Securing Public Health Record using Attribute Based Encryption for Data Storage in Cloud

1. Shubham Prakash Chaudhari, Information Technology Department, MIT College of Engineering, Pune
2. Akshat Jain, Information Technology Department, MIT College of Engineering, Pune
3. Bhavesh Kalal, Information Technology Department, MIT College of Engineering, Pune
4. Kautuk Mishra, Information Technology Department, MIT College of Engineering, Pune
5. Chudaman D. Sukte, Information Technology Department, MIT College of Engineering, Pune

Abstract

Cloud Computing has been increasing in popularity over the past couple of years. There has been extensive use of various software's and applications with the cloud platform acting as the backbone for these activities. As more and more organizations and individuals make use of the Cloud platform, the data warehouses that support the platform are heavily strained. Therefore, these warehouses are staffed full of employees that handle the cloud, this leads to the data of the cloud to be open to attackers and also the people working there. Therefore, the security of the data on the cloud is imperative, to this end, this paper proposes a model for an attribute-based encryption technique in which the public and secret key are generated from the hash key based on the user profile's personal attributes, randomly. The random characters are essential for the generation of the private and public keys. The reverse cipher algorithm also increases the security of the model by enabling stronger encryption.

Keywords: *MD5, RSA, Reverse Circle Cipher, Data security.*

1. INTRODUCTION

The popularity of computer network comes out with EMR (electronic medical records). Early day in the past, hospitals mainly used Electronic Medical Records (EMR). It contains the past, present, future, physical and psychological status records of patients. Using electronic digital format to record the disease status of patients and check the test results instead of the original paper medical

records. The main purpose is to assist medical or its related services, providing information for the executive nurses in clinical medical use. After infirmaries adapted EMR, they soon overcome the restriction on traditional PMR (paper medical records) had caused, and earn them extra benefit never appeared on traditional paper medical records. If the operation of storage and transmission been figured out on traditional paper medical records, and directly track and manage medical records through EMR, both do not only enhance the greater medical efficiently but the few mistakes taken by human beings. However, EMR is an information system primarily based on Local Area Network (LAN), electronic medical records still emphasize on how to manage and transmit, and only part of it can make achievement on the switch between medical institutions. It's hard to satisfy with modern medical development on demand if greatly confine information sharing, monitoring and quick reacting. But they all operate and manage in perspective of medical information suppliers, not the patients. Patients obtain the source of medical records only from doctors and they do not hold the authority to the information which results in incapable of getting over their health condition quickly. As for improving personal health record and the coming diseases, it turns out helpless without enough information.

Nowadays the need for the sharing of health data between health care teams such as doctors, nurses, researchers, students, and family members is increasing so that the professionals, guardians can get a complete overview of the medical history of the patient. Medical data can be needed by various kinds of users. Patients, their close relatives (guardians or adults son/daughter), any other authorized person) may access the data to know about the patient's present conditions. Hospitals, special clinics or diagnostic labs can access the health records for further treatments.

Recently, the aging society has now become one of the obvious traits in developing countries. According to the a standard set by World Health Organization(WHO), the population over 7% up to age 65 in a nation is named aging society; over 14% it is called aged society; when over 21% it is called super-aged society. Developed countries – Japan, become a member of super-aged society where already has 21.2% of the population at least 65. On the other hand, German and Italy or more countries also reach the standard of aged society. However, aging society leads to the phenomenon that chronic diseases rapidly growth, people regard management and prevention as a necessity, many medical services have gradually centered on patients. Many countries take PHR seriously.

