IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 1, June 2022

Security Requirements for Electronic Health Record (EHR) Sharing in Public Clouds

Umamageshwari R[1], Reni Hena Helan R[2], Harini N[3], Lakshmi V[4], Mahalakshmi K[5]

Assistant Professor, Department of Computer Science and Engineering[1,2]
Students, Department of Computer Science and Engineering[3,4,5]
Dhanalakshmi College of Engineering, Chennai, India

Abstract: *Hospital health care supplier is also moving from paper records to electronic health records (EHRs) or may be mistreatment EHRs already. EHRs permit suppliers to use info additional effectively to boost the standard and potency of your care, however EHRs won't amendment the privacy protections or security safeguards that apply to your health information. Our project focuses on developing secure cloud framework for evolving and accessing trustworthy computing services all told levels of public cloud readying model. Thus, eliminates each internal and external security threats. These leads to achieving knowledge confidentiality, data integrity, authentication and authorization, eliminating both active and passive attacks from cloud network environment. To develop a secure cloud framework for accessing trustworthy computing and storage services all told levels of public cloud readying model.*

Keywords: EHR, Privacy Protection, Secure cloud Framework, Security Threads, Trusted computing, Storage services, public cloud, private cloud.

I. INTRODUCTION

With the explosive growth of information, it's an important burden for users to store the sheer quantity of data locally. Therefore, a lot of and more organizations and people would really like to store their data within the cloud. However, the information keep in the cloud could be corrupted or lost because of the inevitable package bugs, hardware faults and human errors in the cloud. so as to verify whether or not the data is stored properly in the cloud, several remote data integrity auditing schemes are proposed. In remote data integrity auditing schemes, the information owner foremost must generate signatures for data blocks before uploading them to the cloud. These signatures are accustomed prove the cloud really possesses these data blocks within the part of integrity auditing. So the data owner uploads these data blocks beside their corresponding signatures to the cloud. The information hold on in the cloud is commonly shared across multiple users in several cloud storage applications, adore Google Drive, Dropbox and iCloud.

Data sharing jointly of the foremost common options in cloud storage, permits variety of users to share their information with others. However, these shared data hold on within the cloud may contain some sensitive info. For instance, the Electronic Health Records stored and shared in the cloud sometimes contain patients' sensitive information (patient's name, signaling and ID number, etc.) and also the hospital's sensitive information (hospital's name, etc.). If these EHRs are directly uploaded to the cloud to be shared for analysis purposes, the sensitive info of patient and hospital are going to be inevitably exposed to the cloud and also the researchers.

Besides, the integrity of the EHRs must be secured thanks to the existence of human errors and software/hardware failures within the cloud. Therefore, it's vital to accomplish remote data integrity auditing on the condition that the sensitive info of shared data is protected. a possible technique of finding this downside is to cipher the full shared file before causation it to the cloud, then generate the signatures accustomed verify the integrity of this encrypted file, finally transfer this encrypted file and its corresponding signatures to the cloud. This method will notice the sensitive information activity since solely the info owner can decipher this file.

However, it'll build the entire shared file unable to be utilized by others. For example, encrypting the EHRs of communicable disease patients will defend the privacy of patient and hospital, however these encrypted EHRs can not be effectively utilized by researchers any more. Distributing the coding key to the researchers appears to be a doable answer to the higher than problem. However, it's unfeasible to adopt this methodology in real eventualities because of the subsequent reasons. Firstly, distributing decryption key desires secure channels, that is tough to be happy in some

DOI: 10.48175/IJARSCT-4618

instances. Furthermore, it appears very troublesome for a user to grasp that researchers can use his/her EHRs within the close to future once he/she uploads the EHRs to the cloud. As a result, it's impractical to cover sensitive info by encrypting the total shared file. Thus, a way to understand knowledge sharing with sensitive information concealing in remote data integrity auditing is incredibly vital and valuable. Unfortunately, this downside has remained unknown in previous researches.

II. LITERATURE REVIEW

Securely Outsourcing Attribute-Based Encryption with Checkability.

Attribute-Based encoding (ABE) could be a promising cryptologic methodology that greatly will increase the range of access management measures. because of the intensive quality of ABE laws, the procedure issues of ABE key supply and decoding are getting too big. though existing Outsourced ABE systems will offload some expensive computing tasks to a 3rd party, the verifiability of the third-party outputs has however to be addressed. We have a tendency to propose an distinctive Safe Outsourced ABE system to handle the issue, that allows for secure outsourced key issuance and decryption. In our innovative solution, all access policy and attribute connected actions within the key-issuing or decryption processes are offloaded to a Key Generation Service supplier (KGSP) and a decoding Service supplier (DSP), exploit solely the encoding process.

Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records.

We have discovered the mission of conserving patient privacy in digital document structures for fitness. we have a tendency to argue that security in such structures ought to be implemented through coding additionally to getting the proper of access to control. Additionally, we advocate techniques that enable users to get and buy encryption keys, so compromising user privacy with the want for host knowledge to be compromised. The well-known argument for such a procedure is that encryption might have an effect on the capability of the machine. However, we show that we are able to build a inexperienced machine that enables patients to access the rights of others and search their records in partial proportion. We formalize the wants of a patient-driven coding theme and supply varied instances, largely primarily based entirely on current scientific discipline primitives and protocols, every achieving a novel set of properties.

