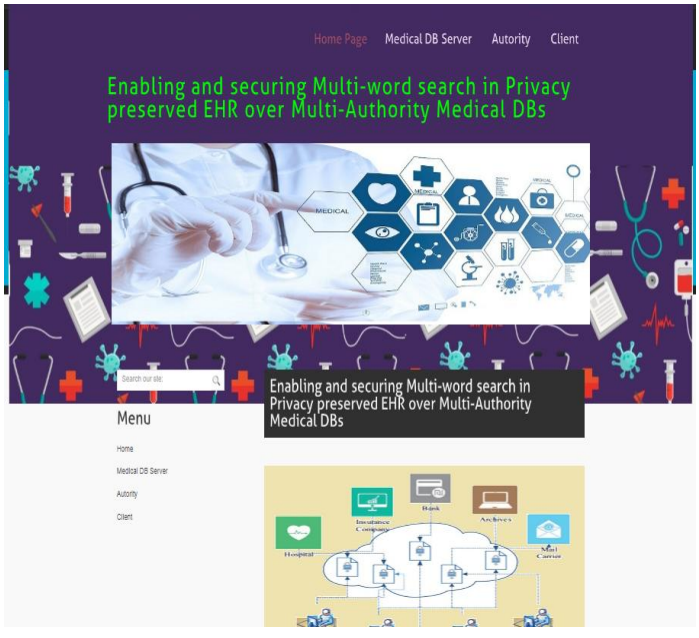
4. Data encryption:

Data that got uploaded by the data owner into the remote server needs to maintain data integrity and high-security standards to obtain reliability.

V PROJECT EXECUTION AND TESTING

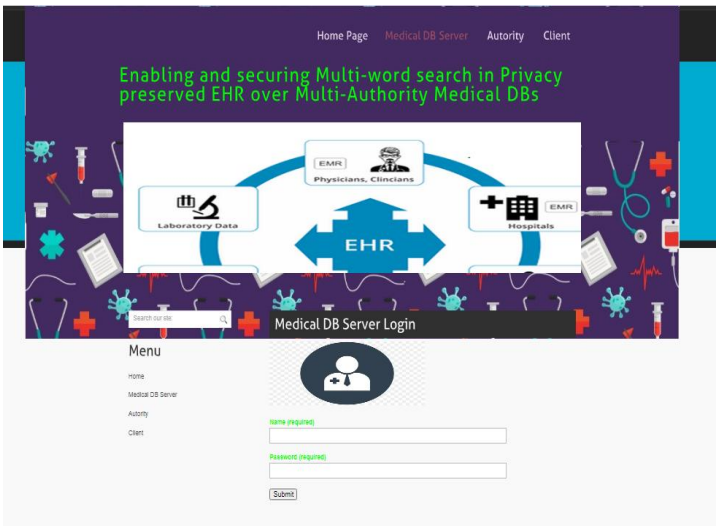
Welcome screen:

This is a welcome page of the project that is enabling and securing multi-word searches in a privacy preserved manner over multi-authority medical databases.



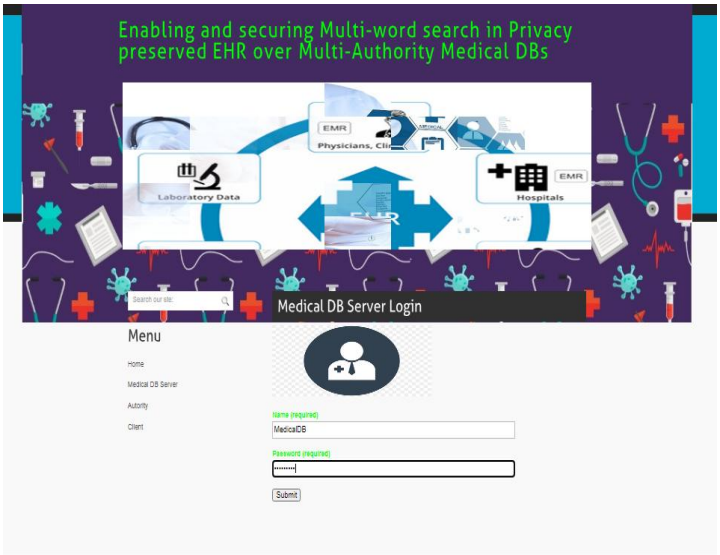
Medical database server page:

Among the three models available in the project medical database server is a high priority service platform, here is a login page related to that.



