International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Authorized and Encrypted in Health Care Records Using Fine – Grained Access Control in Distributed System

Mr.Satish .T.Pokharkar1[1], Dr.L.K.Vishwamitra[2], Mr.Krushna.M.Borude[3], Mr.Suyog.S.Medhe[4], Mr.Sachin.R.Kolase[5]

Submitted:14/03/2024 **Revised**: 29/04/2024 **Accepted**: 06/05/2024

Abstract: today, many applications are being developed in the medical field to overcome the complexities of previous research. The digitization of healthcare is enhanced using information technology and computing, providing a variety of new technologies and medical devices. While existing systems have seen many more advances to save patients time and money, provide accurate care, and keep sensitive patient records secure, the biggest significant issue is confidentiality. To address the current security concerns in order to develop and construct the prototype model for security research work. For sensitive patient health records on database web servers. Existing efforts only data encryption can protect patient records from insider threats. First, put in place front-end security in proposed research work using Key logging techniques, second to prevent insider attacks, store users or patient's sensitive information or data across multiple data servers or chunks, and third, and most importantly, implement a multi-authority search policy for encrypted data. In the present research work is being added to securely clearly state the format of patient data records in multiple chunks (small pieces) and to use cryptosystems because of confidentiality of a patient's medical information's. Specifically, proposed research task benefits to use the SHA hashing technique each user to allow access to specific data records. This study investigates the proposed Role Base Access Control (RBAC) and the proposed Advanced Encryption Algorithm (AES)-256 bit encryption techniques for secure data storage and sharing for end-user strategies for securing access to the data. This work also included the implementation of a backup server strategy, which functions as an all distributed data servers use an ad hoc network data recovery for proxy storage server. We talked about the data protection for a medical database and identified which entities could and could not access the database. We discussed several encryption schemes, especially proxy re-encryption based, and signature Techniques such as the bilinear aggregate authentication protocol are examples of such strategies, that can be used to ensure data confidentiality and integrity. A secure medical database prototype was created, developed and tested to make a comparison the security performance of and insecure medical databases. Our contributions include a theoretical discussion of medical database security, the development the development of a proposed design to represent a secure medical database, and the outcomes of some studies were performed we carried out. This work shows that ensures the integrity and confidentiality of a medical database has a significant impact on performance. The prototype is relatively slow, but should have little real-world impact. If he only has to wait a second for a doctor to retrieve patient information, instead of milliseconds for an insecure the security implications of a medical database exceed the performance impact. Additionally, as part of the decryption process, by employing a re-encryption strategy, i.e. Re-encryption can be assigned to a proxy, thus spreading the computational cost. Furthermore, we showed that the prototype scales linearly, an important property when backing up large databases. From this we can conclude that it is possible to secure a medical database without trusting the database itself.

Keywords: *User data privacy, ABE (Attribute-Based Encryption), Paillier encryption, forward security, Multi-authority, SHA Algorithm, Hashing Functions, encrypted data search, Wireless network, etc.*

1. Introduction

The primary goal of an information distribution centre is to protect data integrity. It also has a TTP audition for illegal access. The proposed work implements included data protection and data regeneration in the event that it was mishandled. To deal with these concerns, data will be temporarily held on a proxy server. This information remains saved in the data server's public and private sectors by users. As a result, patients or users confidential data has been safely stored in private database server, and user as well as patients used only public server data [6]. Primary data are obtained from the Proxy Server on the private server and returned after unauthorized modification has been made. Data storage normally allows customers to maintain the desired balance between achievements including faults tolerance in different roundness configurations. In this research, the proposed Role Base Access Control (RBAC) and AES algorithm and are explored to securely store and share data with a safe data obtain system for the user's. This system also includes a backup server solution for all distributed data servers that acts as an ad hoc data recovery proxy storage server. Experimental testing in private and public server storage environments have been proposed communication, there are two main techniques cryptography and information hiding, as shown in Figure.1 [2].Cryptography is the science of converting elements

