A LITERATURE SURVEY ON HOW CYBER SECURITY MIGHT BE IMPROVED IN HEALTH CARE

1* Supriya Bhosale,2Ashwini Kale,3Sunita Patil

1,2 Department of IT, 3 Department of E&TC, DYPCOE, Talegaon, Pune,India
(*supriya.bhosale@dyptc.edu.in)

Abstract: — It has become progressively certain that Cyber security is a risk factor in health care services information. Therefore, many common threats keep on being problematic in medical care. There are deep insights to understand those threats. Another growing threat in the medical information is the medical devices. Medical devices more and more connected to the internet, hospital networks, and alternative medical devices to produce options that improve health care and increase the power of health care suppliers to treat patients. A deep literature survey has been carried out for the techniques and the theories that are been proposed to improve Cyber security in healthcare.

Key Words: Cyber security, Medical information, Healthcare Devices, Information Security, Vulnerabilities, Threat, Risk factor

I. INTRODUCTION

Earlier the health care information was in the paper format. Later, this paper format information was transformed into the electronic medical record systems. The electronic health care records management offers advantages related to easy accessibility and use of the patient information, no limitation in time, space and human resources for monitoring patients [1]. As we all know that Cybersecurity plays an important role in maintaining authenticity and security of the information. This field has become a lead in securing the data. Its main goal is to prevent the data from the unauthorized access and usage for any unfair means. Similarly, Cybersecurity also plays a vital role in the health care. The information that is authentic and secured may consists the information about the patient. As there is inclusion of various devices in the health care, it has become more important to secure the devices for the health care providers. Health care industries are slow to respond and are lagged behind other industries in terms of Cyber security.

II. LITERATURE REVIEW

A Security Approach for Health Care Information Systems, Iuliana Chiuchisan, Doru-Gabriel Balan, Oana Geman, Iulian Chiuchisan, Ionel Gordin.From the perspective of services to the population, with vast social implications, in which the security, confidentiality, and access to personal data represents a critical region, the medical services and information systems that are on the base of the strategic management in health care systems, are a theme of maximum interest and rather less approached. In particular, the prospect of at-home health care systems for screening and rehabilitation has raised enormous interest and is seen as a new method to approach the disease more efficaciously. With the development of Information Technology and its major breakthroughs in health care information systems, bringing the rehabilitation and monitoring of the elderly patients from in hospital to more advanced at-home health care systems, information security measures has been raised. A survey of security measures and data communication security involved in health care systems in order to ensure information protection is presented in this paper. The specific security issues involved in the development of a health care system that manages data to support monitoring and rehabilitation of patients with Parkinson's disease is subject of this paper [1].

POStCODE Middleware for Post-market Surveillance of Medical Devices for Cyber Security in Medical and Healthcare Sector in Australia, Junaid Chaudhry, Michael Crowley, Peter Roberts, Craig Valli, Jon Haas.Postmarket surveillance for cyber security of medical devices is an area within the critical infrastructure of health care and public health that has been largely neglected. In developed countries post market quality assurance is passive following complaints from the health care institutions to the manufacturers of the medical devices. Recently, the individual devices can be made traceable allowing any malfunctions to be uniquely identified in each device. There is a lack of clarity on post-sale ownership and management of devices and the updates to the device software. These devices, once plugged into Healthcare Information Systems (HIS) act as FDA approved black boxes that cannot be patched, updated, or secured by anyone other than the manufacturer. Moreover, these unpatched devices provide back doors to cyber criminals to invade the HIS. These devices are soft targets for cyber criminals. So far, we have not come across any mechanisms that address the surveillance of these devices for cyber security. In this paper, we analyzed the post-sale surveillance regulations in Australia. Based on our findings, we present fog-based POSTmarket SurveillanCe Of DEvices (POStCODE) middleware that provides the operational details(excluding

the private data of patient) of the devices directly to the manufacturers. The introduction of the POStCODE will give device manufacturers the means to closely monitor the functioning of their devices. Manufacturers will be able to upgrade devices, patch security vulnerabilities and monitor device performance thereby enhancing health care outcomes. The POStCODE middleware enhances device security whilst building partnerships between the health care facilitators and the device manufacturers [2].

