International Journal of Advanced Science and Technology
Vol. 29, No. 7, (2020), pp. 2844-2855

Privacy and Security Implementation in Existing Cloud Based Electronic Health Records - A DetailedReview

S. Prathima[1],Dr.C. Priya[2]
Research Scholar[1],
School of Computing Sciences, Department of Information Technology, VELS Institute of Technology
and Advanced Studies (VISTAS),Chennai, India, prathismanian@gmail.com

Associate Professor and Research Supervisor[2],
School of Computing Sciences, Department of Information Technology, VELS Institute of TechnologyandAdvanced Studies (VISTAS),Chennai, India, drcpriya.research@gmail.com

Abstract

Over the recent years, cloud computing has emerged as a powerful means for providing automated healthcare facilities. Cloud helps in massive sharing of information between doctors and hospitals using Electronic Health Records. This major transformation has changed the way doctors and hospitals deliver quality and effective service to their patients. Using Cloud storage inhealthcare services has revolutionized health industry, making it more efficient. Apart from the primary driving factors of cloud like flexibility in cost of maintenance, infrastructure and development, on-demand scalability of storage centers and pay on use schemes are proven to be most effective. More and more digitalization of data causes breech of security and privacy.Because healthcare information is a highly sensitive data which cannot be compromised,the future of healthcare relies in providing secure and trustworthy sharing of data by safeguarding privacy and trust. This paper gives an extensive review of the existing security mechanisms for Cloud based healthcare systems.

Keywords: *Security, Health Care, Electronic Health Records, Privacy Preservation, CloudComputing.*

1.INTRODUCTION

T.Muhammed et al.,(2018) [1], Health Care isexperiencingasignificant,large-scale and momentouschange due to the progressof technologies inthelastfewyears.

R. Shende et al., (2016) [2], The tremendous increase of cloud computing techniques, has enabled the users right of entry to their outsourced information from the faraway cloud registry server from anyplace. The essential gain of cloud registry is its universalclient access and potentially un-limited data storehouse abilities.

A.Ibrahim et al., (2016) [3], Healthcare providers utilize Electronic Health Records (EHRs) scheme for the many advantages it offers. Distribution of EHRs among various health-care providers has turned into a fascinating subject, and Cloud Computing provides the best medium for such a distri-bution and assistance due to its scalability as well as availability.

L.A.Tawalbeh etal.,(2018) [4], The concept of Cloud Computing (CC)depends on a shared interconnected chain of resources to boost resource availability and lessencommercial and administrative costs.

M.Shanmugam et al.,(2017) [5], With the aim of remaining competent, the cloud owners find alter-nate ways of providing numerous cloud services at an affordable cost, indirectly paving way for re-source depletion. The next main threat in this type of cloud setup is data lock-in (i.e.) when the pro-vider company chooses to lock-in his/her cloud assistance, the cloud users will be compelled to transfer their information to a different medium.

L. Liu et al., (2015) [6], For safeguarding confidential clinical information, encryption of delicate information is necessary before being passed to the cloud storage. This safety mechanism makes it more difficult to access information over the cloud. To improve the usage of these encrypted information, various encryption exploration approaches are considered.

As health care is completely migrating towards Cloud based systems, along with the numerous advantages several risks are also associated with it in spite of the many precautions taken.

2. STUDY MECHANISMS

2.1 KEY CHALLENGES

The most prevalent hurdles identified in Cloud based Health Care are:

1. Uncertainty in Data Security and Privacy Protection: Electronic Health Records are said to carry sensitive information about a patient's medical history, which is aabsolute priority and relevance in Health Care. Frequent issues like data breeches, loss of data and inconsistent data updates are causes of uncertainty in data security and privacy protection.

2.Governance or Control: Cloud infrastructure should follow certain guidelines pertaining to storage, updation and maintenance of health information. Because Cloud is governed by a third party at a remote place, concerns raise in the control of data.

3. Reluctant Data Standards: ThoughHealth Care has become more portable, traditional health care providers are reluctant to share data. Also, with the participation of many entities a common management control is becoming more difficult in terms of service level agreement that do not match the client's requirements.