[1] *Oriental University, Indore – India*
ORCID ID: 0009-0007-4428-9001
[2] *Oriental University, Indore-India*
ORCID ID: 0000-0001-6019-8117
[3] *Adsul's Technical campus Chas Ahmadnagar, India*
[4] *Adsul's Technical campus Chas Ahmadnagar, India*
[5] *Pravara Rural Engineering College Loni, India*
** Corresponding Author Email: satishpokharkar37@yahoo.com*

values of secret message from any format (text, Image or sounds.... etc.) into a different values [3]. Information hiding is imbedding information into the cover carrier, e.g. image, or video is imperceptible to the human beings [4].Here better way is the cryptosystem, and that encrypts data first (converting plain-text to cipher-text) before uploading it. The Secure Hashing algorithm, like the Paillier cryptosystem, distributes user data in various chunks and stores them for backup and recovery use a proxy server. Finally, at most trusted users with an access key can obtain and decrypt data records. The most significant module in this research effort is safety at the front end. Thus, Key logging technology is used in healthcare applications for frontend safety considerations. This strategy is used to prevent the use of password security phishing attempts. Thus, application of healthcare is safer. Secondly, the storage of data and the accessibility of information. The Secret Shamir hash and keyword technique, as well as content-based encryption, can be used for this.

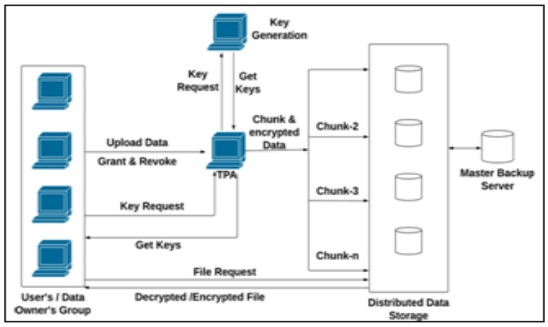

Fig.1.System overview

1.1 What is Medical Data?

Medical data includes everything by patient records and diagnosis and treatment to raw visual information like EEG monitoring samples. We divide medical information into two classifications. Non-sensitive data and important information that includes patient records or can be related with a patient. Sensory data, also defined as measurement data, consists solely of sensor samples and is thus classified as non-sensitive. Sensory data so in event of EEG is made up of numerical values indicating voltages evaluated on a user's scalp. In certain situations, such as when preserving EEG readings in EDF+ format [20], patient data is often kept in the data file, successfully placing the whole data file at risk. Healthcare information can be kept in a database to prevent the above. The sensory data from EEG measurements is secured to such a file; however the personal info is eliminated. Only those recognizing details are stored in a medical database, which contains links to sensory data files. Metadata refers to data contained in a medical database that describes the real statistics.

1.2 Usage of Medical Data

Medical databases that manage patients' health information, visual information, and meta-data, are the focus of this course. Patient information is private and should be securely stored. Sensors and metadata are also not highlighted in this section, but the link that binds them must be safeguarded against corruption. First we look at electronic medical records in general, then he looks at a special medical database known as MeDIA.

1.3 Electronic Health Records:

A medical database as an e.g. of electronic health records (EHRs). EHR, as said by [20], seems to be "a digital collection of patients' health information that is collected and processed as well as transferred and accessible to several legitimate user. "Medical professionals and administrative staff have access to medical records through the EHR system. [20] Distinguishes between several types of electronic patient records. B. Healthcare data records and 2 different electronic medical records (EMR). Others do not differentiate among electronic medical records and electronic medical records and do not consider them equivalent. The EMR contains data entered from her single department of the hospital, all or part of the hospital, and even data from multiple hospitals. Usually only hospital staff enter data into her EMR.

The main distinguish among EMR and PHR might it be all of that PHR system requires health records to be presented in such a case which the patients could also quickly grasp the data provided. Patient's control those someone else's medical documents as well as make the choice who might receive them has access to them. Presenting a patient record may differ from presenting a paper patient record because only physicians and administrative staff have access to the EMR system. Personal medical records are not considered in this task. Instead, consider a hospital's electronic medical record system. This type of electronic patient file is widespread [16, 20]. On the other hand, connecting these systems to the Internet can introduce security gaps [20]. Therefore, securing the It is critical to have servers which store electronic health information. To illustrate the safety and security of electronic health records, consider MeDIA, a healthcare database service.

