Research on E-healthcare Security Evaluation in Cloud-Based System

Gopichand G, Kohinoor Jain, Shashwat Kumar Dev

Abstract—As healthcare adopts electronic methods of storing patient health records, cloud technology allows mining and analyzing this data and accessing the general public health information. Patient's privacy and security of personal information is crucial when considering using electronic health records in the healthcare industry (E-Healthcare). The need of the hour is to be able to store and recover patient's data efficiently. However, moving patient's medical information to the Cloud involves major security risks and destructs robust data privacy of health records. The threat of data breaches and the need to manage huge amounts of data are issues that have affected the healthcare industry for years. The privacy issues and threats faced by E-healthcare systems include network attacks and threats to hosts and unsanctioned access to EHR records. The major EHR system functions such as appointment scheduling, dietary planning, admission and discharge, transfer radiology/lab orders and prescription order entry are vulnerable to security threats. Security issues need to be assessed thoroughly in order for hospitals and other such medical institutions to shift to electronic standards of maintaining patient's data.

Before moving to a cloud-based architecture, health organizations should perform a risk assessment. This will help to identify the security measures required to mitigate these risks. This approach provides a valid assessment of the security risk management procedure approved by field experts. It not only identifies threats to E-healthcare but also allows for a structured flow in risk management. The risk management process is documented and reported in an efficient and easy way for concerned stakeholders of the E-healthcare to understand. It will compare existing solutions on how to protect the confidentiality of patient information. Some of these methods include implementation of a Role-Based Access Control (RBAC) model, digital encryption and signature for cloud security and EHR service continuity management. Moreover, it will consider security matters that CSP's should look into while storing patient's record. Ultimately, it will come up with the most suitable solution to make E-Healthcare systems more secure. In this paper, the focus will be on identifying security encounters that E-health systems face by discussing means in which these systems are susceptible to attacks.

KEYWORDS: Efficiency; Robust; Confidentiality; RBAC; Digital Encryption

I. INTRODUCTION

The term e-Health is meant for communication, sharing and removal of health information.Some papers discuss how electronic health records indirectly influence HIT's, which stands for Healthcare Information Technology [1].

Revised Version Manuscript Received on 10, September 2019.

Gopichand G, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India.(Email: gopichand.g@vit.ac.in)

Kohinoor Jain, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India.

Shashwat Kumar Dev, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India.

Stakeholders' expectations have changed regarding how patient's information should be processed and accessed [2]. EHR plays a major role in this context. Storing information on paper is highly inefficient and just increases storage andrecovery complexity. Thus, EHR's should be used as they can be recovered anywhere, anytime[3].

EHR services are simplified with cloud computing services. Though cloud-based systems bring one of the most demanded thing on the table, flexibility, there are still several areas of improvement. The reason cloud-based systems should be implemented is because any medical institution can share patient's information instantly amongst themselves, wherever they might be located. [4] The only precautions one must take into consideration when deploying a cloud-based is the privacy and security against threats.

Maintaining online security is extremely important. Security administrators working in the IT department must be trained to be able to handle the kind of threats encountered. There is continuous growth of data breaches in healthcare over the last 2–3 years, which is the reason that promptedthisresearch[5].Theexistingmethodsandtechnology beingusedtosolvecybersecurity threatsandcrisisneedtobeanalysedindetail.Attackershavewidenedtheirscopeofattacks.The need for improvement of existing solutions and using latest and trending technologies to provide solutions that are more sophisticated would only be clearer after a proper analysis into this [6]; which this paper aims toprovide.

Cloud computing is defined as using resources over a secure network provided by a network service [7]. Users now have the capability to store, retrieve their data on the go, wherever they need to access it, if their service providers have that range. An organization called Cloud Security Alliance [8] mention several important threats and breaches of data to cloudplatforms which miscreants target themost.

Even with the various benefits of E-healthcare, the platforms vulnerability is primarily based on its usage. The discordancy between different databases remain a threat to assimilate records [9]. The majority of the population happens to be uneducated on privacy of medical records, and it is thislackofeducationthatcreatesaflawinthecloud-baseddesign[10].It isthenuptotheservice providers to secure patient's data, as a vast majority would not be aware of their health records being tampered with and will easily become a victim of misuse of their private data [11]. Human DNA information is private and must be secure, this is also a major concern [12]. Thus, securing cloud data is of utmostimportance.

