Nat. Volatiles & Essent. Oils, 2021; 8(5): 9064-9077

NVEO
Natural Volatiles & Essential Oils

Framework Design and Implementation of Novel Healthcare SecuritySystems

P. Ganesh[1], Shobha K R[2], Rajesh Jagdish Sharma[3], R.Sundarrajan[4], K. Geetha[5], Ovi OmkarParadkar[6]

[1]Department of MCA, BMS Institute of Technology and Management, Bengaluru, Karnataka 560064, India
[2]Department of Electronics and Telecommunication Engineering, Ramaiah Institute of Technology, Bengaluru, Karnataka -560054, India
[3]Department of Biotechnology, Vidya Pratishthan's Arts, Science and Commerce College, Maharashtra-413133, India
[4]Department of information Technology, Kalasalingam Academy of Research and Education, Krishnan koil, Tamil Nadu- 626128, India
[5]Department of Computer Applications, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu - 641021, India
[6]Department of Pharmaceutical Chemistry, Yashwantrao Bhonsale College of Pharmacy Sawantwadi, Maharashtra – 416510, India

ABSTRACT

In a summary, some unique improvements in the design of Security Oriented Frameworks for e- Health based medical systems for procurement of pre-diagnosis information access to hospitals for biomedical engineering problem solutions are provided in this research article. NOVEL Healthcare security approaches for maternal hospitals & Pah labs for the purchase of pre-diagnosis information access to hospitals have been developed. The study article outlines various development tactics that might be used to ensure that the created security architecture is successfully implemented in medical applications employing a NOVEL Bot. The paper serves as a ready reckoner for those who are pursing research in this exciting field of medical access data. The simulation results (quantitative results depicted in the form of a table) presented in this paper shows the efficacy of the methodology that is being proposed by us.

Keywords —Cyber Physical system, Maternal Medical data, Simulation, Real Time, NOVEL Bot

INTRODUCTION

Cyber-physical medical systems (MCPS) are essential to life in the sense that greater preference should be given to networked medical device systems that participate in the care of a patient. In hospitals, these technologies are increasingly used to provide high-quality continuing care to patientsin complex clinical scenarios. There have been many challenges in the face of the need to develop complex MCPSs that are both secure and efficient, including achieving high levels of system software assurance, interoperability, contextual decision support, security and confidentiality. MCPS explicitly combines the computing power and the means to contact the physical environment of health systems.

Recently, the 2 main developments in medical devices have been a high degree of reliance on software-defined functionality and extensive network connectivity. Early development means that software plays an increasingly important role in the overall protection of the system. , used individually to treat patients, distributed network medical devices can simultaneously monitor and regulate various aspects of patient physiology. MCPS aims to improve the efficiency of patient care

by providing personalized treatment with patient referral. Such approaches offer new possibilities forMCPS and, more generally, for integrated technologies and for CPS researchers..

Building an eHealth application system with the smooth integration of cloud and mobile technologies and easy to use the UI for elderly patients could be treated as one of the main objectives of security design frameworks. Building security into an eHealth application system which contains users' personal identifiable information and health records is very critical. For elderly users, they are much proned to make user-oriented errors. The purpose of the design framework could be to enable end-to-end strong security layers in the infrastructure of the eHealth application systems. These layers include secure storage, secure access, and secure transmission along with taking adequate measures to avoid unauthorized uses of eHealth application systems, which could be implemented in real time applications also.

For this purpose, one can develop or propose to use a variation of the security testing methodology oriented to communication protocols with the objective to evaluate the robustness of Web Services against XML Injection attacks. For this purpose, security features could be developed using scripts for different types of fault injectors. This Web Service tool can emulate different types of attacks such as XML Injection, Cross-site Scripting (XSS), Brute Force attacks, Middleware Hijacking, among others, thus serving the purpose.

