|| Volume 5 || Issue 11 || November 2020 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

SCALABLE AND SECURE DATA SHARING OF SENSITIVE INFORMATION PRESERVATION WITH EFFECTIVE SEARCH MECHANISM

Syed Asghar Hussain[1], Dr Shaik khaleel Ahamed[2]

Research Scholar, Dept. of Computer Science & Engineering, LIET, Hyderabad[1]
Associate Professor, Dept. of Computer Science & Engineering, LIET, Hyderabad[2]
syedasgharhussain123@gmail.com[1]
khaleelska@gmail.com[2]

--- ***---

Abstract:- In the cloud computing domain, remote data users need to get facilitated with committed data integrity policies where the data gets stored in the Cloud Servers. In the present-day cloud computing data service utilization of identical and entrepreneur enormous computational power and scalability over data storage facilities that encourage big data utility applications to empower domains like insurance, public Health Care, and Research and Development areas needs to focus on Security attributes. When the system is handling private sensitive information in public domain data Hiding strategies has to get effectively driven to increase the reliability and trustability of the system. 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 conventional systems, data retrieval of data stored in public clouds could be handled with the same formatted data. The keyword-based searching mechanism couldn't be effectively driven if data users don't follow the same formatted data that is been stored in the data store off the cloud. To the present circumstances wherein data needs to get encrypted and preserved in the data store of the database as well data, users could be in a situation to search the data with the daily utility formats irrespective of the format stored in the data store. In this project, we recommend a keyword top-k searching mechanism engage in encrypted data formats effectively and efficiently inter not violating the security policies. This index-based structural keyword search can be effectively performed over encrypted data formats only when searching keywords and data storage format should come to oneness in the runtime without losing the security precautions taken over the data. In the proposed secure keyword search mechanism with the tree indexing, facilitate a significant and defective system in such a way we can emphasize preventing the privacy breaches, data scalability, and time effectiveness in search query keyword processing could be achieved.

Keywords:- *Cloud storage; Data integrity auditing; Data sharing; Sensitive information hiding*

--***--

I INTRODUCTION

Cloud computing is having a massive demand to fulfill the present day necessities which is been incorporated with identical benefits like high flexibility and pay as you utilize manner facilitating data users to invest in procuring computational resources as users services based on situation null Expectations so that the data uses don't worry about out misusing of computational facilities and typical hardware platform architectural facilities[1][3]. 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[4] as well as effective query processing is on demand[2][6]. When we are dealing with user sensitive data we may need to carefully e and has the privacy policies[5] 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[9] 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[8]. 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[7]. 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[10]. 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.

When we try to adopt this kind of typical encryption strategy to bring privacy as a primary e element we may face and overload or computational overhead in the process of multi-keyword search. To deal with this trouble we adopt tree indexing over multiple keywords under search using Top-k priority search and effectively filter the appropriate data. When we implement the above-said process effectively and efficiently data owners are widely kept in a trustable platform. To bring this into practice several schemes for methodologies carbon in which situated in such that the whole search process of encrypted data is been effectively driven in such that the user is privileged to utilize it with the multi-keyword boolean search strategy. In the conventional methods, users are facilitated with a single key such process mechanism which is not well suited in practically addressing the present-day ongoing cloud paradigms. In these conventional single key schemes are not providing an efficient search mechanism and lacks in data security factors.

In the present day, big-data data utilities demand flexible, effective, and efficient challenges towards the sensitive data stored needs to get addressed. That we adopt an attribute index-based multi-keyword searchable encryption scheme with an implicit ranking facility to optimize the time taken to access the desired resource from the cloud servers. Hindi recommended system we should also think effectively implement random Travels scheme in such that cloud data access control can comfortably it travels on the index and reflects a variety of results with the very same multi-keyword query. Show the data owner of the cloud should be facilitated with and has search capabilities not violating or compromising on security and accuracy.

By adopting this multi keywords scalable search scheme data on ASA protected with hai data privacy policies and divide scalability over a huge volume of data sets. In public clouds analysis over data retrievals along with security, parameter pushes data into Cloud Servers in an encrypted format with an encrypted index-based methodology which reduces access time significantly. Securing the sensitive data of the cloud server by converting user compatible formats into secure formats using ciphertext-policy greatly avoids malicious user attack over sensitive data significantly.

II LITERATURE SURVEY

SecSVA: **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

Public key encryption with a keyword search: by D Boneh

When we emphasize the demanding circumstances of cloud computing especially in that data as a service utility it is required to maintain the data owner resource securely and facilitate flexible data access strategies to meet the data user expectations more effectively and efficiently. More or less when data security e parameter comes in front of us in a cloud computing environment we should adopt a typically high standard encryption policy at the data owners end to protect data integrity in cloud platforms. To address the above-said scenario by extracting the facts from recent research works power data security paradigm we ought to move on to public-key encryption of the facilitated data. This typical scenario that got adopted over share data makes a barrier in filtering the share data using a keyword search mechanism which could be handled by adopting proper index mapping technique.

