IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Comprehensive Architecture for Securing Information Disseminated by Wearable Devices in Health Informatics

Dr. Badr Almutairi[1], **Dr. Abdulgader Almutairi**[2]

College of Computer and Information Sciences, Majmaah University, Kingdom of Saudi Arabia[1]

College of Sciences and Arts in ArRass, Qassim University, Kingdom of Saudi Arabia[2]

Abstract: Health information is one of the most critical data to manage and disseminate. Securing this information is a big challenge. Many vendors today are providing wearable devices, which collect different information and display them to the end-user, but the information provided by these wearable devices is not secured and encrypted. Information is extracted from various variable devices having different sensors to extract specific information from the human body. This information is further stored on the web servers which hold the records of individuals. Securing the dissemination of information from wearable devices to the web servers is a big challenge in the wearable industry today. In this research project, we are focusing on designing a comprehensive architecture for securing information dissemination and management of the end-users' health data. We will be using optimization and encryption algorithms to protect the privacy of information which is being disseminated by wearable devices to the web servers which hold critical data related to the end-users. Our research project will collect data from various wearable devices and convert it to XML data sheets which, in turn, will help in information collaboration between various application software applications available for health information management.

Keywords: Security;Optimizatin; Encryption; Wearable Devices ; Health Information; XML.

I. INTRODUCTION

As the number of vendors for wearable devices is increasing, the cost of purchasing a wearable device is going down. New devices and vendors will make it cheap to monitor human activities in real-time and upload the data to a health informatics data warehouse. Some of the available variable devices such as Fit-bit and jawbone monitor various human actives in real-time and send alerts based on the wearer's health conditions. E-health monitoring and prevention approaches revealed to be among the top promising solutions [1]. With the evolution of technology and small sensors, it's now becoming easy to monitor various parameters of a human body such as the heartbeat, calories burned and steps taken. All this information is computed and stored on web servers so that the doctors associated with the patient can look into the patient's activity tracker program and give them alerts based on what they should do next so that the patient can take care of themselves try avoiding the risks associated with a human body. As health information is very personal to an individual, it's becoming risky to manage and disseminate information over the Internet channels. Hence, in this research project, we are focusing on securing information dissemination and management of contents, which is provided by the wearable devices. The transmission of information from wearable devices to the web server should be encrypted. We will be providing a middleware solution to protect information exchange between the web servers and wearable devices, thus securing the critical path of a data breach. This middleware solution will have tuner and transmitter, which will handshake with each other through a private key to exchange the encrypted data which flows over the Internet TCP/IP and UDP protocols. This can be effective since more patients and physicians are relying more on data generated from wearable devices which help them in taking precautionary measures for protecting their health from various type of diseases. These devices generate real-time data which can be further analyzed and computed to get the exact prescription for the patient. Gone are those days when a doctor would drop by your home to give you a quick check-up for your health related issues.

The emergence of new technology has created physicians as avatars that can interact and monitor your health related issues by virtually assisting the patients. As VOIP is becoming faster, it has become easy to collect voice data from wearable devices and sensors which monitor the heart beats and pulse rates. As the vendors in health care increase, they will come up with new wearable devices such as rings which can monitor skin-related issues. The biomedical sensors are typically involved in monitoring vital-sign parameters by converting physical values [2].Application software is being designed to communicate with the hardware of these tiny devices, which hold crucial health data that can be used by the consultants and doctors to cure the patient in real time and help him take his medication on time. The data feeds which come from these devices need to be secured and hence this research project will provide a middleware framework

DOI10.17148/IJARCCE.2017.6685

architecture, which will secure data transmission channels over the network protocols to main secrecy and privacy of patient's data which is coming out from wearable devices which are being used in health informatics.