4.Compliance: Finally, there is always an uncertainty of the provider meeting compliance norms like: Standards, Contracts, Policy Changes, Guidelines and Regulations set up by the concerned government.

2.2 COMMON SOLUTIONS AVAILABLE

1.Integrity: It is the responsibility of the Cloudproviders to ensure that data shared is in the same form as its saved form so that data is neither corrupted nor illegally edited. To ensure this data is encrypted and several cryptographic algorithms are used for the same.

2.Infrastructure Security : Clouds should be run by certain protocols, policy statements and constructive measures. Robust infrastructure is seldom subject to hacking and vulnerabilities. This is a group initiative and cannot be followed by a single provider.

3.Storage Management: Continuous data updates, audit logs of each data access are done by a secure and continuous interface for the maintaining data. Information shared or exchanged obey the laws of Health Regulatory Authority in the local jurisdiction.

4.Service - level Agreement: Many Service- level Agreement (SLA) are reached between the Cloud Providers, Health Care Organizations and various service providers in the network so as to provide a free passage of data.

2.3 RESEARCH QUERY

1.Does the paper resolve Data Integrity Challenges?
2.Is Infrastructure Security Considered?
3.Are Audit Logs and Management Control
Guaranteed?
4.Are Service Level Agreements followed?

2.4 RESEARCH METHOD

In this paperaorganized study to examine the security threats in cloud computing was carried out. The main focus was on security and privacy challenges related to cloud healthcare together with the existing implementations for a safe Health Care with ancoordinated review of 100research journalspresented between 2015 and 2020 out of which 50 journals were selected.Finally analysis curtailed to only 34journal papers, because they were found to be more relevant to the research considerations and also reviewing all the papers was not practically possible. The journals that were taken into consideration are: IEEE, Science Direct, Springer and other Scopus Journals.

2.5 FOUNDATION FOR PAPER COLLECTIONAND EVALUATION

Key words: Reviewed research articlesconsist ofthekeywords relevant to the review.

Date of publication: The research articles publishedbetween 2015 and 2020 are examined.

Type of Study: This review article has methodicallyreviewed only research papers and review articles related to the research problem and other sources were not taken into discussion.