I. BACKGROUND OF ELECTRONIC HEALTH RECORD DESIGN PROCESS

In this section, a brief background regarding the electronic health record design process is presented in a nutshell. Electronic Health Records (EHRs) are digital versions of paper-based patient's health information. EHR applications are increasingly being adopted in many countries. They have resulted in the improved quality in healthcare, convenient access to histories of patient medication and clinic visits, easier follow up of patient treatment plans, and precise medical decision-making process. EHR applications are guided by measures of the Health Insurance Portability and Accountability Act (HIPAA) to ensure confidentiality, integrity, and availability. However, there have been reported breaches of Protected Health Identifier (PHI) data stored by EHR applications. In many reported breaches, improper use of EHRs has resulted in disclosure of patient'sPHI data.

Inefficient application design threatens the integrity of EHRs, which leads to fraud and endangering patient's health. To solve such problems, one can identify HIPAA technical requirements, evaluate an open source EHR application (OpenEMR) for security vulnerabilities using open-source scanner tools (RIPS), and map identified vulnerabilities to HIPAA technical requirements. Security vulnerabilities discovered later in the development cycle are more expensive to fix than those discovered early. Therefore, software developers should strive to discover vulnerabilities as early as possible. Unfortunately, the large size of code bases and lack of developer expertise can make discovering software vulnerabilities difficult. To ease this difficulty, manydifferent types of techniques have been devised to aid developers in vulnerability discovery. One important point in this type of research is to improve the vulnerability detection by comparing the effectiveness of vulnerability discovery techniques and to provide specific recommendations toimprove vulnerability discovery with these techniques.

One can conduct different case studies on different type of electronic health record systems to compare four discovery techniques: systematic and exploratory manual penetration testing, static analysis, and automated penetration testing.

It could be found that a systematic manual penetration testing finds the most design flaws, while static analysis found the most implementation bugs. Finally, one can find the most effective vulnerability discovery technique in terms of vulnerabilities discovered per hour was automated penetration testing. At the end, it could be seen that the results suggest that if one has limited time to preform vulnerability discovery one should conduct automated penetration testing to discover implementation bugs and systematic manual penetration testing to discover design flaws.

Through the development of a black box security test plan, software testers who are not necessarily security experts can work proactively with the developers early in the software development lifecycle. The team can then establish how security will be evaluated such that the product can be designed and implemented with security in mind.

In the next section, we present what are the goals of the research that is presented in this research paper.

I. GOALS OF THE RESEARCH WORK

The goal of the research work taken up in this research paper is to improve the security of applications by introducing a methodology that uses the software system's requirements specification statements to systematically generate a set of black box security tests. A methodology could be developed for the systematic development of a security test plan based upon the key phrasesof functional requirement statements.

The methodology developed could use it on a public requirement specification to create numerous tests & then execute these tests on a number of electronic health record systems. Once tests conducted, it could reveal that quite a number of successful attacks on these five systems, which are used to manage the clinical records for approximately millions of patients, collectively. If non-expert testers can surface the more common vulnerabilities present in an application, security experts can attempt more devious, novel attacks.

Security experts use their knowledge to attempt attacks on an application in an exploratory and opportunistic way in a process known as penetration testing. Penetration testing and similar techniques require the security expert's knowledge to be effective. For example, a security tester might browse through a web application, find a form, and submit several attacks to test that the system properly validates input. She will use the knowledge of successful attacks to drive her next attempt.

A software tester with no security training would lack the knowledge to pursue defects the same way an expert does. Due to time and resource constraints, building security into a product must bethe responsibility of the whole team, not just the security experts who are often only involved in the final phases of testing. One can present different methodologies that uses a software system'sfunctional requirements specification in order to formulate a set of security test cases that assesses the system/s ability to protect itself and its data from malicious intruders.

Everyone from the independent test team, to the developer writing unit tests, should be enabled to emulate attacker behavior and work towards security throughout the development process. Through the development of a black box security test plan that is based on functional requirements specifications, software testers who are not necessarily security experts can work proactively withthe developers early in the software development lifecycle.