Medical database login page:

This page by filling appropriate medical database server credentials that is username: MedicalDB and password: MedicalDB, just click on submit in such that we can migrate into the medical database server home page.

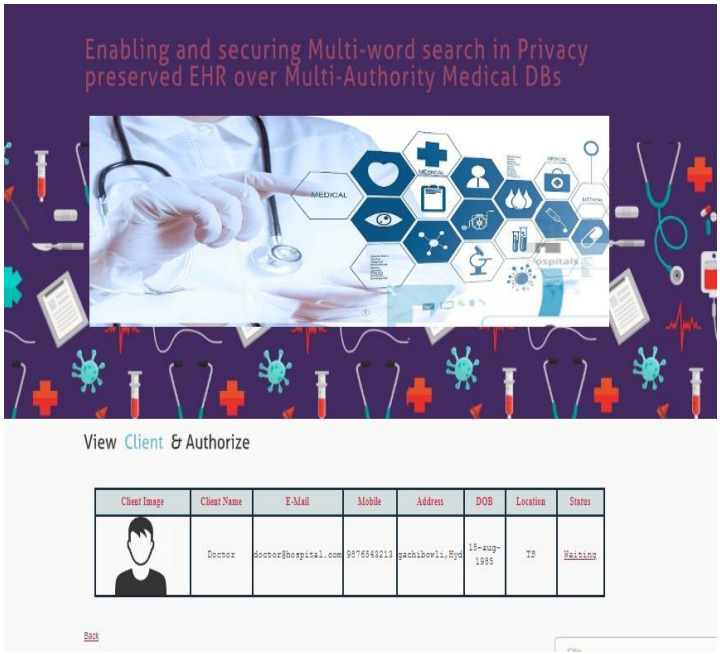


Medical database homepage:

After successfully entering medical database login credentials in control migrate to this page here authority and authorize, view clients and authorize, view client requests, view cloud server files, view transactions, view attackers are been facilitated for the administration of database server.

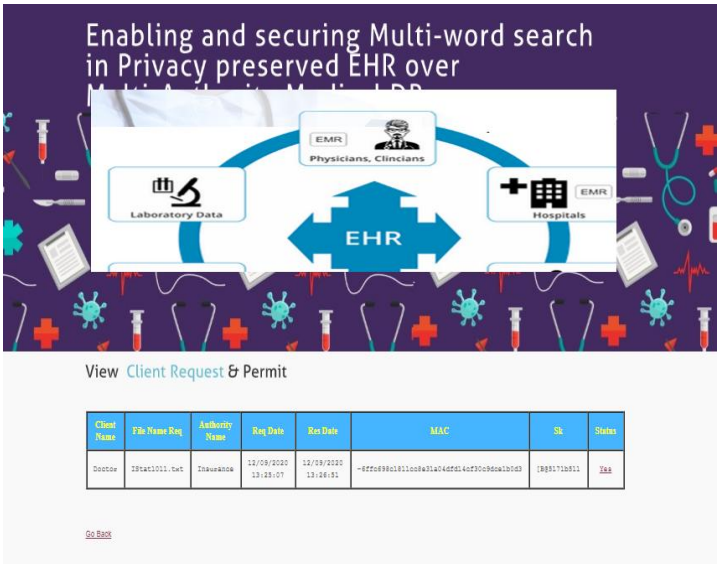
View client and authorized page:

A list of all client personal information and their authorization status is been visualized for administrative purposes.