Language of Study: Only research papers published in English were reviewed

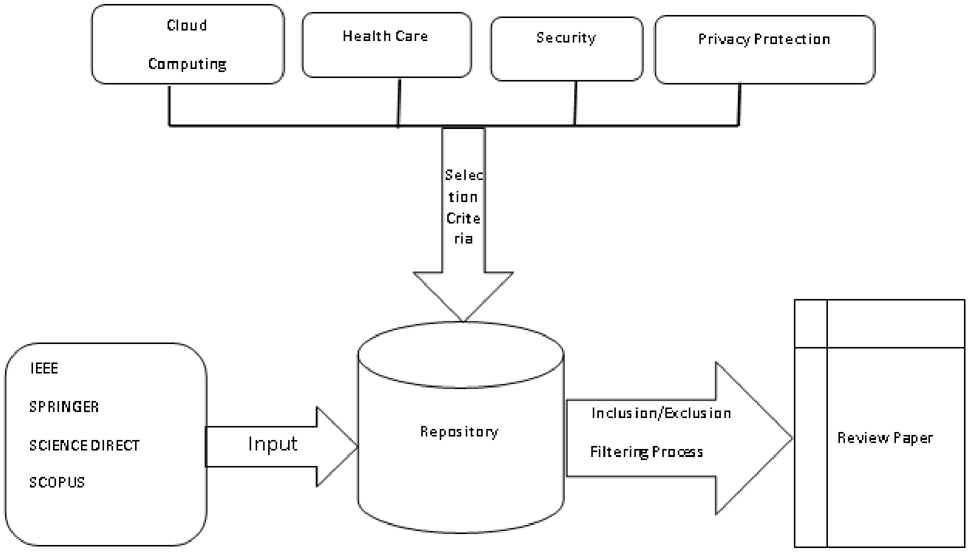

Figure 1:Review Paper Selection Process

3.DISCUSSION

3.1 Research Query 1:

C.Xu et al., (2019) [7], proposed a new privacy protecting electronic health records distribution method, that allowed entry as well as exploration of Personal Health Information (PHI) documents safely and effectively by HSPs. Searching and en-crypting techniques with keyword scope along with multi-keyword searching are used. This sug-gested privacy protection identity check protocol allowed various kinds of numerical correlation searching over encoded information. Likewise, an alternate of Bloom Filter, notice verification code for classifying of PHI records and filtering fake information, as well as checking authenticity of explored conclusions are taken into consideration.

Mayank Kumar Kundalwal et al., (2019) [8], recommended a hybrid approach that features two various interpretation management techniques: question set -size restraint along with k-anonymity that monitored individual confidentiality. The question set-size restraint is employed to prevent sensitive information against suspicion invasion, the k-anonymity is enforced to shield info from associating invasions. Together the suggested techniques achieve an explicit confidentiality alongside satisfactory info usage. A rule set is generated which will increase the privacy of health-care data.

D.C. Nguyen et al., (2019) [9], proposed an innovative EHRs sharing schema which combined blockchain along with a decentralized interplanetary file system (IPFS) over a mobile cloud medium. Notably, a dependable entry regulatory method layout that uses smart agreements to guarantee safe EHRs distribution across various clients and health care regulators were suggested. Simulation application applying Ethereum- blockchain in ac-tual information distribution scheme over a portable application with Amazon cloud - computing is suggested.

J.Liu et al., (2019) [10], suggested a lightweight together with privacy-preserving medicinal assistance access schema relying on multi-authority ABS for health-care clouds called LPP-MSA. According to this schema, MSRs may gain entry to private health assistance with only partial disclosing of his/her integrity info.

Abdullah Al Omara et al., (2019) [11], presented a patient pivotal health-care information administration arrangement, that used blockchains technique for stocking thereby aiding confidentiality. Cryptographed operations help to encode patient’s information as well as satisfy anonymity. Also, information preparing measures as well as the price efficiency of the smart-contracts utilized in the proposed structure are evaluated.

P.K.Maganti et al ., (2019) [13], various cryptosystems were studied that provides guarantee to all health documents that are static as well as dynamic. Also, a new secure mobile healthcare application was suggested that has IBBE schema. In this schema, the patient selects specialist of his/her decision, then encodes the electronic reports and transfers it to the cloud, this information can only be decoded by the entitled specialists. Added to this, in order to gain entry rights secure CP-ABPRE and close-grained techniques is made use of. At the receiving end, the doctor will set up a decoded key and the intermediate server will execute a de-cryption. By doing so, the end-user will be relieved from the computational overload. The de-cryption can also be carried out by an expert fulfilling the characteristics.

ShaoanXie et al., (2020) [19], surveyed the latest developments in block-chain techniques that bestowed opportunities to override the drawbacks of cloudexchange. In spite of this, the combination of blockchain with cloud-exchange continues to be in starting stages and indepth analysis attempts are required that can override various experi-mental demands.

H.Zhang et al., (2018) [26],proposed a unique cloud storage system for EHRs that absolutely ensured the information protection using the Shamir's Secret Sharing. According to the stated sharing, a particular EHR was divided into various sections by a health-care society, and thereafter these sections were shared via various cloud helpers. After restoring the EHRs, the health-care cloud protects sections from limited cloud-servers, then initiate recreating EHRs.

A.N.Vinodhini et al., (2017) [27], suggested a Minutiae Map (MM) design implementation for the handling of finger print established verification. In this design, users kept personal files that are saved in the open free multiple cloud stacks like Drop-box, Cloud Me and applying the dual technique of dividing and conbining techniques. RC4 algorithm was employed to boost the security in cloud-based environments. The techniques were: Crosssite - request forgery (CSRF), Crosssite - scripting (XSS) prevention.