The team can then establish how security will be evaluated such that the product can be designed and implemented with security in mind. A black box security test plan is fundamentally different than a black box functional test plan. A security test plan focuses on ensuring a malicious user is not able to force unintended functionality in the system. A functional test plan focuses on ensuring intended functionality is present for a benevolent user.

In the next section, we present a brief literature review or survey of the works that has been carried out by various researchers across the globe.

II. LITERATURE SURVEY

A large number of research papers were collected, referred & studied on the chosen research topic on CBIR and here only a few of them which are going to be used in our future work is being cited & referred to in the references from [1] to [30]. The following paragraphs, gives a brief insight into the detailed survey carried out till date one after the other in succession, in the sense this survey relatesto the study of CBIR and HSV characteristics based on color and shape of images in a brief manner.

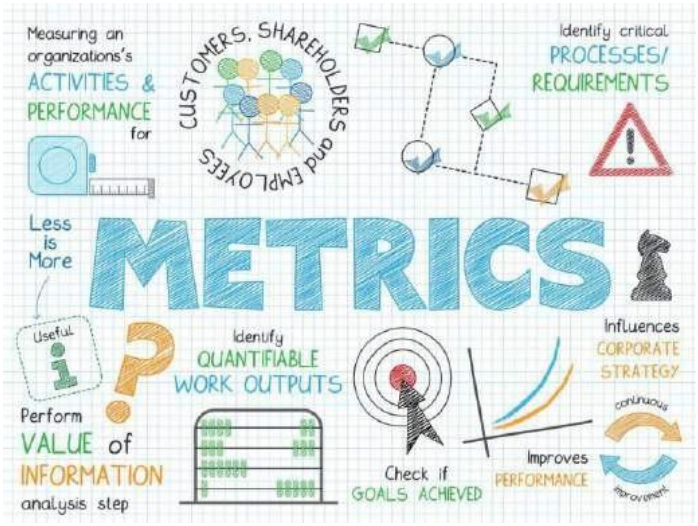

Fig. 1 : Different types of metric groups employed in the security design concepts.

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics, as shown in Fig. 1. OWASP Top 10 Application Security Risks – 2017 is shown in the Fig. 2. Basic metric groups could be classified as follows.

1. Exploitability metrics (attack vectors, attack complexity, privileges required, user interaction)

2. Impact metrics (Confidentiality impact, integrity impact, availability impact)

3. Temporal metric groups (exploit code maturity, remediation levels, report coincidence)

4. Environmental metric groups (modified base metrics, Confidentiality impact, integrity impact,availability impact)

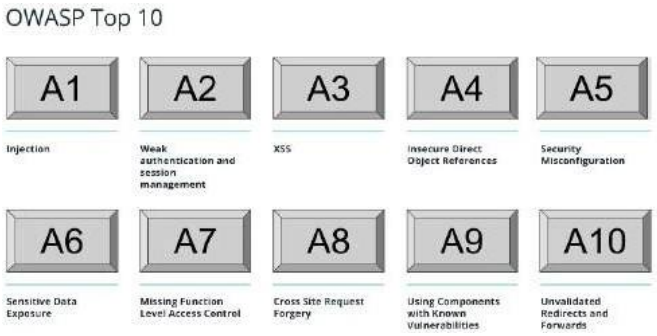

Fig. 2 : OWASP Top 10 Application Security Risks – 2020

A brief literature review w.r.t. the developed research work is as follows. The authors in [1] worked on the Standardized SOA for Clinical Data Interchange in a Cardiac Telemonitoring Environment & produced some significant results. Later on, this work was extended in [2] by the team of researchers who worked on the topic of Security Oriented Design (SOD) Framework for eHealth Systems. In [3], the researchers researched upon the Security Testing Methodology for Evaluation of Web Services Robustness - Case: XML Injection & produced some novel results. Later, the work on Static Analysis of HIPPA Security requirement in EHR Applications was put forth by researchers in [4] with some practical application-oriented problems. In [5], the authors researched upon the technique is not enough: Comparison of Vulnerabilities discovery techniques with some examples.

