Prevention of Cyber-Attacks in Healthcare Informatics

R. Varalakshmi

Abstract*: *Healthcare Informatics (HCI) empowers patient to deal with their own therapeutic records in a digitalized and centralized path. The main aim of this paper is accessing this stored information on cloud by authorized personnel, anywhere, anytime through any device. Healthcare Informatics contains sensitive patient data, clinical history that should to be protected against unauthorized users on cloud. In this study, role-based access control and fine-grained access control were proposed. The results of this study are utilized in the policy enforcement and the access control policies. With the help of cryptographic techniques, the proposed algorithm in this study, provides the higher-level privacy and prevention of cyber-attacks in healthcare informatics.

Keywords*: *Access control, Cloud computing, Cyber-attacks, Healthcare informatics.

I. INTRODUCTION

Cyberattacks has become an important issue for all organizations and also for individuals. The individuals information are available in many sector like Government sector, Banking sector, Online services, Healthcare organizations etc., Out of this, Healthcare organizations hold the most sensitive information about an individual including name, age, gender, date and place of birth, contact details, medical records, medical insurance details, social security details, etc. Due to limitation in Healthcare organization like lack of IT knowledge, low budget, etc., the healthcare industry has little security on data and hence, they become easy targets for hackers, results in more threats from hackers.

The term Healthcare Informatics (HCI) has been connected to maintaining information about the patients using both paper based and digital system. The recent technological development suggests an electronic application used to gather and store health information. An electronic record of health-associated data on personal can able to access by multiple doctors at identical time for discussion and treatment for the patients. The doctors can able to collaborate in critical cases, experiences can be shared and managed through cloud. Electronic Health Record (EHR) could be a computer-based record that originates and managed by doctors, and utilized by a general practioner, nurses, lab technicians, patients, pharmacists and relevant medical personnel.

In figure 1 the Healthcare Informatics model is shown and it is based on the role-based access control technique. These techniques introduced many roles like patient information, medical records, medical examiner, pharmacy, insurance policy and sensitive information. In this technique will include another method which is called role-based authentication. This method is used for website will be created the role fields such as patient information contains name, age, gender, height, weight, patient id etc., all the personal information are presented here and the medical history contains health conditions, medicated prescriptions, allergies etc., and medical examiner contains physical examine, lab test, laboratory test and insurance policies and sensitive information like HiV, cancer, tumor etc.

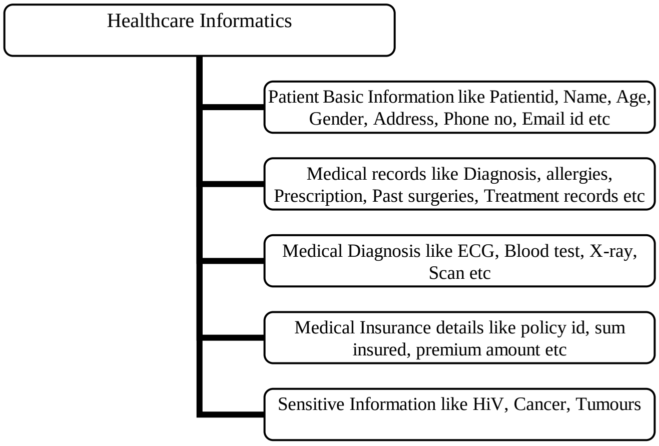
Healthcare Informatics
Patient Basic Information like Patientid, Name, Age, Gender, Address, Phone no, Email id etc
Medical records like Diagnosis, allergies, Prescription, Past surgeries, Treatment records etc
Medical Diagnosis like ECG, Blood test, X-ray, Scan etc
Medical Insurance details like policy id, sum insured, premium amount etc
Sensitive Information like HiV, Cancer, Tumours

Fig. 1.Healthcare Informatics model

A. TYPES OF CYBER ATTACKS

The threats in healthcare organization is classified into two categories namely untargeted attacks and targeted attacks. Without knowing what kind of information is available in the healthcare organization, if the attacker attacks then it can be said as untargeted attacks. After getting the data like patients healthcare informatics, active medical devices etc, the attacker will try to maximise the profit with the minimum effort. As the attack is more generic, the attackers may spend little amount of time and resources to breach the security. Also, it is expected that the attacker may be novice.