Ensuring security and privacy preservation: ACM Computing Surveys

When we focus on the present-day emerging demands power facilities of cloud computing whether an independent or corporate utilization of shareable privileged data in Cloud Service suffers from a lack of security e standards. Data of data users that is been kept for service into the data service of public cloud must meet high security and reduce risk factors over privacy preservation on how to search for data. To meet the above said expectations advancements and sufficient research is to be done to emphasize privacy protection strategies that deal with the current security threats and facilitates reliable data service capability with a high-level focus. At the bottom line, recommendations are framed on challenges on an open basis and significant research parts in every significant area. These enhancements are being driven from the present-day research that in that is been done on untrusted data access scenarios to facilitate high-level privacy protection over shared data.

III SYSTEM ANALYSIS

Existing system:

When a data user prepares to outsource sensitive data on public cloud data access it is recommended to encrypt data before uploading into the cloud server to obtain data confidentiality and protect the integrity of data users in cloud environments. Along with that data uses should get privileged with searchable strategies power encrypted shareable cloud data that is searchable encryption to address variety threat models and meet typical search functionalities with single key similarity search. Remote data that got stored in the cloud server contributed by data owner needs to get facilitated with some dynamic ok operations like data inserting and removal activities.

Disadvantages of the existing system:

- ➢ Factors involved in data utilization needs high operational costs can operate on keyword based data retrieval process because the plain data contributed by data owner couldn't be stored exactly as it is into the data server and needs to get cipher-text converted to meet requirements of high-security standards.
- ➢ In the above-said process, there are some technical non-feasibility issues like huge computational stress to the cloud server that reflects onto the data user when he attempted to access the resource.

Proposed system:

A fully secure keyword-based tree search scheme is being adopted over shareable data of data owner which is been driven with keyword index ranked similarity search over searchable operations of cloud server data. Train text mapping and keyword ranking process for effective query handling are to be systematically driven by the administrative policies of cloud Service Provider to get public cloud server end. So this index-based structural keyboard search is been effectively performed on towards encrypted data format only when searching keywords and data storage format should come to Oneness in the runtime without losing the security precautions taken over the data.

Advantages of the proposed system:

- ➢ We emphasize preventing privacy breaches, data scalability, and time effectiveness over search query keyword processing is been achieved.
- ➢ Modularizing the whole data into subsets and performing encryption over the data outsourced by the data owner empowers the reliability and trustability of data Services.

IV IMPLEMENTATION

Modules:

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

1. Personal Health Owners Module:
2. Public Attribute Authority
3. Emergency
4. Data encryption

1. Personal Health Owners Module:

This is the Personal Health Owners module Login Authentication process verified through which Personal Health Owner can able to use his services by entering their credentials like ID and password as well there is an option to make a new registration to create a new user account. 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. After entering appropriate Personal Health Owner credentials in Personal Health Owners login page control will get navigated to Personal Health Owners home service that facilities like Entry personal health records and Maintain personal health records are been provided for the Personal Health Owners

2. Public Attribute Authority Module:

This is Attribute Authority Login Module Authentication process verified in which Attribute Authority can be able to perform his administrative operations by entering their credentials like ID and password. If the entered credentials are not correct it will be access rejected. If the Attribute Authority enters the right credentials will get migrated to the Attribute Authority home service area successfully and can utilize specified services provided by the server. After entering appropriate Public Attribute Authority credentials in Personal Public Attribute Authority login control will get navigated to Public Attribute Authority home service that facilities like Health Records Details, Personal Health Records Owners Details, Emergency clients are been provided for the Public Attribute Authority.

3. Emergency

In the emergency module, users are privileged with some glass breaking services that are directly requesting for a secret key and searching for a specified file carbon facilitated effectively.

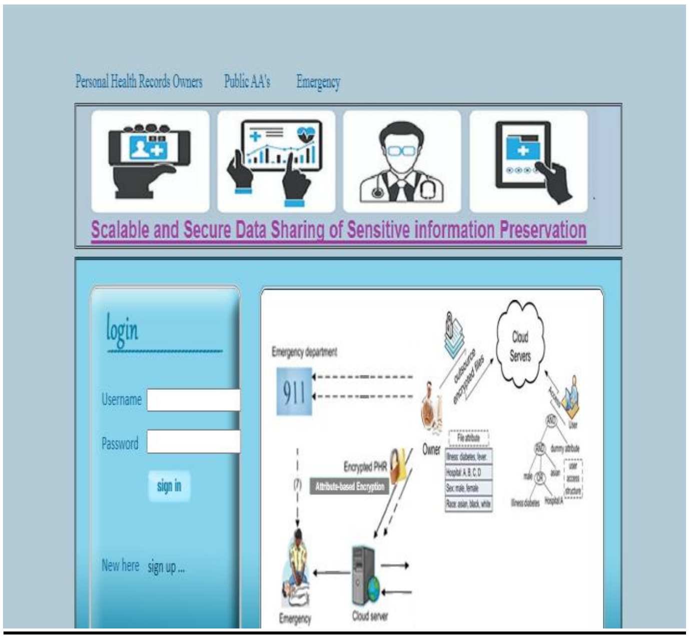
4. Data encryption:

Data that got uploaded by the data owner into the remote server needs to maintain data integrity and high-security standards to obtain reliability and a Long committed walk with the service provider.

