Proceedings of the Third International Conference on Intelligent Sustainable Systems [ICISS 2020]
IEEE Xplore Part Number: CFP20M19-ART; ISBN: 978-1-7281-7089-3

Centralized and Automated Healthcare Systems:
A Essential Smart Application Post Covid-19

Rama Moorthy H
ramamoorthy.h@ieee.org

Sahana Udupa
sahana.udupa22@gmail.com

Samanvitha A Bhagavath
samanvithabhagavath@gmail.com

Shreesha
shreeshakannantha@gmail.com

Varun Rao
varunrao72@gmail.com

Department of Computer Science and Engineering,
Shri Madhwa Vadiraja Institute of Technology and Management, Bantakal, India.

2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) | 978-1-7281-7089-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICISS49785.2020.9316103

Abstract- **At an era of Industry 4.0 revolution, when it is said that the automation is buzzword among the all the devices/applications available. Still automation in Hospital Management System are far from reality in most developing nations. Automation in the field of Healthcare is the need of today's generation. This would help in providing a lot of functionalities to a patient with the help of a mobile application and other devices (Wearable devices to complex devices in testing centers). Here in our framework, patient details, which can be collected regularly from wearable devices and/or collected from Testing Centers(Clinics) and the case history from any hospital visited previously, all these vital details are stored in central repository irrespective of the hospital he/she visits. At the case of emergency, the patients case history which is stored in Central repository(Cloud). These details at any point of time if made available in any hospital, it can fast track the process in handling the patient. Also, understanding the secrecy level to be maintained in the Electronic Health Record and the way the HSM operates nowadays. This research work proposes to have a framework wherein, Patient related data collected from the wearable devices to the data stored in the CR (Cloud), utilizes Audio-Steganography as tool for Security aspect. The framework proposed would be an ideal solution during the current pandemic COVID-19 situations, with Doctors Forum proposed in the framework would be utilized to the most extent possible way to benefit each citizen at large.**

Keywords- Industry 4.0, Automation, EHR, HSM, Audio-Steganography, Healthcare, Security, Wearable Devices, COVID-19.

I. INTRODUCTION

Science and technology are growing rapidly hence providing new ways to cause security threats. Also many users are depositing their data on the cloud. Hence security of confidential information is a topic which needs attention [1]. In many of the Healthcare Management Systems that are observed today, there is a huge requirement for automation. Automation is the use of control systems and information technologies to reduce the need for human work in the development of services. Some of its advantages are labor saving, improved quality and consistency, reduced waste, increased predictability of outcomes, higher throughput, and reduction of manual errors and so on. As more and more users keep depositing data on the cloud, the security problems related to cloud increases. There are a large number of characteristics of Cloud Computing, such as, scalability, multi-user, virtualization etc. Due to these characteristics, the normally used security measures are not effective and it does not make the cloud computing system totally safe from third party unauthorized access. Usage of Homomorphic Encryption algorithm for cloud computing data security is also one of the methods adopted in various works [1]. It ensures that the data transmitted between the cloud and the user is safe from attacks. Also, it ensures that the data in the Security in IoT is another issue in the present day scenario of Healthcare Management Systems. It is all about safeguarding of the confidential data of the patient which is to be stored and transmitted over the internet. Security measures have to be implemented to ensure safety of networks when IOT devices are connected to them.

Ensuring that a patient is taken care of and given the required treatment at the right time is must. Timely reminders of tests to be conducted for the patient at the testing center needs to be given. Maintenance of the patient's reports and also sending them to the caretaker of the patient is very important. Taking necessary actions in case of emergencies by automatically calling the caretaker is one of the main objectives of this work Apt data of the patient will be collected and sent from or to the testing centers. This will help in maintaining the health conditions. Maintaining the confidentiality of the patient data by using audio steganography methods during the transmission of data and also during the storage of data builds a more secure network. Having a decision making system which suggests the best kind of treatment to be given to a patient among the various decisions put-forth by the certified doctors in the Doctors' Forum will ensure that a patient would not be given unnecessary treatment and will prevent the doctors from taking advantage of some uneducated and poor patients, ensuring that the confidentiality of the case will not be misused.