Targeted attacks are used to retrieve a specific information from the organization. The adversaries have a primary objective in hacking the health care system. After getting the data, the attackers gain more profit through blackmailing, sale of a random health records etc. As the attack is targeted and specific, the attackers will spend more amount of time and resources in breaking the security for the date theft. It is expected that the attackers are more expertise and try different algorithm to break the security.

Revised Manuscript Received on April 25, 2020.
* Correspondence Author

Dr. R. Varalakshmi*, Assistant Professor, Department of Computer Science and Applications, The Tamil Nadu Dr. Ambedkar Law University, India Email: rvaralakshmi697@gmail.com

Though limiting the security breach is sufficient for untargeted attacks, a more advanced security policy is highly essential to prevent targeted attacks. Thus, irrespective of the nature of the attacks, the healthcare organisation is expected to take necessary steps to enhance the security and to prevent attacks.

B. CLOUD COMPUTING

Cloud computing Technology one of the creating field that is been joined into different fields in the Information Technology [1]. The modern booming growth of the Internet-based techniques has up a revolution of network-oriented applications. A connected surroundings additional drives the merger of assorted techniques, like edge computing, cloud computing and Internet-of-Things (IoT) [2]. These days, digital storage of computer information is moving toward cloud computing that is a set of infrastructure provides information storage for organizations and people [3]. cloud computing is one amongst the rising technologies. It represents a true paradigm shift within the manner during which systems are deployed Cloud computing incorporates virtualization, on-demand deployment, web delivery of services, and open supply software [4]. Figure 2 shows the three layer cloud Architecture [5].

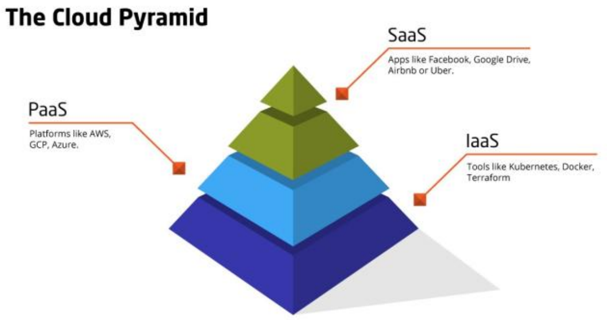
The Cloud Pyramid
SaaS
Apps like Facebook, Google Drive, Airbnb or Uber.
PaaS
Platforms like AWS, GCP, Azure.
IaaS
Tools like Kubernetes, Docker, Terraform

Fig. 2.Three- Layer Cloud Architecture / Cloud Pyramid

SaaS- (Software as a service) To utilize the supplier's applications running on a cloud foundation and open from different customer gadgets through a slight customer interface, for example, a Web program.

PaaS- (Platform as a service) To convey onto the cloud infrastructure consumer-created applications victimization programming languages and tools supported by the supplier (java, python, .Net).

IaaS- (Infrastructure as a service) To provision process, storage, networks, and other basic computing resources wherever the consumer is in a position to deploy and run whimsical software, which might embrace operational systems and applications.

C. ACCESS CONTROL

Access control is a security system that manages who or what can view or utilize assets in a processing situation. It is a crucial idea in security that limits hazard to the business or association. Access control mechanism permits one application to confide the identity of another application. Access control contains six models [6,7], they are

i. Identity based access control
ii. Role based access control
iii. Attribute based access control
iv. Risk adaptable access control
v. Trust based access control and
vi. Rule based access control.

Role-based access management (RBAC) restricts network access supported a personality's role at intervals a company, colleges, hospitals etc.it has become one amongst the most strategies for advanced access management. The roles in RBAC ask the amount of access that patient got to the network. patients square measure solely allowed to access the knowledge necessary to effectively perform their health record details. Access is supported many factors, like authority, responsibility, and job competence. additionally, access to pc resources is restricted to specific tasks like the flexibility to look at, create, or modify a file.