Cross-Domain Data Sharing in Distributed Electronic Health Record Systems

Cross-employer or cross-area cooperation takes house usually in Electronic Health Record (EHR) device for essential and super affected person treatment. Cautious layout of delegation mechanism got to be in area as a constructing block of cross-area cooperation, as a results of the cooperation inescapably entails dynamical and sharing applicable affected person knowledge which can be taken into thought tremendously personal and confidential. The delegation mechanism presents permission to and restricts get entry to rights of a cooperating partner. Patients are unwilling to simply accept the EHR device except their fitness info are assured right use and disclosure, that can't be simply dead while not cross-area authentication and fine-grained get entry to manage. In addition, revocation of the delegated rights got to be viable at any time at some purpose of the cooperation. throughout this paper, we have a tendency to tend to advocate a stable EHR device, whole} completely on field constructions, to allow stable sharing of touchy affected person knowledge at some purpose of cooperation and hold affected person info privacy. Our EHR device equally consists of superior mechanisms for fine-grained get entry to manage, and on-call for revocation, as upgrades to the basic get entry to manage provided through the delegation mechanism, and therefore the basic revocation mechanism, respectively. The projected EHR device is established to satisfy targets precise to the cross-area delegation state of affairs of interest.

Privacy-Preserving Multi-Keyword Ranked Search Over Encrypted Cloud Data.

With the rise of cloud computing, statisticians are being enticed to their sophisticated data management systems from shut sites to the economical public cloud for larger flexibility and worth savings. excluding preserving information privacy, sensitive data got to be encrypted before being outsourced, that renders ancient data consumption totally obsessed on plaintext key-word retrieval. As a result, allowing Associate in Nursing encrypted cloud statistics get supplier is crucial. Given the large choice of statistics customers and files within the cloud, it' essential to allow multiple key words within the request, request and are available files in the order of their affiliation to those key phrases. connected studies

DOI: 10.48175/IJARSCT-4618

on searchable secret writing consciousness on single key-word search or man of science key-word search, and often kind the introduce low overhead on computation and communication.

Privacy-Preserving Cloud-Based Personal Health Record System Using Attribute-Based Encryption and Anonymous Multi-Receiver identity -Based Encryption.

The cloud-based entirely private fitness record (CB-PHR) system has huge promise for empowering patients and making certain more economical delivery of health care as a growing patient-centric style of fitness records exchange. we have a tendency to propose a unique CB-PHR gismo during this work. It allows PHR homeowners to firmly store their fitness knowledge at semi-reliant cloud service providers, further on by selection share their fitness data with a large vary of PHR purchasers. PHR clients are divided into 2 protection domain names: public space and personal area, to cut back the vital factor management complexity. PHR owners code their fitness data for public use employing a ciphertext-coverage attribute-based absolutely secret writing technique, whereas encrypting their fitness knowledge for personal usage using a ciphertext-coverage attribute-based altogether encryption scheme.

III. SYSTEM ARCHITECTURE

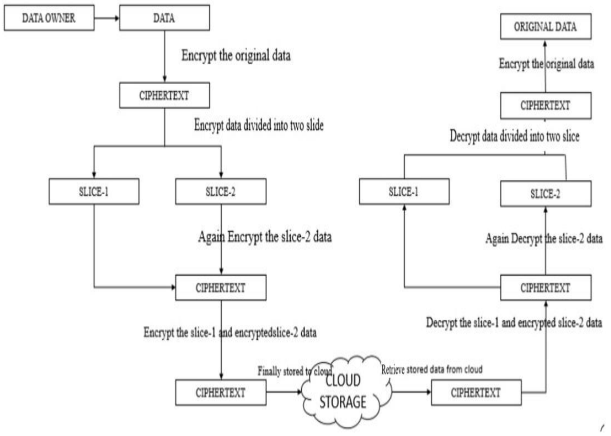

DATA OWNER
DATA
Encrypt the original data
CIPHERTEXT
Encrypt data divided into two slide
SLICE-1
SLICE-2
Again Encrypt the slice-2 data
CIPHERTEXT
Encrypt the slice-1 and encryptedslice-2 data
CIPHERTEXT
Finally stored to cloud
CLOUD STORAGE
Retrieve stored data from cloud
CIPHERTEXT
Decrypt the slice-1 and encrypted slice-2 data
CIPHERTEXT
Again Decrypt the slice-2 data
SLICE-1
SLICE-2
Decrypt data divided into two slice
CIPHERTEXT
Encrypt the original data
ORIGINAL DATA

Figure 1: Architecture diagram

Trust Store is one of the first stable cloud storage engines that offers Confidentiality, Integrity and Availability (CIA) for data stored in the cloud. The main features of the Trust Store can be summarized as follows: supports some great garage deals from cloud providers. Therefore, it is much more viable to augment redundant and hybrid digital document structures by using replication for excess data availability. It helps in key control as an unbiased provider that can be implemented in a (semi) dependent environment. It supports an unbiased integrity check provider that helps with both online and offline integrity check. Supports great APIs so many packages can be developed and deployed on great platforms. Trust store consists of three main tiers: a software tier, the trust store client, the server-side trust store offerings, and the cloud storage offerings. Below we describe each level and its core components and functionalities functionalities. It is important to note that within the procedure defined above, non-public keys cannot be recovered if the password is lost if they are considered encrypted when using the password. It can best be changed when the consumer knows the current password so that the non-public key can be decrypted first. The consumer can also select a document from the document list in the store to open it.