To decide the future work and input required for E-healthcare security, a detailed analysis of existing methods is required. Through this paper, we aim to identify threats to healthcare online services by discussing the threats posed to them and we shall give our evaluation of existing methods to counter these attacks as well as our own solution if needed. After reviewing existing research, this paper seeks to discuss the most prominent security techniques for healthcare organizations. The intent is to identify the most efficient method as an opportunity for industry- wide efforts to secure data for its patients.

II. RELATED WORK

In 2017, Muhammad Ehsan Rana [13]. discussed various access control models, their merits, limitations,androlestopromoteprivacyincloud-basedsolutions .Mostsuitablemodelformilitary andgovernmentorganizations.ApplicationsofmodelsofRBAC incloud basedEHRsystemsare discussed.

FloydandLeizel[14]focusedtheirworkoninvestigatingsecurity measuresthatmedicalpersonnel shouldtakeintoconsiderationtoprotectpersonalEHRswhileaccessingfromsmartphones.Three uniquethreatstothedatasecuritywereindicatedwhichcontainstheuser,infointransit,andstored data.M-healthsecurityframeworkwastakenintoaccounttogive 10measuresthatcanbeusedto indicatehowthesedataprivacythreatscouldbehandledbythehealthcareprovidersandpatient.it is concluded that both of them should contribute in providing and increasing privacy in thehealth records and also data in transit should be wellprotected.

Patience and Mary (2016) [15] recognized threats in the health records system, by identifying vulnerabilitiesofthesystemandareaswhicharepronetoattack.Various solutionswerediscussed by comparing journals and articles on unauthorized entry in PEHR. The paper also provided its own solution and compared efficiency of the proposed solution with existingones.

In 2017, Vaikunth Pai T released a paper on Cloud Computing Security Issues – Challenges and Opportunities[16]whereinfirstadvantagesofthecloudstorageareshownwhichincludesstorage facility, efficiency, easy data retrieval, elasticity, atomicity etc. in this model third party cloud service providers owns the infrastructure and customers/patient use theirservices. A solution model is proposed using data fragmentation without much overhead.

Prerna and parul [17] discussed encryption method to add security in the cloud. Symmetric and non-symmetric keys are discussed, their advantages and disadvantages and a new encryption technique is proposed. Its efficiency is tested and results are shown.it also talks about the limitations of encryption method.

Yaw Marfo Missah [18] discussed the advantages of moving paper based records to cloud based data storage facility. It also provides guidelines and precautions to be taken care of while moving records. They did a case study on an eye-hospital, interviewed medical personnel regarding the challenges they face in handling the data. Techniques such as action research and appreciative inquiry were used in interviews.it helped them to get an overview and define scope of EMR and know the expectations of EMR system.

III. CASE STUDY MODEL

In this paper, a case study-based model is implemented. Our ultimately goal is toprovide a solution to the problems mentioned above in this paper and look into the various ways that exist for implementing security measures for threats. In addition, it will help to understandhowitwillbebeneficialforthecloudserviceproviders .Inordertoimplement this,wehavereviewedsomeresearchpapersandtriedtoidentifywhichmethodsaremost suitable for security implementation. We aim to propose our own combined solution of thefollowingexistingsolutions,andplantoproposeourownsolutioniftheexistingones are not upto themark.

Case Study 1

MinkyuChoi,byusingCloudTechnology[19],aimsatprovidingbiometricasasolution to healthcare security. Two leading process in this will be identification and authentication.Methodthroughwhichthepatientsrecognizetheirindividualitybygiving ausernameisidentificationi.e.someparticulartypeofidentityandauthentication.The process of confirmation or checking to get assured that the patient is authentic. Three authentication factors are passwords, token device, and badge. The third pertains to biometrics which is the most reliable in the fact that most organizations still battle to providesecurepasswordstrategiesandifbadgesoranytypeoftokensareused,thenthey are generally lost by the users. To provide Access control, different mechanisms can be used such as recognition of voice and face which only needs a normal camera and recognition software. USB sticks can be integrated with biometric access control. Hard drives can also be used for access control and for encryption using in-builtalgorithms.