II. LITERATURE REVIEW

This section has reviewed the research works considering three aspects:

- **Towards Centralized EHR**

Allan Hasley[2] has mentioned the *National Project* planned in the year 2005. In this article, he mentioned the motive to have a reliable IT Infrastructure for EHR of all authorized users and the project has to adopt to the new technologies in the future. The project failed due to mismanagement, technical issues etc. The project was started with the estimation of 6 billion Pounds. But eventually was stopped from further completion in 2011 with almost spending not less than 13 billion Pounds[3].

In Abby et al work [4], authors investigated the relationship between EHR usage and the quality provided in the hospital. Here in this work, authors had taken 10 process indicators & 3 clinical conditions as parameters as the investigating tools with the Propensity Score algorithm. Authors found that the quality parameter derived with study did not match with the Hospital' theoretical claims.

Margret Hansen in his work stressed the benefits of using medical history in any emergency cases [5]. Authors introduced a 'Health Smart Card' concept, which would retrieve the case history of any particular individual person from wherever required. A practical implementation framework has not been discussed in this work. But nevertheless one can provide any framework for this approach.

Gabriel et al, were more concerned with the recent pandemic situation witnessed across the globe. There is a strong sentiment to centralize all the data-set of hospitals for all kinds of research works. Thus to kick start the process, such that the EHR's which were stored separately in the Hospital Server space needs to be stored in a Centralized data center[6]. With this intention a consortium has been formed with initially 96 hospitals from five countries around the globe and the framework is designed towards Centralization of EHR data-sets. Here, harmonized data were analyzed locally and later it was converted to a shared aggregator to have faster analysis and other purposes. Work also highlights the limitation of decentralization in data generations.

- **Security Concern in Centralized EHR as a Cloud Storage**

In the work highlighted by Rui et al, a reference model through a Use-Case scenario for security models of EHR applications in the cloud was being proposed with the integration issues in the model. The work lacked any implementation of the application mentioned in the real world scenario [7].

The work proposed by Gul et al, is that of a framework designed for a nationwide EHR system[8]. Authors in this work thrusted on the Cloud Computing model to ensure easy access with scalable and demand available resources. With the proposed framework, data interoperability between heterogeneous data sources were the challenges. Other than this, security and confidentiality factors have not been adopted here.

Abdul et al highlighted the importance of Privacy of patients records in the cloud platforms[9]. Work proposed to have a better access control mechanism. It was achieved by restriction on participants' access, forming a distinctive encryption parameter. The work proposed had the Key Management issues providing the access control mechanism.

With the increase in IoT application in healthcare systems and Cloud Computing technologies, Anam et al showcased the future deployment of Wireless Body Area Networks (WBANs)[10]. The thrust of the study here was more focused on the data privacy of EHR in various frameworks. Author also mentioned the need for Light-Weight algorithms to overcome security issues like access control and data privacies in the IoT application and cloud computing.

Alyami et al proposed the study in the United States about how the Personal Health Record is being adapted and accepted by both the persons and the institutions handling the PHR. The study was conducted for the period between 2008 to 2016, categorizing into six parameters. The work was aimed to ease out the misconception in the mind of persons & motivating them to utilize PHRS [11]. Here once the collection process from various personal medical records were done then automation, interfacing & secure storage of PHR in the cloud were suggested.

Ziglari et al analyzed certain security concerns of deployed models for cloud storage of EHR (Data Sets). Study conducted analyzed different set of models which were deployed for EHR likes of, Separation models, Availability Models, Migration Model, Tunnel and Cryptograph model [12]. Authors proposed to have a Collaboration Model. Their findings also highlighted to have mix security algorithms and protocols for future works.