IV. SYSTEM IMPLEMENTATION

This paper shows the implementation of

- MODULE 1: Login
- MODULE 2: Registration
- MODULE 3: Creation Storage and Instance
- MODULE 4: Data Protection
- MODULE 5: Data Recovery Module

Module Description

1. Login Module

This is the primary pastime that opens while person open the internet site. User desires to offer a accurate touch range and a password, which person enters even as registering, if you want to login into the internet site. If records supplied via way of means of the person fits with the information withinside the database desk then person effectively login into the internet site else message of login failed is displayed and person want to reenter accurate records. A hyperlink to the signup pastime is likewise supplied for registration of recent users**.**

2. Registration Module

A new consumer wishing to access the website must first register before being able to log in. by clicking on the register button in the case of interest in logging in, the interest in registering opens. A new consumer registers by entering their full name, password and different phones. A consumer wants to re-enter the password in the password verification text box for confirmation. When the consumer enters the records in all of the text fields, pressing the record button transfers the information to the database and instructs the consumer to log in again. The registered consumer then wishes to log in to gain access to the website. Validations of all text fields are performed for the correct functioning of the website. Just like the logs in each text box, whether it's your name, touch, password, or password verification miles, this text box is now no longer blank while you log in. If this text box is empty, the application provides the required record message in each text box. the information in the fields Password and Password check must also be compared with a hit data record. Further validation is the need for a wide tactile array to be legitimate, this is 10 digits. If such validation is breached, registration may fail and the consumer may wish to register again. Message that the website displays when one of the topics is empty. If all of these records are correct, the consumer can be redirected to the login interest to login to the website.

3. Creation Storage and Instance

The record owner no longer has control over the records after their miles have been uploaded to the cloud. In this module, unique records are encrypted with specific values. Records in each bucket can be encrypted using specific cryptographic algorithms and encryption keys before being stored in the cloud.

4. Data Protection

In this module, the approach is to keep information in a right steady and secure way so as to keep away from intrusions and information assaults in the meantime it'll lessen the value and time to keep the encrypted information withinside the Cloud Storage.

5. Data Recovery Module

In this module, user can use unique techniques to get better data from cloud server.

V. ALGORITHM USED

SHA 1 Algorithm

Secure Hash algorithmic program one (SHA-1) could be a cryptological hash algorithm that generates a 160-bit (20-byte) hash price from associate degree input. A message digest is that the name given to the present hash value. This message digest is thus unremarkably diagrammatical as a 40-digit positional notation number.

Step 1: Append Padding Bits.

Message is “padded” with a one and as several 0’s as necessary to bring the message length to sixty four bits fewer than a fair multiple of 512.

Step 2: Append Length....

64 bits are appended to the top of the cushioned message. These bits hold the binary format of sixty four bits indicating the length of the first message.

DOI: 10.48175/IJARSCT-4618

Step 3: Prepare Processing Functions….

SHA1 requires 80 processing functions defined as:

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)

f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)

f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)

f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

Step 4: Prepare Processing Constants....

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999	(0 <= t <= 19)
K(t) = 0x6ED9EBA1	(20 <= t <= 39)
K(t) = 0x8F1BBCDC	(40 <= t <= 59)
K(t) = 0xCA62C1D6	(60 <= t <= 79)

Step 5: Initialize Buffers….

SHA1 requires 160 bits or 5 buffers of words (32 bits):

H0 = 0x67452301

H1 = 0xEFCDAB89

H2 = 0x98BADCFE

H3 = 0x10325476

H4 = 0xC3D2E1F0

Step 6: Processing Message in 512-bit blocks (L blocks in total message).

This is the most task of SHA1 algorithmic program that loops through the soft and appended message in 512-bit blocks.

Input and predefined function:

M[1, 2, ..., L]: Blocks of the padded and appended message f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 Processing Functions K(0), K(1), ..., K(79): 80 Processing Constant Words

H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values.

VI. RESULTS

OUTPUT FOR HOME PAGE

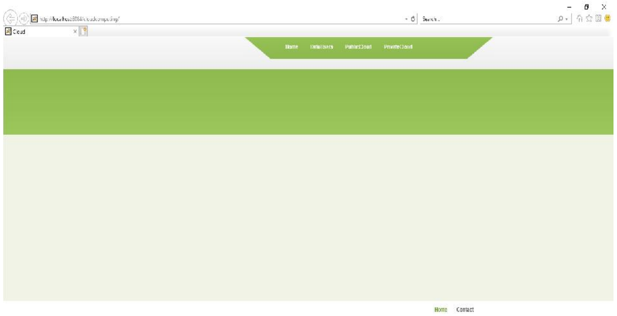
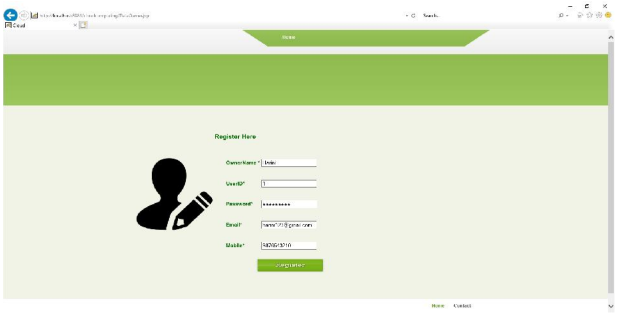


Figure 2. Output for Home page

DOI: 10.48175/IJARSCT-4618

OUTPUT FOR REGISTRATION PAGE

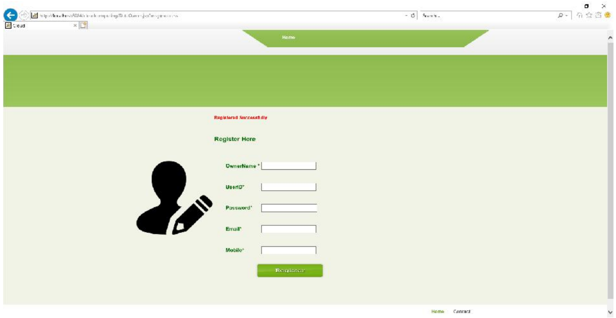


Register Here

OwnerName * Harini
UserID* 1
Password* ••••••••••
Email* harini123@gmail.com
Mobile* 9876543210
Register