N.S. Kumar et al., (2017) [28], storing of the unorganized infowithin the cloud by usage of an efficient directorycalled the MongoDB, that is a type of NoSQL was proposed. Enforcement of dual mode safety for each verification, retrieving of information from the records are strictly followed.

S.J..Nadaf etal., (2016) [29], Privacy protectioninformationrepository by encryption of the information at the customerahead of saving information on a distant cloud- server is emphasized. AES algorithm for encryption and decryption utility is selected. AsAES is a symmetric key encryption the same key was used for encryption and decryption purpose. In addition, keyword-search method to scanthrough encrypted file was done. The important maintenance issue isresolved by distributingprivate key to enduser's mail.

AqeelSahiet al., (2016) [30], suggested three com-pletely different approaches: Security-Preserving approach, Privacy - Preserving approach, and Disaster-Recovery plan approach. The Security-Preserving approach is a powerful way of enabling the safety and purity of Electronic Health Records, and the Privacy-Preserving approach being a ca-pable verification scheme which protects the privacy of Personal Health documents. The combined methods along with Disaster-Recovery plan approach ensures accountability as well as safety related to the cloud model.

P.Pace et al., (2019) [33], proposed *BodyEdge*, a new model applicable for humanity based applications, in the relation to the evolving healthcare sector. A mini mobile client segment and an oper-ating Edge gateway aiding Multi-Radio and Multi-Technologyconnection to gather and narrowly process information returning from various schemes are suggested. Moreover, it also utilizes the efficiency made possible by both private and public Cloud medium thereby ensuring a improved extensible, durable and flexible service levels.

J. Zhou et al., (2015) [34], suggested a safe and effective privacy-protecting lively therapeutic text mining and image feature extraction scheme PPDM in cloud-assisted e-healthcare systems.

3.2 Research Query 2:

G.Yang et al.,(2018) [14], formulated a block-chainbaseplanning for electronic health-record (EHR) systems. The design model was constructed to utilize existing databases managed by health providers and implements a block-chain solution to improvise interchange of the existing EHR systems, avoid damageand suspicious misapply of EHRs by means of tracing all transactions in the database.It also introduced a new stimulus method for the creation of new blocks in the block-chain. The architecture is independent of any specific block-chain platforms and are applicable to further updates.

YefengRuan et al., (2019) [18], built a novel security-based measure of trustability (trust–reliability) along with an advanced method to determine it. Trustability quantifies how much a framework can be relied under a particular attack direction. Likewise, the method could be utilized to investigate the pattern space of source structure in order to select the exact contract amidst reliability and cost of reoccurrence. Depending on, the actual-time trust report, cloud authority can transfer load from doubtful hubs to reliable hubs, progressively allot a reserve, and deal with the exchange off between the level of repetition and the expense of the reserve.

A.Mehmood et al.,(2018) [22], proposed a new validation method .For this, a rotating group signature structure based on Elliptic-Curve Crypto method (ECC) to give invisibility to the patients is used. To add an additional layer of security, the Onion Router (TOR) was included to give protection at the networks layer.

S.Roy et al., (2019) [23], proposed a different design which gives a consolidated methodology of fine-grained entry authority over cloud based multi-server records alongside a provably portable client validation tool for the Health-care sector 4.0.

L.Selvam et al., (2018) [24], utilized improved Attribute-Based Encrypting (ABE) techniques. Fine-grained data gathers the privilege of access to control is ensured on un-confided servers. In these design schemes, the information holders are responsible for encoding the information before transfer or downloading them on the cloud and furthermore second encryption is done when there is an adjustment in customer accreditations.

M.Marwan et al., (2016) [31], designed an approach based on Secure Multi-Party Computation (SMC) protocol approach to guarantee protection and safeguarding of the collective frameworks. Various systems collaborate together to achieve shared objectives without permitting any individual to see and uncover another person's unique information. A system design dependent on SMC for security safeguarding collective settings in the health-service segment was proposed. The recommended result is based on the Paillier method to provide data safety. This is guaranteed by making use of the additive homomorphic property of this public key cryptosystem.