The work conducted by Dallal et al, proposed to have Hybrid Data Security methods with Multi-Layered encryption data security approach for multiple segments of EHR's. However the method is tested with fewer records and searchable encryption methods. With large data sets and considering the centralized approach of EHR [13], this method will lack the efficiency mentioned.

Shekha et al, reviewed the security and privacy concepts in e-health systems managing EHR in the Cloud. Authors

reviewed works conducted for the period 2000-2018[14]. Most of the work were categorized into: Security and privacy in EHR; Security and Privacy in e-Health data in Cloud; EHR Cloud Architecture; EHR Cryptography and Non-Cryptographic methods. The study conducted highlighted the need of Comprehensive Security mechanism and techniques to ensure integrity in EHR systems

- **Steganography as a security tool**

Srinivasan et al. [15], concluded from their study that an image steganography method can be efficiently used as an alternative to cryptography for transmitting medical records securely. Steganography also uses the redundancies in the image to good effect and reduces the amount of information to be transmitted by combining the secure information into the redundancies of the image.

Lavania et al. [16] discussed about the implementation of Steganography on Medical images using Integer Wavelet Transform method, which consumes less memory space.

Wankhade et al. [17], say that many of the current audio and network steganography algorithms are theoretically applicable but in practice only some of them are feasible or applicable taking in mind available equipment and technology. As with the human Auditory Range(HAS), audio – steganography is a challenge as HAS operates over a wide dynamic range.

The Following table 1, gives the comparative analysis of the topics discussed.

Table 1: Comparative Analysis:

Towards Centralized EHR		
Work by:	Work Proposed on:	Findings/Limitation of the research identified:
Allan Hasley [2]	**National Project UK**	Project which was initiated in 2005, was further stopped during 2011[3].
Abby et al [4]	Relationship between EHR usage and quality provided in the Hospitals. Used Propensity Score algorithm	Quality Score observed mismatched with the claimed quality.
Margret Hansen [5]	Proposed a framework on Health Smart Card	Framework limited to One Nation was proposed.
Gabriel et al [6]	A Consortium of 96 Nations Proposed Centralized data center, during Covid-19 pandemic.	For the current COVID-19 pandemic, framework is proposed and 96 contries' major hospitals are part of this centralization. But heterogeneous data dependencies are the main issue.
Security Concern in Centralized EHR as a Cloud Storage		
Rui et al [7]	Use-Case scenario for security models of EHR applications in Cloud	Real time implementations lacked with integration issues
Gul et al [8]	Nationwide EHR system using Cloud Computing Model	Issues in Data interoperability. No Security framework deployed/discussed.
Abdul et al [9]	For better access control mechanisms in the cloud for EHR.	Key Management Issues were to be observed

Anam et al [10]	IoT application, further with Wireless Body Area Networks (WBANs)	Encryption techniques are of heavy weight protocols/ algorithms. Not fit for WBAN's or IOT applications
Alyami et al [11]	Study of Personal Health Record under 6 categories.	automation, interfacing & secure storage of PHR in the cloud were lacking.
Ziglari et al [12]	**Analyzed** deployed models for cloud storage of EHR(Data Sets).	Need of mix security (Homomorphic) algorithms and protocols were the findings of this work.
Dallal et al[13]	Hybrid Data Security for EHR on clouds.	Didn't reach the efficiency required.
Shekha et al [14]	Reviewed security and privacy concepts in e-health systems managing EHR in the Cloud.	need of a Comprehensive Security mechanism and techniques in ensuring integrity of EHR systems.
Steganography as a security tool		
Lavania et al. [17]	Image Steganography for Medical Images using IWT.	IWT processing in smaller devices takes longer time to execute and generate Stego-file.
Srinivasan et al. [16],	Medical records in image steganography application	Proposed framework is a manual work, which can not be utilized for automation of the HMS.
Wankhade et al. [15]	Investigated the possible audio/network steganography.	Restriction of several techniques due to HAS.