Figure 3: Output for Registration page

OUTPUT AFTER SUCCESSFUL REGISTRATION



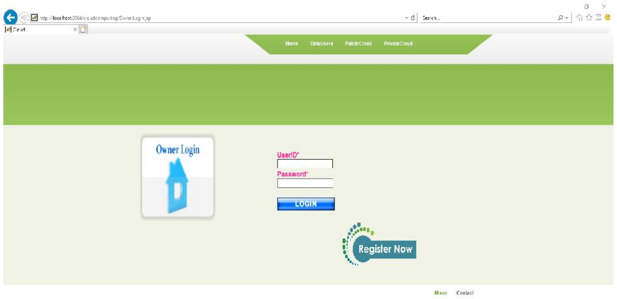
Registered Successfully

Register Here

OwnerName *
UserID*
Password*
Email*
Mobile*
Register

Figure 4: output for After Successful Registration

OUTPUT FOR LOGIN PAGE

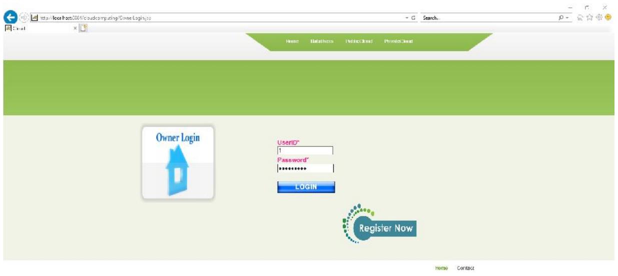


http://localhost:8084/cloudcomputing/OwnerLogin.jsp

UserID*
Password*

Figure 5: output for login page

OUTPUT FOR DETAILS ENTERED IN LOGIN PAGE



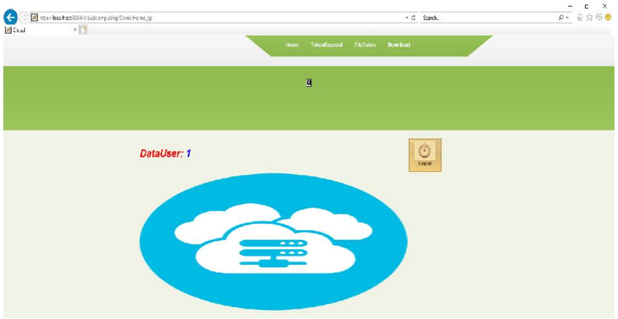
http://localhost:8084/cloudcomputing/OwnerLogin.jsp

UserID* 1
Password* ••••••••••

Figure 6: output for Details Entered in Login Page

DOI: 10.48175/IJARSCT-4618

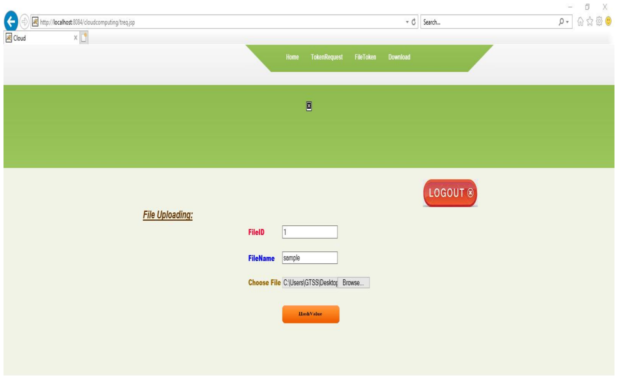
OUTPUT FOR DATA USER HOME PAGE



DataUser: 1

Figure 7: Output for Data User Home Page

OUTPUT FOR FILE UPLOAD PAGE



File Uploading:

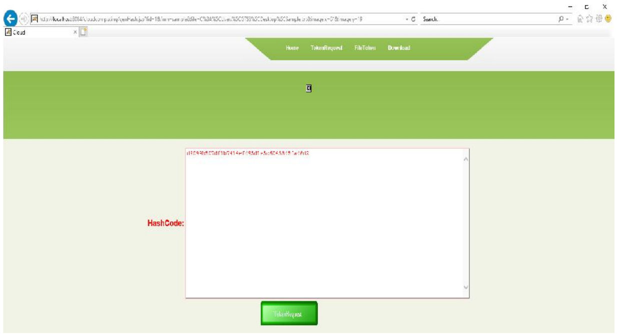
FileID 1

FileName sample

Choose File C:\Users\GTSS\Desktop

Figure 8: output for file upload page

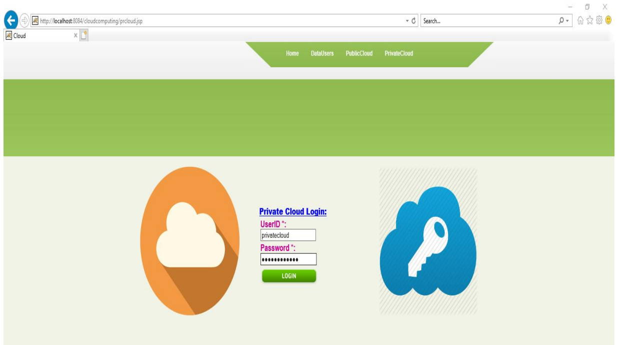
OUTPUT FOR TOKEN GENERATION PAGE



HashCode: [illegible]

Figure 9: Output for Token Generation Page

OUTPUT FOR PRIVATE CLOUD LOGIN PAGE



Private Cloud Login:

UserID *: privatecloud

Password *: ●●●●●●●●●●●●●

Figure 10: Output for Private cloud Login Page

OUTPUT FOR PRIVATE CLOUD HOME PAGE

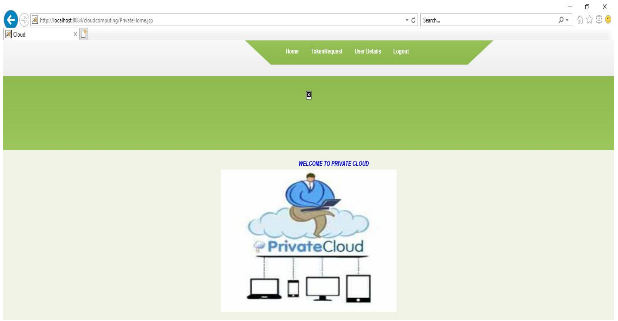
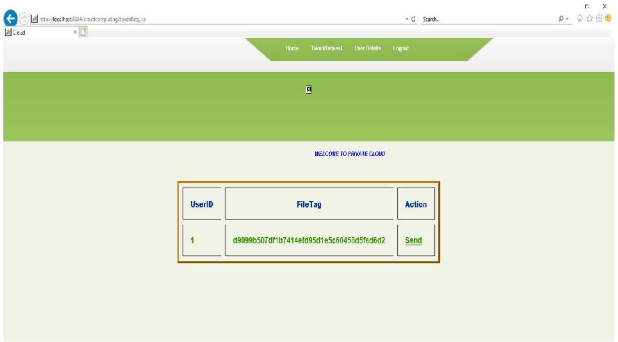


Figure 11: Output for Private cloud Home page

OUTPUT FOR BEFORE SEND TOKEN REQUEST PAGE

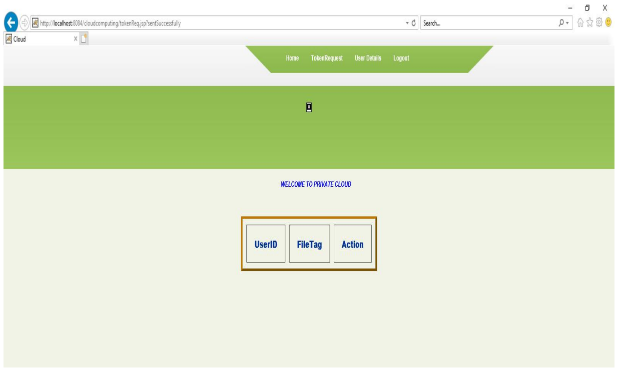


UserID	FileTag	Action
1	d9099b507df1b7414efd95d1e5c60458d5fad6d2	Send

Figure 12: Output for Before send Token request page

DOI: 10.48175/IJARSCT-4618

OUTPUT FOR AFTER SEND TOKEN REQUEST PAGE

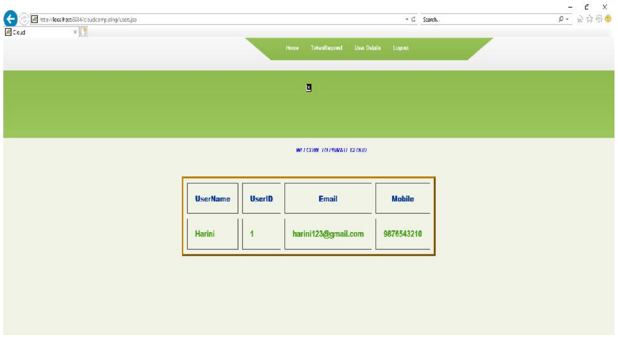

http://localhost:8084/cloudcomputing/tokenReq.jsp?sentSuccessfully
Search...
Cloud
Home
TokenRequest
User Details
Logout

WELCOME TO PRIVATE CLOUD

UserID	FileTag	Action

Figure 13: Output for After Send Token Request Page

OUTPUT FOR USER DETAIL PAGE

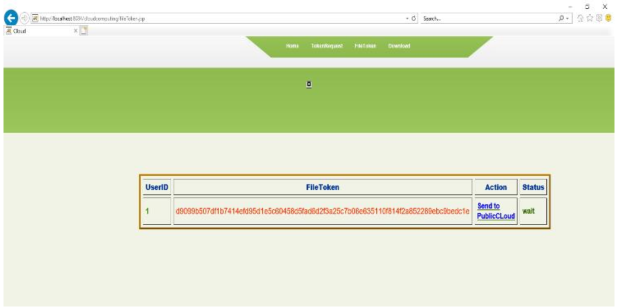


WELCOME TO PRIVATE CLOUD

UserName	UserID	Email	Mobile
Harini	1	harini123@gmail.com	9876543210

Figure 14: Output for User Detail Page

OUTPUT FOR FILE TOKEN PAGE

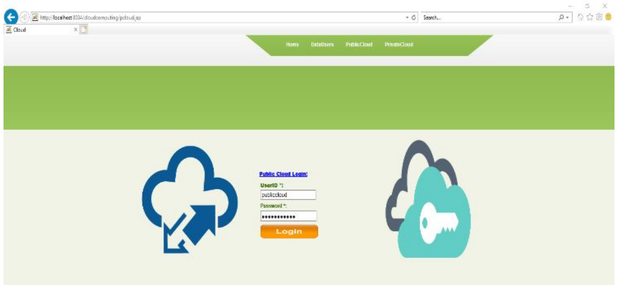


UserID	FileToken	Action	Status
1	d9099b507df1b7414efd95d1e5c80458d5fad8d2f3a25c7b08e635110f814f2a852289ebc9bedc1e	Send to PublicCLoud	wait