The deployment and maintenance of large data storage infrastructures are costly. As a result, data storage is usually

Outsourced to third-party providers. Cloud computing is a paradigm that provides this kind of service. It became a trend and is one of the fastest growing technological services. With the fastest development of cloud computing, a large number of companies and individuals utilize the public cloud to store and share data. By externalization of data in the cloud, the users no longer required to maintain the local storage. Instead, users can store the information in a pay-per-use manner and save the cost of hardware and software deployment. Cloud computing centralizes, virtualizes separable one-side network, server, operating system, storage space, application, and et cetera to become a database that IT department can immediately be processing dynamic service depend on demand what client need. Cloud computing technology contains the utilization of computing reservoir that is distributed as a service over a network. In cloud computing model users must provide access to their information for storing and playacting the specified business operations. Hence cloud service supplier should give trust and security, as there's valuable and sensitive information in large quantity holds on the clouds. There are considerations regarding versatile, climbable and fine-grained management inside the cloud computing.

Cloud computing provides with cross-platform, saving of time, lower the cost and other factors. Therefore, PHR implement achieved various services with an elastic adjustment under the computing power and storage. This perception of sharing not only obviously lower IT investment by medical institutions, increase using efficiency and strengthen system stability, but also improve the original standard of service IT held and evaluate more flexible service. The prediction of Markets and Markets indicates that there is a huge growth if health IT works on cloud computing, which profit will grow to $5.4 billion in health care by 2017, and the user will step up from 4% to 20.5%. More and more PHR suppliers are willing to shift their application and data-storage to the Cloud, like Microsoft, IBM, and SAP.

The problem related to the empowering of patients to keep them updated with respect to their health records is acceptable that is termed as PHR (Personal Health Record). PHR is considered to be as a better solution for the management of the health of an individual. This is also that toll that empowers the reaction of patient & health providers by providing his/her complete medical past. Attribute dependent encryption (ADE) is defined as public key encryption within which the user secret key and ciphertext are based upon attributes. In this type of system, ciphertext decryption is feasible when the attributes of the ciphertext equivalent to attributes set of the user key. A collision resistance is a critical safety aspect of attribute dependent encryption. A contender that constrains multiple keys ought to solely be ready to access information if a minimum of one individual key grants access. In cloud computing, an attribute dependent encryption is the best algorithm. Constrain of a numerous of attribute dependent encryption technology are to be analyzed. Attribute dependent encryption commonly involves the encryption of attributes only neither encrypting the entire information. Encryption in ABE is simple and safe and cheap in comparison to other encryption. The ABE is safe because the encrypted information carries the attributes instead of data. The information is not at all leaked in case of malicious attacks also. The attribute-based encryption performance is also high in comparison to other encryption method and it makes the application safe also. It is the best solution for all cloud applications.

This research paper dedicates section 2 for analysis of past work as literature survey, section 3 deeply elaborates the proposed technique and whereas section 4 evaluates the performance of the system and finally section 5 concludes the paper with traces of future enhancement.

II LITERATURE SURVEY

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

Chia-Hui Liu, Fong-Qi Lin, Dai-Lun Chiang, Tzer-Long Chen, Chin-Sheng Chen, Han-Yu Lin,Yu-Fang Chung, Tzer-Shyong Chen [1] proposed a program about key management on Bilinear pairing, which perfectly switch in patient-centered PHR (Personal Health Records) in Cloud computing environment, and establish partial order to direct every user, an arrangement to ensure every patient can manage and share their own medical record, they design access control based on patients, also give the solution of Multi-user access and lower the difficulty of key management. With these advantages, users can retrieve PHR in the legitimate and authorized environment on their own. For PHR to develop well in the Cloud computing environment, must confirm where the information comes from and the integrity of content, also provide multi-user dynamic access mechanism. They design the unique public formula FU (x, y), and by access control matrix to pick qualifier, only with the trusted authority (TA) or certification authority (CA) can get authorized access of encrypted information. They give users minimum authority on the basis of their need, accordingly, they can prevent the danger from unexpected events, errors and unauthorized events may bring to users. They design and combat the equation problem attack, external attack and reverse attack perfectly with the help of access control scheme.

