iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6369

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

Study of Data Security Features in Healthcare Sector

Priyanka Bhimrao Lade[1], Chetana Achar[2]
[1, 2]*Mumbai Education Trust (MET), Mumbai, India*

Abstract: The objective of this research paper is to compare the security features of healthcare applications. Applications are created for doctors as well as patients to make their lives easy. Android applications are developed as it is widely used and very user friendly. But at the same time security is a major issue. Various applications exist in market but security is an aspect we need to work upon. When it comes to healthcare application the security concern is higher, as it contains patient's confidential information. There are various levels at which security need to be checked. In this paper we will consider various vulnerabilities in an application with regard to security and also solution to them.
Keywords: Healthcare, Android application, Privacy, Security.

I. INTRODUCTION

"Privacy" may be defined as the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others. Privacy is your right to control what happens with personal information about you. In Australia there is no general right to privacy. Some protection is afforded through the operation of certain Federal and State legislation, together with the law of contract, tort and confidential information. [1]

Information security and privacy in the healthcare sector is an issue on rise. The method of turning to digital patient records, increased regulation, provider consolidation and the increasing need for information exchange between patients, providers and payers, all point towards the need for better information security.[2] Health care environments today have turned to be technology-oriented. Also mobile devices and their usage have increased manifold in recent times. Today we have an abundant increase in the development of Science and Technology, which in-turn made the humans even to carry a mini-Computer in their palms with screen touch. To make a doctors life easy and efficient we combine technology and healthcare. Although in healthcare there are many security and data privacy problems to be overcome. [3]

We have various Android Application a secure and privacy preserving framework such as Dr.Pad, Medical Records, Medical records, etc. Many applications available in the market are free and easy to use but not secure enough to protect patient's data or prove the authenticity of the doctors.

The various security aspects are:

A. Access control
B. Integrity
C. Confidentiality

To safeguard the application against these attacks we need to find the vulnerabilities, loopholes and glitches in the security system. The various points where these vulnerabilities may creep in are login, remote server, analysis, and patient's data. Through the research we found these loopholes in various applications and special measures are undertaken to overcome them in many healthcare applications are there for a doctor. These applications are developed to ease the life of a doctor.

II. LITERATURE REVIEW

Healthcare applications have some benefits as well as some barriers also. Before healthcare application comes in market there was paper based system at healthcare center and hospitals. Where for patient's information, health related information, medical reports, prescriptions, bills, etc. paper was used. Because of that data collection was one issue if we consider time factor. And another important issue was storage of collected data and loss of important data.

Major barriers to the adoption of healthcare applications are resistance to innovation, lack of infrastructure, and cost of technology acquisition and ownership.[4] One of the major concerns about the use of healthcare application is the security of the health information being accessed through and residing on mobile devices. Healthcare applications provides mobility and remote

connectivity, but it also brings in significantly more security threats than the traditional wired networks. Other policy barriers to healthcare applications are cost of implementation and infrastructure maintenance, liability, and security issues. HIMSS[5] has postulated additional obstacles as lack of business model, security, standards, and regulatory compliance guidelines for healthcare applications. The mobile devices due to their small size can be lost or slide out of pocket, stolen or given for replacement or upgrades. Ever expanding storage capabilities of mobile devices leading to storage of corporate sensitive data on healthcare applications. All devices can connect to any network outside the company's control. This proliferation of wireless interfaces exposes ever-increasing attack surface that can be used to compromise devices by the attack vectors.

Healthcare applications can collect, report and analyses the data in real-time and cut the need to store the raw data. This all can happen over cloud with the providers only getting access to final reports with graphs. Reports and alerts give a firm opinion about a patient's condition. It also helps make well-versed decisions and provide on-time treatment. In event of an emergency, patients can contact a doctor who is many kilometers away with a smart app. Healthcare application can also be used for research purposes. It's because it enables us to collect a massive amount of data about the patient's illness which would have taken many years if we collected it manually. This data thus collected can be used for statistical study that would support the medical research.

III. ANALYSIS

According to the U.S. Department of Health & Human Services (HHS), access to ePHI should be limited to the "minimum necessary" for employees to do their jobs and care for patients. This is where many organizations fail. It's all too common for health facilities to share large datasets across the organization simply because they lack the resources or time to manage access properly.