II. SYSTEM DESIGN FOR SECURING DATA TRANSMISSION

The users' health related data, being the most crucial entity petabyte of data, is generated every day, which is important and needs secrecy and privacy of the data; we also need to disseminate the data to various stakeholders based on their requests. The system provides continuous monitoring of the user's electrocardiogram (ECG), respiratory status and activity [3]. This raw data, when disseminated over the network channels, is prone to tampering and there are chances that it might be misused. In this research, we are designing a system which has a secure channel for data transmission and handshake protocol between both the end-users. The architecture for securing the healthcare data is as follows:

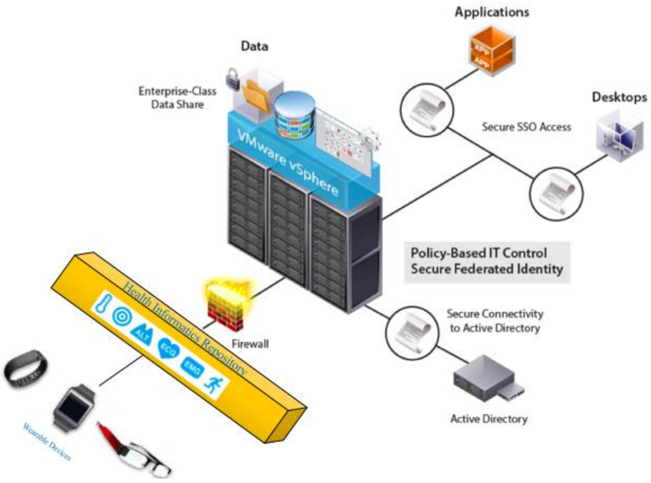


Fig. 1. Architectural layout for securing healthcare data

In the given figure 1, wearable devices are collecting real time data with the help of sensors mounted on the devices. This data is then forwarded to the health informatics repository, but unfortunately we need to filter this data via firewalls and create a secured environment for the ethical data to enter the enterprise servers. The enterprise servers have many VMs (Virtual Machines) running, each of which has a specific task to execute in order to secure the data. Now, the tuners and the transmitters are responsible for exchanging the data between application software, which are requested for the health care data of the patient. Such a secure channel will help to build trust between all the stakeholders.

The above layout focuses on three major aspects which are as follows:
A. Data from wearable devices
As wearable devices have small sensors which produce huge amounts of real-time data, it becomes mandatory to secure the collected data from these devices. As the amount of power consumed by the sensors in wearable devices is very less, the data which it will produce is really tiny. Sensors can be weaved or integrated into clothing, accessories, and the living environment [4]. But this data holds a huge amount of information which is crucial and needs to be maintained in health informatics repository. Securing this RAW data generated by the sensors is a major challenge as syncing this information after processing back to the devices requires secure access channels for data transmission. Most of the wearable devices available in the market today produce the following kind of data:

a) Steps taken;
b) Calories burned;
c) Blood pressure;
d) Skin tone monitoring;
e) Pulse rate monitor.

These data are then displayed to the end user on his screen, based on the device which he or she holds. This information can then be utilized by the patient to take his medicine on time and also to keep a track of his health and fitness. Most of the doctors today are focusing on the fitness of human beings and it is evident that the vendors are adding more fitness-tracking sensors to the wearable devices. These sensors consume very little power from the wearable devices and produce real-time data, which is related to human health. Vendors also have applications for the iOS and Android operating systems so that the fitness trackers can connect to your mobile handset and disseminate the information about

DOI10.17148/IJARCCE.2017.6685

your health. The patient can also share his data using the social channels to his doctors so that the doctor can prescribe some medicine based on the patient's health conditions.

B. Health Informatics repository

The data repository is important to maintain records in the digital form so that they can be referred to easily access the patients' records and keep a track of the patient's history. Healthcare repository holds huge amounts of data which are recorded through the sensors or the wearable devices. Doctors can search for patient records by secure two-way authentication. To search records in the repository, many data-mining algorithms run in parallel. Healthcare repository holds health related information of each patient. Information about the patient can be collected from various sources such as wearable device data, medical records, private medication and much more. This repository serves as a centre point for all the health related issues of the patients. when one needs help and monitoring related to his health, the physicians and consultants can login to this repository and gain access to the health related history of the patient. Chronic diseases such as stroke, arthritis, asthma and obesity are very costly to get rid of. Thus, these wearable devices can help monitor the patient's activity and give suggestions from time to time for taking the proper medicine at appropriate intervals so as to avoid further problems caused by these chronic diseases.

C. Enterprise level security for healthcare data

Security of health related information being a major concern, the medical and healthcare world today needs special attention.

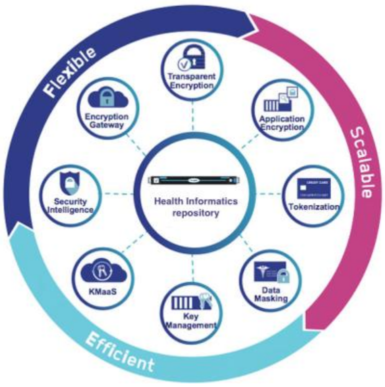


Fig. 2. Optimized Security for healthcare data.

The above figure 2 shows the optimized architecture for securing healthcare data management and information dissemination system using algorithms which encrypt and decrypt the data flowing through and fro the wearable devices used in medical data collocation. This is important from an administrative point of view as he will have a control over the data optimization. Information that is sent by the wearable devices to the web servers is secured with the primary key, which is decoded at the server-end. Each tuple data that is sent from a wearable device to the web-server will have to pass through the middleware software, which will encrypt the data and then transmit it through a secure channel to the web-server. Once the data is received at the server end, the decryption algorithm at the server end will decrypt the data and collect information from the data and store the data and information securely on the web-server.

III. REPOSITORY AND COMMUNICATION CHANNEL DESIGN AND DEVELOPMENT

This research project design mainly focuses on database security and dissemination of information on a secure channel so that the patients' data is not leaked to unwanted sources. The design mainly comprises of three major components which include data, information, the private key for encrypting the data (Data encryption algorithms) with optimization and end-to-end protection mechanism for dissemination of the data back to the wearable devices.

Steps to collect information and secure it are as follows:

a) Connecting to the wearable decive via a secure channel.
b) Classification of health realted data.
c) Index data according to the type.
d) Transmitting data over secure channel to the webserver.
e) Analyzing the data based on patients record present in the health informatics repository.
f) Consulting the physician and consultant for any health

DOI10.17148/IJARCCE.2017.6685

g) related issues by providing realtime updated data to the doctor
h) Transmitting back the information to the patient based on the diagnosis

All the steps mentioned above are important and need a secure channel of communication and data security for transmission.

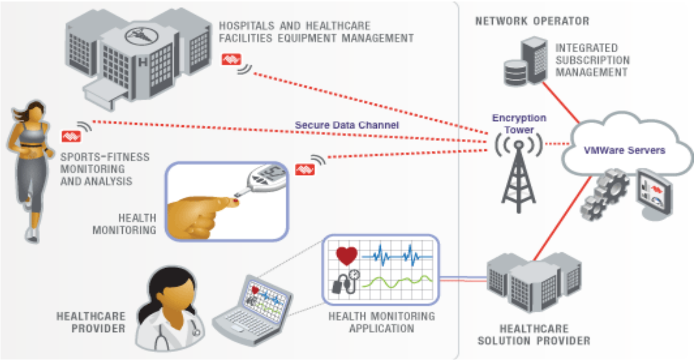

HOSPITALS AND HEALTHCARE FACILITIES EQUIPMENT MANAGEMENT
NETWORK OPERATOR
INTEGRATED SUBSCRIPTION MANAGEMENT
Secure Data Channel
Encryption Tower
VMWare Servers
SPORTS-FITNESS MONITORING AND ANALYSIS
HEALTH MONITORING
HEALTHCARE PROVIDER
HEALTH MONITORING APPLICATION
HEALTHCARE SOLUTION PROVIDER

Fig. 3. Communication with the optimization servers.

As shown in the above figure 3, the user or patient's data is collected from various sensors which are built upon wearable devices, which he or she is wearing, for example the fitness data such as steps taken, calories burnt and pulse monitoring system all of this data is transmitted to the VM-ware servers over the secure channels in an encrypted form. The system architecture, details of the monitoring sensor nodes, hardware design of the ZigBee module and data packet structure definition of wireless communication are introduced [5]. The encryption tower is responsible for running various data encryption algorithms, which will secure the data being transmitted to the VM-Ware servers which act as health informatics repositories. Real-time encryption of data is required on the fly as the sensors keep producing data every second and update it to the health informatics servers. Intern the VM-Servers can be accessed by the health care solution provides who can get real-time data of the patient and monitor his activity. This will help them in suggesting the necessary action related to chronic diseases, which might affect the patient's health, based on this activity monitored by the system. A two-way communication system is set up in such a manner that if any activity is detected that might affect the patient, an alert signal is generated by the system and sent to the patients' wearable device, which he or she is using.

IV. PATIENT RECORD MANAGEMENT REPOSITORY AND REPORT GENERATION SYSTEM

Petabytes of data are generated every day by the wearable devices, which are used by the end users. This huge amount of data needs to be secured and maintained in informatics repositories and used when ever required by the stakeholders of the system.

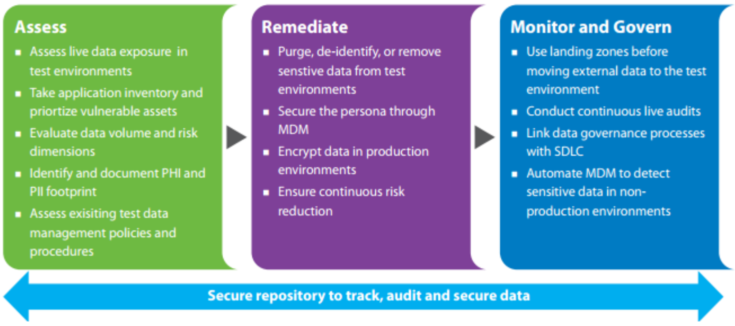

Assess
Assess live data exposure in test environments
Take application inventory and priortize vulnerable assets
Evaluate data volume and risk dimensions
Identify and document PHI and PII footprint
Assess exisiting test data management policies and procedures
Remediate
Purge, de-identify, or remove senstive data from test environments
Secure the persona through MDM
Encrypt data in production environments
Ensure continuous risk reduction
Monitor and Govern
Use landing zones before moving external data to the test environment
Conduct continuous live audits
Link data governance processes with SDLC
Automate MDM to detect sensitive data in non-production environments
Secure repository to track, audit and secure data

Fig. 4. Health Informatics Secure Repository.

Fig. 5.

The above figure 4 shows that a secure repository channel is created to manage huge amounts of data. Moreover, auditing of the data is also performed by the systems running on the VM-Ware server. This system is sub divided into the following tracks:

- Assessing the data

This sub-system runs on a VM and is responsible for assessing the live data streams which come from the wearable devices. It also needs to validate the patients' data and keep a track of the trend that is going on with the patients and also

DOI10.17148/IJARCCE.2017.6685

generate reports based on the activities, which the system is accessing. If there is any vulnerability found in the records, the system should take necessary actions to rectify the vulnerability and provide solutions to the stakeholders using this system. It should identify the volume of the data and provide a report on the risk dimensions. Also, the system should access the record and forward the information to the concerned department to get the exact medication required and suggest the same in the report which will be generated by the system.

- Remediate the data

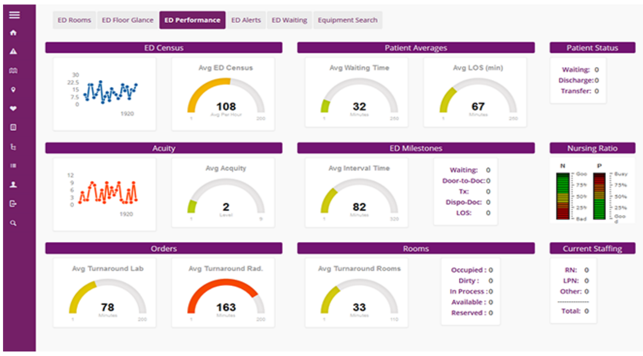
This sub system should remove sensitive data from the information, which collected from the wearable devices. Data analysis algorithms will be running on the VMs to identify the sensitive data and encrypt this sensitive data so that it can be shared with the authenticated stakeholders over a secure channel. The test environment is set to identify the crucial data from the repository. The persona of the patient is secured on the servers, which host this module. MDM is responsible for collecting and managing this information so that the exact records can be fetched easily from the system using the Hashed Indexing system when information is being received by the system over the secured channels, which is the production environment. VMs will encrypt the data and secure it in the healthcare repository. These VMs run encryption algorithms that validate the information received and acknowledge the end terminal about the information mitigation and management. Many European and American countries have healthcare data breach, which is a major setback to the country's citizens and its government. The medical authorities need to be notified about the number of records which have been breached and thus provide proof and remedies for the same. Our system is end-to-end encrypted with a 128-bit encryption key; also, an optimized algorithm is used to compress the key I in such a way that it cannot be breached easily. Also, the availability of the system is 24x7 and the system is highly scalable.