In [6], the authors researched upon the Systematizing of the Security Test Planning Using Functional Requirements Phrases. Further, the research team in [7] worked on the Plug-and-Play in the Operating Rooms. In [8], the authors worked on the the IEEE 1073 Standard for Medical Device Communications which was used by a number of researchers as a platform for referencing their standard works. In [9], the authors worked on the Interoperable End-to-End Remote Patient Monitoring Platform based on IEEE 11073 bus standards and produced novel results. In [10], the authors worked on the Implementation of an end-to-end standard-based patient monitoring solutions, which was used for a host of science applications.

In [11], the authors worked on the development of an Open Test Bed for Medical Device Integration and Coordinations. In [12], the authors proposed an Information Architecture For Telehealth System Interoperability. Further, work Towards the Technical Interoperability in Telemedicine was developed by the research team in [13]. Work on Interoperable infrastructure and implementation of a health data model for remote monitoring of chronic diseases with comorbidities was developed in [14]. Then, the Interoperability of eHealth System Networked Components which could be used for a host of securital applications was developed by the research team in [15].

In [16], the Health CPS's usage in the Healthcare Cyber-Physical System Assisted by Cloud and Big Data was developed by the engineers. Perspective of health data interoperability on cloud-based medical cyber-physical systems was researched upon by the team in [17]. Challenges and

Research Directions in Medical Cyber-Physical Systems was studied by authors in [18]. Then, the Cost- Efficient Resource Management in Fog Computing Supported Medical Cyber Physical Systemwhich was used for a number of security purposes was studied upon by the team in [19]. A brief Review of Cyber-Physical System in Healthcare was surveyed upon in an excellent survey paper in [20], which was used by majority of the researchers to know about the health care system reviews.

In [21], Interoperable End-to-End Remote Patient Monitoring Platform Based on IEEE 11073 standards was studied upon with, which was extended to the development of secured health care application architecture for cyber-physical systems in [22]. Secure and scalable cloud-based architecture for e-health Wireless sensor networks was developed by the engineers in [23]. Cyber- physical systems which is base for the next computing revolution was developed by researchers in [24]. Then, the Network QoS management in cyber-physical systems was coined by a number of researchers in [25] which lead to the development of an adapted customer relationship management implementation framework for facilitating value creation in nursing homes in [26] in a structured manner.

An Agile and RESTful approach to healthcare information exchange was developed in [27]. A systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: taxonomy, open challenges motivation and recommendations was studied upon in [28], which was extended to providing the service for the pseudonymization of Electronic Healthcare Records Based on ISO/EN 13606 for the Secondary Use of Information in [29]. In an excellent research article published in [30], the implementation experience of a Patient Monitoring Solution based on End-to-End Standards was developed. Standard-based IoT platforms interworking: implementation, experiences, and lessons learned was categorized by the research team in [31].

Then, the challenges and Research Directions in Medical Cyber-Physical Systems was stated in [32]. Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data was studied upon with in [33]. A cloud-based algorithm for detection of injected object in data in motion was researched in [34]. Finally, the auditing of the XSS defense features implemented in web application programs was studied in [35]. Like this, a large number of authors had worked on the similar works, but here only a few of the base works which has been referred to has been presented in a nut-shell.

In the next section, the top 10 OWASP tests with vulnerabilities & the security risks that have been faced is presented with is being taken care of in our research work to arrive at the modified results.

III. OWASP TOP 10 TESTING WITH VULNARABILITIES & THE TOP 10 APPLICATION SECURITY RISKS FACED

The Open Web Application Security Project is a non-profit global community that strives to promote application security across the web. A core OWASP principle is that their knowledge base be freely and easily accessible on their website. With its tens of thousands of members and hundreds of chapters, OWASP is considered highly credible & developers have come to count on it for essential web application security guidance. Testing for OWASP vulnerabilities is a crucial part of secure application development. The sheer number of risks and potential fixes can seem

overwhelming but are easy to manage if you follow a few simple steps as follows.