V PROJECT EXECUTION AND TESTING

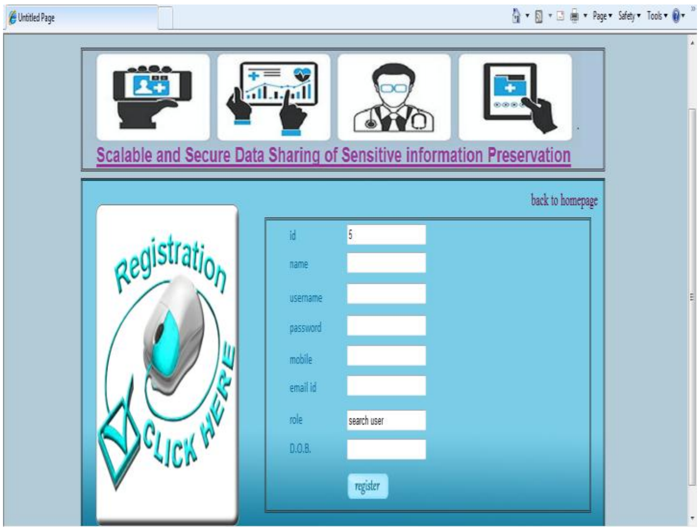
Welcome screen:

This is a welcome page of the project that is Scalable and Secure Data Sharing of Sensitive information Preservation with an Effective Similarity Search Mechanism.



Registration page :

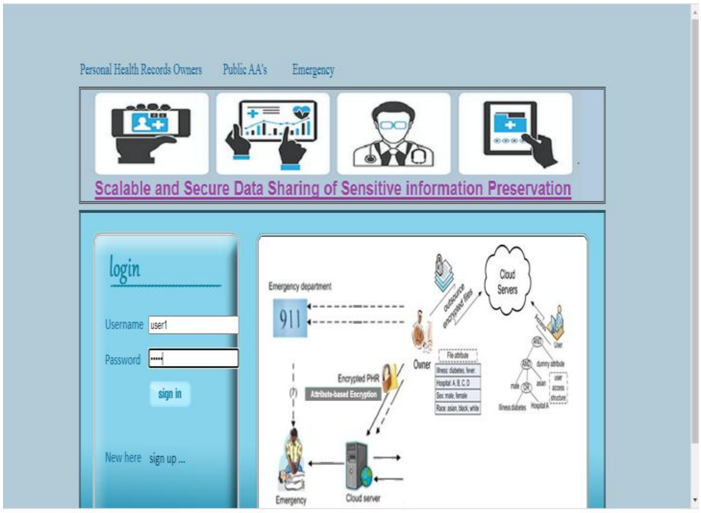
Using this registration page the person could be able to create his cloud user registration with his personal information which could be reused in logging into his account it with the credentials entered on this page. This is the page where all users have to use to create the account in the database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



id: 5
role: search user

User Login page :

This is a user login page through which a user 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.

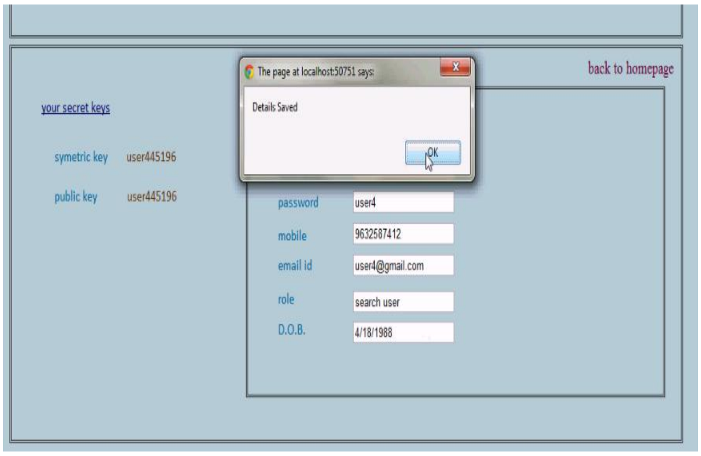

Personal Health Records Owners
Public AA's
Emergency
Scalable and Secure Data Sharing of Sensitive information Preservation
login
sign in
New here
sign up ...
Emergency department
911
Cloud Servers
outsource encrypted files
Owner
Encrypted PHR
Attribute-based Encryption
File attribute
Emergency
Cloud server
User