- Monitor and Govern the data

This sub system is responsible for securely moving the data from one source to another. The requesting source should be governed by the procedures and policies of the system and should imply the rules of the SDLC so that proper migration of the healthcare data can be achieved. The MDM system should detect sensitive data and transmit it to the requesting server over a secured channel. Health related information management and redundancy can be achieved by optimizing the crucial information present on the servers. Various optimization algorithms based on efficiency have been implemented an example of which is the K-means clustering algorithms that provide optimized data storage and remove redundancy from the repository so that only the useful information is stored on the servers.

V. INFORMATIC REPOSITORY DASHBOARD

The centre console is provided to all the stakeholders of the system so that they can access the health-related data over a secure channel. Encrypted data is stored in the informatics repository. The stakeholder can login by using their two-way authentication process. Once the stakeholders are logged in, they can gain access to the patient-data and use this data for analysis and give the patient medical recommendations based on the record analysis done by the physicians and consultants. The doctors can select the patient record and view his full history. The patient can also get real-time updates from the wearable devices, which they are using. Data such as activity records and other health related data can be viewed by the doctor in real-time using this software. A lot of precaution is taken in terms of security to secure the collected data.



Waiting: 0
Discharge: 0
Transfer: 0

Waiting: 0
Door-to-Doc: 0
Tx: 0
Dispo-Doc: 0
LOS: 0

Occupied : 0
Dirty : 0
In Process : 0
Available : 0
Reserved : 0

RN: 0
LPN: 0
Other: 0
Total: 0

Fig. 6. Dashboard for the medical repository.

VI. CONCLUSION

Wearable devices are disseminating huge amounts of health-related data to the users but it is really important to secure and store this data in the health informatics repositories. This research helps in solving this issue by providing a secure

DOI10.17148/IJARCCE.2017.6685

channel for data communication and stored repository, which can hold petabytes of data and secure this data on the repository. Access to this health related data can be given to authentic stakeholders of the system and further processing can be done on this data to avoid further chronic diseases in the patients. The doctors can investigate this real-time health data, which is collected by the wearable device so that early alerts can be given to the patient, which will ensure that he or she takes precautions and preventive measures to avoid the chronic diseases beforehand.

ACKNOWLEDGMENT

This research work would not have been successful without the help of the resource persons and software, hardware requirement and procurement. We would like to thank the department of computer and information sciences Majmaah University for giving us all the required resources in time and helping us achieve this opportunity in adequate time. Our Dean **Dr. Hisham Alsaghier** has been very co-operative and has guided us in the various phases of this research work. He always motivated us to complete this research project in time and with the available resources. At last but not the least, we would also like to thank our lab assistants who worked with us tirelessly and helped us assemble all the equipments in time.

REFERENCES

[1] Abdelghani Benharref, "Novel Cloud and SOA-Based Framework for E-Health Monitoring Using Wireless Biosensors",IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, January 2014.pp. 46-55.

[2] Sasan Adibi, "Biomedical Sensing Analyzer (BSA) for Mobile-Health (mHealth)-LTE", IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, January 2014, pp. 345-351.

[3] Jianfeng Wu, "A Wearable Health Monitoring System with Multi-parameters", IEEE 6th International Conference on Biomedical Engineering and Informatics (BMEI 2013), pp. 332-336.

[4] Ya-Li Zheng, "Unobtrusive Sensing and Wearable Devices for Health Informatics", IEEE Transactions On Biomedical Engineering, Vol. 61, No. 5, May 2014, pp. 1538-1554..

[5] Zhang-qi Wang, "Wearable health status monitoring device for electricity workers using ZigBee-based wireless sensor network", IEEE 7th International Conference on BioMedical Engineering and Informatics (BMEI 2014), 2014, pp. 602-606.

DOI10.17148/IJARCCE.2017.6685