Priyanka Bansal, Bhavna Sharma, Mohit Saxena [2], introduced the system for enhancing the safety of PHR by an implementation of DWT that is based over Steganography. Steganography is that process in which information can be hidden in a picture. Steganography has the ability to insert more information into one image. PHR data will be hidden in one image by Steganography. In the Steganography encryption & decryption process will be executed by DWT. They are working for hiding the PHR data into a single image for the security reasons. They proposed Wavelet-based Steganography for hiding the PHR data into an image. In the results, Elapsed time and Error rate get reduce up to 80-90%.

Mohd Anwar [3], introduced the concept of observing daily living (ODLs) and execute EMA (Ecological Momentary Assessment) along OSNs (Online Social Networks). The ODLs is utilized to enhance diagnosis and treatment. EMA is introduced to discover health connected behavior specimen to diagnose health issues and treat them. The user content and activity logs present in OSNs are visualized to derive ODLs and execute EMA. The "apps" are developed to record health associated data, supported by an open platform of vital OSNs. The data collected by an app transfer to cloud build server which processes the data and extracts ODLs from that data and enters them into PHRs (personal health records) and to execute EMA.

George Hsieh and Rong-Jaye Chen [4] proposed the blueprint of cloud-based PHR service that is safe and practical. They used the CCD (Continuity of Care Document) for exchanging and storing the PHR data of an individual to increase portability and practicability. A broad spectrum of the safety system that include encryption, access control, and a digital signature is applied in an embedded, integrated and fine manner, depend on standards like XML, XML Encryption, XML key management, and XML signature. They used attribute depended on encryption, ciphertext policy and public key encryption with search schemes keyword in the embedded, integrated and fine-grained way.

Fuhu Deng, Yali Wang, Li Peng, Hu Xiong, JiGeng, and Zhiguang Qin [5], presents private health information may be exposed to unauthorized organizations or individuals since the patient lost the physical control of their health information. Ciphertext-Policy Attribute-Based Sign Cryption (CP-ABSC) could be a promising resolution for coming up with a secure PHR sharing system with cloud support. It provides complete management of access, confidentiality, believability, and privacy of PHR knowledge. However, an oversized variety of pairing and standard mathematical operation and calculations lead to serious overhead throughout the encryption process of the planning. They proposed an outstanding scheme in order to reconcile the conflict of high calculation overhead and low potency within the blueprinting encryption method. In the proposed scheme the significant computations outsourced to CTS (Ciphertext Transformed Server), solely going a tiny low process elevated for the PHR user. At a similar time, the additional communication overhead in their theme is really tolerable. In the random oracle model hypothetical analysis and also the needed safety properties together with unforgeability, confidentiality, and verifiability have been tested formally. Experimental analysis indicates that the planned theme is sensible and possible.

Lucas de Melo Silva, Roberto Araujo, Felipe Leite da Silva and Eduardo Cerqueira [6], proposed a novel design for secure sharing and storage of health information in the cloud. Their solution makes possible secure storage with file sharing managed by the user based on access policy. Also, it allows access to revocation and doesn't need users to continuously store keys. The new proposal also enables patient and clinician sovereignty over PHR and EHR. In addition, it allows collaboration through health record sharing and it allows simple access revocation. It is thus a step towards secure sharing and storage of health information in the cloud. A more complex access revocation is still a challenge. As future work, they will improve the architecture to consider different configurations. IdPs may assume the AA role and AAs may perform as SPs. In addition, they will consider other ABE protocols and will provide proof of concept implementation for the proposed architecture.

Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk [7], proposed a PHR sharing plan which is patient-centric and attribute depended. It provides access to both personal and professional users in a flexible way. In the proposed method every individual data of PHR is encrypted and then saved in a healthcare cloud accompanying a policy which attribute-based and that controls the encrypted information access. An authorized based mechanism is introduced to authorize the user's retrieval request for PHR information to depend on the connected access scheme while using a proxy re-encryption plan to smooth the users to decrypt the needed PHR files. The proposed scheme is successful in overcoming the flexibility issues for accessing the file in relation to past ABE based PHR sharing plan while sustaining ample safety level and privacy.