1.4 MeDIA

MeDIA (**Medical Data Integration Application** [15]) seems to be the current name of a healthcare system for managing databases under development. MeDIA can store sensory data such as EEG, MRI, and CT scans, moreover related Patient health information and annotations are examples of metadata. MeDIA's main advantages over simply storing binary data are its ability to handle descendants, unpredictability, and refactoring, or must integrate various data types such as EEG and MRI. Additionally, if a user wants to view her EEG data and her MRI data for one of her patients, she can use MeDIA instead of querying different databases separately. MeDIA differs

from traditional electronic medical record systems in his three ways: lineage, uncertainty, and version control.

Lineage can be employed to indicate for which a specific piece of data came from. eg, if they exist three data elements a, b, and c, so c is described as c = a + b, then c comes directly by a and b. This can be employed, e.g., in diagnostic tables. Each diagnosis is accompanied by a list of sensory data that supports it. If for some

Reason it is necessary to reject a particular set of sensory data due to erroneous capturing, it is simple to figure out whether diagnoses should be revaluated.

Database uncertainty which indicates each element whereas in database is assigned a reasonable chance. Probabilities are used, eg, when collecting elements forecasts in a database. The forecast might be "80\% possibility of clear skies, 15\% possibility of clouds, 5% possibility of rain". In the database stores probabilities for each of the three possibilities (sun, cloud, rain).

Versioning: The possibility to keep record of existing versions of data element is known as versioning. Suppose a university saved all wages of its employees in a database. Employee Monica got a raise. Monica's previous salary is archived and versioning is used to update her "current" salary. As a result, the database contains not only the current salary, but also all past salaries for each employee. This can be used to preserve older diagnoses in more medical settings.

2. Proposed methodology

Computer security is an important concern in today's world because computers are used to keep and analyze confidential information all across. Particularly in healthcare, virtual offices, education, business, e-commerce, e-learning, e-banking, distributed, cloud computing, computing, as well as several internet-based services. Passwords can protect Keystroke the dynamics access control approach protects against a variety of attacks. This method has been conceived on how people type their passwords. Keystroke dynamics does not necessitate the use of any additional hardware. Password protection requires only software-based technology. The end result emphasizes pleasure security, which is in high demand in web-based applications. Existing works can provide protection of user data during transmission but cannot prevent an internal assault on the database of users administrator illustrates sensitive user information. Medical database reports are extremely sensitive in the medical field, so there is a need to secure them and provide strong privacy to avoid unauthorized access to the information. When we upload the PHR record to the cloud, there is a risk of data leakage; therefore, to avoid malicious attacks on personal data and health records, we must provide strong security, proper authentication, and end-to-end encryption to only those with authority to access data. As a result, only the authorized person has access to the available information, and the data is kept secure. To avoid all of these conditions, our system must perform flawlessly as expected. To put in place a system that will solve the security issue. Our system will be able to solve problems, eliminating the need for hacking scenes. Because of the security provided by the AES algorithm, the information is end-to-end encrypted and cannot be accessed or stolen by unauthorized users. By utilizing the TPA (Third Party Auditor) and AES encryption and decryption process. In this search work is to address critical challenges in healthcare database security and privacy. The research aims to design and implement a secure database framework that incorporates multi-authority mechanisms, allowing for efficient and authorized encrypted searches while preserving the privacy of sensitive healthcare information. The primary goals include enhancing the security infrastructure of healthcare databases to safeguard against unauthorized access and potential breaches. By employing multi-authority techniques, the research seeks to distribute trust and control across multiple entities, mitigating the risks associated with a single point of compromise. The focus on encrypted search functionality aims to strike a balance between data accessibility for authorized users and the imperative to protect individual privacy. Furthermore, the research aims to contribute to the development of advanced privacy-preserving techniques, ensuring that sensitive healthcare data remains confidential even during search operations. This is particularly crucial in healthcare settings where the protection of patient information is paramount. Ultimately, the purpose of this research is to advance the state-of-the-art in healthcare database security, providing a robust and privacy-preserving solution that facilitates authorized access for healthcare professionals while safeguarding sensitive patient data from potential adversaries. The outcomes of this research have the potential to significantly impact the field of domain of secure database systems.