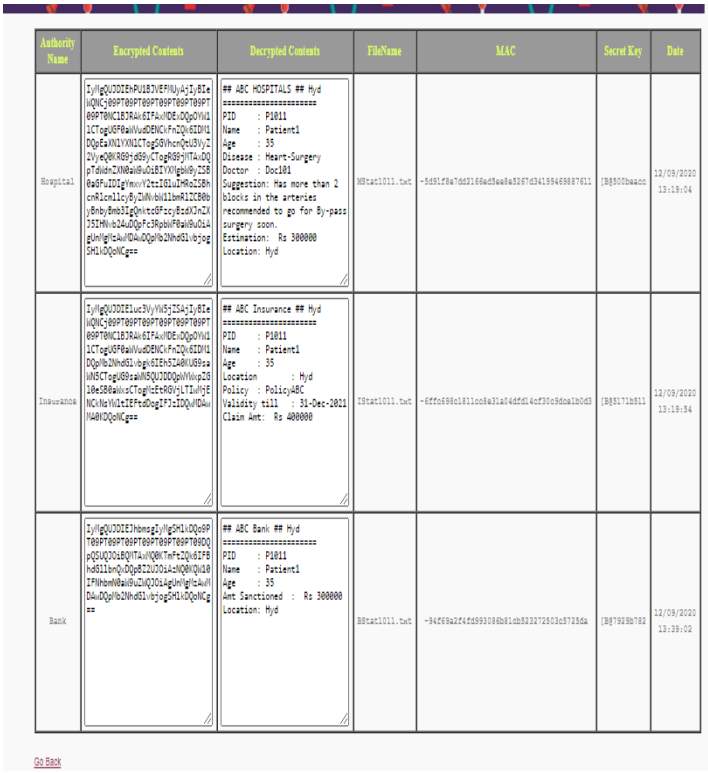
View client request and permit page:

Here on this page, client-specific requests for a file without the written name, request date, response date, mac key, secret key, and permission status have been visualized.



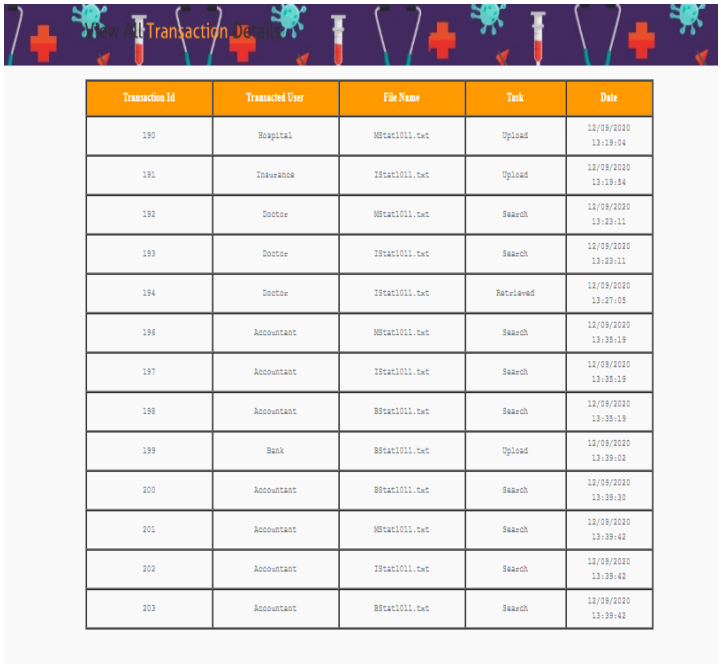
View cloud server files page:

On this page, every file related to encrypted content, decrypted contents, file name, MAC key, secret key, and date of upload are been visualized.



View transaction page:

All transactions of a user towards a file have been listed here. It could be upload or search for data retrieval that is visualized in a tabular form.