Mitu Kumar Debnath, Saeed Samet and Krishnamurthy Vidyasankar [8], presents the execution of a framework for sharing of PHR (personal health records) in a secure way by using a variety of generic CP-ABE encryption scheme named mCP-ABE. To accomplish their goal they implemented the Java library of this CP-ABE scheme with the help of jPBC library. This framework would allow users to share, manage, and process PHR data with the fine refined access control mechanism. Moreover, this framework efficiently handles the fundamental challenge of key management which is introduced by multiple PHR users and owners. Furthermore, it handles the efficient and on-demand attribute revocation. As a future direction to this work, we are going to add the NoSQL database system (e.g., MongoDB, Oracle NoSQL Database, etc.) in place of MySQL RDBMS. NoSQL database is suitable for PHR applications, because there is no limitation for the number and type of properties a patient's record can have, and each PHR is different from one another by its nature with a different number of properties. Also, to make the system more robust, and to overcome the issue of sole point of failure, single Trusted Authority (TA) can be replaced by (k, n) threshold scheme, such that at least k TAs should participate to generate the user secret keys.

Samydurai, Revathi K, Prema P, Aruhnozhiarasi D S, Jency J and Hemapriya S [9], presented a HCI (Health Care Information) sharing system which is used to store sensitive health information which can be outsourced in the cloud with high security. The patients can send queries to specified doctors which are updated in the cloud. The doctors can reply to the queries which are updated and then encrypted by the admin. The patients view the details after proving the encryption key. The details remain encrypted to other users who view health care information, ensuring increased security.

Md. Rafiqul Islam, Mansura Habiba and Mir Injamamul Ibne Kashem [10], proposed a framework for securing the PHRs of an organization. Through the classification of data according to the sensitivity levels, it has been demonstrated that the system can save its overhead and enhance its performance. Implementation issue especially related to obtaining control has been demonstrated here. For future work, they will collect data from different hospitals and clinics and compare our hypothetical consideration with the survey data. On the hand, they will do a detailed experiment for the proposed purpose.

III PROPOSED METHDOLOGY

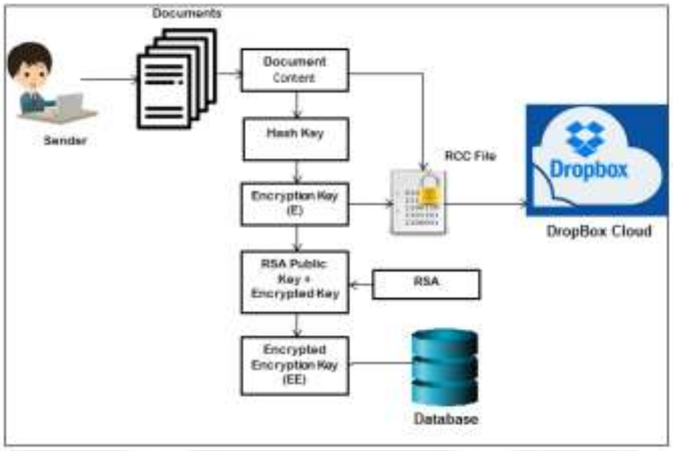


Figure 1: System Overview of the proposed technique

The figure above depicts the presented technique for hiding sensitive data and maintaining the integrity of the cloud. The various steps to achieve the methodology have been elaborated below.

Step 1: Key Generation–The technique being discussed here has been implemented on a Java-based platform on a real-time public cloud entity. The various signup formalities and setup were obliged to on the public cloud “Dropbox” website before integrating it with the framework developed on Java through the use of an Access token.

After the successful implementation of the framework, and authenticating the credentials on the public cloud, the framework generates MD5 hash key based on the user credential.

After the generation of the hash key, the deployed model is allowed to randomly select 7 characters from it and create an E_{KEY}which is an Encryption key. Furthermore, the RSA algorithm is utilized to generate K_{PUB} and K_{PRI} an Asynchronous key. The generated RSA key $K_{PUB}$is utilized to encrypt the E_{KEY}into EE_{KEY}that is extremely complicated and thus increases the security of the key. The key generation process is depicted in algorithm 1.