3.3 Research Query 3:

C.Esposito et.al., (2018) [15], examined the capability to use the Blockchain technology to preserve health-care information hosted within the cloud. The study also dealt with the practical threats of such a proposition and further research that is needed.

S.Sharaf et.al., (2019) [16], proposed a safe, effec-tive structure for the public Electronic Health Records framework, in which fine-grained right of entry was utilized depending on Multi-Authority Ciphertext ABE called the CP-ABE, along with a hierarchal system, to authorize right of entry protocols. The recommended model will be able to allow authorized persons in the Government of Saudi Arabia to set up the health-care services and take advantage of the current e-government cloud-based computing medium ―Yasser, which is in charge of providing distributed service through a profoundly able, dependable, and safe condition. This structure intends to provide health-related support and provisions from the Government-to-citizens (G2C).

I.Singh et al., (2019)[17], presented a design for e-Healthcare structured governance. In this, details of the concerned person's info is recorded in a focal datastore. The concerned government collaborates with health care organizations and experts to build a successful medical framework.

H.Liu et al., (2019) [20], a collaborative confidentiality preserving plan was intended for wearable machines with identification approval and entry control of information study in the space-aware and time-aware techniques. In the space-aware edge-computing technique, anonymous and Min-Hash related confirmation is deployed to upgrade privacypreservation and similarity computations without advertising unique information.

M.K.Kundalwal et al., (2018) [21], proposed a privacy ensured structure that manages the data-privacy and authenticity. Also, it makes sure only particular individuals have entry to their respective health related information. Apart from that, it also overrides the privacy challenges and also manages a safe healthcare structure.

J.Park et al., (2018) [25], introduced models for trustworthy datainterpretation in the efficient decision of health-care cure. For this, a blockchain structure for gathering records, which is characterized by stability was devised. Secondly, a crypto-currency based compensation model on the role of new research titles and data improvement to acti-vate un-interrupted participation was also introduced. Lastly, an architectural design for web based services was also developed..

3.4 Research Query 4:

Josep Domingo-Ferrer et al., (2019) [12], conducted a survey of the prevailing security and privacy- enabling solutions focusing on cloud, with empha-sis on those that protect cloud service perfor-mances, such as the capability to redistribute en-quiries and metrics on reserved data towards the cloud.

Dr. Sunil Bhutada et al., (2018) [32], due to multi-tenancy, there are many privacy and security problems with health-related data. A systematic model for multi-tenancy and health care process is created[35,36] and role-based access are provided to the users. Amazon simple storage service (Amazon S3) was used to store the records. As access to respective records for the respective roles are pro-vided, this resolves the security-related issues that are caused due to multi-tenancy by providing access control[37,38].

Table 1. Summary of Reviewed Articles with Significant Investigation Issues

S. No	Ci-ta-tion	Research Contributor	Year	Research Title	Queries			
					Q1	Q 2	Q 3	Q 4
1	[7]	C.Xu et al	2019	Achieving Searchable and Privacy-Preserving Data Sharing for Cloud-Assisted E-Healthcare System	Y	N	N	N
2	[8]	Mayank Kumar Kundalwal et al	2019	An improved privacy preservation technique in health-cloud	Y	Y	N	N
3	[9]	D.C. Nguyen et al	2019	Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems	Y	Y	N	N
4	[10]	J. Liu et al	2019	Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud	Y	N	N	N