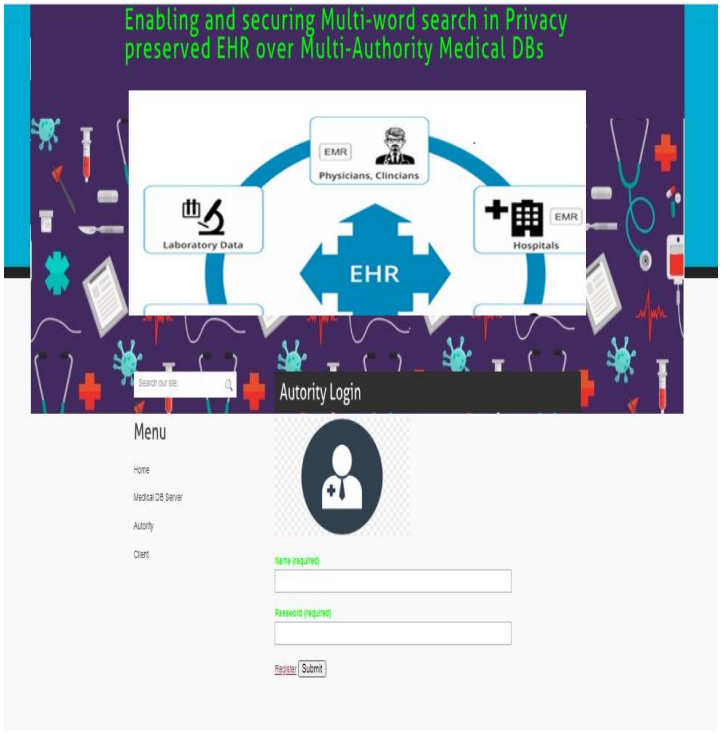


View All Transaction Details

Transaction Id	Transacted User	File Name	Task	Date
190	Hospital	MStat1011.txt	Upload	12/09/2020 13:19:04
191	Insurance	IStat1011.txt	Upload	12/09/2020 13:19:54
192	Doctor	MStat1011.txt	Search	12/09/2020 13:23:11
193	Doctor	IStat1011.txt	Search	12/09/2020 13:23:11
194	Doctor	IStat1011.txt	Retrieved	12/09/2020 13:27:05
196	Accountant	MStat1011.txt	Search	12/09/2020 13:35:19
197	Accountant	IStat1011.txt	Search	12/09/2020 13:35:19
198	Accountant	BStat1011.txt	Search	12/09/2020 13:35:19
199	Bank	BStat1011.txt	Upload	12/09/2020 13:39:02
200	Accountant	BStat1011.txt	Search	12/09/2020 13:39:30
201	Accountant	MStat1011.txt	Search	12/09/2020 13:39:42
202	Accountant	IStat1011.txt	Search	12/09/2020 13:39:42
203	Accountant	BStat1011.txt	Search	12/09/2020 13:39:42

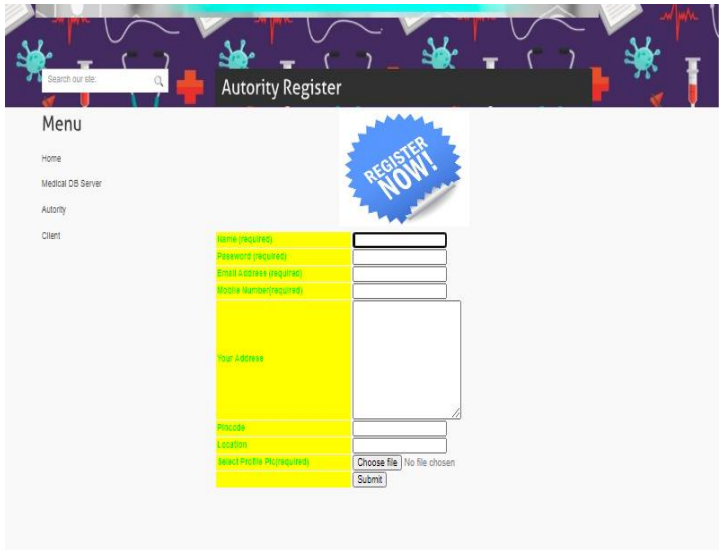
Authority login page:

Authority login page is an Authority service entry page if we enter appropriate credentials we can migrate into other Authority homepage.