The healthcare industry historically lags behind other industries when it comes to adopting technology. Hospitals and medical practices often use outdated operating systems, elementary backup systems, manually carry all the reports and previous health records and consumer-grade routers. Additionally, they offer unsecured guest networks for patients and visitors.

Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable [6-10]. For instance, the patient's physiological vital signals are very sensitive (i.e., if a patient has some embarrassing disease), so any leakage of individual disease data could make him/her embarrassed. In fact, sometimes revealing disease information can result in a person losing his/her job, or make it impossible for him/her to obtain insurance protection [11]. Further, wireless medical sensor networks cover a broad range of healthcare applications, such as physiological data monitoring, and activity monitoring in health-clubs, location tracking for athlete, etc. Therefore, unauthorized collection and use of patient data by potential adversaries (such as insurance agents, for political reasons, rival coaches, personal enemies etc.) can cause life-threatening risks to the patient, or make the patient's private matters publicly available [11]. For example, in a simple scenario, a patient's body sensors transmit his/her body data to a nurse/caregiver; it may happen that an attacker is also eavesdropping the patient data while the data is transmitting, and consequently the patient's privacy is breached. Later that attacker can post the patient data on s social site (Facebook or Twitter, etc.), and thus pose risks to the patient's privacy.

Moreover, traditional security mechanisms needed unlimited resources, so they cannot be directly applied to the extremely resource-constrained sensor nodes. While WMSNs' security requirements are the same as those of traditional networks, namely availability, confidentiality, integrity, authentication, data freshness and non-repudiations, thus resource conscious security protocols have emerged as one of the critical issues in healthcare applications using wireless medical sensor networks. There are other survey studies on security and privacy issues in wireless healthcare applications [7-10,12-15] . However, these studies discuss limited information about these security issues.

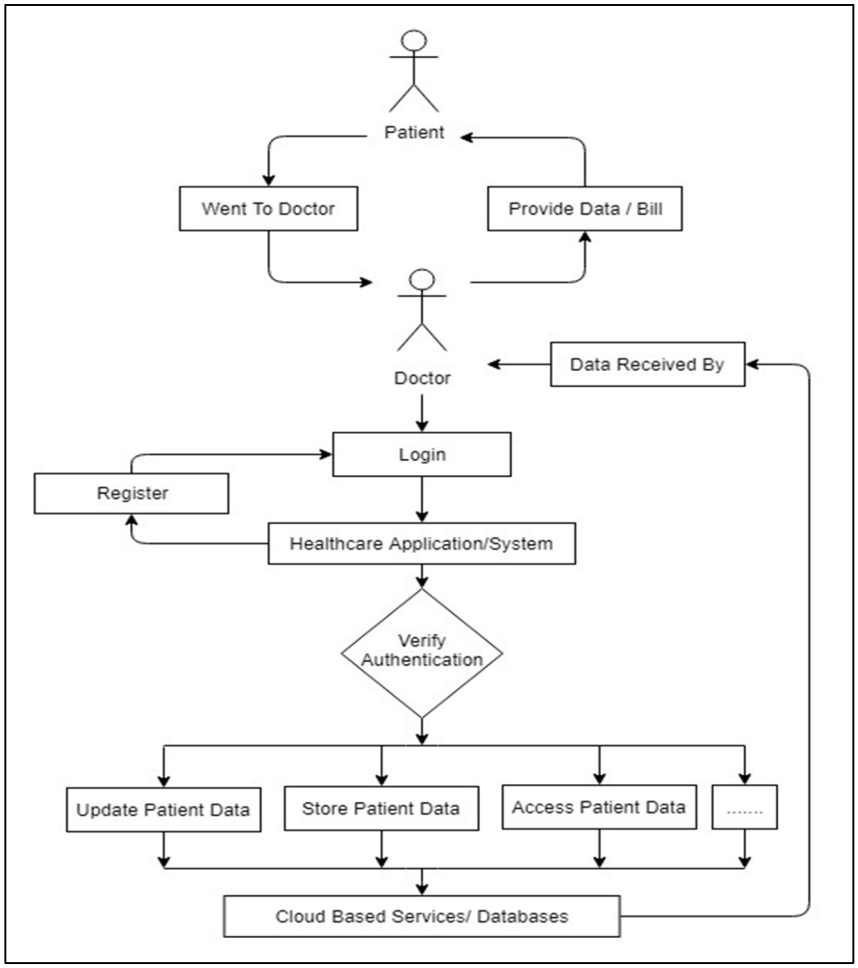
IV. DESIGN

To carry out this research work, the method of survey, statistics, study of use of apps were taken into consideration. The survey was directed towards the doctors. The aim of survey was to understand the need from their perspective. Based on the need, the security aspects were shaped and put into consideration while developing the android application.