3. Working Architecture

3.1 Working Modules

First Module: Secure Login & Password (Account) Authentication Key logging, also known as the process of keystroke acquiring is secretly recording (or logging) the keys pressed on a keyboard. It is also extremely useful in studies communication between humans and computers. A few numerous Key logging strategies, ranging from software- and hardware-based methods to signal testing. Human inclusion in authentication mechanisms, whereas guaranteed, is difficult due to their limited calculation and memory capacity. We demonstrate how a careful visualization illustration could also enhance all these security and convenience and its benefit of access control. Two visual authorization protocols have been proposed: one

with a one-time password and the other with a password. Our strategy for authentic scheme: we were able to achieve an abnormal level of usability while legal structures security requirements. Like, account verification & validation, trusted data transmission, node mobility support, and rapid event detection, data delivery on time, power management, node computation, and middleware are all examples of services provided by the platform. Furthermore, implementing technological innovations in data transmission apps without regard for security are.

Second Module: Access Control List (ACL) using Cipher Text Policy-Attribute based Encryption (CP-ABE) to manage the patient-managed PHR access control mechanism, a strategies known as Secure Sharing of PHRs in the Cloud (SeSPHR) is used. By restricting unauthorized users, the approach protects the PHRs' privacy. The PHR owner defines the Access Control List (ACL) levels of permission provided to various user categories. For example, the owner may grant full access to the PHRs to the patients' family members or friends. Similarly, Health insurance delegates may only have access to segments such as PHRs that encompass info on medical health coverage claims, while some private health data, eg. Patient's medical history might well be limited for those kinds of users.

Third Module: Database security with Multi-Instance In this research work, we discuss a realistic solution to preventing inside attacks by storing user data on multiple data servers. This systems main contribution is the secure distribution of user or organizational data across multiple data servers, as well as the use of either Paillier and ElGamal cryptosystems or SHA algorithm for conduct research on user/organizational information without compromising its confidentiality.

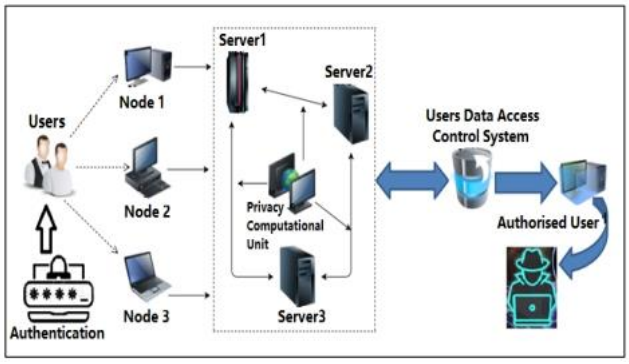

Fig.2: Proposed System Architecture

4. Problem Definition:

The development of an authentication and wireless data transmission application presents numerous novel challenges frequently made users/organizations privacy vulnerable. The above problem can be addressed by proposing a practical approach to preventing inside attacks by using multiple data servers to store patients' confidential info and using privacy protection on data transmission and database of Key logging strategy.

5. Implementation details

In the previous chapter, we described the System Design without going into detail about the system's security requirements. The building blocks for implementing the CIA properties are identified in this chapter (Confidentiality, Integrity and Availability). But first, we'll go over some terminology that will be used throughout the chapter.

5.1 Cryptography

Cryptography plays a pivotal role in safeguarding sensitive healthcare information within the proposed secure database system. The concept involves the use of encryption and decryption algorithms to protect data at rest and during authorized searches. The system employs symmetric and asymmetric encryption methods to secure the stored healthcare records, ensuring that only authorized entities can access and retrieve the information.

5.2 Proposed Algorithm

In this work, we contrasted the existing method with our proposed Secure Hash Generation Algorithm (SHA) -256 bit based hashing method. The SHA-256 (Secure Hash Algorithm 256-bit) algorithm is a widely used cryptographic hash function that produces a fixed-size output of 256 bits. Below is a step-wise pseudo code for the SHA-256 algorithm:

Algorithm: SHA-256

Require: number of data chunks, Encrypted information, data chunk member counter, probability,Threshold, data transmission interval, Secure hash functions.