Various model has been proposed like

i. Team- based access control
ii. Group-oriented Access Control
iii. Temporal Role based access control
iv. Location - based Role based access control
v. Spatio-temporal Role based access control.

Attribute based access management extends role-based access management, in general, with the subsequent features:

i. Delegation of attribute authority
ii. Decentralization of attributes and
iii. Interference of attributes.

II. LITERATURE REVIEW

According to previous studies, a comparative analysis was prepared for Healthcare Informatics. It can be analysed by using various cloud technologies, algorithms, comparative analysis, methodologies are noted down. Mostly cryptography algorithms are used in Healthcare Informatics for security purpose, an encryption and decryption timing analysis are made. The general framework mechanism for secure sharing of Healthcare Informatics in proposed by different authors [8-10].

Ciphertext Policy-Attribute Based Encryption (CP-ABE) scheme is used for to transfer the encrypted information however solely authorized users who satisfy the access policy will decrypt [11]. The curiosity of our development is that properties can be from two security areas: social space (for example family, companions, or individual patients) and expert area (for example specialists or medical caretakers). F. Xhafa proposed a multi authority Ciphertext-Policy ABE scheme which has been used for access policy can be hidden and user access privacy has been protected. This scheme can be very secure and efficient [12]. The security framework of cloud computing [13] and secured transmission of key in group hierarchy in multicast communication has been discussed in [14].

Fine grained access control is proposed in which the proxy decryption to enforces sticky policies and furnished clients with compose benefits for HCIs [15]. Whenever clients complete the process of composing information to their HCIs, they sign the altered HCIs. Notwithstanding, clients sign the HCIs utilizing the signature key of the HCI owner and it is along these lines hard to accurately check who signed the HCI. Patient-centric access control scheme had confidentiality, integrity, authenticity of personal health data in cloud storage [16]. Key aggregate cryptosystem has been used for revocation of access control.

For secure hold on transmission of the private health records to the approved entities within the cloud storage is proposed using SeSPHR[17]. Healthcare Informatics owner stores the encrypted data on cloud storage and only authorized person can be access the valid re encryption keys provided by a semi trusted proxy can be decryption of Healthcare Informatics. Healthcare Informatics modify customers to electronically store, create and share their own health data, isolated from electronic or paper medical records maintained by their health care suppliers [18]. The elgamal encryption and proxy decryption scheme are proposed and can be used for privacy purpose [19].

III. PROPOSED ALGORITHM

In Healthcare Informatics system there are many risks involved for the patient security. But the patients are in dilemma whether they can share and store their personal records which are stored in third party server. But there is alternate method that works in semi trusted servers to ensure patient that is fine grained access control technique. The fine-grained access control technique increases the level of security and privacy for the data owners and data entity that can be access the data. the technique is very flexible and it allows access control policies. The finegrained access control technique is very simple and efficient to use. So, Patients may be comfortable to share their records when their disease is fully cured. Hence all patients wish that their health record is fully secured. In order to secure this, there is a system called HCI cloud computing system. With this method patients are very free and comfortable to store their Healthcare Informatics.

In order to enhance the security for the HCI's data to be stored in cloud, the data are encrypted with RSA Algorithm. RSA uses two keys i.e Public key and Private key, the data are encrypted using public keys and the encrypted information are stored in cloud. The private keys are distributed to the authorized personnel. In order to retrieve the patient information, the encrypted data has to be decrypted using private key. As the data are in cloud, the user can access the data anytime, anywhere. The data can be retrerived using thin clients with minimum process capabilities, memory and bandwidth. Thus, the data are stored and accesed in safe and secure way

From the hospital, a patient will get his data's like disease history, laboratory records, x-rays, and other data after due authentication. The patient can choose his family doctors or specialist who can treat his/her disease. The doctor can able to access the patient's information available on the cloud using Access Control List (ACL). ACL is nothing but a set of permission that is embedded on the medical data. From this permission different user can be provided with different level of rights for the patient data access. The ACL is regulated by Mandatory Access Control (MAC).