Algorithm 1: Key Generation Generation

```
// Input :  Hash Text $H_T$
// Output :  Random Key $E_{KEY}$
Function :randomKeyGenrator($H_T$)
Step 0: Start
Step 1: $E_{KEY}$ =Ø
Step 2:  HashKey $H_K$=MD5 ($H_T$)
Step 3: K=$H_K$ length MOD  7
Step 4: If  K<7, THEN
Step 5: P=K+1
Step 6:for i=0 to $E_{KEY}$ length < 7
Step 7:  i=i+P
Step 8:  If  i< $H_K$ length, THEN
Step 9: $E_{KEY=}$ $E_{KEY+}$ $H_K$ [i]
Step 10: $H_{K =}$rotate($H_K$ )
Step 11: End if
Step 12: Else
Step 13: i=0
Step 14: End For
Step 15: End if
Step 16: return $E_{KEY}$
Step 17: Stop
```

Step 2: Reverse Circle Encryption – After the generation of the various different keys in the previous step, this step provides the proposed model with a plain-text file that is used in conjunction with the generated $EE_{KEY}$to be encrypted by the Reverse Circle Cipher Algorithm. The Algorithm encrypts the plain-text file and outputs a ciphertext.

The prescribed steps of the Reverse Circle Cipher start with segregating the input plain-text into blocks. The indices of these boxes, all of size 10 are utilized to constantly rotate them. At every rotation, the $E_{KEY}$is used on the blocks by summarization followed by neutralization of the ASCII values and then subsequently replaced with the original blocks. The process is elaborated in the algorithm 2 outlined below.

Algorithm 2: Reverse Circle Cipher

```
// Input :  Plain Text $\mathbf{PL_T}$, Random KEy $E_{KEY}$
// Output : Cipher Text $\mathbf{CR_T}$
Function :reverseCircleCipher($\mathbf{PL_{T,}}$ $\mathbf{E_{KEY}}$)
Step 0: Start
Step 1: $BLK_{STR}$ =Ø, $BS_{SET}$ =Ø
[$BLK_{STR:}$ Block String , $BS_{SET:}$ Block Set ]
Step 2:  for i=0 to length of $PL_T$
Step 3: $BLK_{STR\,=}$ $BLK_{STR}$ + $P_{Ti}$
Step 4: If  $BLK_{STR}$ size =10 THEN
Step 5:  $BS_{SET\,=}$ $BS_{SET}$ + $BLK_{STR}$
Step 6:  $BS_{SET\,=}$ =Ø
Step 7: End for
Step 8:for j=0 to size of $BS_{SET}$
Step 9:  If j >=10 , THEN
Step 10: K=j MOD 10
[K: number of Character to rotate ]
Step 11: $BS_{SETj\,=}$rotate($BS_{SETi\,,}$K)
Step 12:  T= ∑ $\mathbf{E_{KEY}}$ MOD 20
Step 13: $BS_{SETj[E]\,=}$$BS_{SETj}$+ T
Step 14: $CR_{T=}$ $CR_{T+}$$BS_{SETj[E]}$
Step 15: End for
Step 16: return $\mathbf{CR_T}$
Step 17: Stop
```

After the encryption with the Reverse Circle Cipher is complete, the file is then uploaded onto the cloud service, such as Dropbox here. The file is highly secure in the cloud storage, and when needed, the user can download the encrypted file from the cloud and decrypt it using the private key + EE_{KEY}which outputs the $E_{KEY}$with the help of the Reverse Circle Cipher. The proposed technique is quite efficient and fast and doesn't require heavy computational capabilities from the user machine.

IV RESULT AND DISCUSSIONS

The proposed methodology for enhancing the security and maintaining the data on the cloud has been extensively tested and deployed on a public cloud called Dropbox in real-time. The presented technique was coded using the Java Platform, on a NetBeans Integrated Development Environment. The methodology was implemented on a machine on which the Central Processing Unit was a Core i5, with the primary memory of 6 GB. The various tests performed to evaluate the performance of the presented model has been outlined below.