Username user1

Password •••••

Symmetry key generation page:

In this Symmetry key generation page, the user attempts to register an account with his personal information to fulfill the security policies a symmetric key and public key are generated which are associated with user account information



The page at localhost:50751 says:

Details Saved

symetric key user445196

public key user445196

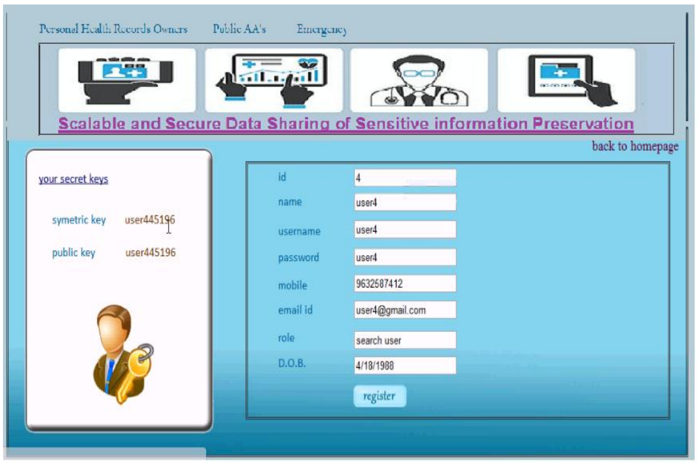
password user4

mobile 9632587412

email id user4@gmail.com

role search user

D.O.B. 4/18/1988


Personal Health Records Owners
Public AA's
Emergency
Scalable and Secure Data Sharing of Sensitive information Preservation
back to homepage
your secret keys
register

symetric key user445196

public key user445196

id 4

name user4

username user4

password user4

mobile 9632587412

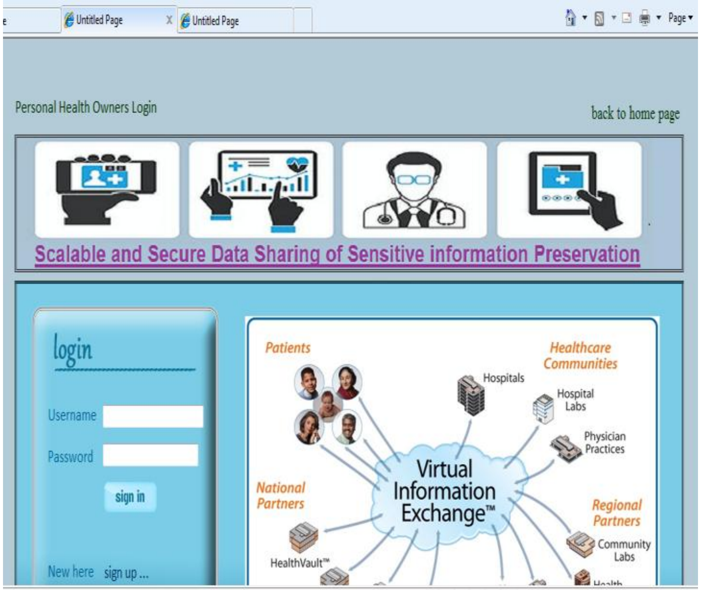
email id user4@gmail.com

role search user

D.O.B. 4/18/1988

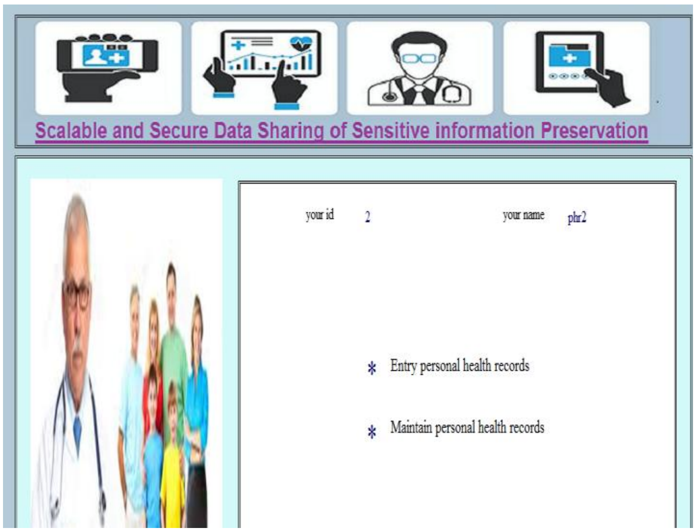
Personal Health Owners Login page:

This is Personal Health Owners login page through which Personal Health Owner can able to use his services by entering their credentials like 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.