Procedure:

Step 1.Start

Step 2.Initialize

Constants H0 = 0x6a09e667

H1 = 0xbb67ae85

H2 = 0x3c6ef372

H3 = 0xa54ff53a

H4 = 0x510e527f

H5 = 0x9b05688c

H6 = 0x1f83d9ab

H7 = 0x5be0cd19 Step

Step 3. Pre-processing

Pad the message

Append a single '1' bit to the end of the message Append '0'

bits until the length of the message in bits is 448 (mod 512) Append the original message length as a 64-bit integer.

b. Initialize variables

W [0...63] - Message schedule

a..h - Working variables

Step 4. Main loop

For each 512-bit block of the padded message. Prepare the message schedule

b. Initialize the working variables with the previous hash value

c. Compression function

For t = 0 to 63:

If t in [0, 15]:

W[t] = Block[t]

Else:

W[t] = Sigma1 (W[t-2]) + W[t-7] + Sigma0(W[t-15]) + W[t-16] Update working variables using logical functions

d. Update hash values

H0 = H0 + a

H1 = H1 + b

H2 = H2 + c

H3 = H3 + d

H4 = H4 + e

H5 = H5 + f

H6 = H6 + g

H7 = H7 + h

Step 4. Output

Concatenate H0, H1, H2, H3, H4, H5, H6, and H7 to obtain the final hash value.

Step 5. Stop

6. Result analysis

The goal of the present system is to develop a web-based approach for the medical network toward use in order to avoid number of attacks on patients along with the storage and transmission of confidential data records. The following parameters are used in the analysis of the results:

Time consumption

Response Time.

Computation Cost.

Performance accuracy.

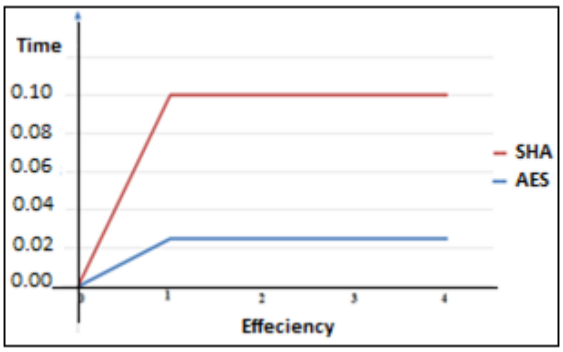

Fig.3: Time and Efficiency Chart

Present entire setup get captured the greatest number of qualities or input data parameters, although the focus is mostly on Performance of Operation and its Time. Here to receive the following analytical conclusion for our proposed system if we support a few of attributes.

Parameter	Existing	Proposed
A	10	4
B	10	5
C	8	8
D	10	3
E	8	2

Table 1: Result Table

Where,

A = Time Consumption.
B = Response Time.
C = Computation Cost.
D = Performance accuracy
E = Scalable & User Friendly.

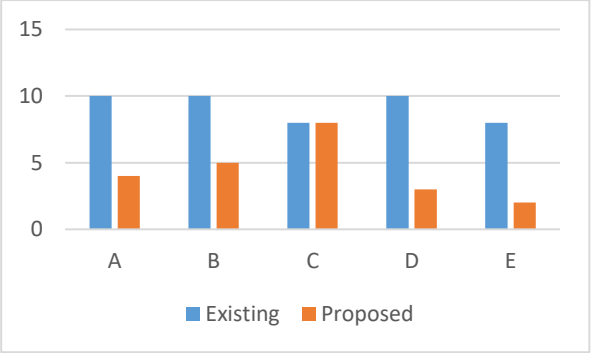

Fig.4: Time line chart of Result Analysis

Calculation of the amount of time required to accomplish those tasks:
Here to calculate the required time for AES encryption approach to encrypt (cipher text) the information as well as a result time required to hashing operation on particular information.