5	[11]	Abdullah Al Omar et al	2019	Privacy-friendly platform for healthcare data in cloud based on blockchain environment	Y	Y	N	N
6	[12]	Josep Domingo-Ferrer et al	2019	Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges	Y	Y	Y	Y
7	[13]	P.K.Maganti et al	2019	Secure Application for Sharing Health Records using Identity and Attribute based Cryptosystems in Cloud Environment	Y	Y	N	N
8	[14]	G.Yang et al	2018	A Design of Blockchain-Based Architecture for the Security of Electronic Health Record (EHR) Systems	Y	Y	Y	N
9	[15]	C.Espositio et al	2018	Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?	Y	Y	Y	N
10	[16]	S.Sharaf et al	2019	A Secure G-Cloud-Based Framework for Government Healthcare Services	Y	Y	Y	N
11	[17]	I.Singh et al	2019	Improving The Efficiency of E-Healthcare System Based on Cloud	Y	Y	Y	N
12	[18]	YefengRuan et al	2019	A trust management framework for clouds	Y	Y	Y	N
13	[19]	ShaoanXie et al	2020	Blockchain for cloud exchange: A Survey	Y	Y	Y	N
14	[20]	H.Liu et al	2019	Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-Based Smart Health	Y	Y	Y	N
15	[21]	M.K.Kundalwal et al	2018	A Privacy Framework in Cloud Computing for Healthcare Data	Y	Y	N	N
16	[22]	A.Mehmood et al	2018	Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications	Y	Y	N	N
17	[23]	S.Royet al	2019	Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Serversin Mobile Cloud Computing Based Healthcare Applications	Y	Y	N	N
18	[24]	L. Selvam et al	2018	Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained and Enhanced Attribute-Based Encryption	Y	Y	N	N
19	[25]	J.Park et al	2018	CORUS:Blockchain-Based Trustworthy Evaluation System for Efficiacy of Healthcare Remedies	Y	Y	Y	N
20	[26]	H.Zhang et al	2018	Cloud Storage for Electronic Health Records Based on Secret Sharing With Verifiable Reconstruction Outsourcing	Y	Y	N	N

21	[27]	A.N. Vinodhini et al	2017	Prevention of personal data in cloud computing using bio-metric	Y	N	N	N
22	[28]	N.S. Kumar et al	2017	Secured Repertory of Patient Information in Cloud	Y	N	N	N
23	[29]	S.J..Nadaf et al	2016	Cloud based privacy preserving secure health data storage and retrieval system	Y	N	N	N
24	[30]	Aqeel Sahiet al	2016	Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan	Y	N	N	N
25	[31]	M.Marwan et al	2016	Applying Secure Multi-Party Computation to Improve Collaboration in Healthcare Cloud	Y	Y	N	N
26	[32]	Dr. Sunil Bhutada et al	2018	Access Control for Multi-Tenancy in Cloud-Based Health Information Systems	Y	N	Y	Y
27	[33]	P.Paceet al	2019	An Edge-Based Architecture to Support Efficient Applications for Healthcare Industry 4.0	Y	N	N	N
28	[34]	J. Zhouet al	2015	PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems	Y	Y	N	N

Y-Accounted, N- Not Accounted

4. CONCLUSION

From the above systematic review, it is obvious that data security is the primary cause of concern for cloud based Electronic Health Records and almost all of the reference papers concentrate on providing safe and secure data transfer along with the aim of privacy guarantees for preserving personal information. Because cloud is hosted over the internet via a third party vendor, case of data breeches, loss of data and hacking are very common. Several cryptographic algorithms and robust frameworks have been suggested that can improve data mobility and store data without being compromised.Secondly, it is observed that protecting sensitive information of medical records, in Cloud based Healthcare system is a collaborative effort of all the participating entities like physicians, cloud providers, Government Organizations, Health care professionals and organizations. Each one of the entities is equally responsible to assure data integrity, data-security and privacy-preservation. Added to this a number of things has been discussed and evaluated about compliance standards and effective infrastructure and service level agreements. As cloud is expanding so is the scope of research on Cloud based Health Care has increased.

4.1 RECOMMENDATIONS

From the above discussion it is inferred that though a lot of attention is given to build a robust framework for ensuring security in Electronic Health Records(EHRs) there is always a setback in providing the same. Also, for interoperability to be fruitful, more responsibilities should be given to each role in the system.

The following recommendations hold good for data integrity, infrastructure security and Privacy Preservation schemes:

(I).Robust framework for ensuring infrastructure security, such that the cloud is less vulnerable to cyber-attacks.

(II).Having common agreement protocols between various service providers to safeguard data and privacy.
(III).Adoption of authentication schemes and strong license agreements with time stamps.
(IV).Clean and appropriate architecture for Cloud EHR mobility.
(V)Distinction of data security protocols and Cloud applications.