4.1 Character assignment for Encryption Comparison

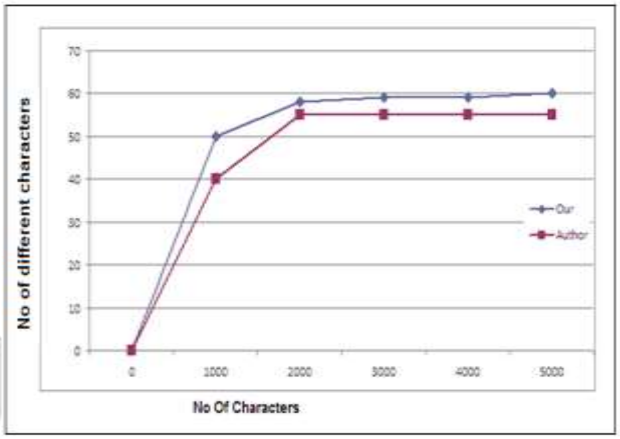
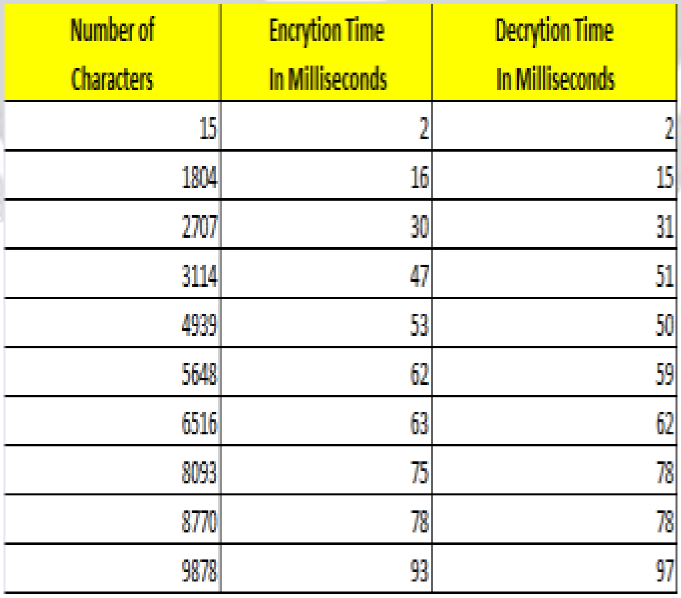


Figure 2: No of File character versus No of Using different characters for the encryption and decryption

The Graph in figure 2 above depicts the difference in performance when different characters are being used for the algorithm and the number of characters that are being utilized for encryption and decryption purposes. The proposed methodology has been compared with the conventional techniques for encryption on the cloud and the results indicate that a larger number of characters are utilized in the method elaborated in this paper in comparison with the traditional technique of [11], which enhances our encryption model by a large margin.

4.2 Encryption and Decryption Time performance

The performance time of the proposed model's encryption and decryption is tested extensively, and the results are compared and tabulated in the table below.



Number of Characters	Encrytion Time In Milliseconds	Decrytion Time In Milliseconds
15	2	2
1804	16	15
2707	30	31
3114	47	51
4939	53	50
5648	62	59
6516	63	62
8093	75	78
8770	78	78
9878	93	97