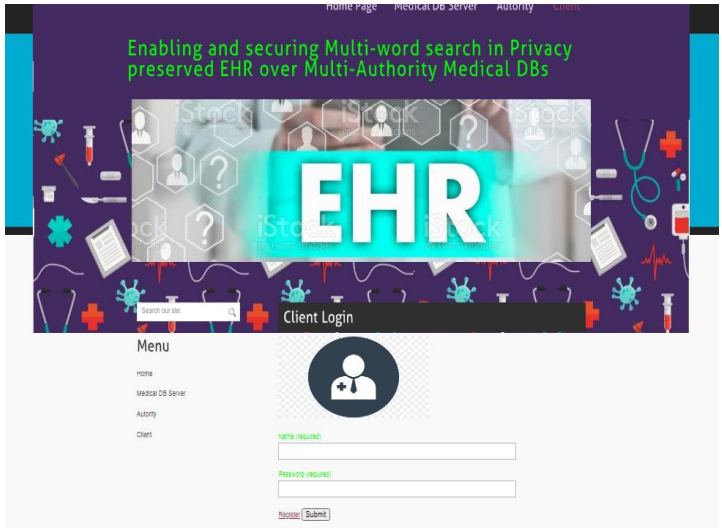
Authority registration page:

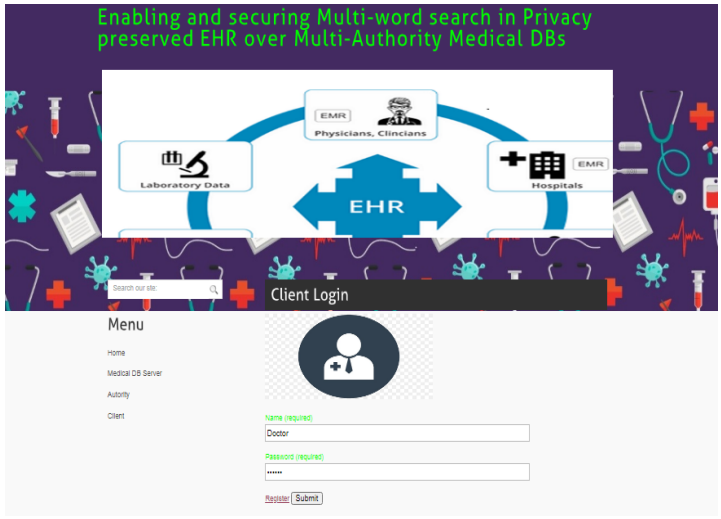
ITI registration page facilitates the creation of a new account into the database with Authority personal information.



Client login page:

The client login page is a client service entry page if we enter appropriate credentials we can migrate into another client homepage.



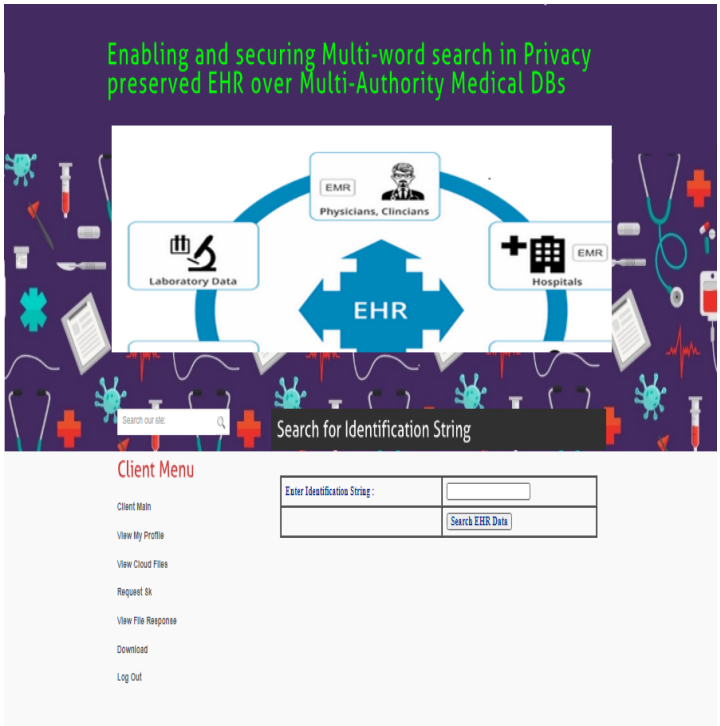


Client home page:

On this page, client-related facilities are been provided like view profile, search string, view cloud files, request SK, view file response, and download are been empowered.