Personal Health Owners home page:

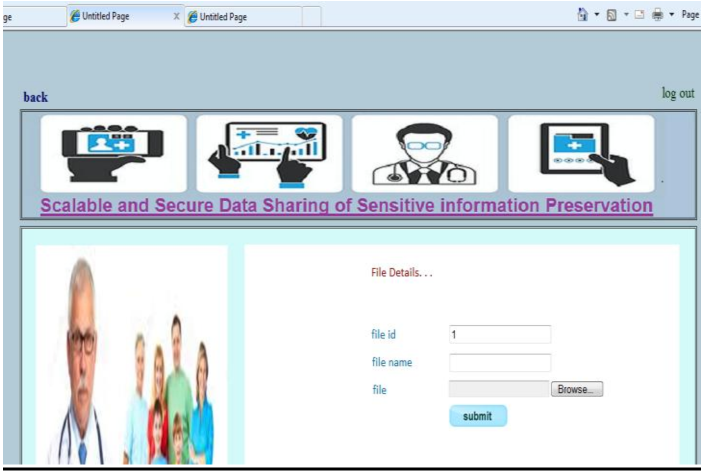
After entering appropriate Personal Health Owner credentials in Personal Health Owners login page control will get navigated to this page. In this Personal Health Owners homepage facilities like Entry personal health records and Maintain personal health records are been provided for the Personal Health Owners


Scalable and Secure Data Sharing of Sensitive information Preservation
Entry personal health records
Maintain personal health records

your id 2

your name phr2

Entry personal health records Page:


Untitled Page
Untitled Page
back
log out
Scalable and Secure Data Sharing of Sensitive information Preservation
Browse...
submit

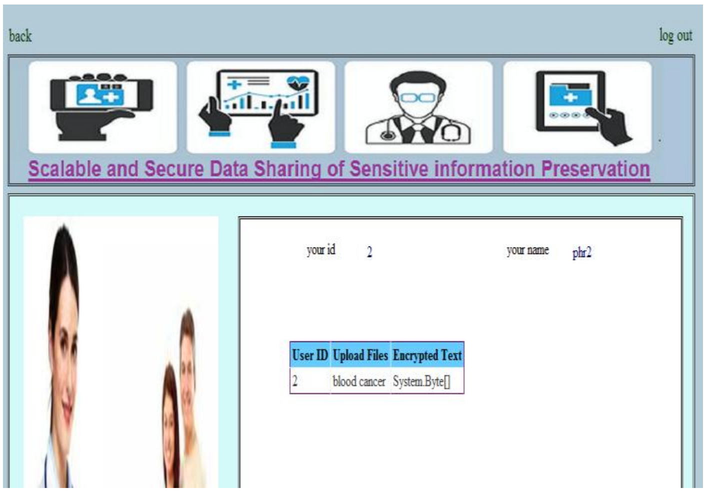
File Details. . .

file id 1

file name

file

Maintain personal health records page:

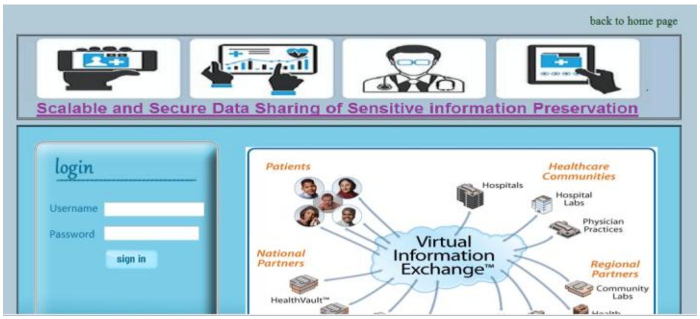

back
log out
Scalable and Secure Data Sharing of Sensitive information Preservation

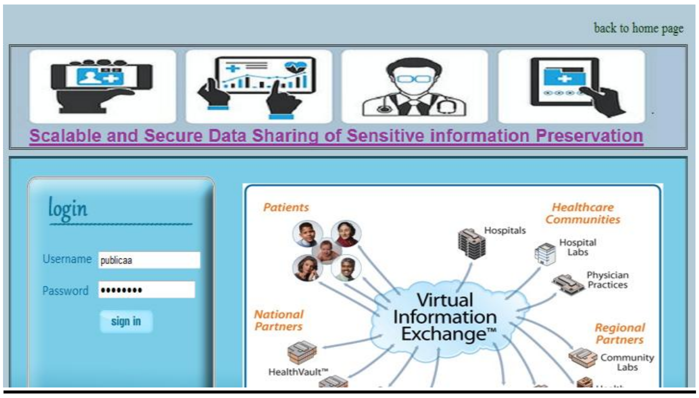
your id 2 your name phr2

User ID	Upload Files	Encrypted Text
2	blood cancer	System.Byte[]

Public Attribute Authority Login Page:

This is Attribute Authority Login page through which Attribute Authority can able to use his administrative facilities by entering their credentials like ID and password. 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 Attribute Authority home page successfully and can utilize specified services provided by the server.