The various aspects under scrutiny are:

A. Authenticating a doctor
B. Adding record about a patient in the database
C. Retrieving data about patient
D. Analysis
E. Device lost

The first step to safeguard an application would be to give it in the right hands. To implement this, we need to make it accessible to authentic users. For a healthcare application made for doctors' the only authentic user would be a doctor itself. So, to log into the application, the user must prove to be a doctor. For that purpose, healthcare applications have a Registration form which a doctor needs to fill to get access to the application. The doctor will give all the necessary details about oneself like name, address, registration number and also needs to provide reference of few doctors who already are using the application. In a particular duration those doctors need to verify the newly added doctor. Only after the verification process is complete the doctor will get access to the application. This satisfies the first security aspect of access control.



An application created for doctors' will surely help them in their day-to-day task like keeping patients records. The data need not be typed but just selected from the dropdown menus. The disease, medicines, precautions etc. need not be manually typed. This helps to avoid spelling mistakes and wrong information to be stored in the database. It also saves doctors time and efforts. The reports generated will be kept in a unique folder with patient's name and alphanumeric id which could be accessed only using the One Time Password. The secure authentication is made possible through adding two steps, first, a user recognizes and verifies the SMS on arrival, and then the user confirms again after the initial authentication. In other words, the proposed method provides advantages including the features for mutual authentication and non-repudiation, has a secure means of multi-channel authentication, and can be safely used in the given android app. [17] This safeguards the privacy of the patient's data. As the data could be misused if leaked.

The doctors' application is created to ease the task of a doctor. One of the features of the application is to store the patient's data on the server to avoid manually carry all the reports and previous health records. As we save all the data on cloud to ease the task of both doctor and patient, we call for a security threat. Data breaches, Data loss, Account hijacking, Denial of service, Malicious insiders, Insufficient due diligence etc. [18] Most of these security concerns also apply to a healthcare organization's self-hosted IT infrastructure. These issues should give pause to healthcare organization and spur them to ensure that prospective cloud providers expertly and completely mitigate these risks, and that a strategy and action plan are in place to identify and address evolving and emerging security and privacy risks.

Another feature of healthcare applications are broadcasting a message and using forums to communicate and find answer to a query. When considering a secure text messaging for healthcare solution, facilities should evaluate the following to ensure an effective answer for their concerns:

1) Patient risks with current policies
2) Healthcare staff's mobile device usage
3) Current administrative approaches
4) Sample policies or templates for implementing secure healthcare texting

All the data collected needs to be utilized in such a manner that it helps doctors and scientist to prevent it in future. To prevent it we need to study present in detail. For this reason, analysis functionality is developed in healthcare applications. Analysis helps the doctor to understand and send the personal, regional or larger unit of data to scientist for Research & Development purpose. [19] When this data is sent to laboratories it is very important to hide the patients' detail and only the necessary information is passed. [20] Here, some healthcare applications use big data to implement this functionality. The big data allows only the higher-level information to be sent for analysis preventing the patients' personal detail.

These data are stored in the cloud and can be shared with an authorized person, who could be a physician, your insurance company, a participating health firm or an external consultant, to allow them to look at the collected data regardless of their place, time, or device [21]. After creating security at each stage what would happen if the device itself is lost or stolen. In this situation we need to ensure that patients' private health information remain secure during such an event. [8] In these cases, we do not need to worry as the data is not stored in the device but on the cloud or remote server. And patients' information cannot be accessed until the OTP is entered. Security accomplished.

V. ETHICS

To establish the presence of healthcare apps, a survey was conducted on the basis of questionnaire mention in the Section V. Appendix. The report of the survey is as follow.

A. Does your Profession Demand use of IT?

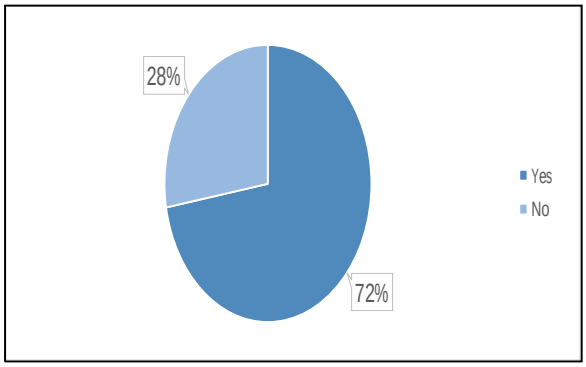


Figure 1 : (72% people think IT is required for their field where as 28% people thinks IT is not required for their field.)