- Build security into your development process, rather than making it an afterthought
- Test your code against security standards repeatedly throughout development
- Use IDE and CI Pipeline integrations to automate testing
- Identify known vulnerabilities in third-party code to ensure your program does not rely on insecuredependencies

In the following paragraph, the top 10 applications in the security risks that are faced are presented in a nutshell. The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. ... Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Further, the OWASP top 10 vulnerabilities in the year 2020 could be summarized as follows.

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

Finally, it could be discovered almost no individual vulnerabilities with multiple discovery techniques was present. It could also be found that systematic manual penetration testing found the most design flaws, while static analysis found the most implementation bugs. Finally, it was found the most effective vulnerability discovery technique in terms of vulnerabilities discovered per hour was automated penetration testing. These results suggested that if one has limited time to preform vulnerability discovery, one should conduct automated penetration testings to discover implementation bugs and systematic manual penetration testing to discover design flaws. Based on the results of their proposed research, they felt strongly that there is room for improvement for implementing secure EHR systems. This improvement could be accomplished by augmenting the security criteria that EHR systems implement and by taking the time to do a thorough security

Injection

11. Broken Authentication
12. Sensitive Data Exposure
13. XML External Entities
14. Broken Access Control
15. Security Misconfiguration
16. Cross-Site Scripting
17. Insecure Deserialization
18. Using Components with Known Vulnerabilities
19. Insufficient Logging and Monitoring

Finally, it could be discovered almost no individual vulnerabilities with multiple discovery techniques was present. It could also be found that systematic manual penetration testing found the most design flaws, while static analysis found the most implementation bugs. Finally, it was found the most effective vulnerability discovery technique in terms of vulnerabilities discovered per hour was automated penetration testing. These results suggested that if one has limited time to preform vulnerability discovery, one should conduct automated penetration testings to discover implementation bugs and systematic manual penetration testing to discover design flaws. Based on the results of their proposed research, they felt strongly that there is room for improvement for implementing secure EHR systems. This improvement could be accomplished by augmenting the security criteria that EHR systems implement and by taking the time to do a thorough security

analysis using vulnerability discovery tools suited to finding both design- and implementation-levelsecurity vulnerabilities.

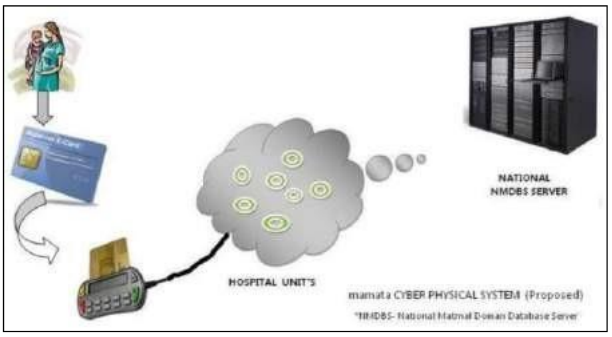

Fig. 3 : The proposed cyber physical system for implementing the security system in the health sector

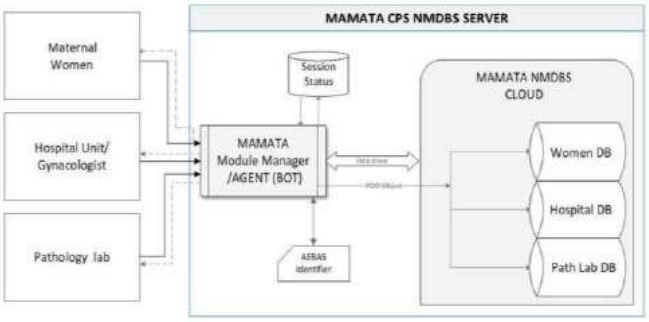

Fig. 4 : The designed & developed NOVEL Bot CPS NMBDS Server for the biomedical applications

	Vulnerability name	Before	After
	Injection	Yes	Yes
	Broken authentication	No	No
	Sensitive data exposure	No	Yes
	XML external entities (XXE)	No	Yes
	Broken access controls	No	Yes
	Security mis-configurations	No	Yes
	Cross-site scripting XSS	Yes	Yes
	Insecure deserializations	Yes	Yes
	Using components withknown vulnerabilities	No	Yes
	Insufficient logging & monitoring	No	Yes

Table 1 : 1st Pen Test PRE-POST Status showing Not Vulnerable (Safe-Green) & Vulnerable(Unsafe-Brown)

IV. PROPOSED RESEARCH WORK

In this section, the proposed research work is presented in which the software implementation process is also carried out. The server was demonstrated & it was advised to identify performance parameter & test for the NOVEL Bot framework with reference to existing system. The final advice to improve those parameters by algorithm or method for diff scenario was carried out. The proper terminologies that were used was checked out before inputting to the algorithm. Performance Parameter - Load/Stress Test was carried out along with the +*performance +89+parameter (Security).

Technical Security Threats findings - as per OWASP was also found out. Pen-Test, i.e., security attacked made on NOVEL Bot Server was used for these purpose & the results being improved and compared with SOA to show the SOD frameworks of few more eHealth systems. The proposed cyber physical system for implementing the security system in the health sector is shown in the Fig.3 along with the designed & developed NOVEL Bot CPS NMBDS Server for the biomedical applications in Fig. 4.

V. CONCLUSIONS / REMARKS

The main objective of the proposed research was to carry out an integrated analysis & to develop some novel features for incorporating the security features in the *e*-health applications of the medical related problems. In view of this objective, which is to be achieved, first step was to carry out a brief review of the survey of the works done in the chosen field (literature survey) by various authors & the final result is the outcome of this output-oriented research paper, which is further used to define the our research problem statement, observing some of the lacunas in the already done works, leading to our main objective and finally to solve it.

Hence, in a nutshell, a brief review of the related research work done in the field of the incorporating of the security features in the *e*-health application were presented in this research paper. Also, some of the drawbacks or the dis-advantages of the works done were also portrayed herewith along with the advantages of the authors works. These lacunas or the demerits could be taken up as some of the identified problems that could be solved upon defining the problem and arriving at good optimized solutions. This developed research paper is definitely going to serve as a ready reckoner or as a base for the researchers.

The literature survey presented in this research work could be used further to define the research problem & verify it through effective simulation results in the Matlab / LabVIEW / Scilab environment in order to substantiate the research problem undertaken in comparison with the work done by the earlier authors in the relevant field, in the sense to solve the desired objective & arrive at the solution of the research work. Further, extensions can be done for the real time implementation ofthe simulated works in order to validate the simulated results. .

Finally, it was concluded that to perform one more Pen test from other security expert (Ethical hacker) & (to observe vulnerabilities severity and findings …if any) and the flexibility points to cover up all gears of NOVEL Bot were developed. In this research article, a brief introduction to the NOVEL Bot Cyber physical system was presented in pictorial form as well in descriptive form alongwith the work-flow. The 2nd pen test (security test) was conducted; results were obtained

andcompared with the older results. The performance metrices were also obtained from which it could be judged that the work done by us is far more superior to the researches carried out by the earlier ones.

REFERENCES

[1] Gazzarata, R., Vergari, F., Cinotti, T. S., & Giacomini, M. (2014). A Standardized SOA for Clinical Data Interchange in a Cardiac Telemonitoring Environment. *IEEE Journal of Biomedical and Health Informatics*, 18(6), 1764–1774.

[2] Yu, W. D., Davuluri, L., Radhakrishnan, M., & Runiassy, M. (2014). A Security Oriented Design (SOD) Framework for eHealth Systems. *2014 IEEE 38th International ComputerSoftware and Applications Conference Conference*.

[3] Marcelo Invert Palma Salas, Paulo Lício de Geus, Eliane Martins, Security Testing Methodology for Evaluation of Web Services Robustness - Case: XML Injection, *2015 IEEE World Congress on Services*, Brazil.