III.SYSTEM DESIGN

With the above study conducted, a centralized, automated and secured framework is proposed for the collection of medical data, storing of medical data and making that medical data available at any point of time and place. Thus the system is built with the following main modules and a centralized repository (CR), which maintains all the data of the patient. The modules of the system are:

- Patients Module (PM)
- Caretakers Module (CM)
- Testing Centre's Module (TM)
- Doctors Forum Module (DM)
- Hospitals Module (HM)

To showcase the security aspects in our framework, we have considered the least possible device which is used, i.e., wearable device. Having concern about Security Threats involved and constraints in this device, we are proposing to have Audio Steganography to be utilized, such that wearable device in the patient module will transfer the data with the help of audio captured randomly from min of a wearable device and sent to the Patient Module. Thus to achieve automation throughout the framework, we have utilized steganography techniques across the application (Mobile Apps) [18] [19] [20]. In our work LSB Audio Steganography is considered to hide the original message from hackers [21]. A pictorial representation of all the modules is shown below in the fig 1. It clearly depicts that they are all interconnected. Each module is explained in detail below.

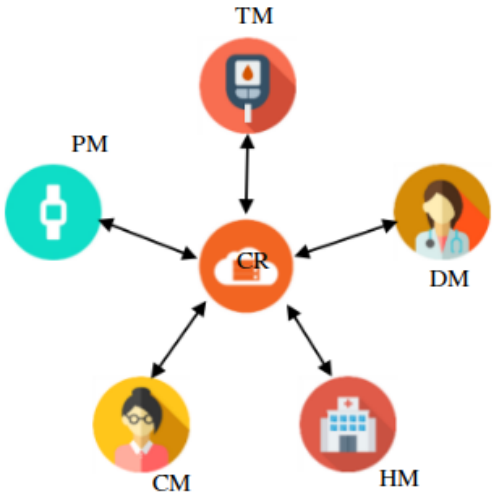

Fig 1: Proposed Framework

Patient Module: This is an application that is to be used by the Patient. This application provides proper authentication

while logging in and thus ensures that no random person can gain access to the patient details. After logging in, the patient's health parameters like heart rate, blood pressure, ECG, sugar level, height and weight will be collected periodically from wearable device and will be displayed. Some of the parameters will be updated after each test in the testing center. An option called as 'CHECK HEALTH' checks if any parameter value is above the prescribed limit. If so, a call will be automatically placed to the caretaker, who will then take care of the remaining necessities. In the 'About' page, the patient's basic details will be present. The patient can call the caretaker and in case of emergencies even call the ambulance by himself. In 'History' page, the previous test details, the upcoming test dates will be put. This will remind the patient of the next test date.

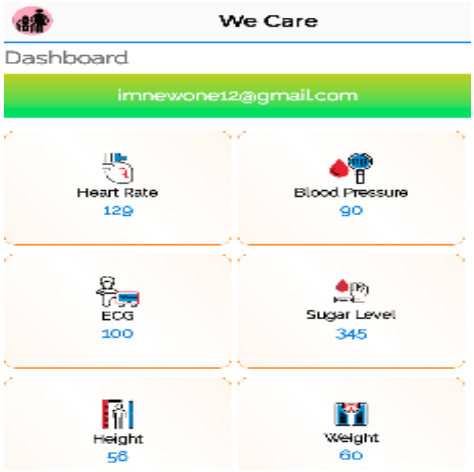

Fig 2: Patient Dashboard

There is also a notification feature, which reminds the patient to take medicines.
If the patient responds positively, the tablet count gets decremented. Hence this will remind the patient when he is going to be out of tablet stock. A logout feature also provided in the application as shown in fig 2.