B. Do you use Information Technology?

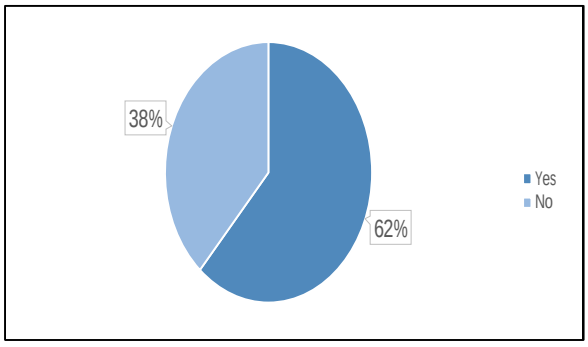


Figure 2. (According to survey 62% people use IT and 38% people still not using IT.)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

C. Which Software Application are you Using?

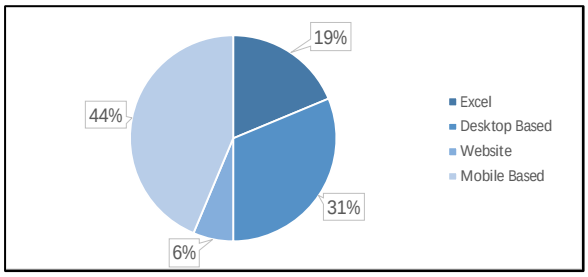


Figure 3. (There are 44% users of mobile based application,31% users of desktop-based application, 19% users of excel application and 6%users of website.)

D. Since How Many Years Are You Using Information Technology?

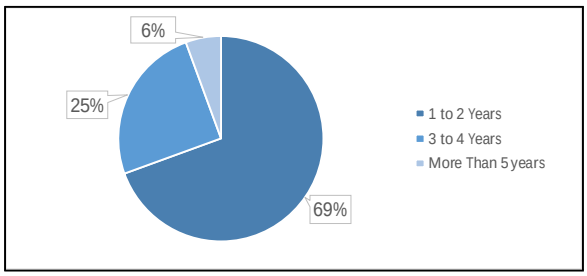


Figure 4 : (69% users are using IT from 1 to 2 years,25% are using IT from 3 to 4 years and 6% are using IT from more than 5 years.)

E. Information Technology Is Used By You For

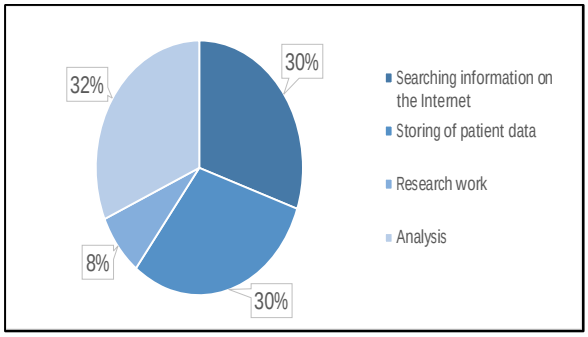


Figure 5 : (IT used by 30% users for searching information on internet,30% users for storing of patient data,32% users for research work and 8% users for analysis.)

F. Does the Application allow to Track the Patient History?

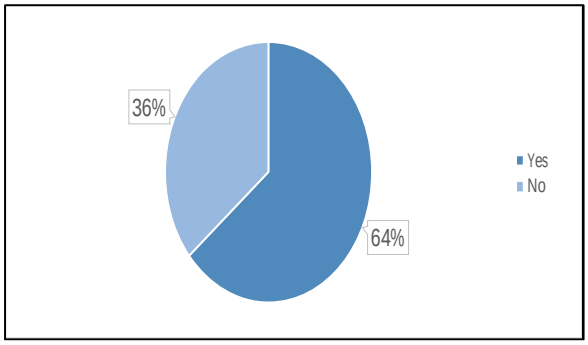


Figure 6 : (64% users used application which track the patient history where 36% users are not using such applications.)