4.1.1 RECOMMENDATIONS FOR FUTURE WORK

(I).Guarantee efficient, secure and robust virtual clouds.
(II). Ensure common service level agreements between various vendors.
(III). Periodical check and renewal of cryptographic algorithms, policies etc.
(IV). Define clear cut roles and responsibilities to all.

REFERENCES

1. T. Muhammed, R. Mehmood, A. Albeshri and I. Katib, "UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities", in IEEE Access, vol. 6, pp. 32258-32285, 2018
2. R. Shende, S. Kamble and S. Kakde, "Health data access in cloud-assisted e-healthcare system", International Conference & Workshop on Electronics & Telecommunication Engineering (ICWET 2016), Mumbai, 2016, pp.169-173
3. A. Ibrahim, B. Mahmood and M. Singhal, "A secure framework for sharing Electronic Health Records over Clouds", 2016 IEEE International Conference on Serious Games and Applications for Health (SeGAH), Orlando, FL, 2016, pp. 1-8
4. L. A. Tawalbeh and S. Habeeb, "An Integrated Cloud Based Healthcare System", 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, Valencia, 2018, pp. 268-273
5. M. Shanmugam and M. Singh, "A comparitive study on traditonal healthcare system and present healthcare system using cloud computing and big data", 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, 2017, pp. 269-273
6. Lu Liu, Jingchao Sun, Jianqiang Li, Rong Li, Juan Li, Xi Meng, Huifang Li, Jijiang Yang, "A Privacy Enhanced Search Approach for Cloud-Based Medical Data Sharing", 2015, IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, 2015, pp. 1032-1037
7. C. Xu, N. Wang, L. Zhu, K. Sharif and C. Zhang, "Achieving Searchable and Privacy-Preserving Data Sharing for Cloud-Assisted E-Healthcare System", in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8345-8356, Oct. 2019
8. Mayank Kumar Kundalwal, Kakali Chatterjee, Ashish Singh, "An improved privacy preservation technique in health-cloud", ICT Express (2019),Volume 5,Issue 3,September 2019, Pages 167-172
9. D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems",in *IEEE Access*, vol. 7, pp. 66792-66806, 2019
10. J. Liu, H. Tang, R. Sun, X. Du and M. Guizani, "Lightweight and Privacy-Preserving Medical Services Accessfor Healthcare Cloud", in IEEE Access, vol. 7, pp. 106951-106961, 2019
11. Abdullah Al Omar,MdZakirulAlam Bhuiyan, Anirban Basu,Shinsaku Kiyomoto,Mohammad Shahriar Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain

environment", Elsevier, Future Generation Computer Systems Volume 95, June 2019, Pages 511-521