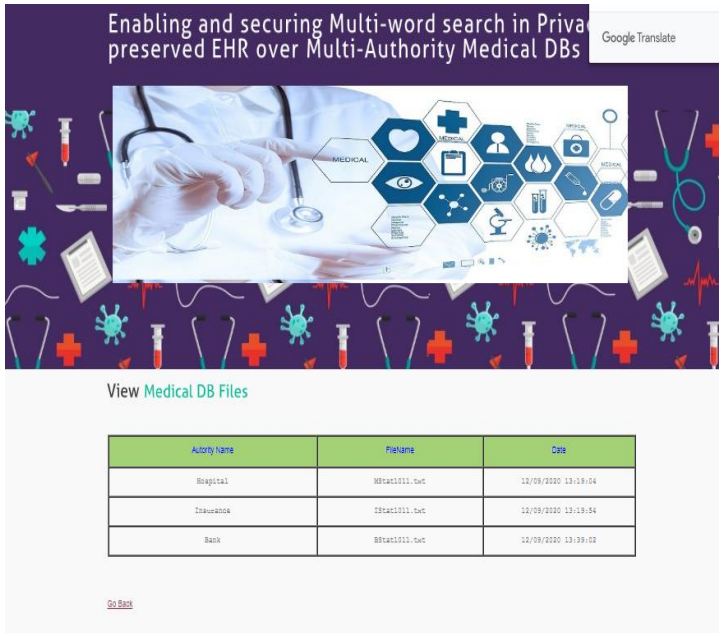
String search page:

One of the primary facilities is a crucial service facilitated to clients as multi-keyword identification brings search over sensitive information like EHR data is been facilitated here.



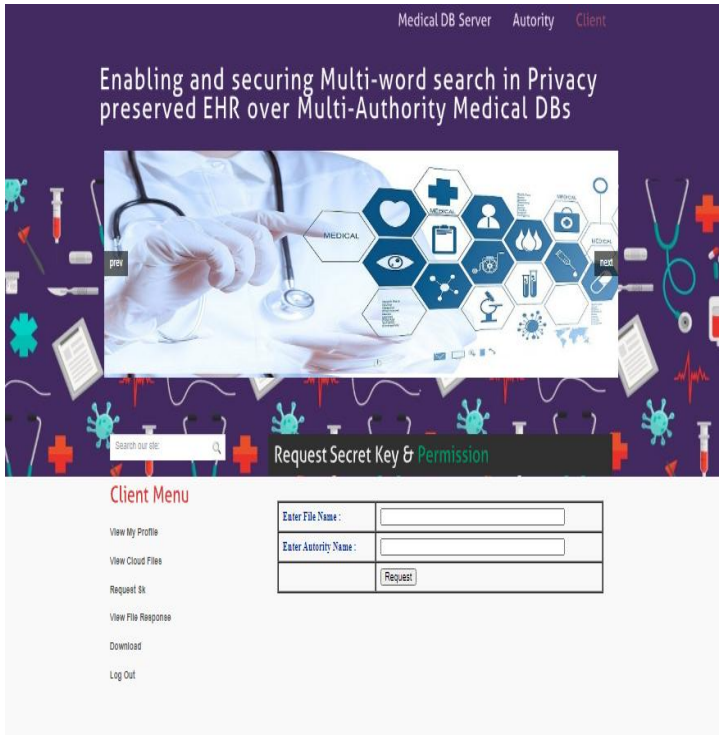
View medical database files page:

On this page, all medical files that got uploaded are visualized within an associated authority name.