G. Do You Have E-Prescription Facility? (Y/N)

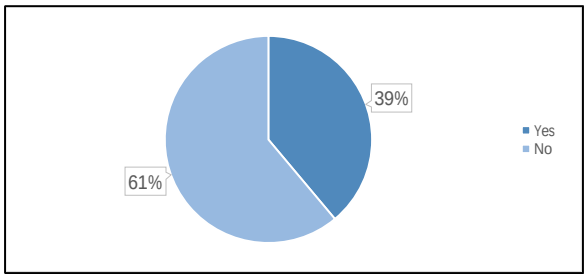


Figure 7 : (39% users are using e-prescription facility where 61% users are still not using e-prescription facility.)

H. Do You Send/Receive alerts or Reminders Electronically? (Y/N)

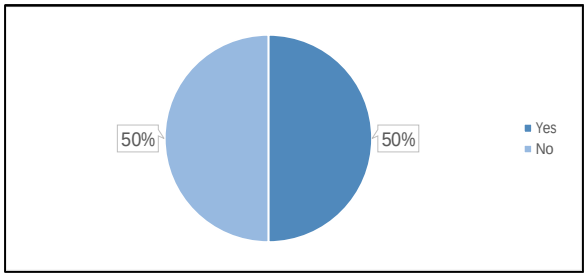


Figure 8 : (50% users are sending/receiving alerts or reminders electronically and 50% users are not sending/receiving alerts or reminders electronically.)

I. Do you Communicate Electronically with Patients to Support remote Consultation and Diagnosis? (Y/N)

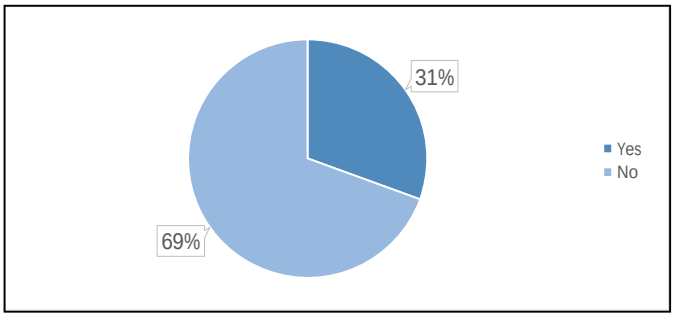


Figure 9 : (31% users communicate electronically with patients and 69% users are not communicate electronically with patients.)

J. Is There Any Specific Reason Why this Software Application is Used by You?

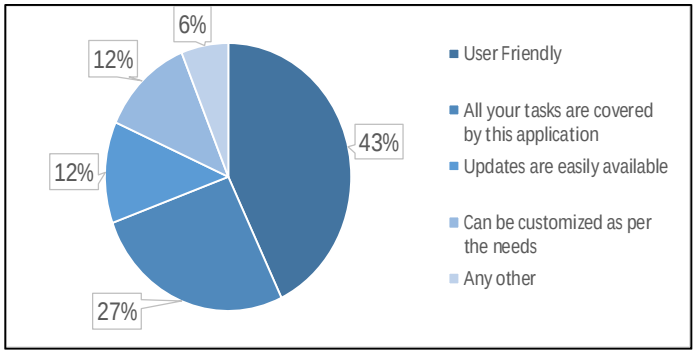


Figure 10 : (Software application used by 43% users because it is user friendly, used by 27% users because all tasks are covered by applications, used by 12% users because updates are easily available, used by another 12% users because it can be customized as per the needs and used by 6% users because of another reason.)

VI. CONCLUSION

In conclusion, the use healthcare application, systems in healthcare sector has several benefits including collecting, storing, manipulating, updating patient's data, analysis of patient's data and help them to diagnose the disease, generate appropriate reports, communicate with patients ,etc. Along with benefits healthcare applications and systems has serious issue regarding with data security. The solution for this issue is using appropriate applications/systems where only authorized users can access them and other important thing is creating awareness and importance about data and security of data as well as educate people about in healthcare sectors.

On the basis of reports of survey, we can conclude that there are some people who are aware about the data and security of data in healthcare sectors and they are using various kinds of application to protect their data. There are some people still not using any application or system to protect their data. May be because of lack of awareness, education or lack of training or may be people are aware but because of some factors like cost, maintenance, etc.

So, gradually number healthcare application/system users are increasing year by year to secure their data. Finally, there is security along with privacy to patient's data by healthcare applications/systems so that the patient can feel secure while sharing or disclosing their data.