12. Josep Domingo-Ferrer, Oriol Farràs, Jordi Ribes-González, David Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges", Computer Communications 140–141,May 2019Pages 38–60.
13. P. K. Maganti and P. M. Chouragade, "Secure Application for Sharing Health Records using Identity and Attribute based Cryptosystems in Cloud Environment",20193rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 220-223
14. G. Yang and C. Li, "A Design of Blockchain-Based Architecture for the Security of Electronic Health Record (EHR) Systems", 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia, 2018, pp. 261-265
15. C. Esposito, A. De Santis, G. Tortora, H. Chang and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" in IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018
16. S.Sharaf and N. F. Shilbayeh, "A Secure G-Cloud-Based Framework for Government Healthcare Services", in IEEE Access, vol. 7, pp. 37876-37882, 2019
17. I. Singh, D. Kumar and S. K. Khatri, "Improving The Efficiency of E-Healthcare System Based on Cloud", 2019, Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 930-933
18. YefengRuan, Arjan Durresi, "A trust management framework for clouds", Elseiver, Computer Communications, Volume 144, 15 August 2019, Pages 124-131
19. ShaoanXie, Zibin Zheng, Weili Chen, Jiajing Wu, Hong-Ning Dai, Muhammad Imran, "Blockchain for cloud exchange: A Survey", Elseiver, Computers & Electrical Engineering, Volume 81, January 2020, 106526
20. H. Liu, X. Yao, T. Yang and H. Ning, "Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-Based Smart Health", in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1352-1362, April 2019
21. M. K. Kundalwal, A. Singh and K. Chatterjee, "A Privacy Framework in Cloud Computing for Healthcare Data",2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida (UP), India, 2018, pp. 58-63
22. A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston and Y. Zhang, "Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications", in IEEE Access, vol. 6, pp. 33552-33567, 2018
23. S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay and J. J. P. C. Rodrigues, "Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications", in IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 457-468, Jan. 2019
24. L. Selvam, R. J. Arokia, "Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained and Enhanced Attribute-Based Encryption", 2018 IEEE International Conference on Current Trends toward Converging Technologies (ICCTCT), Coimbatore 2018, pp.1-6
25. J. Park, S. Park, K. Kim and D. Lee, "CORUS: Blockchain-Based Trustworthy Evaluation System for Efficacy of Healthcare Remedies", 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia, 2018, pp. 181-184
26. H. Zhang, J. Yu, C. Tian, P. Zhao, G. Xu and J. Lin, "Cloud Storage for Electronic Health Records Based on Secret Sharing With Verifiable Reconstruction Outsourcing", in IEEE Access, vol. 6, pp. 40713-40722, 2018
27. A. N. Vinodhini and S. Ayyasamy, "Prevention of personal data in cloud computing using biometric", 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT), Coimbatore, 2017, pp. 1-6

28. N. S. Kumar, P. Harini, G. D. Kumar and G. Rathi, “Secured repertory of patient information in cloud”, 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, 2017, pp. 1-4
29. S. J. Nadaf and R. Patil, “Cloud based privacy preserving secure health data storage and retrieval system”, 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, 2016, pp. 1-6
30. AqeelSahi, David Lai,Yan Li, “Security andprivacypreservingapproachesintheeHealthcloudswith disasterrecoveryplan”,Elseiver, Computers in Biology and Medicine, Volume 78, November 2016, Pages1-8
31. M. Marwan, A. Kartit and H. Ouahmane, “Applying secure multi-party computation to improve collaboration in healthcare cloud”, 2016 Third International Conference on Systems of Collaboration (SysCo), Casablanca, 2016, pp. 1-6
32. Dr. Sunil Bhutada, T.Ramakrishna Reddy, S.Shabarish, YaramAnuja,“Access Control for Multi-Tenancy in Cloud-BasedHealth Information Systems”,Volume 6 Issue IV, April 2018,IJRASET.
33. P. Pace, G. Aloi, R. Gravina, G. Caliciuri, G. Fortino and A. Liotta, “An Edge-Based Architecture to Support Efficient Applications for Healthcare Industry 4.0”, in IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 481-489, Jan. 2019
34. J. Zhou, Z. Cao, X. Dong and X. Lin, “PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems”, in IEEE Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp. 1332-1344, Oct. 2015
35. A.Vidhyalakshmi and Dr.C.Priya, “A Study on Supervised Learning in Medical Image Grading using IoT, International Journal of Recent Technology and Engineering, ISSN:2277-3878, Vol 7, Issue 5C, 274-79, Feb 2019
36. Dr.C.Priya, “TAAS: Trust Management Model for Cloud-based on QoS”, Journal of Advanced Research in dynamical and Control Systems, Vol 9,1336-45, Sep 2017
37. Dr.C.Priya, et.al., “Trusted Cloud Computing Platform in IaaS for Closed Box Execution Environment to VM, Journal of Advanced Research in dynamical and Control Systems, Vol 10,193-8, Nov 2018
38. R.Cristin,B.Santhosh Kumar,C.Priya,K.Karthik,”Deep Neural network based rider-Cuckoo Search Algorithm for plant disease detection”, Artificial Intelligence Review, feb 2020, https://doi.org/10.1007/s10462-020-09813-w