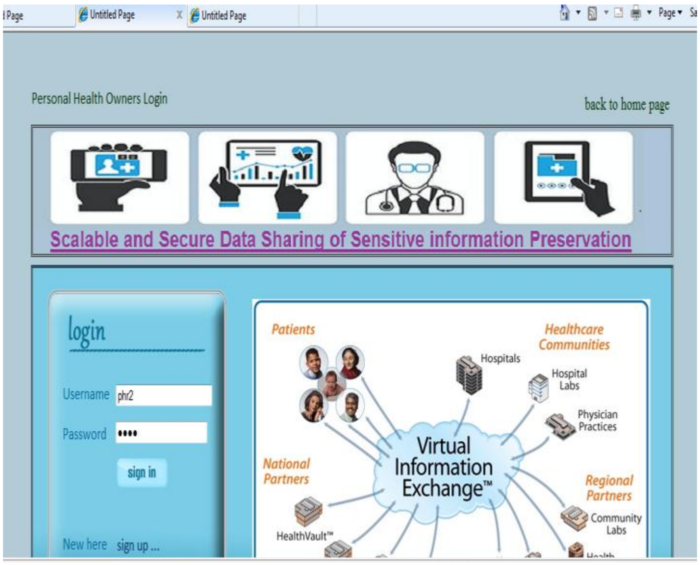


Username publicaa

Password ••••••••

Public Attribute Authority home page:

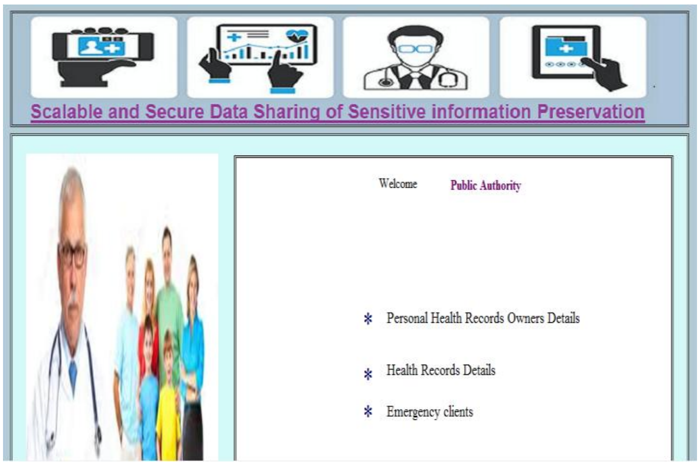
After entering appropriate Public Attribute Authority credentials in Personal Public Attribute Authority login page control will get navigated to this page. In this Public Attribute Authority homepage facilities like Health Records Details, Personal Health Records Owners Details, Emergency clients are been provided for the Public Attribute Authority.



Personal Health Owners Login

Username phr2

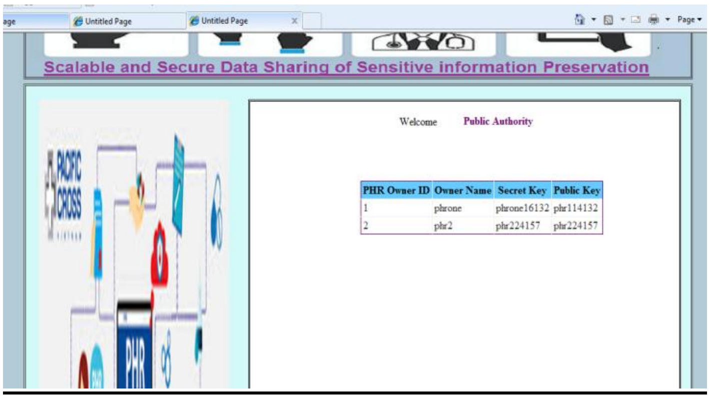
Password ••••


Scalable and Secure Data Sharing of Sensitive information Preservation

Welcome Public Authority

- Personal Health Records Owners Details
- Health Records Details
- Emergency clients

Health Records Details Page:

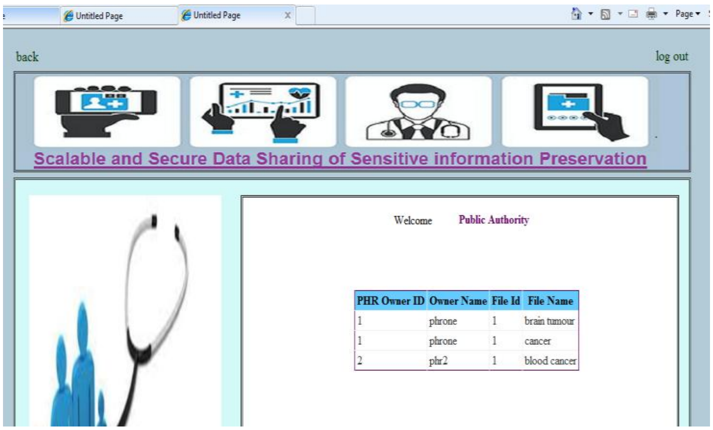


Scalable and Secure Data Sharing of Sensitive information Preservation

Welcome Public Authority

PHR Owner ID	Owner Name	Secret Key	Public Key
1	phrone	phrone16132	phr114132
2	phr2	phr224157	phr224157