Mandatory Access Control (MAC) will be at the level of user operating system and it makes the operating system to perform an operation on the given data files, memory of I/O devices.

A. Algorithm

The main objective of this proposed algorithm is to prevent cyber-attacks in healthcare informatics. This algorithm is used to encrypt and decrypt the health care data and it is an asymmetric cryptographic algorithm. In this algorithm there are two keys. i.e., Public key and Private key. Public key is public to all user in the network. Every user in the network having both the keys. Private key should not sharable between all. It must be kept secret.so only user can use the private key. If one key is used in encryption side and the other key of same way in decryption process. public key is used at encryption and a private key of same user is used in the decryption process.

The proposed algorithm is classified into four processes there are set up, key generation, encryption algorithm, decryption algorithm.

Let

$CK=g^{\chi} \, mod \; n$ (1)

$Mk=g^{y} \, mod \; n$ (2)

B. Setup

The bilinear mapping group of prime order N=PQ and e: $B*B\text{->}B_1$ is a non-degenerate bilinear map, that is

(i) Bilinear: for all $b_1,b_2 \epsilon B$ and ɏ $x,y\text{<-}L$, $e(b_1^{\chi},b_2^{\gamma})=e(b_1,b_2)^{\chi\gamma}$.

(ii) Nondegenerate: for generator b of B, e(b,b) generator B_1.

Let Bp and Bq denotes the subgroups of B of order p and q respectively. Then B=Bp * Bq. If b is a generator of B then bp and bq denotes the generators of Bp and Bq for all random elements Lp ϵ Bp and Lq ϵ Bq. So e(Lp,Lq) =1 because $e(Lp,Lq)=e(bp^{\chi},bq^{\gamma})$. $e(bq^{\chi},b^{P\gamma})=e(b,b)^{P9\chi y}=1$ for some generator b in B.

C. Key Generation

Generate bilinear group B of order N=PQ.public key and private key are generated by the bilinear mapping group which is pk and sk.

Pk=(B,N,b,bp) and sk=(p) here pk is the public key and sk is the secret key.

D. Encryption

Enc(pk,x) here pk and x is a public key.

$V\text{<-}L*n$ and $F\text{<-}b^{\chi}(bp)^{v} \epsilon B$. Here V is random variable and it is belong to L*n.

The Healthcare Informatics is logically partitioned into the following five portions. They are

i. Private Information.
ii. Medical Records.
iii. Medical Examination.
iv. Insurance Policy.
v. Sensitive Information.

Here the random variables $v_1,v_2,v_3,v_4,v_5 \epsilon L*n$ are generated and variable v_i is used for encrypt ith partition of HCI.

$Fp_i=L^{v}{}_1.HCIp_i$ (3)

Retrieval Number: D7858049420/2020©BEIESP
DOI: 10.35940/ijeat.D7858.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fp_i is the semi encrypted file that contains the private information partition as encrypted text. $HCIp_i$ is private information of Healthcare Informatics.

$Fmr=L^{v}_{2}.HCImr$ *(4)*

Fmr is the semi encrypted file that contains the medical record patition as encrypted text in addition to the Fpi that was encrypted in the previous step. HCImr is medical record of Healthcare Informatics.

$Fme=L^{v}_{3}.HCIme$ *(5)*

Fme is the semi encrypted file that contains the medical examine patition as encrypted text in addition to the Fpi , Fmr that was encrypted in the previous step. HCIme is medical examine of Healthcare Informatics.

$Fip=L^{v}_{4}.HCIip$ *(6)*

Fip is the semi encrypted file that contains the Insurance Policy partition as encrypted text in addition to the Fpi , Fmr, Fme that was encrypted in the previous step. HCIip is insurance policy of Healthcare Informatics.