File Size in KB	AES(256)	SHA-256	Time in m/s
12KB	6.6ms	20.595ms	27.195ms

25KB	12.3ms	37.370ms	49.67ms
5KB	2.77ms	9.040ms	11.81ms

According to the comment, the time required to conduct the data action depends on the configuration of the system. The Intel (R) Core (TM) i5 – 8th generation 8250U CPU @ 1.80GHz, 8GB RAM, Windows 10 64-bit OS Version 1909. I have further noticed that it took longer to conduct the procedure on a system that had less setup than an above mentioned.

7. Conclusion

This research work examined medical database security and identified medical database security requirements. We explained the encryption method in order to stop information leaks and the signature method facing ensure the purity of the information. A prototype was created to gauge the effectiveness penalties of medical database safety. The findings demonstrate notable performance degradation. Security delays are significant when only a few patient records are requested. E.g., retrieving complete patient data for It takes less than 1.5 seconds for five patients, compared toward 0.5 ms on the outside of safety security. After all, the safety-adding delay should be considered as an absolute number, not as a percentage of unsafe delay situations. He considers 1.5 seconds to be acceptable for patient information from 5 patients. When requesting large amounts of data using a safe database, every request execution time increases linearly with the number of patients requested. I have listed some questions for research that need to be resolved in the introduction. The initial query was, "How can I encrypt patient information so that it cannot be decrypted by the database? "The foundational elements for providing confidentiality were outlined in working architecture. We came to the conclusion that type-based proxy rekeying was the ideal response for maintaining privacy while permitting access to be revoked if necessary. Type-based proxy re-encryption was put into place, and evaluated the effectiveness of different algorithms.

The next following query was, "How can we ensure the security of medical data in untrusted databases?" In working architecture describes how to verify data integrity and how to verify query results. We encourage you to discuss how to sign your data using the Bilinear Aggregate Signature Scheme and have your customers verify its integrity. We investigated the impact of aggregation on signing performance and found that it can speed up verification by up to twenty five percent. The third investigational query was, "What are the performance implications of maintaining information integrity and discretion?" To test the performance of our additional security, we set up an experiment and put a prototype into practice. In Implementation describes experiments and prototypes. In result analysis, we discussed the experimental results and concluded we set up an experiment and put a prototype into practice. How the database is used. A doctor's performance who needs to decipher a patient's record while treating a patient her penalty is her 1 second at most. Performance degrades significantly when physicians and patient administrators request data for a large number of patients. For example, it takes up to 5 minutes to decrypt and verify the full names of 5000 patients. In case or not this is acceptable is entirely dependent on the circumstances under which is what the system is employed.

Acknowledgements

I am grateful to all of those with whom I have the pleasure to work during this and other related projects. I thankful to my guide Dr.L.K.Vishwamitra sir and Dr. Amit Saxena Associate Dean Research of University have provided me extensive personal and professional guidance and taught me a great deal about the research. I especially thankful to computer department in oriental university for providing the resources.

References

[1] H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system," Journal of Computer and System Sciences, vol. 90, pp., 46-62, 2017.

[2] Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach, "Future Generation Computer Systems, vols. 4344, pp. 99-109, 2015.

[3] Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.

[4] Li, "Electronic personal health records and the question of privacy," Computers, 2013, DOI: 10.1109/MC.2013.225.

[5] S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, "Secure Dynamic access control scheme of PHR in cloud computing," Journal of Medical Systems, vol. 36, no. 6, pp. 4005– 4020, 2012.

[6] Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 1–17, Jul. 2012.

[7] Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing (Collaboration), 2012, pp. 711-718.

[8] N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, "Incremental proxy re-encryption scheme for mobile cloud computing environment," The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.

[9] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "A research agenda for personal health records (PHRs)," Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9

[11] Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.

[12] Shamim Hossain, Ghulam Muhammad, et al. "Cloud-assisted Industrial Internet of Things (IIoT) –Enabled framework for health monitoring." 2016 evier B.V.

[13] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions On Parallel and Distributed Systems 2012.

[14] IEEE 2012 paper on "Improving the interoperability of healthcare information system through HL7 CDA and CCD standards".

[15] Ibrahim, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, Cipher text-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes‖2009

[16] Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, Worcester Polytechnic Institute, 2011.

[17] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[18] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving PHE system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[19] Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in SecureComm'10, Sept. 2010, pp. 89–106.

[20] Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.