Table 1: Encryption and Decryption time performance

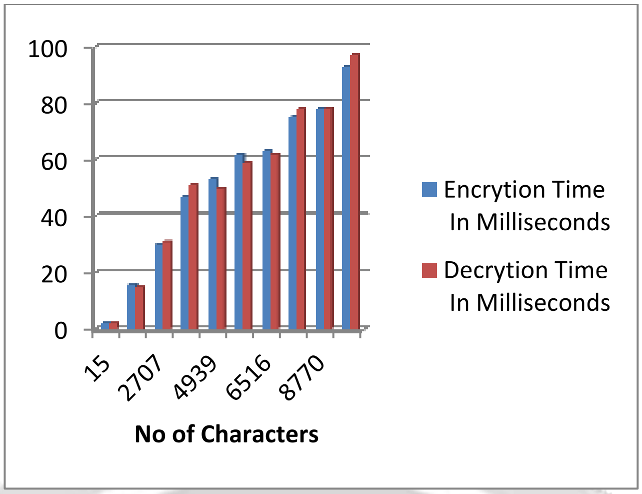


Figure 3: Encryption and Decryption Time

Table 1 and Graph in figure 3 confirms that the proposed methodology has inconsistent timings corresponding to encryption and decryption in terms of the number of characters. This is an indication that the encryption algorithm is performing as expected and has been deployed properly in the domain.

V CONCLUSION AND FUTURESCOPE

The security in the cloud is more concern than anything in its operational paradigm. This is due to more complicated and huge size of the cloud. So to overcome this data is always kept in encryption format. So the proposed system uses the Reverse circle cipher encryption technique which is enhanced in its structure of rotation to yield good secured encrypted data. This encryption scheme is using the random characters that are generated for the user attributes to maintain the more security. Encryption key is secured using the RSA public and private keys to ensure the authentication of the system.

In the future this system can be applied on more format of the files of big size in terms of GB.

REFERENCES

[1] Chia-Hui Liu, Fong-Qi Lin, Dai-Lun Chiang, Tzer-Long Chen, Chin-Sheng Chen, Han-Yu Lin, Yu-Fang Chung, Tzer-Shyong Chen," Secure PHR Access Control Scheme for Healthcare Application Clouds" 2013 42nd International Conference on Parallel Processing.

[2] Priyanka Bansal, Bhavna Sharma, Mohit Saxena, "Low Error Rate Based Secure Sharing of Personal Health Record in Cloud Computing using DWT Steganography", 2016 8th International Conference on Computational Intelligence and Communication Networks.

[3] Mohd Anwar, "Leveraging Online Social Media for Capturing Observations of Daily Living and Ecological Momentary Assessment", IEEE IRI 2014, August 13-15, 2014, San Francisco, California, USA.

[4] George Hsieh and Rong-Jaye Chen, "Design for a Secure Interoperable Cloud-Based Personal Health Record Service", 2012 IEEE 4th International Conference on Cloud Computing Technology and Science.

[5] Fuhu Deng, Yali Wang, Li Peng, Hu Xiong, JiGeng, and Zhiguang Qin, "Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records", DOI 10.1109/ACCESS.2018.2843778, IEEE Access.

[6] Lucas de Melo Silva, Roberto Araujo, Felipe Leite da Silva and Eduardo Cerqueira, “A New Architecture for Secure Storage and Sharing of Health Records in the Cloud Using Federated Identity Attributes”, 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom).

[7] Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk, “A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing”, 2016 IEEE 2nd International Conference on Collaboration and Internet Computing.

[8] Mitu Kumar Debnath, Saeed Samet, and Krishnamurthy Vidyasankar, "A Secure Revocable Personal Health Record System With Policy-Based Fine-Grained Access Control", 2015 Thirteenth Annual Conference on Privacy, Security and Trust (PST).

[9] Samydurai, Revathi K, Prema P, Aruhnozhiarasi D S, Jency J, and Hemapriya S, "Secured Health Care Information Exchange on CloudU sing Attribute-Based Encryption", 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN).

[10] Md. Rafiqul Islam, Mansura Habiba, and Mir Injamamul Ibne Kashem, "A Framework for Providing Security to Personal Healthcare Records", Department of CSE, BUET. 5-8 January 2017.

[11] Ebenezer R.H.P. Isaac ; Joseph H.R. Isaac ; J. Visumathi " Reverse Circle Cipher for personal and network security ",2013 International Conference on Information Communication and Embedded Systems (ICICES), 2013.

****