$F=L^{v}_{5}.HCIsi$ *(7)*

F is the completed encrypted file that contains all the partition in the encrypted form. HCIsi is sensitive information of Healthcare Informatics.

The above stated encryptions the client also calculate the following parameters.

$Vpi\_p= b^{v}_{1}{}^{\chi}p.$ (8)

$Vme\_p= b^{v}_{2}{}^{\chi}p.$ (9)

$Vmr\_p= b^{v}_{3}{}^{\chi}p.$ (10)

$Vip\_p= b^{v}_{4}{}^{\chi}p.$ (11)

$Vsi\_p= b^{v}_{5}{}^{\chi}p.$ *(12)*

Here Xp is the private key of the patient and Vis the parameter which is used to produce the decryption key for the partition indicates in the subscript of each V and P is the user. The parameter Vpi_p, Vme_p, Vmr_p, Vip_p, Vsi_p are transmitted to the decryption key along with the file identification for which there parameters are generated.

E. Decryption

Calculates the decryption keys (Vk) and V and transmits it to the user I. $F^{p}=[b^{\chi}]^{p}.[bp^{v}]^{p}=[bq]^{\chi}$

The decryption keys and V are calculated below.

$Vkp\text{->}I =b^{\chi}I/^{\chi}P$ *(13)*

Here $^{\chi}I$ and $^{\chi}P$ are the private keys of I and P.

V is the parameter corresponding to the user I are calculated according to the following equations.

$$Vpi\_I = e(Vkp\text{->}I, Vpi\_p)$$
$$= e(b^{\chi}I/^{\chi}P, b^{v}_{1}{}^{\chi}p)$$
$$= e(b,b)^{v}{}_{1}{}^{\chi_i}$$

Therefore, L = e(b,b)

$Vpi\_I =L^{v}{}_{1}{}^{\chi_i}$ *(14)*

Where Vpi_I is the parameter used to decrypt the partition Private Information and it is applicable for the user I. similarly V parameters for other partitions corresponding to the user I are calculated.

$$Vme\_I = e(Vkp\text{->}I, Vme\_p)$$
$$= e(b^{\chi}I/^{\chi}P, b^{v}_{2}{}^{\chi}p)$$
$$= e(b,b)^{v}{}_{2}{}^{\chi_i}$$

Therefore, L = e(b,b)

$Vme\_I= L^{v}{}_{2}{}^{\chi_i}.$ *(15)*

$$Vmr\_I = e(Vkp\text{->}I , Vmr\_p)$$
$$= e(b^{\chi}I/^{\chi}P, b^{v}_{3}{}^{\chi}p)$$
$$= e(b,b)^{v}{}_{3}{}^{\chi_i}$$

Therefore, L = e(b,b)

$Vmr\_I= L^{v}{}_{3}{}^{\chi_i}$ *(16)*

$$Vip\_I = e(Vkp\text{->}I , Vip\_p)$$
$$= e(b^{\chi}I/^{\chi}P, b^{v}_{4}{}^{\chi}p)$$
$$= e(b,b)^{v}{}_{4}{}^{\chi_i}$$

Therefore, L = e(b,b)

$Vip\_I= b^{v}{}_{4}{}^{\chi_i}.$ *(17)*

$$Vsi\_I = e(Vkp\text{->}I , Vsi\_p)$$
$$= e(b^{\chi}I/^{\chi}P, b^{v}_{5}{}^{\chi}p)$$
$$= e(b,b)^{v}{}_{5}{}^{\chi_i}$$

Therefore, L = e(b,b)

$Vsi\_I= b^{v}{}_{5}{}^{\chi_i}.$ *(18)*

The above given parameters are provided to the user I that decrypts each of the partitions based on the following equations.