Secret key page and permission page:

To fetch the file from DB, file name and authority name are entered to raise a request for it.

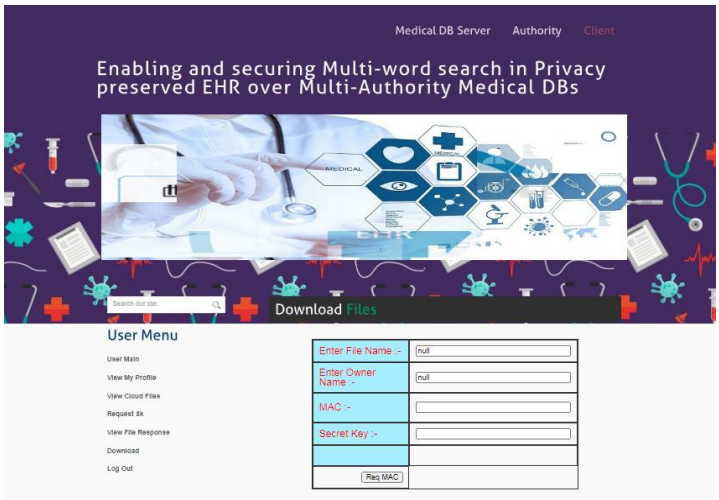


Request status page:

All the requests that got raised towards a specific file related to an associated are been listed with dates and security keys.

File download page:

The user has a right to download a specific file if he had a filename, enter the owner name, MAC KEY, and secret key, which could be driven from this page.



VI 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 mechanisms are been effectively driven. Sensitive data access policies over-optimized and liberalized achieving trustability and reliability over both data owners and data users are 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 to bring reliability and usability in wider boundaries. Thus we facilitated 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 on improvising security strategies by adopting optimal encryption methodologies that might bring overhead and are barricades to search techniques of encrypted data formats is achieved successfully.

REFERENCES

[1] J. Liu, X. Huang, and J. K. Liu, “Secure sharing of personal health records in cloud computing: Ciphertext-policy attributebased signcryption,” Future Generation Comput. Syst., vol. 52, pp. 67–76, 2015.

[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.

[3] Y. Zhang, J. Katz, and C. Papamanthou, “All your queries are belong to us: The power of file-injection attacks on searchable encryption,” in Proc. of 25th USENIX Secur. Symp., 2016, pp. 707– 720.

[4] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, “Private information retrieval,” in Proc. of 36th Annu. Symp. on Foundations of Comput. Sci., 1995, pp. 41–50.

[5] X. Yuan, X. Wang, C. Wang, C. Qian, and J. Lin, “Building an encrypted, distributed, and searchable key-value store,” in Proc. of the 11th ACM on Asia Conf. on Comput. and Commun. Security, 2016, pp. 547–558.

[6] S. Lai, S. Patranabis, A. Sakzad, J. K. Liu, D. Mukhopadhyay, R. Steinfeld, S.-F. Sun, D. Liu, and C. Zuo, “Result pattern hiding searchable encryption for conjunctive queries,” in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 745–762.

[7] S.-F. Sun, X. Yuan, J. K. Liu, R. Steinfeld, A. Sakzad, V. Vo, and S. Nepal, “Practical backward-secure searchable encryption from symmetric puncturable encryption,” in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 763–780.

[8] L. Xu, X. Yuan, C. Wang, Q. Wang, and C. Xu, “Hardening database padding for searchable encryption,”

in Proc. of the 2019 Conf. on Int. Conf. on Comput. Commun. IEEE, 2018.

[9] S. K. Kermanshahi, J. K. Liu, and R. Steinfeld, "Multi-user cloudbased secure keyword search," in Proc. of 22nd Aus. Conf. on Inf. Secur. and Privacy, 2017, pp. 227–247.

[10] X. Yang, T. Lee, J. K. Liu, and X. Huang, "Trust enhancement over range search for encrypted data," in Proc. of 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 66–73.