Figure 15: Output for File Token Page

DOI: 10.48175/IJARSCT-4618

OUTPUT FOR PUBLIC CLOUD LOGIN PAGE



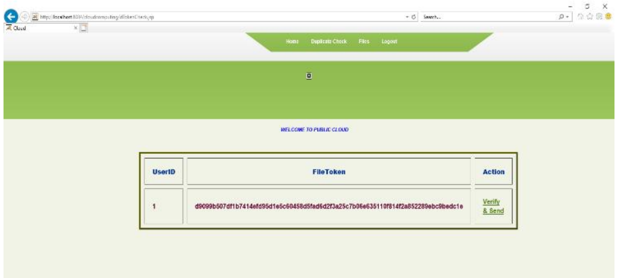
Public Cloud Login:

UserID *: publiccloud

Password *: ●●●●●●●●●●●●

Figure 16: Output for Public cloud Login Page

OUTPUT FOR FILE DUPLICATE CHECK PAGE

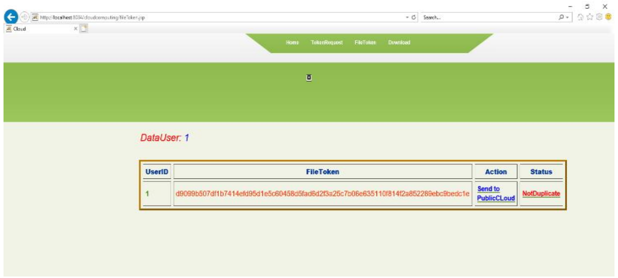


WELCOME TO PUBLIC CLOUD

UserID	FileToken	Action
1	d9099b507df1b7414efd95d1e5c60458d5fad6d2f3a25c7b06e635110f814f2a852289ebc9bedc1e	Verify & Send

Figure 17: Output for File Duplicate Check Page

OUTPUT FOR AFTER CHECKING FILE DUPLICATE PAGE

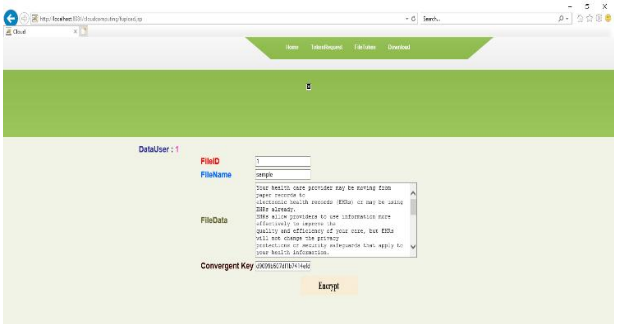


DataUser: 1

UserID	FileToken	Action	Status
1	d9099b507df1b7414efd95d1e5c60458d5fad6d2f3a25c7b06e635110f814f2a852289ebc9bedc1e	Send to PublicCLoud	NotDuplicate

Figure 18: Output for After Checking File Duplicate Page

OUTPUT FOR FILE UPLOAD PAGE SLICE (ENCRYPTION)-1



DataUser : 1

FileID: 1

FileName: sample

FileData:

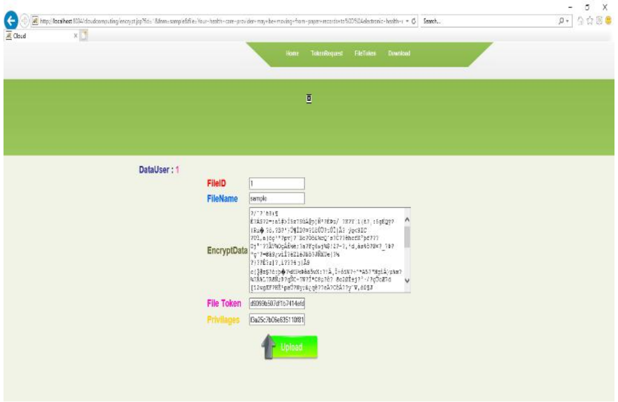
```
Your health care provider may be moving from
paper records to
electronic health records (EHRs) or may be using
EHRs already.
EHRs allow providers to use information more
effectively to improve the
quality and efficiency of your care, but EHRs
will not change the privacy
protections or security safeguards that apply to
your health information.
```

Convergent Key: d9099b507df1b7414efd

Figure 19: Output for File Upload Page Slice (Encryption)-1

DOI: 10.48175/IJARSCT-4618

OUTPUT FOR SLICE (ENCRYPTION)-2



DataUser : 1

FileID: 1

FileName: sample

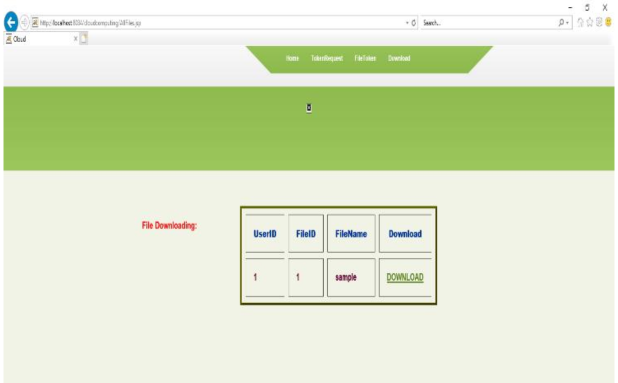
EncryptData: [illegible]

File Token: d8099b507d1b7414efd

Privilages: f3a25c7b06e635110f81

Figure 20: output for Slice (Encryption)-2

OUTPUT FOR FILE DOWNLOAD PAGE

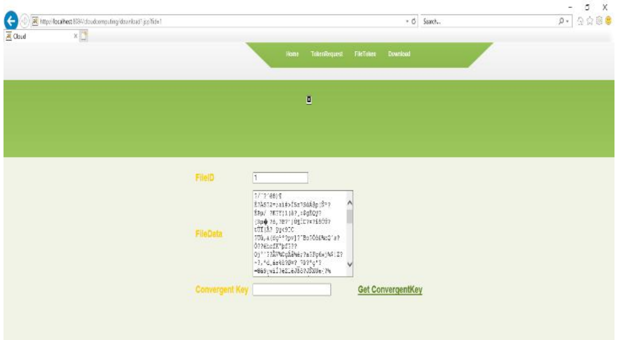


File Downloading:

UserID	FileID	FileName	Download
1	1	sample	DOWNLOAD

Figure 21: Output for File Download Page

OUTPUT FOR SLICE (DECRYPTION)-1



FileID: 1

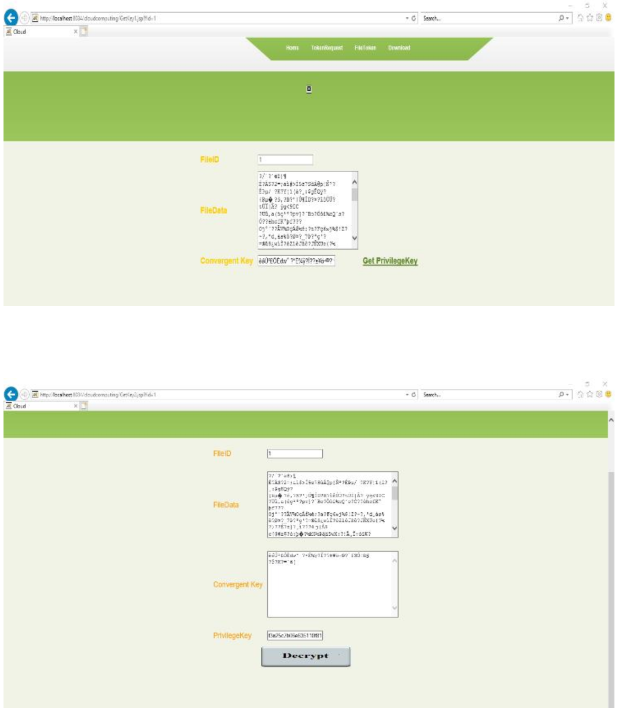
FileData: [illegible]

Convergent Key:

Figure 22: Output for Slice (Decryption)-1

DOI: 10.48175/IJARSCT-4618

OUTPUT FOR SLICE (DECRYPTION)-2



FileID: 1

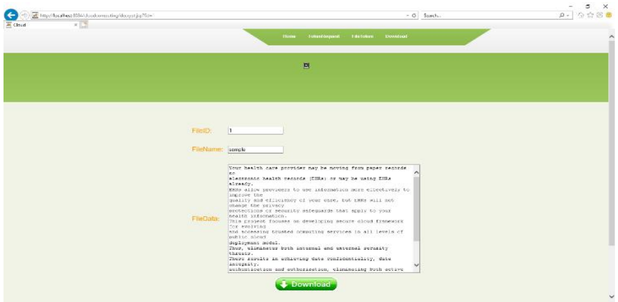
FileData

Convergent Key

PrivilegeKey

Figure 23: Output for Slice (Decryption)-2

OUTPUT FOR GET ORIGINAL FILE PAGE



FileID: 1

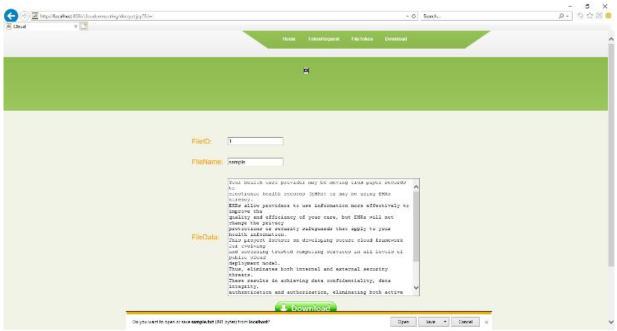
FileName: sample

FileData:

```
Your health care provider may be moving from paper records
to
electronic health records (EHRs) or may be using EHRs
already.
EHRs allow providers to use information more effectively to
improve the
quality and efficiency of your care, but EHRs will not
change the privacy
protections or security safeguards that apply to your
health information.
This project focuses on developing secure cloud framework
for evolving
and accessing trusted computing services in all levels of
public cloud
deployment model.
Thus, eliminates both internal and external security
threats.
These results in achieving data confidentiality, data
integrity,
authentication and authorization, eliminating both active
```

Figure 24: Output for Get Original File Page

OUTPUT FOR AFTER DOWNLOADING PAGE



FileID: 1

FileName: sample

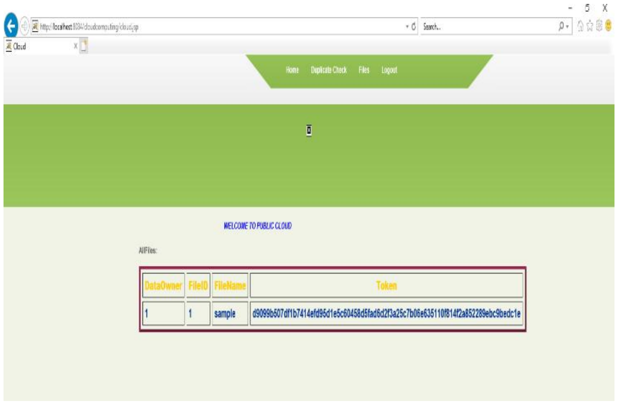
FileData:

```
Your health care provider may be moving from paper records
to
electronic health records (EHRs) or may be using EHRs
already.
EHRs allow providers to use information more effectively to
improve the
quality and efficiency of your care, but EHRs will not
change the privacy
protections or security safeguards that apply to your
health information.
This project focuses on developing secure cloud framework
for evolving
and accessing trusted computing services in all levels of
public cloud
deployment model.
Thus, eliminates both internal and external security
threats.
These results in achieving data confidentiality, data
integrity,
authentication and authorization, eliminating both active
```

Do you want to open or save **sample.txt** (INI bytes) from **localhost**?