ImprovementtoEHRinformationsecurityiseasedbyuseofbiometrictech.Utilizingthe cloud technology for better security, and the biometric methods for patient's authentication, will fortify the security on getting to EHR on the web. Therapeutic specialists from various human services offices can get to this data on the web. Enlisted client can get these records by biometric techniques. Verification will be done through database. Records can be protected and redundancy can be removed. Likewise, Doctors and patients will be distinguished after getting to such records. There is a positive future for security in healthcare by using Cloud technology also it gives efficient way to exchange information on the web.

Case Study 2

Iuliana Chiuchisan [20], presented an outline of security threats and proposed various actions to be implemented:

Signature and authentication on the web:

This system can be accessible through internet through access control mechanisms such as RBAC. Through various methods such as encryption and cryptography, client/user security can be guaranted; and this will be utilized to avert threats to the network.

Secure file transfer:

Network protocols such as FTPS is implemented to resolve privacy issues encountered while while transferring Patient records to the cloud.

Securing Database:

Open source databases such as Maria DB is used for securing data online. This database provides encryption techniques which makes it difficult for accessing the old data by an illegal person. Encrytping data is made fairly easy via this method.

Arrangement of secure network:

Virtual Private Network (VPN) is the method which is already offering establishment of secure connection amongst two endpoints.

So in conclusion, the three critical principles suggested by paper which confirms privacy ofusers:encryptionisthebasisforsecuringalldatamovedtothecloud,insuringsecurity of storage over these networks; insuring authenticity; and digital verification techniques to access patient data.

Case Study 3

Another paper proposed some already existing techniques such as authentication and encryption. Other techniques proposed by this paper are [21]:

Data masking:

Thepurposeofthistechniqueistoprotecttherealdatawhilehavingafunctionalsubstitute for occasions when the actual data is not required. Masking changes delicate information withananonymousvalue.Sincemaskedvaueisn'tanauthenticencryptintechnique,there is no chance of retrieving original data from it. For live data anonymization, it is one of the most popular approach. Obscurity protects against relieving identity but failed to protect against detailed data revelation. A major advantage of this system is that the expense of verifying major information is diminished. Through proper masking techniques, security is ensured for cloud-basedplatforms.

Access control:

Accesscontrolwillsancionrightstodifferentusersofthesystembasedontheirclearance level. It gives approval to users to be able to access required patient's information in a limitedcapacity.Rolebasedaccesscontrolandattributebasedaccesscontrolaretwomost wellknownmodelsforEHR.Foruserstobeabletosharetheirdata overthecloud,certain keys shall be provided with repect to the cloud sharing policies [22]. There is some work that needs to be done on deciding how much contant someone may be able to elicit using a patient's uniquekey.

Monitoring and auditing:

Methodofcollectinginformationandobservingflawsinthenetworktofindtheintruders is what is involved in monitoring. Patient's records must be audited at regular intervals and should be accessible at any time. Network traffic should not prevent record retrieval and if any changes to the data are made, they must berecorded.

IV. RESULTS&DISCUSSION

Hereby, comparing all the aforementioned solutions, we have provided an effective overall solution on how to counter attacks on the network while transferring data to the cloud and how to keep it secure while on the cloud for easy and smooth access and recovery.

Table 1: Major required Security mechanisms

Requirements	Description
Authorized access	Identificationsystemneedstobeimplemented forthecloud service providers and patients registered under them. Identification has to be convenient among various bodies that have access to the user's data. A role based access control mechanism should be implemented to allow authorized users to access information based on theirroles.
Patient's consent	Patients should be able to allow/deny access to their health record information. A security mechanism must be constructed in case of an Emergency to allow access without patient's consent.
Secure Cloud- based Environment	The Cloud service provider (CSP) must providetechniques toensurenetworksecurity.Genericnetworksecuritythreats and attacks should behandled.
Audits	A register to store all accesses and updates made to the electronic health records of patients. Should be interoperable and should allow constant monitoring of accesses.
Archive Process	Aim is to archive patients HER for as long as possible. Unadvisable to delete records after a certain period of time.