$Vpi\_I = L^{v}_{1}.\chi_i$

$L^{v}_{1} = Vpi\_I / \chi_i$

$Fp_i = L^{v}_{1}.HCIp_i$

$HCIp_i = Fp_i/L^{v}_{1}.$

$HCIp_i = Fp_i . \chi_i / Vpi\_I$ (19)

$Vme\_I = L^{v}_{2}.\chi_i$

$L^{v}_{2} = Vme\_I / \chi_i$

$Fme = L^{v}_{2}.HCIme$

$HCIme = Fme/ L^{v}_{2}.$

$HCIme = Fme . \chi_i / Vme\_I$ (20)

$Vmr\_I = L^{v}_{3}.\chi_i$

$L^{v}_{3} = Vmr\_I / \chi_i$

$Fmr = L^{v}_{3}.HCImr$

$HCImr = Fmr/ L^{v}_{3}.$

$HCImr = Fmr . \chi_i / Vmr\_I$ (21)

$Vip\_I = L^{v}_{4}.\chi_i$

$L^{v}_{4} = Vip\_I / \chi_i$

$Fip = L^{v}_{4}.HCIip$

$HCIip = Fip/ L^{v}_{4}.$

$HCIip = Fip . \chi_i / Vip\_I$ (22)

$Vsi\_I = L^{v}_{5}.\chi_i$

$L^{v}_{5} = Vsi\_I / \chi_i$

$Fsi = L^{v}_{5}.HCIsi$

$HCIsi = Fsi/ L^{v}_{5}.$

$HCIsi = Fsi . \chi_i / Vsi\_I$ (23)

IV. SIMULATION RESULT

The existing and proposed algorithm are simulated using MATLAB Software.

Table 1 shows the simulation result. Figure 3 shows the successful attacks gained by the adversary. It is understood that the proposed algorithm is preventing the security breach than the existing algorithm.

Table 1. No. of Successful attacks

No. of Successful Attacks	Existing	Proposed
0	0	0

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication
© Copyright: All rights reserved.

5	24	7
10	79	26
15	143	63
20	297	123

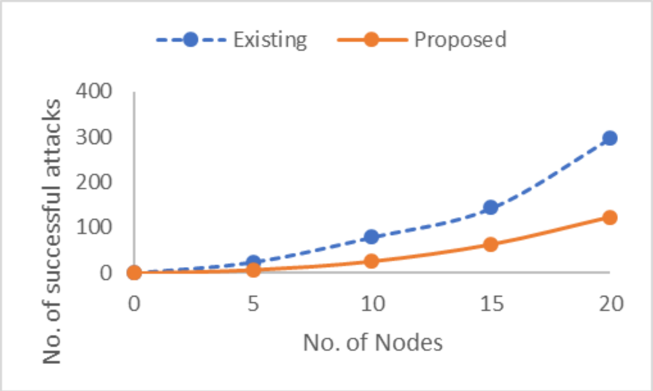

Fig. 3.No. of Successful attacks Vs No. of Nodes

V. STEPS TO ENHANCE CYBERSECURITY IN HEALTHCARE

i. During working hours, the doctors, and other members has to access database in front of the patients with their credentials. Hence use of multi-factor authentication.
ii. Any unused terminals may be switched off or logged out to prevent data breach.
iii. The system / Wi-Fi password may be updated frequently.
iv. Hospital can have a specialized IT team, to reduce the vulnerabilities.
v. The hospital management can organize training programmes for the Doctors, employees, system administrator.
vi. Awareness campaign can be conducted to give awareness about the risk faced if any security is breached.
vii. Can employ a consultant or an expert member to study and monitor if any vulnerabilities are found.
viii. Antivirus software / Firewalls helps in prevention of these sort of attacks.

VI. CONCLUSION

In this paper, the safe and secure way of storing and accessing the Health Care Informatics (HCI) data in cloud are discusses. The sensitive HCI data like patient details, medical history, lab results, etc., are stored in cloud. During emergency, the doctor can provide medical advices to the patient remotely by accessing this data. To prevent the unauthorized access, the data are encrypted using cryptographic technique and the authorized personnel can access using their access control. The HCI information is divided into five categories, the encryption and decryption of these data are explained. From the simulation the proposed shows improvements. Also, the preventive measures to enhance the cybersecurity in healthcare is presented.