Figure 25: output for After Downloading Page

OUTPUT FOR FILE PAGE IN PUBLIC CLOUD



WELCOME TO PUBLIC CLOUD

AllFiles:

DataOwner	FileID	FileName	Token
1	1	sample	d9099b507df1b7414efd95d1e5c60458d5fad6d2f3a25c7b06e635110f814f2a852289ebc9bedc1e

Figure 26: Output for File Page In Public Cloud

VII. CONCLUSION

These consequences in attaining statistics confidentiality, statistics integrity, authentication and authorization, putting off each energetic and passive attacks from cloud community environment. To develop a steady cloud framework for getting access to depended on computing and storage offerings in all stages of public cloud deployment model.

REFERENCES

[1]. C. Chu, S. Chow, W. Tzeng, J. Zhou, R. Deng, “Key-aggregate cryptosystem for scalable data sharing in cloud storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, Feb. 2014.

[2]. Y. Tong, J. Sun, S. Chow, P. Li, “Cloud-assisted mobile-access of health data with privacy and auditability”, IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, Mar. 2014.

[3]. Z. Pervez, A. Khattak, S. Lee, Y. Lee, “SAPDS: Self-healing attribute-based privacy aware data sharing in cloud”, The Journal of Supercomputing, vol. 62, no. 1, pp. 431´lC460, Oct. 2012.

[4]. C. Fan, V. Huang, H. Rung, “Arbitrary-state attribute-based encryption with dynamic membership”, IEEE Transactions on Computers, vol. 63, no. 8, pp. 1951-1961, Apr. 2013.

[5]. D. Boneh, G. Crescenzo, R. Ostrovskyy, G. Persianoz, “Public key encryption with keyword search”, in Eurocrypt 2004, Interlaken, Switzerland, May 2-6, 2004, pp.506-522.

[6]. N. Cao, C. Wang, M. Li, K. Ren, W. Lou, “Privacy-preserving multi keyword ranked search over encrypted cloud data”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222-233, Nov. 2013.

[7]. S. Seo, M. Nabeel, X. Ding, E. Bertino, “An efficient certificateless encryption for secure data sharing in public clouds”, IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 9, pp. 2107-2119, Sept. 2014.

[8]. L.A. Dunning, R. Kresman, “Privacy preserving data sharing with anonymous ID assignment”, IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp.402-413, Feb. 2013.

[9]. X. Chen, X. Huang, J. Li, J. Ma, D. Wong, W. Lou, “New algorithms for secure outsourcing of large-scale systems of linear equations”, IEEE Transactions on Information and Forensics Security, vol. 10, no. 1, pp. 69-78, Jan. 2015.

[10]. X. Chen, J. Li, J. Weng, J. Ma, W. Lou, “Verifiable computation over large database with incremental updates” IEEE Transactions on Computers, vol. 65, no. 10: 3184-3195, Oct. 2016.

[11]. C. Gao, Q. Cheng, X. Li, S. Xia, “Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network”, Cluster Computing, to be published. DOI: 10.1007/s10586-017-1649-y.

[12]. J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, Y. Tang, “Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks”, Journal of Network and Computer Applications, vol. 106, no. 15, pp. 117-123, Mar. 2018.

[13]. J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. Hassan, A. Alelaiwi, “Secure distributed deduplication systems with improved reliability,” IEEE Transactions on Computers, vol. 64, no. 12, pp. 3569-3579, Dec. 2015.

[14]. J. Li, Y. Zhang, X. Chen, Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing", Computers & Security, vol. 72, pp. 1-12, Jan. 2018.

[15]. J. Li, X. Huang, J.W. Li, X. Chen, X. Xiang, "Securely outsourcing attribute-based encryption with checkability", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201-2210, Aug. 2014.

[16]. Y. Zhang, X. Chen, J. Li, D. Wong, H. Li, I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing", Information Sciences, 379: 42-61, Feb. 2017.

[17]. W. Sun, S. Yu, W. Lou, Y. T. Hou, H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," in INFOCOM 2014, Toronto, Canada, Apr. 27-May 2 2014, pp.226-234.

[18]. A. Rosenthal, P. Mork, M. Li, J. Stanford, D. Koester, P. Reynolds, "Cloud computing: a new business paradigm for biomedical information sharing", Journal of Biomedical Informatics, vol. 43, no. 2, pp. 342-353, Apr. 2010.

[19]. M. Li, S. Yu, Y. Zheng, K. Ren, 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, pp. 131-143, Jan. 2013.

[20]. J. Benaloh, M. Chase, E. Horvitz, K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records", in CCSW 2009, Chicago, Illinois, USA, Nov. 13, 2009, pp. 103-114.

[21]. J. Sun, 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, Jun. 2010.

[22]. A. Bahga, V. Madisetti, "A cloud-based approach for interoperable electronic health records (EHRs)", IEEE Journal of Biomedical and Health Informatics, vol. 17, no. 5, pp.894-906, Sept. 2013.

[23]. D. Anthony, A. Campbell, T. Candon, et al., "Securing information technology in healthcare", IEEE Security & Privacy, vol. 11, no. 6, pp. 25-33, Nov. 2013.

[24]. M. Canim, M. Kantarcioglu, B. Malin, "Secure management of biomedical data with cryptographic hardware", IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 1, pp. 166-175, Jan. 2012.

[25]. M. Lesk, "Electronic medical records: confidentiality, care, and epidemiology", IEEE Security & Privacy, vol. 11, no. 6, pp.19-24, Nov. 2013.

DOI: 10.48175/IJARSCT-4618