[4] Maryam Farhadi, Hisham M. Haddad, Hossain Shahriar. Static Analysis of HIPPA Security requirement in EHR Applications. *IEEE 42nd Int Conf. on Computer Software & Application*- 2018.

[5] Andrew Austin and Laurie Williams, One Technique is not enough: Comparison of Vulnerabilities discovery techniques. *2011 IEEE Int. Symposium on Empirical software engineering and measurement.*

[6] Ben Smith, Laurie Williams North Carolina State University Systematizing Security Test Planning Using Functional Requirements Phrases, *2011 IEEE Conference*

[7] Julian M. Goldman, Richard A. Schrenker, Jennifer L. Jackson, Susan F. Whitehead, Plug-and- Play in the Operating Room of the Future, *Journal of Biomedical Instrumentation And Technology And Journal of Association Of Advanced Medical Instrumentation*. June 2005, pg 194-199.

[8] Robert J. Kennelly Chair," T*he IEEE 1073 Standard for Medical Device Communications"*

IEEE 1073 General Committee Principal, Eden Shores Consulting, 1998.

[9] E, Joost de Folter, Vivek Verma, Hulya Gokalp , Interoperable End-to-End Remote Patient Monitoring Platform based on IEEE 11073 PHD and ZigBee Health Care Profile, TBME-00143-2017 1 *IEEE Transactions on Biomedical Engineering.*

[10] Martmez, J. Fernandez, M. Galarraga, L Serrano, P. de Toledo "Implementation of an end-to- end standard-based patient monitoring solution, *IET journal of communication*, 2014

[11] Andrew King, Sam Procter Dan Andresen, John Hatcliff‡, Steve Warren Kansas State University, "An Open Test Bed for Medical Device Integration and Coordination", *ICSE'09*, May 16-24, 2009, Vancouver, Canada.

[12] Steve Warren, Ph.D.,L Richard L. Craft, M.S.,2 Raymond C. Parks , Proposed Information Archetechture For Telehealth System Interoperability. US Govt Initiative I.E Sandia Labs Project Ponsored By USA Government., *IEEE Engineering In Medical*

[13] Mary Ann Liebert, Inc. Sandia labs, Toward Technical Interoperability in Telemedicine, *IEEE Conf Engg In Medicine & Biology*, Volume 11, Number 3, 2005 © Project ponsored by USA Government

[14] Dameron, R. Le Bouquin Jeannès, Université de Rennes France , Interoperable infrastructure and implementation of a health data model for remote monitoring of chronic diseases with comorbidities.

[15] Alexandru Soceanu, Alexandru Egner, Florica Moldoveanu Towards Interoperability of eHealth System Networked Component. *IEEE Conference on Control Systems And Computer Science* 2014

[16] Yin Zhang, Meikang Qiu, Senior Member, IEEE, Chun-Wei Tsai, Member, IEEE, Mohammad Mehedi Hassan, and Atif Alamri, Member, IEEE "HealthCPS: Healthcare Cyber-PhysicalSystem Assisted by Cloud and Big Data" *IEEE Systems Journal*, Vol. 11, No. 1, March 2017

[17] Mona A. Alhumud1, M. Anwar Hossain and Mehedi Masud, "Perspective of health data interoperability on cloud-based medical cyber-physical systems", *Department of Computer Science, Taif University, KSA*

[18] Insup Lee, Fellow, IEEE, Oleg Sokolsky, Member, IEEE, Sanjian Chen "Challenges and

Research Directions in Medical Cyber-Physical Systems", *IEEE Conf. Paper.*

[19] LIN GU, DEZE ZENG, Cost Efficient Resource Management in Fog Computing Supported Medical Cyber-Physical System" 2168-6750 2015 IEEE. *Transactions on emerging computing*, Vol 5, NO. 1, MARCH 2017

[20] Shah Ahsanul Haque, Syed Mahfuzul Aziz, andMustafizur Rahman Review of Cyber-Physical System in Healthcare Hindawi Publishing Corporation, *International Journal of Distributed Sensor Networks*, Volume 2014, Article ID 217415, 20 pages.