Personal Health Records Owners Details Page:_



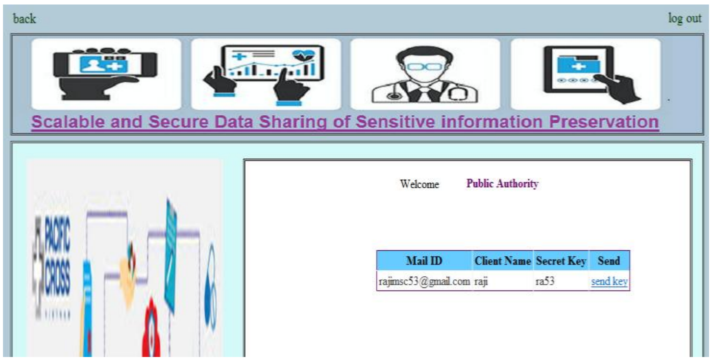
back log out

Scalable and Secure Data Sharing of Sensitive information Preservation

Welcome Public Authority

PHR Owner ID	Owner Name	File Id	File Name
1	phrone	1	brain tumour
1	phrone	1	cancer
2	phr2	1	blood cancer

Emergency clients :



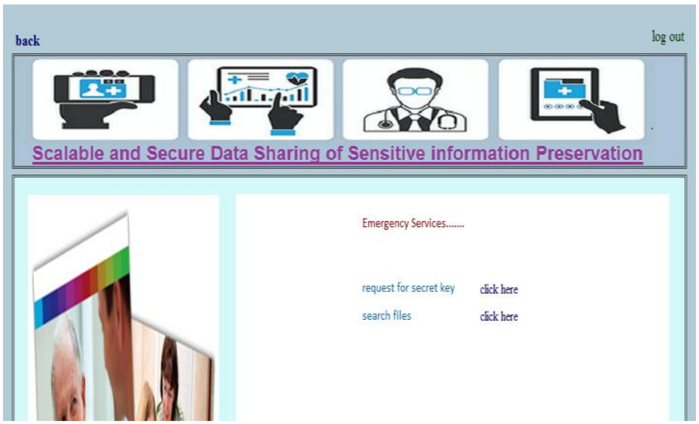
back log out

Scalable and Secure Data Sharing of Sensitive information Preservation

Welcome Public Authority

Mail ID	Client Name	Secret Key	Send
rajimsc53@gmail.com	raji	ra53	send key

Emergency Page:



back log out

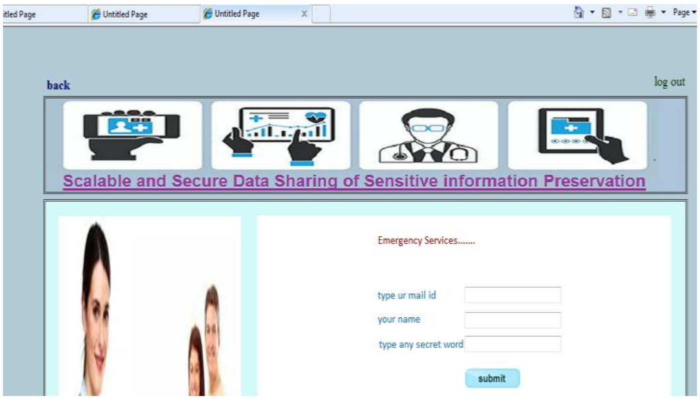
Scalable and Secure Data Sharing of Sensitive information Preservation

Emergency Services.......

request for secret key click here

search files click here

Request for Secret Key Page:



back log out

Scalable and Secure Data Sharing of Sensitive information Preservation

Emergency Services.......

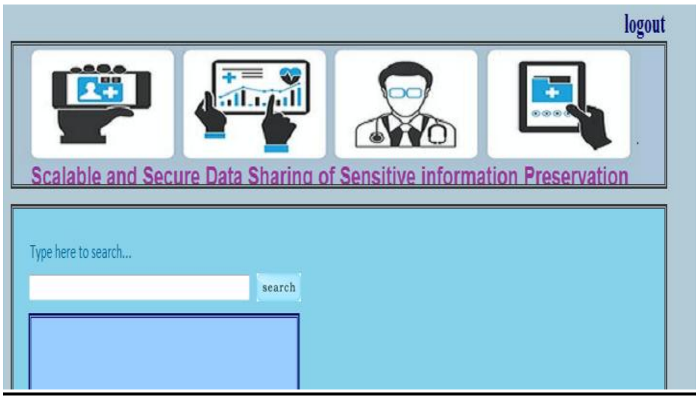
type ur mail id

your name

type any secret word

submit

Search Files Page :



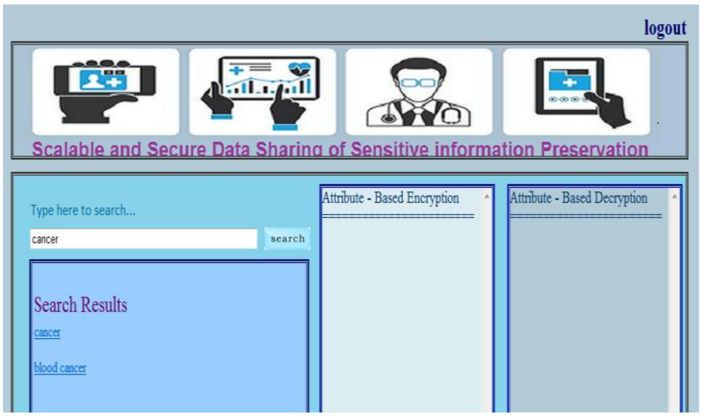
logout

Scalable and Secure Data Sharing of Sensitive information Preservation

Type here to search...

search

Encryption and Decryption Key Visualization:



logout

Scalable and Secure Data Sharing of Sensitive information Preservation

Type here to search...

cancer

search

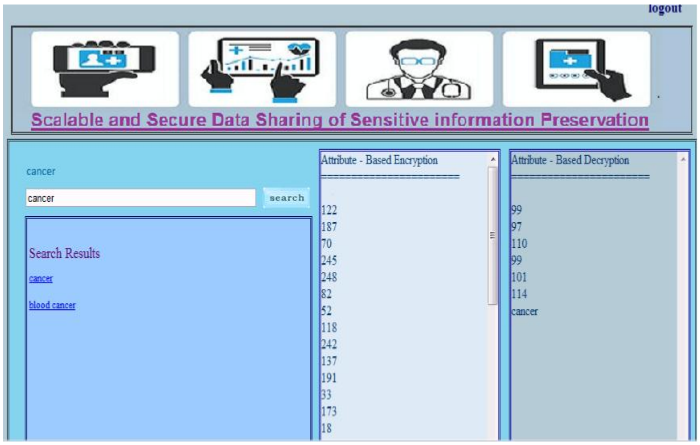
Search Results

cancer

blood cancer

Attribute - Based Encryption
========================

Attribute - Based Decryption
========================



logout

Scalable and Secure Data Sharing of Sensitive information Preservation

cancer

cancer

search

Search Results

cancer

blood cancer

Attribute - Based Encryption
========================

122
187
70
245
248
82
52
118
242
137
191
33
173
18

Attribute - Based Decryption
========================

99
97
110
99
101
114
cancer

VI CONCLUSION

In this paper, we focus on improving the efficiency and the security over data storage facilities to encourage big data utility applications in such that service utilization of identical and entrepreneur enormous computational power and scalability got improvised greatly. Demerit in conventional systems i.e data retrieval of data stored in public clouds could be handled with the same formatted data. The keyword-based searching mechanism couldn't be e effectively driven if data uses doesn't follow the same formatted data that is been stored in the data store of the cloud got overcome by the below said approach. Data needs to get encrypted and preserved in the data store of the database as well as data users could be in a situation to search the data with the daily utility formats irrespective of the format stored in the data store. In this project, we implemented a keyword searching mechanism to engage in encrypted data formats effectively and efficiently inter not violating the security policies. When the system we attempt in handling private sensitive information in public domain data Hiding strategies has to get effectively driven to increase the reliability and trustability of the system. This index-based structural keyword search can be effectively performed over encrypted data formats only when searching keywords and data storage format should come to oneness in the runtime without losing the security precautions taken over the data is done. To enhance the security policies, we move ahead by modularizing the whole data into sub-parts and perform encryption then stored so that when data user attempt to retrieve the very Same data could be done in a segment based manner so that reliability and trustability of the Stored data got achieved.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2007, pp. 598–609.

[3] A. Juels and B. S. Kaliski, “Pors: Proofs of retrievability for large files,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser.CCS ’07, 2007, pp. 584–597.

[4] H. Shacham and B. Waters, “Compact proofs of retrievability,” J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul. 2013.

[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou,“Privacy-preserving public auditing for secure cloud storage,” IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[6] S. G. Worku, C. Xu, J. Zhao, and X. He, “Secure and efficient privacy-preserving public auditing scheme for cloud storage,” Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, Jul. 2014.

[7] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, “Symmetric-key based proofs of retrievability supporting public verification,” in Computer Security – ESORICS 2015. Cham: Springer International Publishing, 2015, pp. 203–223.

[8] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao,“Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,” Journal of Network and Computer Applications, vol. 82,pp. 56–64, 2017.

[9] J. Sun and Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” IEEE Transactions on Parallel and Distributed Systems, vol.21, no. 6, pp. 754–764, June 2010.

[10] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2008, pp. 1–10.