REFERENCES

[1] Westin AF, Privacy and Freedom New York: Athenaeum, 1967, page 7.
[2] (2013) Secure healthcare data sharing among federated health information systems. International Journal of Critical Computer-Based Systems
[3] Information & Communications Technology, 2006. ICICT '06. ITI 4th International Conference
[4] Mehregany M. Opportunities and obstacles in the adoption of mHealth. In: R. Krohn, D. Metcalf., editors. mHealth. Health Information and Management Systems Society (HIMSS); 2012. pp. 7–20.
[5] Health Information and Management Systems Society (HIMSS) Advances in wireless technologies for healthcare. 2012 Webinar, June 27.
[6] Dimitriou, T.; Loannis, K. Security Issues in Biomedical Wireless Sensor Networks. In Proceedings of 1st International Symposium on Applied Sciences on Biomedical and Communication Technologies (ISABEL'08), Aalborg, Denmark, 25–28 October 2008.
[7] Xiao, Y.; Shen, X.; Sun, B.; Cai, L. Security and Privacy in RFID and Applications in Telemedicine. IEEE Commun. Mag. 2006, 44, 64-72.
[8] Venkatasubramaniam, K.K.; Gupta, S.K.S. Security for Pervasive Health Monitoring Sensor Applications. In Proceedings of 4th International Conference on Intelligent Sensing and Information Processing (ICPSIP 2006), Bangalore, India, 15–18 December 2006; pp. 197-202.
[9] Leon, M.D.L.A.C.; Garcia, J.L. A Security and Privacy Survey for WSN in e-Health Application. In Proceedings of Conference on Electronics, Robotics and Automotive Mechanics (CERMA'09), Cuernavaca, Morelos, Mexico, 22–25 September 2009; pp. 125-130.
[10] Halperin, D.; Benjamin, T.S.H.; Fu, K.; Kohno, T.; Maisel, W.H. Security and Privacy for Implantable Medical Devices. Pervas. Comput. 2008, 7, 30-39.
[11] Meingast, M.; Roosta, T.; Sastry, S. Security and Privacy Issues with Healthcare Information Technology. In Proceedings of the 28th IEEE EMBS Annual International Conference, New York, NY, USA, 31 August–3 September 2006; pp. 5453-5458.
[12] Meingast, M.; Roosta, T.; Sastry, S. Security and Privacy Issues with Healthcare Information Technology. In Proceedings of the 28th IEEE EMBS Annual International Conference, New York, NY, USA, 31 August–3 September 2006; pp. 5453-5458.
[13] Ng, H.S.; Sim, M.L.; Tan, C.M. Security Issues of Wireless Sensor Networks in Healthcare Applications. BT Tech. J. 2006, 24, 138-144.
[14] Weippl, E.; Holzinger, A.; Tjoa, A.M. Security Aspects of Ubiquitous Computing in Healthcare. Available online: http://www.springerlink.com/content/et5gt8088j388115/fulltext.pdf (accessed on 10 June 2011).
[15] Ameen, M.A.; Liu, J.; Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. J. Med. Syst. 2010, doi: 10.1007/s10916-010-9449-4.
[16] Misic, J.; Misic, V.B. Security Issues in Wireless Sensor Networks Used in Clinical Information Systems. Wirel. Netw. Secur. Sign. Commun. Tech. 2007, doi: 10.1007/978-0-387-33112-6_13.
[17] Ubiquitous Intelligence and Computing, 2014 IEEE 11th Intl Conf on and IEEE 11th Intl Conf on and Autonomic and Trusted Computing, and IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UTC-ATC-ScalCom)
[18] The notorious nine: Cloud computing top threats in 2013
[19] Secure-text-messaging-for-healthcare
[20] Computer and Information Technology (ICCIT), 2014 17th International Conference
[21] Mobile, Ubiquitous, and Intelligent Computing (MUSIC), 2012 Third FTRA International Conference
[22] Healthcare: applications, benefits, and challenges.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