[21] Malcolm Clarke; Joost de Folter; Vivek Verma; Hulya Gokalp "Interoperable End-to-End Remote Patient Monitoring Platform Based on IEEE 11073 PHD and ZigBee Health Care

Profile" *IEEE Transactions on Biomedical Engineering*, Year: 2018, Volume: 65, Issue: 5 Pages: 1014 – 1025.

[22] J. Wang, H. Abid, S. Lee, L. Shu, and F. Xia, "A secured health care application architecture for cyber-physical systems," *Control Engg. and Applied Informatics*, vol. 13, no. 3, pp. 101– 108, 2011.

[23] Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and scalable cloud-based architecture for e-health Wireless sensor networks," *Proceedings of the International Conference on Computer Communication Networks* (ICCCN '12), Munich, Germany, 2012.

[24] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," *Proceedings of the 47th Design Automation Conference* (DAC '10), pp. 731–736, June 2010.

[25] F. Xia, L. Ma, J. Dong, and Y. Sun, "Network QoS management in cyber-physical systems," *Proceedings of the International Conference on Embedded Software & Systems Symposia*(ICESS'08), pp. 302–307, July-08.

[26] S. R. Gulliver, U. B. Joshi, and V. Michell, "Adapted customer relationship management implementation framework: facilitating value creation in nursing homes," *Total Quality Management & Business Excellence*, vol. 24, pp. 991-1003, 2013.

[27] HL7 Duane Bender, Kamran Sartipi "FHIR: An Agile and RESTful approach to healthcare information exchange" *IEEE 26th International Symposium on Computer Based Medical Systems* (CBMS) ISBN: 978-1-4799-1053-3, ISSN: 1063-7125.

[28] O.S. Albahri, et al., "Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: taxonomy, open challenges motivation and recommendations", *J Med Syst*, 42 (5) (2018), p. 80

[29] Roberto Somolinos; Adolfo Muñoz; M. Elena Hernando; Mario Pascual; et.al., "Service for the Pseudonymization of Electronic Healthcare Records Based on ISO/EN 13606 for the Secondary Use of Information" *IEEE Journal of Biomedical and Health Informatics*, Year: 2015, Volume: 19, Issue: 6, pp. 1937 – 1944.

[30] Martmez, J. Fernandez, M. Galarraga, L Serrano et"Implementation Experience of a Patient Monitoring Solution based on End-to-End Standards" *29th Annual International Conference IEEE Engineering in Medicine and Biology Society*, Lyon, France 2007.ISSN:1094-687X

[31] Jaeho Kim,Jaeseok Yun, Sung-Chan Choi, Dale N. Seed Standard-based IoT platforms interworking: implementation, experiences, and lessons learned, *IEEE Communications Magazine*, Volume: 54, Issue: 7, Print ISSN: 0163-6804, Pages 48-54, July 2016.

[32] Insup Lee, Oleg Sokolsky, "Challenges and Research Directions in Medical Cyber-Physical Systems", *Proceedings of the IEEE* 100(1), 75-90. January 2012.

[33] Y. Zhang, M. Qiu, C. Tsai, M. M. Hassan and A. Alamri, "Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88-95, March 2017, doi: 10.1109/JSYST.2015.2460747.

[34] Thouhedul Islam; Rashidah Funke Olanrewaju; Othman O. Khalifa MotionSure: A cloud-based algorithm for detection of injected object in data in motion, *2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application* (ICSIMA), Year: 2017, Pages: 1 – 6.

[35] Auditing the XSS defence features implemented in web application programs L. K. Shar; H. B.

K. Tan, *IET Softwar*e, Year: 2012, Volume: 6, Issue: 4 Pages: 377 - 390, Print ISSN: 1751- 8806.