Caretaker Module: This is an application that is to be used by the Caretaker of the patient. This application authenticates the identity of the caretaker before they get access to the patient details. Once they login, all the patient details and health parameters which were being displayed in the patient's application will be displayed to the caretaker. After the patient's test in the testing center is completed, the test reports will be updated to the application. The caretaker will be reminded about the next date when they have to take the patient for a check-up in the test center. They will also be reminded whether the patient has taken the tablet or not. If not, they can remind the patient to take medicines. If yes, the medicine count will be decremented. Once the tablet count reaches a minimum, the caretaker will be reminded about the same. Whenever the patient's health parameter's crosses a particular limit, a call will be placed to the caretaker from the patient's phone automatically. The caretaker will then have to take necessary measures by taking the patient to the hospital. Snapshot of the screen is shown in the fig 3.

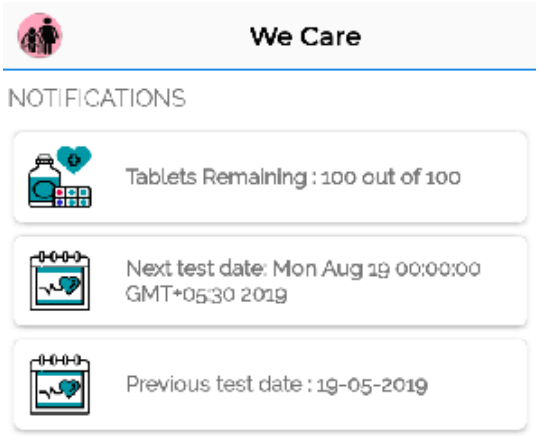

Fig 3: CareTaker Dashboard

Testing Center Module: This is an application that is to be used in the Testing Center. A Testing Center is where tests will be conducted to the patient. Once the tests are done, the results of the tests will be updated in this application. These will be updated to that particular patient's Identification Number. The report consists of Patient Id, Patient's Name, Blood Pressure, Weight, Sugar Level, ECG and Heart Rate. These details will be updated to the application in the Patient Module as well as in the Caretaker Module, which is shown in fig 4.

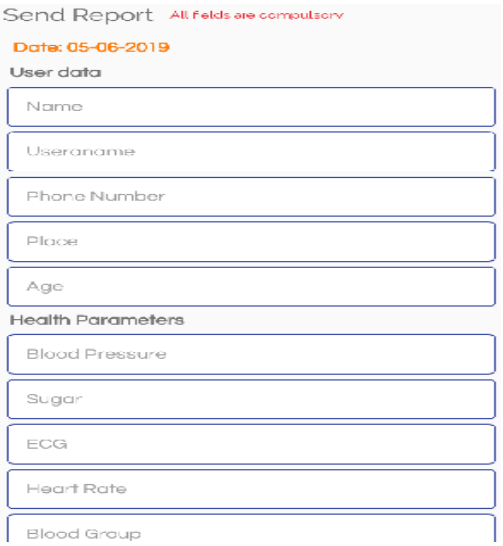

Fig 4: Testing Center Dashboard

Doctors Forum Module: This is a Forum that can be used by Doctors who do not work in that hospital where the patient visits. Only Certified Doctors can be a part of the Forum. This feature is helpful in the current pandemic situation when patient admitted in one hospital will get second opinions from doctor situated remotely. In order to ensure this, when the doctors enter into the forum, their details, success rates etc. will be taken. Whenever there is a complicated case, the case details will be put up by the hospital, into the Doctors Forum. However, in this process, the patient's personal details will not be leaked (identity of the patient). Once the case details are put into the Forum, the doctors present in the Forum can give their suggestions on what can be done to solve the case, as shown in fig 5. This will help the doctor in the hospital to handle the case in an efficient manner. These suggestions put forth by the doctors in the forum will be sent to the Hospital's application.

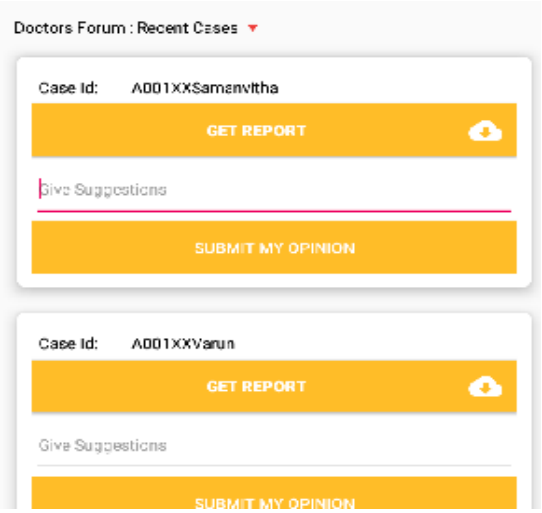

Fig 5: Doctor's Forum Dashboard

Hospitals Module: This is an application to be used by the hospital authorities. Here, there is an option to 'Add Patient'. This allows to add a new patient into the hospital records. This contains basic details of the patient like name, age, place, blood group and the reason for which they have come to the hospital. There is also another option called 'Patient details'. This contains details of the patients and also their case details. In case of a complicated case, the doctor treating the patient might need some second opinion on how the case could be handled more efficiently. Such case This is done in order to maintain the confidentiality of the details are sent to the Doctors Forum where certified doctors put forth their opinion about the case. In the option called as 'Second Opinion', the case details will be sent to the Forum and then the opinions obtained from the Doctors Forum will be displayed. In the 'Get Opinion' option, the best solution among the many solutions given by the certified doctors of the Forum is selected and displayed. The selection of the best solution is done by looking at the experience of the doctors, success rate of the doctors in the past years and so on. Once the second opinion is obtained, a proper decision on what kind of treatment is to be given to the patient is decided and the right treatment is given. It also prevents the doctors from giving unnecessary treatment to the patient. Hence it prevents the Hospital from taking advantage of the patient's less knowledge on the case, which are shown in the following fig 6, 7 & 8.

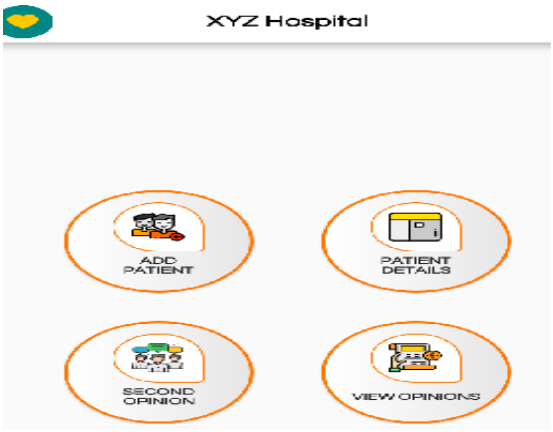

Fig 6: Hospital' Dashboard

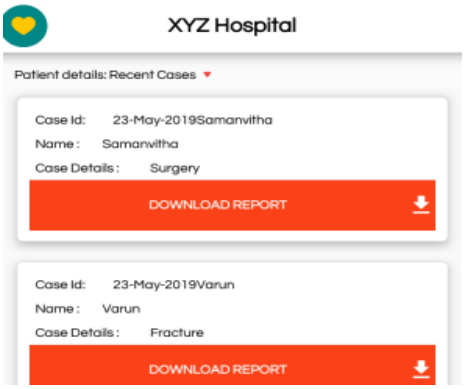

Fig 7: Extracting Details from/to Central Repository

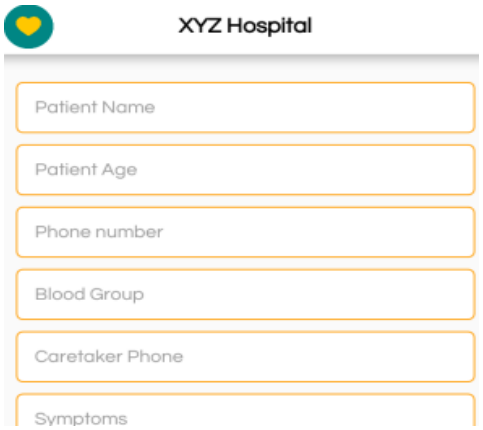

Fig 8: Sending Patient Details to Doctors Forum

Centralized Repository: The Centralized Repository is the heart of the entire system. It stores the medical data of the patient securely and ensures that no third party can get access to the confidential data of the patient. The data is stored in the server in the form of audios, which is the stego file. Thus, even if somebody does get access to the server, they will just be able to access the audio files. They will not realize that these audio files contain confidential medical data of the patient. Even when the data is being sent, the audio files will be sent. When the data is required, the decryption process will take place there and then the data can be extracted. This thus ensures security of the data.

The following figure fig.9 , gives the glimpse of how the proposed framework functions with the help of flowchart diagram.

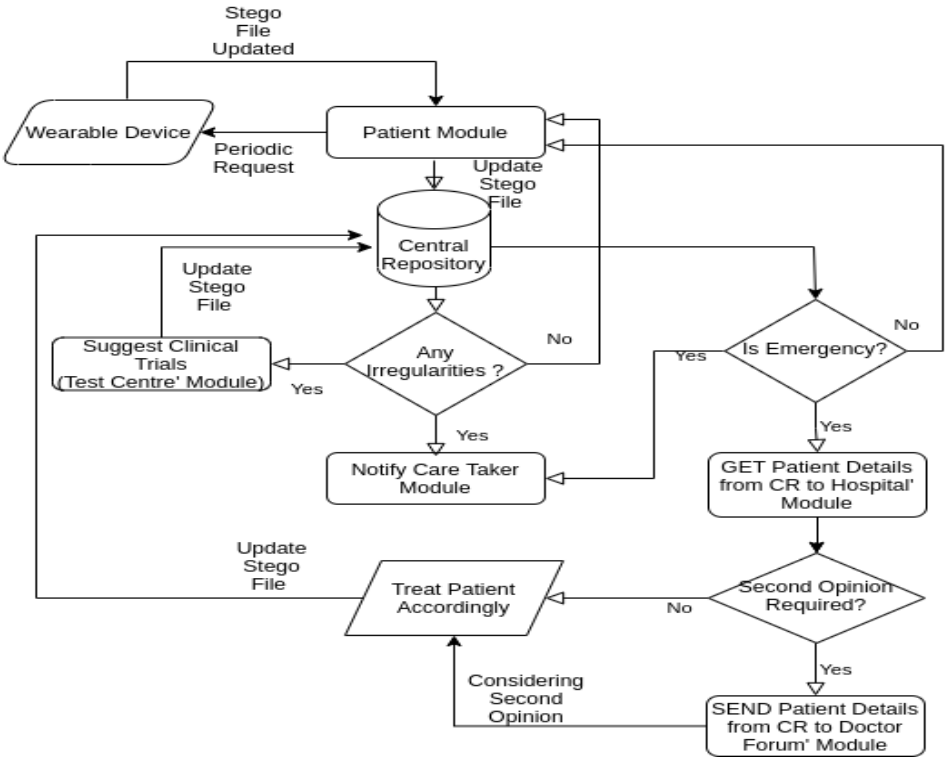

Fig 9: Flowchart for the Proposed framework.

IV. CONCLUSION AND FUTURE ENHANCEMENTS

We have implemented the concept of Audio Steganography for ensuring the secrecy of the confidential medical data. Another concept that has been proposed through this work is the process of Automation in the Healthcare Management System. Near Field Communication (NFS) could be used for authentication of a patient and also utilized for faster transfer of data from central repository in health care

sectors. In order to combat the (a) ageing factor of elderly citizens/patients, (b) their caretakers, (c) the employees of the hospital and (d) testing center easier, android applications have been developed for the modules. In the current pandemic situations when all hospitals, clinic centers, doctors are all engaged in their respective works, the automated framework proposed would be very useful application.

REFERENCES

[1] F. Zhao, C. Li and C. F. Liu, "A cloud computing security solution based on fully homomorphic encryption," 16th International Conference on Advanced Communication Technology, Pyeongchang, 2014, pp. 485- 488.doi: 10.1109/ICACT.2014.6779008

[2] Alan Hassey, " The National Programme for IT in the NHS.", British Journal of General Practice, 2005, 55(210),58.

[3] Expensive mega-projects that went wrong, can be found at https://www.lovemoney.com/gallerylist/88014/expensive-megaprojects-that-went-wrong

[4] Abby S. Kazley, Yasar A. Ozcan, "Do Hospitals With Electronic Medical Records (EMRs) Provide Higher Quality Care? An Examination of Three Clinical Conditions.", Medical Care Research and Review Volume 65 Number 4 August 2008 496-513

[5] Margaret Hansen, "Smart Card Technology and Healthcare Information: A Dynamic Duo.", CIN: Computers, Informatics, Nursing • September/October 2008.P No:254-257.

[6] Gabriel A. Brat, Griffin M. Weber, Nils Gehlenborg et al, "International electronic health record-derived COVID-19 clinical course profiles: the 4CE consortium.", npj Digital Medicine (2020) 3:109

[7] Rui Zhang, Ling Liu, "Security Models and Requirements for Healthcare Application Clouds.", 2010 IEEE 3rd International Conference on Cloud Computing.

[8] Omniyah Gul, Mahmoud AI-Qutayri, Chan Yeob Yeun, Quang Hieu Vu, "Framework of a National Level Electronic Health Record System.", 1ntemational Conference on Cloud Computing, Technologies, Applications & Management, 2012.

[9] Abdulatif Alabdulatif, Ibrahim Khalil, Vu Mai, "Protection of Electronic Health Records (EHRs) in Cloud.", 35th Annual International Conference of the IEEE EMBS, 2013.

[10] Anam Sajid & Haider Abbas, "Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges.", J Med Syst (2016) 40:155.

[11] Mohammed Abdulkareem Alyami, Yeong-Tae Song, "Removing Barriers in sing Personal HealthRecord Systems.", ICIS 2016.

[12] Hajar Ziglari, Arefeh Negini, "Evaluating Cloud Deployment Models Based on Security in EHR System", ICET2017

[13] Kushal Rashmikant Dalal, "A Novel Hybrid data security algorithm for Electronic Health Records security", 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS), 2019

[14] SHEKHA CHENTHAR, KHANDAKAR AHMED, (Member, IEEE), HUA WANG ,FRANK WHITTAKER, "Security and Privacy-Preserving Challenges ofe-Health Solutions in Cloud Computing", IEEE Access, VOLUME 7, 2019.

[15] Yeshwanth Srinivasan, Brian Nutter, Sunanda Mitra, Benny Philips and Darron Ferris, Secure Transmission of Medical RecordsUsing High Capacity Steganograhy

[16] Shubham Lavania, Palash Sushil Matey and Thanikaiselvan, Real-Time Implementation of Steganography in Medical Images using Integer Wavelet Transform, School of Electronic Engineering, VIT University, Vellore, Tamilnadu, India.

[17] Shilpa Sunil Wankhade and Ramesh V Shahabade, Hiding Secret Data through Steganography in VOIP, Terna Engineering College, Nerul, Navi Mumbai, India

[18] Ramasamy, Balasubramani & k b, Sudeepa. (2017). A Secure Data Transmission using Audio Steganography Based on Randomized LSB Technique. 56-59.

[19] Jayaram P, Ranganatha H R and Anupama H S, Information Hiding using Audio Steganography – A Survey, Department of Computer Science and Engineering, R V College of Engineering, Bangalore, India.

[20] Namita Verma and Vinay Kumar Jain, Audio Steganography – A Review, SSCET Bhilai

[21] Lindawati, Rita Siburian, "Steganography implementation on android smartphone using the LSB (least significant bit) to MP3 and WAV audio.",3rd International Conference on Wireless and Telematics (ICWT), 2017.