Along with this, we also identified major threats to Cloud-Based EHR systems:

Traditional network threats:

Apart from securing the cloud platform, CSP's should guarantee against frequently encountered network attacks.

Table 2: Major security threats

Security Threats	Description of Usage
DDoS attacks (Distributed Denial ofService)	Techniquestocountersuchattacksareavailable inweb services.
MITM attacks (Man in theMiddle)	Secure Socket Layer (SSL) is used to mitigate such attacks as it provides server authentication.
Port Scanning	Violations of scanning unauthorized ports should be recorded and investigated.
IP Spoofing	Firewalls used to control traffic to avoid spoofing.

After reviewing existing solutions and techniques to improve cloud-based EHR security, a combination of the below stated solutions should be able to give maximum security to EHR database systems.

1. EHR security implemented by Role-Based Access Control (RBAC)Model

Patients, hospital representatives and even technicians of the Cloud service provider require the data of patients. For privacy, an RBAC model is required due to different access requirements to the patient information distributed between doctors and other technicalemployees.Tosolvethelevelofclearanceforaccess,ea chindividualshouldbe allotted with an ID number. These ID numbers will be segregated into groups andgroups will be granted access to parts of the patient's records depending on clearancelevel.

To demonstrate, to guarantee patient's privacy, we will give restricted access to CSP technicians; information sufficient for the management system to operate, whereas the patient and their respective doctor shall have full and unrestricted access to the health- care records.

2. EHR Network Security

When moving the patient's health record information to cloud, this data is beingexposed toexternalthreats.Therefore,measuresmustbetakentoensurese curityofcloudprovided byCSP's.

Securing cloud data with digital encryption is one such measure. **Cryptography** is a useful technique that promotes secure shared cloud services and ensures security outside oftheenvironment,whereinthereisnocontrolofdata.Encrypting datapriortouploadis beneficialasitisencryptedbeforemovingittocloudandcanbesou ndlydecryptedby authorized personnel with decryption keys. Digital Signatures primarily promote nonrepudiation; thus it is meant for authenticity verification only. It is necessary to use this technique in cloud data storage to avoid false transactions of data.

3. EHR Service Continuity Management

The CSP should be able to provide continued service. There is certain security related issues that must be taken into consideration to ensure the continuous functioning of the system. Medical centres may face **EHR downtime**, therefore resources must be in place for alternative access [23]. This could lead to a potential transition to manual documentation. To prevent this, following issues must be addressed:

- Aregionhasaclusterofdatasets.Therefore,automate dprocessesmustbeinplace to shift server traffic away from targetednetwork.
- Incident Response should be looked into.24/7/365 technical support must be offered.
- Periodic auditing carried out by an internal audit group is required to ensure continuity.

V. CONCLUSION

In this research paper, our aim was to identify the security threats to cloud-based EHR systems and propose viable solutions for the same. For this, we identified the major security risks to EHR, and shifting patient data to the cloud, which is one of the main reasons why people in the health field prefer not to shift data to the cloud. After this, we reviewed some existing solutions to these problems. Our first case study proposed a biometric system, which is mainly just identification and authorization. The second case study extended from the first one along with secure infrastructure and secure migration overthenetwork,whichincludesusingprotocolssuchasFTP's.w ecametotheconsensus thatnoneofthesolutionswereuptothemark.Lastbutnotleast,wec ameacrossasolution which proposed access control standards and data masking techniques. Although the above solutions we're viable, none of them were fully sufficient when considering them individually. Hence, we proposed a collection of the above solutions to be implemented as a whole. This includes an RBAC model for access control, digital encryption techniques for security over cloud transfer and monitoring and auditing techniques discussed under EHR service continuity management. This solution should be sufficient to counter most threats and issues to Cloud-Based EHR Systems.

REFERENCES

1 Tomines,A.,Readhead,H.,Readhead,A.,&Teutsch,S.(201 3).Applicationsofelectronic health information in public health: uses, opportunities & barriers. eGEMs,1(2).

2 Evans, R. S. (2016). Electronic health records: then, now, and in the future. Yearbook of medical informatics, 25(S 01),S48-S61.

3 Sahama, T., Simpson, L., & Lane, B. (2013, October). Security and Privacy in eHealth: Is it possible ?. In 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013) (pp. 249-253).IEEE.

