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 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]. 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 and recovery 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 prompted this research [5]. The existing methods and technology being used to solve cyber security threats and crisis need to be analyzed in detail. Attackers have wide nd their scope of attacks. 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 to provide.

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 cloud platforms 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 this lack of education that creates a flaw in the cloud-based design [10]. It is the need of the hour to service 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 utmost importance.

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.
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, and role to promote privacy in cloud-based solutions. Most suitable model for military and government organizations. Application of model of RBAC inc loud based EHR systems are discussed.

Floyd and Leizel [14] focused their work on investigating security measures that medical personnel should take into consideration to protect personal EHRs while accessing smartphones. Three unique threats to the data security were indicated which contain heuser, info in transit, and stored data. M-health security framework was taken into account to give 10 measures that can be used to indicate how these data privacy threats could be handled in the healthcare providers and patient. It is concluded that both of them should contribute in providing and increasing privacy in the health records and also data in transit should be well-protected.

Patience and Mary (2016) [15] recognized threats in the health records system by identifying vulnerabilities of the system and areas where cloud storage is inefficient, easy data retrieval, elasticity, atomicity etc. in this model third party cloud service providers own the infrastructure and customers/patients use their services. A solution model is proposed using data fragmentation without much overhead.

Prema 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 to provide 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 understand how it will be beneficial for the cloud service providers. In order to implement this, we have reviewed some research papers and tried to identify which methods are most suitable for security implementation. We aim to propose our own combined solution of the following existing solutions, and implement our own solution if existing ones are not up to the mark.

Case Study 1

Minkyu Choi, by using Cloud Technology [19], aims to provide a biometric solution to healthcare security. Two leading processes in this will be identification and authentication. Method through which the patients recognize the identity of the patient and authenticate the process. 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 provide secure password strategies and biometric solutions. USB sticks can be incorporated with biometric access control. Hard drives can also be used for access control and for encryption using in-built algorithms.

Improvement to EHR information security is a biometric solution that uses biometric technology. Utilizing the 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 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

Iuliiana Chiuchislan [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 guaranteed; 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. Encrypting 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 of users: encryption as the basis for securing all data moved to the cloud, ensuring security 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:
The purpose of this technique is to protect the real data while having an anonymization substitute for occasions when the actual data is not required. Masking changes delicate information with an anonymous value. Since masked data is not authentic, 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-based platforms.

Access control:
Access control is an important principle for the security of electronic health records. It gives approval to users to be able to access required patient’s information in a limited capacity. Role-based access control and attribute-based access control are the most well-known models for EHR. For user to be able to access their data over the cloud, certain keys shall be provided with respect to the cloud sharing policies [22]. There is some work that needs to be done on deciding how much content someone may be able to elicit using a patient’s unique key.

Monitoring and auditing:
Method of collecting information and observing flaws in the system 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 be recorded.

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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized access</td>
<td>Identifications system need to be implemented for the cloud service providers</td>
</tr>
<tr>
<td>Patient’s consent</td>
<td>Patients should be able to allow/deny access to their health record information.</td>
</tr>
<tr>
<td>Secure Cloud- based Environment</td>
<td>The Cloud service provider (CSP) must provide techniques to ensure network security.</td>
</tr>
<tr>
<td>Audits</td>
<td>A register to store all accesses and updates made to the electronic health records of patients.</td>
</tr>
<tr>
<td>Archive Process</td>
<td>Aim is to archive patients’ HER for as long as possible. Unadvisable to delete records after a certain period of time.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Security Threats</th>
<th>Description of Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS attacks (Distributed Denial of Service)</td>
<td>Techniques to countersuchattacksareavailable inweb services.</td>
</tr>
<tr>
<td>MITM attacks (Man in the Middle)</td>
<td>Secure Socket Layer (SSL) is used to mitigate such attacks as it provides server authentication.</td>
</tr>
<tr>
<td>Port Scanning</td>
<td>Violations of scanning unauthorized ports should be recorded and investigated.</td>
</tr>
<tr>
<td>IP Spoofing</td>
<td>Firewalls used to control traffic to avoid spoofing.</td>
</tr>
</tbody>
</table>
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 technical employees. To solve the level of clearance, each individual should be allotted with an ID number. These ID numbers will be segregated into groups and groups will be granted access to parts of the patient’s records depending on clearance level.

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 being exposed to external threats. Therefore, measures must be taken to ensure the security of cloud provided by CSP’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 of the environment, wherein there is no control over data. Encrypting data prior to upload is beneficial as it is encrypted before moving it to the cloud and can be securely decrypted by authorized personnel with decryption keys. Digital Signatures primarily promote non-repudiation; 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:

- A regional cluster of datasets; Therefore, automate dprocessesmustbeinplace to shift server traffic away from targeted network.
- 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 over the network, which includes using protocols such as FTP’s.

REFERENCES

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