APPENDIX

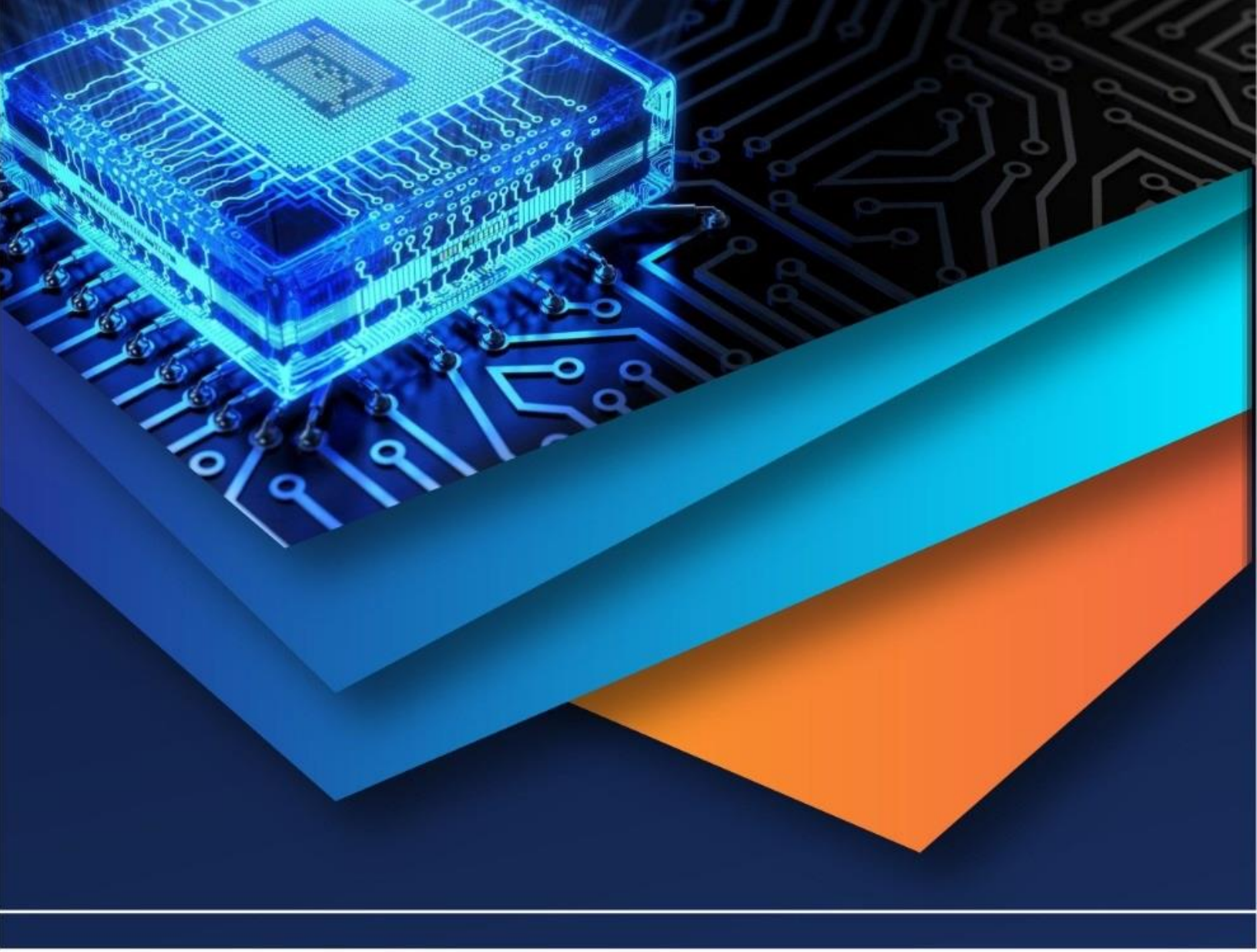
QUESTIONNAIRE

Name:_____
Contact: _____

Email: _____

Specialization: _____ Organization/Hospital attached with: _____
Number of years of practice: _____

1) Does your profession demand use of Information Technology? Y/ N
2) Do you use Information Technology? Y / N
3) Which software application are you using?_____
4) Since how many years are you using Information Technology _____
5) Information Technology is used by you for :
a) Searching information on the Internet
b) Storing of patient data
c) Research work
d) Analysis
e) Means of communication – E-mail
6) Does the application allow to track the patient history? Y / N
7) Do you have e-prescription facility? (Y/N)
8) Do you electronically send/receive referrals to/from health professionals in other organizations? (Y/N)
9) Do you communicate electronically with patients to support remote consultation and diagnosis? (Y/N)
10) Is there any specific reason why this software application is used by you
a) User Friendly
b) All your tasks are covered by this application
c) Updates are easily available
d) Can be customized as per the needs
e) Any other



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY