International Journal of Engineering & Technology, 7 (2.33) (2018) 477-479

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Healthcare information system using cloud security

P. Shobana Pritha [1] *, Dr. A. Sasi Kumar [2]

[1] Research Scholar, School of Computing Sciences,Vels Institute of Science, Technology and Advanced Studies (VISTAS),Chennai
[2] Professor School of Computing Sciences,Vels Institute of Science, Technology and Advanced Studies (VISTAS),Chennai
**Corresponding author E-mail: preetha.30121992@gmail.com*

Abstract

Almost all the human living in Earth forgets to take care of their health. To say specifically, the elder ones and the younger ones need con-tinuous examination to note down the variation in their health issues (either improvement or a decrement). This can be achieved through the digitalization of the data. In the present day scenario information security and privacy in healthcare systems is an issue that is growing at alarming rate. The espousal of digital records of the patient, the enlarged order, provider integration and the growing need to exchange in-formation between patients, providers and payers each targets at the necessity for a developed information system. Inspite of so many measures taken to prevent the theft of patient's healthcare records offenders find some loophole or the other to get the records. This article strives to list certain health issues faced by a majority of people, threats to HIS, the method adopted to store huge amount of data and measures to prevent security threats.

Keywords: *Healthcare Information System (HIS); Cloud; Security.*

1. Introduction

According to Panemon Institute (2016), "The most lucrative information for hackers can be found in patients' medical records". Medical records has valuable information such as name, address, date of birth, credit card information, social security numbers and physical/mental health condition of a person and all these records are called Protected Health Information(PHI).
Cloud Computing has become one of the most important changes in technology and is cost effective. Involving cloud technologies and models in health care monitoring can be a great way for the effective treatment and better patient care. Cloud models can be used to serve as networks, servers or for storage. All the medical records, staff details, doctors prescription can be monitored remotely through a web browser usually.
Wireless sensor networks (WSN) are modern day technology which is still an ongoing research and is efficient enough to change the life of humans (especially elders) more convenient. WSN has many specialities like management, efficiency etc. It have many applications in almost all the fields. The mobile sensors are integrated with these WSN's to examine the elder and younger people. There are also other technology such as WBSN – Wireless Body Sensor Network and WASN – Wireless Body Area Network.
The main aim of these technologies is to examine the elders and the young ones 24X366. Although, this is a good development they have many challenges in this contemporary world such as, there must be constant communication between sensors, the technology must be user friendly and so on.
The most important challenge for these technologies is 'security'. The security risk is a major problem which makes these technologies to develop slowly. Although this is a beneficial approach for the development of technology in the medical field, we tend to ignore it which is not fair. In order to overcome these kind of challenges we have taken an initiative step to make out these technologies into flying colours.
The main reason for this work to be chosen is that we see many people living with atleast one health issue. For instance,
A survey shows nearly 2.1 billion people of world's population are obese. [1] One in four is affected by mental disorder [1]. 2.4% of worldwide diarrhoea and 6% of malaria [2] One in thirteen suffer from anxiety [3].
These are just some of the examples, which has been published by prior researches. There are lot, more which has not been researched. Hence, there is a need in the development of such technologies, a guaranteed and a safe one. So we would like to improve the security in the above defined technology.. The rest of the article is organized as follows. Section I provides a brief background on Risks in Healthcare Management and also illustrates a Key Assets in. security. Section II explains our proposal to improve health care in cloud computing and the introduction of cloud computing. Section III describes the security and key issues in security. Then, Section IV provides an overview about related work. Finally, Section V presents the conclusions.

1.1. Risk in healthcare management

With the aim of assessing the cyber risks involved in the health sector, it is of prime importance to understand which system needs to be shielded, their key assets and the affect of a successful attack. Moreover antagonists also need to be recognized along with their purpose and capabilities. By doing so perils as well as healthcare system vulnerabilities can be better computed.

Copyright © 2018 P. Shobana Pritha, Dr. A. Sasi Kumar. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

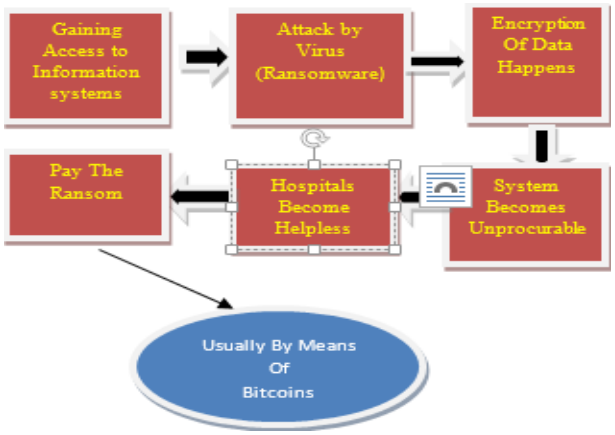


Fig. 1: Steps Involved in Attacking.

1.2. Key assets

The most important asset is the health of the patient. The perpetrator would injure the patient permanently. This would either cause an indefinite or a short term effect on the patient's health. Another method is to damage the medical equipments, cut off power supply, mixing of hazardous gases in the oxygen pipe etc. The actions may be deliberate or done unintentionally. However it results in the exploitation of the patient's health.

Readiness of the healthcare services is a major asset. These services are categorized into two: the critical services and the management services. The former focuses in providing healthcare such as giving necessary medical devices, the necessary medicines, apparatus required for surgery etc. Any disturbance in this service may result in a trauma. The latter is associated with the hospitals' interface. This may include appointments, bills, list of medicines available etc.

Certain hospitals provide research labs. This accounts for the intellectual asset such as innovative procedures for surgery, experimental results, antidote formulae etc. The information acquired from such activities holds great value. Thus they become a victim of cyber attacks. If such data gets stolen then the hard work of the researchers as well as the money invested is exhausted. The worst case scenario is that if the data falls into wrong hands or if the data is altered then it may cost the life of many innocent patients.

Last but not the least, the reputation of the hospital and its practitioners is an inevitable asset. The patients must have faith in the doctors and also need to believe that the facilities available are safe because their health is an issue related to their life. A cyber attack nevertheless of its character will disrupt the fidelity of the institution.

2. Cloud computing

Cloud is the practice of using a remote servers network that is hosted on the internet for managing, storing and processing data other than a local server Cloud in healthcare organizations:

As of now, health care organizations lag behind other industries. To prevent this, the providers can modernize the infrastructures of IT industries and the workflows that are based on paper. Health care organizations are slow in their development. So healthcare organizations can be modernized using cloud technology.

Cloud is not a remedy, it just the way to improvise the efficiency of healthcare industry. If the cloud technology is implemented in the healthcare industries, then it will permit the heath care organizations for better services. So, it is just a operating model for driving down the cost and improving the efficiency.

2.1. For cost effective health care

The cost of the heath care has grown up to the higher extent. Government must take some initiatives to minimize it. Alternative models which is cost efficient can be implemented in order to prevent this issue.

2.2. Government incentives

Government is providing incentives for providing new technologies. Reimbursement, development of standards, introduction of legislation and regulatory compliance are some of their incentives. So there is a increased awareness as well as consideration of new technologies. Increase in the data growth, It is a major issue in this healthcare. If the technology is improvised, the digital information will also become large which is the biggest problem here. So it can be protected by using the cloud technology. By this, there will be a better treatment path for diseases and faster recovery as well. Even though the adoption of big data technologies in healthcare sector carries many benefits and promises, it raises also some barriers and challenges. Indeed, the concerns over the sensitive information security and privacy are increased year by year because of several growing trends in healthcare, such as clinician mobility and wireless networking, health information exchange, cloud computing and so on[8].

2.3. Challenges of cloud in healthcare

By adopting the model of cloud in the healthcare, we will have a considerable change in the issue of management for providers. The current technologies are inefficient which must be modernized.

2.4. Benefits of using cloud technology

This technology provides access to many applications which was previously not applicable. Pathologists can also be accessed by remote services.

3. Security

All paragraphs must be justified alignment. With justified alignSince the usage of electronic devices is at its peak and all the information are stored in computers, these information are at the risk of cyber threats. So security plays an important role in healthcare management.

Some important methodologies in security, Anonymity is the term used here. It means the state of being unidentified within the set of subjects or entities .It gives us assurance that we can use the resource or service without disclosing the identity. Encryption will not alone check for anonymity. Because the user will be able to analyze the traffic eavesdrop the sender. So, healthcare systems must also give us some mechanisms as well such as opaque identifiers.

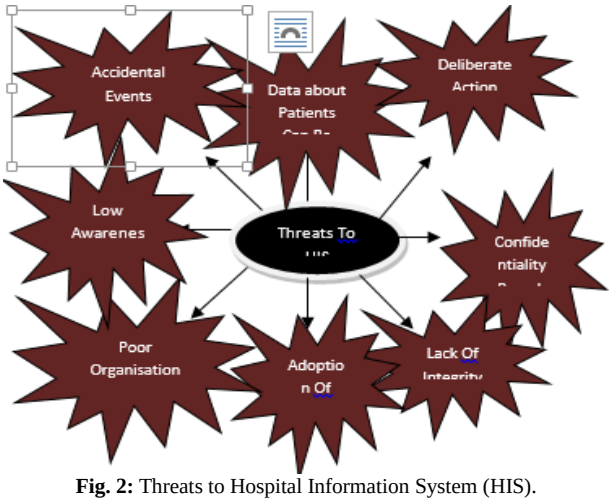


Fig. 2: Threats to Hospital Information System (HIS).