4 Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronichealth record systems. Risk management and healthcare policy, 4,47.

5 Thomson, L. L. (2013). Healthcare data breaches and information security. In American Bar Association (pp.253-267).

6 Martin, C., & Leurent, H. (2017). Technology and Innovation for the Future of Production: Accelerating Value Creation. In World Economic Forum, Geneva Switzerland.

7 Chen,D.,&He,Y.(2010).Astudyonsecuredatastoragestrate gyincloudcomputing. Journal of Convergence Information Technology, 5(7),175-179.

8 Prakash, C., & Dasgupta, S. (2016, March). Cloud computing security analysis: Challenges and possible solutions. In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 54-57).IEEE.

9 Rudin, R. S., & Bates, D. W. (2013). Let the left hand know what the right is doing:a vision for care coordination and electronic health records. Journal of the American Medical Informatics Association, 21(1),13-16.

10 Habib, K., Torjusen, A., & Leister, W. (2015). Security analysis of a patient monitoring systemfortheInternetofThingsineHealth.InTheSeventhInt ernationalConferenceoneHealth, Telemedicine, and Social Medicine(eTELEMED).

11 Apreliminarystudyofacloud-computingmodelforchronicil lnessself-caresupport in an underdeveloped country. Piette JD, Mendoza-Avelares MO, Ganser M, Mohamed M, Marinec N, Krishnan Sam J Prev Med. 2011 Jun;40(6):629-32.
12 Santhi H, Gayathri P, Gopichand G, Venkata Vinod Kumar N, Sailaja G. (2019). A Scalable and Distributed Mechanism for DNA Databases by Aggregate Queries. International Journal of Innovative and Exploring Engineering(IJITEE), 8(6S4), 1474-1477.
13 Rana, M. E., Kubbo, M., & Jayabalan, M. (2017). Privacy and Security Challenges Towards Cloud-Based Access Control. Asian. Journal of Information Technology, 16(2-5),274-281.
14 Els, F., & Cilliers, L. (2017, March). Improving the information security ofpersonal electronic health records to protect a patient's health information. In 2017 Conference on Information Communication Technology and Society (ICTAS) (pp. 1-6).IEEE.
15 Idoga, P. E., Agoyi, M., Coker-Farrell, E. Y., & Ekeoma, O. L. (2016, October). Review of security issues in e-Healthcare and solutions. In 2016 HONET-ICT (pp. 118- 121). IEEE.
16 Pai, T., & Aithal, P. S. (2017). Cloud Computing Security Issues-Challenges and Opportunities.
17 Missah, Y. M., Dighe, P., Miller, M. G., & Wall, K. (2013). Implementation of Electronic Medical Records—A Case Study of an Eye Hospital. South Asian Journal of Business and Management Cases, 2(1),97-113.
18 Yan, L., Rong, C., & Zhao, G. (2009, December). Strengthen cloud computing securitywithfederalidentitymanagementusinghierarchicali dentity-basedcryptography. In IEEE International Conference on Cloud Computing (pp. 167-177). Springer, Berlin, Heidelberg.
19 Choi, M., & Paderes, R. E. O. (2015, November). Biometric application for healthcare records using cloud technology. In 2015 8th International Conference on Bio-Science and Bio-Technology (BSBT) (pp. 27-30).IEEE.
20 Chiuchisan,I.,Balan,D.G.,Geman,O.,Chiuchisan,I.,&Gordi n,I.(2017,June).A security approach for health care information systems. In 2017 E-Health and Bioengineering Conference (EHB) (pp. 721-724).IEEE.
21 Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1),1.
22 P Gayathri, Mayank Agarwal, Santhi H, Gopichand G. (2018). Bone Breakage Identification Using Image Processing Techniques. Journal of Adv Research in Dynamical & Control Systems, 10(09-SI), 1096-1103.
23 Santhi H, Gopichand G, K.Pavan Koushik, A.Nithin Krishna, D. Sai Tharun (2019). Derma Net: An Automated Skin Lesion Analyzer Using CNN with Adaptive Learning. International Journal of Innovative and Exploring Engineering(IJITEE), 8(6S4), 513-515