REFERENCES

1. E. Tuncay, "Effective use of Cloud computing in educational institutions," in Procedia Social Behavioral Sciences, 2010, pp. 938–942.
2. K. Gai, M. Qiu, Z. Xiong, and M. Liu, “Privacy-preserving multi-channel communication in Edge-of-Things,” in Future Generation Computer Systems, 85, 2018, pp. 190-200.
3. Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, Nor Fazlida binti Mohd Sani1, Solahuddin bin Shamsuddin, Farhood Norouzizadeh, “A Survey About Impacts of Cloud Computing on Digital Forensics,” in International Journal of Cyber-Security and Digital Forensics, 2013, pp.1-18
4. Bibin K Onankunju, “Access Control in Cloud Computing,” in International Journal of Scientific and Research Publications, Vol 3, 2013, pp.1-3.
5. Reterived from https://medium.com/@FedakV/what-is-the-cloud-pyramid-the-layers-of-devops-services-730ac137e8b8
6. Yogita Borse, Anushka Chawathe, “A Survey on Access Control in Cloud Computing,” in International Journal of Computer Trends and Technology (IJCTT), vol 59, May 2018.
7. A.R.Khan, “Access Control in Cloud Computing Environment,” in ARPN Journal of Engineering and Applied Sciences, vol 7, no 5, 2012.
8. Rakesh, Harsha Vardhan, “Sharing of Personal Health Records in Cloud Computing,” in Int. Journal of Engineering Research and Applications, Vol. 3, 2013, pp.1769-1773.
9. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou,” Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption,” in IEEE transactions on parallel and distributed systems, Vol:24, 2013, pp.1- 14.
10. M. 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,” in Journal of Computer and System Sciences, vol. 90, 2017, pp. 46-62.
11. L. Ibraimi, M. Asim, and M. Petkovic, “Secure management of personal health records by applying attribute-based encryption”, in Technical Report, University of Twente, 2009.
12. F. Xhafa, Fatos, J. Feng, Y. Zhang, X. Chen, and J. Li, “Privacy- aware attribute-based PHR sharing with user accountability in cloud computing,” in The Journal of Supercomputing, 2014, pp. 1- 13.
13. Dr. R. Varalakshmi, "Cloud Computing Security Framework for Banking Industry", International Journal of Mechanical and Production Engineering Research and Development (IJMPERD), Vol. 8, Special Issue 3, 2018, pp. 1343-1349.
14. R. Varalakshmi, Dr. V. Rhymend Uthariaraj, “Design of Group Hierarchy for Multicast Communication”, Journal of Theoretical and Applied Information Technology (JATIT), Vol. 54, No.1, 2013, pp 20-29.
15. C. Leng, H. Yu, J.Wang, and J. Huang, “Securing personal health records in the cloud by enforcing sticky policies,” in Telkomnika Indonesian Journal of Electrical Engineering, vol. 11,no. 4, 2013, pp. 2200–2208.
16. Prajakta Solapurkar, Girish Potdar, “Patient-Centric Secure Sharing of Personal Health Records in Cloud Storage,” in International Journal of Engineering Research and General Science,Volume 3, 2015
17. Mazhar Ali, Assad Abbas, Muhammad Usman Shahid Khan and Samee U. Khan,“SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud,” in IEEE Transactions on Cloud Computing,2018,pp.1-14
18. J. Li, “Electronic personal health records and the question of privacy,” in Computers, 2013, DOI: 10.1109/MC.2013.225.
19. D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, “A platform for secure monitoring and sharing of generic health data in the Cloud,” in Future Generation Computer Systems, vol. 35, 2014, pp. 102-113.

AUTHORS PROFILE

Dr. R. Varalakshmi, research area includes Cryptography, Network Security, Cyber Security and allied areas. She has vast experience in teaching and research. She has been recognized and awarded by many forms. She is member of various professional bodies. Her research findings have been published in various International, National Journals, Conference etc. She is an active reviewer and editorial board member.