Pseudonymity is the use of pseudonym. The advantage is that it can be accounted for misbehavior if any. It also helps the healthcare providers to link identifiers with real identities so that it could make appropriate decisions if the user commits any mistake.
Unlinkability means it allows the user to use the multiple resources or services without allowing other entities to link these resources or services. Specifically, it allows to interact with multiple organizations. It is important that the Healthcare systems must provide some mechanisms Healthcare systems should provide mechanisms to prevent collaboration in the organizations like by linking a given user profile at one organization and the same profile at another.
Unobservability will permit the user to get accessed with the resources as well as services by avoiding the interference of other entities, especially third parties. It is more or less related to anonymity of subject in the terms of item of interest (IOT).

4. Related works

Lately researcher dedicated much time to the vicinity of wireless medical care systems. Recent projects concentrates on wearable health devices. These projects are taken care of by public and private organizations which swathe many areas in healthcare like glucose level monitoring, stress monitoring, cancer detection, elderly people monitoring, ECG monitoring etc.
CodeBlue [4] is a self-organized platform, which is easy to connect due to its adhoc architecture, and it integrates different wireless devices sensor nodes into disaster response surroundings. In paper [5], a lot of body sensors like pulse oximeter, ECG sensor are connected to Zigbee-enabled transmitters individually, which corresponds with APs. Thus no intra BAN communication takes place in CodeBlue. In this approach, multiple APs are closed to a wall. Without any control from the central unit, its inter BAN communication shapes a mesh structure where physicians subscribe by multicasting to the network and the sensor devices of patients bring out all applicable information. By using these messages, physicians understands the information they need to collect. This model is flexible and secure.
HealthGear [7] are sensors connected to a phone by Bluetooth. It is a wearable real-time health monitoring system to analyse physiological signals.
SMART [7] is deployed to scrutinize physiological signals of patients in the waiting areas of emergency unit. A variety of cases have been seen in waiting room where patient's health deteriorates rapidly while waiting. To solve this, this is used to collect information and wirelessly send it to a central station which accumulates and compute the data to issue an alert signal when the health deteriorates. Thus before the condition get worsens patients receives treatment.
The UNC Health Care (UNCHC), which is a not-for-profit integrated healthcare system in North Carolina that has implemented a new system allowing clinicians to rapidly access and analyze unstructured patient data using natural language processing. In fact, UNCHC has accessed and analyzed huge quantities of unstructured content contained in patient medical records to extract insights and predictors of readmission risk for timely intervention and providing safer care for high-risk patients and reduce readmissions [7].
In Morocco for instance, Pharma Process in Casablanca, ImmCell, The Al Azhar Oncology Center and The Riad Biology Center in Rabat are some medical institutions at the forefront of innovation that have started integrating Sophia to speed and analyze genomic data to identify disease-causing mutations in patients' genomic profiles, and decide on the most effective care. As new users of SOPHiA, they become part of a larger network of 260 hospitals in 46 countries that share clinical insights across patient cases and patient populations, which feeds a knowledge base of biomedical findings to accelerate diagnostics and care.

5. Conclusion

Healthcare systems predominantly aim to make healthcare cost effective while maintaining the quality, security, access and equity. It can also lie as a substructure abolishing duplicated services, minimising error, and otherwise upgrading the care of individual patients by providing basic changes in care delivery models. Each case has its pros and cons. Digitising such information makes them casualities of threats. The data from medical records and personnel files is more beneficial to the perpetrators than the information regarding credit cards. Why hospitals become a pray of such attacks is because of their time sensitivity. If faster access is not made to a patient's health record, the consequences may be large. The case a patient requires may not be provided, which may lead to death. In this paper, we have deliberated some successful related works and have made aware of the risks faced in healthcare management. We have also discussed some important terms in security and given a brief introduction about cloud computing and it's uses. The need of Big data is also discussed and it's security and privacy are considered as a huge obstacle for researchers in this field.

References

[1] www.who.in.
[2] www.ncbi.nlm.nih.gov.
[3] www.futurity.org.
[4] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, Victor C. M. Leung,"Body Area Networks: A Survey, Mobile Networks and Applications, Springer, Vol.16, Issue. Two, pp. 171 – 193, 2011.
[5] Min Chen, Jiafu Wan, Sergio Gonzalez, Xiaofei Liao, Victor C. M. Leung, a Survey of Recent Developments in Home M2M Networks, IEEE Communications Survey and Tutorials, Vol.16, Issue. 1, 2014.
[6] Moshaddique Al Ameen, Kyug-sup Kwan"Social Issues in Wireless Sensor Networks with Healthcare Perspective", The International Arab Journal of Information Technology, Vol. 8, Issue. 1, 2011.
[7] "UNC Health Care relies on analytics to better manage medical data and improve patient care." IBM press release, October 11, 2013.
[8] Karim Abouelmehdi, Abderrahim Beni-Hssane, Hayat Haloumi, Mostafa Saadi, ""Big data security and privacy in healthcare: A Review", The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks, 2017.
[9] Handler, Daniel Tolboe; Hauge, Lotte; Spognardi, Angelo; Dragoni, Nicola, "Security And Privacy Issues in Healthcare Monitoring Systems: A Case Study", Proceedings of the 10th International Joint Conference on Biomedical Engineering Systems and Technologies, Vol. 5, 2017.