Developing Countries and e-Health Services, Leonid. Androuchko, Isao NakajimaThe Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU) has formed the Study Group 2 of the ITU Development Sector to answer the need to implement of Telemedicine which was widely addressed and questioned since the World Telecommunication Development Conference in Buenos Aires. The Conference noted that "the widespread use of telemedicine services could allow universal health access and consequently facilitate the solution of the principal health problems connected with infectious diseases, pediatrics, cardiology etc., particularly in areas where medical structures are inadequate or non-existing." Although Telemedicine will give benefit to any countries, it will be especially very helpful in developing countries, because these countries normally faced with problem of inadequate of lack of medical infrastructure. Implementation of E-Health services requires multidisciplinary collaboration, with the active participation of telecommunication operators and health care professionals. There is a need to bridge the gap between the telecommunication and health care communities at all levels. National Ministries of Health and Telecommunications also need to work together towards introduction of a EHealth/telemedicine policy and achievement of universal service where emergency services, health and social information systems are concerned. The creation of national associations, committees, task forces and the like, with a multidisciplinary composition, is necessary to bring together telecommunication and health professionals, lawyers, industry and others to assist with awareness-raising at national level [3].

Implementation of E-Health Care System using Web Services and Cloud Computing, Unnati Dhanaliya, Anupam Devani For economical, technological and social development of any country needs enhanced health care system. Development of health care system necessitates large no of manpower, especially when a patients needs continuous monitoring. Power of information and communication technology provided efficient and effective solution to health care system. Using Internet of Things (IoT) condition of a patient can be monitored and controlled remotely. In this paper we present E-Health care system by using cloud computing and web services. Use of cloud computing made remote monitoring and controlling possible. It provides automatic update of measured parameter of patient as well as it sends alert mail by using SMTP (Simple Mail Transfer Protocol) [4].

Cyber Attacks Classification in IoT-based-Healthcare Infrastructure, Amir Djenna, Diamel Eddine Saïdouni Internet of Things (IoT) is one of the most promising technologies that has captured the attention of industrials and academics in recent years. This technology offers a huge add value to many sectors such as home automation, transport, energy and especially health. However, IoT-based healthcare suffers from several security issues that are varied from other domains in terms of methodologies, motivation, and consequences, due to the complexity of the environment and the nature of the deployed devices. This paper provides an overview of the most recent security issues for IoT based healthcare. Particularly, we discuss the probable threats and vulnerabilities, and we provide new classification of cyber-attacks that may affect the healthy functioning of such infrastructures [5].

Cyber-physical systems in healthcare networks, Delia Ioana DOGARU, Ioan DUMITRACHE This paper presents the role of cyber-physical systems in healthcare networks, proposes a general framework for the interconnected medical or medical related devices and service and discusses security problems. The motivation for choosing this topic resumes to the evolution of healthcare systems and lack of concern for security in the medical sector [6].

Health care technology management applied to public primary care health, Saulo José Argenta Garcia, Rubia Alves da Luz Santos, Priscila Sousa de Avelar, Renato Zaniboni, Renato GarciaThe Institute of Biomedical Engineering, Federal University of Santa Catarina (IEB-UFSC) for over three years to develop from the Municipal Health Secretariat of Florianopolis (FLN-SMS) a project management technology medical and hospital (gTMH) in establishments health care (EAS) in primary care. This work is conducted by a Local Center of Clinical Engineering (CELEC), supported by the various areas that make up the Centre for Management and Development of Technology Medical and Hospital (TMH-Ceged) of IEB-UFSC. In this center are developed methodologies for the management of hospitalmedical technology that are applied in Health Centers (SC) of SMS-FLN. This methodology is focused on managing a proposal based on analyzing the process that involves the whole cycle of technology healthcare. The deployment of this system in the CS of SMS-FLN has presented an important impact on the quality of health care in public primary care of the municipality of Florianópolis – SC [7].

Cyber-physical systems security—A survey, Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, Bo LuoWith the exponential growth of cyber-physical systems (CPSs), new security challenges have emerged. Various vulnerabilities, threats, attacks, and controls have been introduced for the new generation of CPS. However, there lacks a systematic review of the CPS security literature. In particular, the heterogeneity of CPS components and the diversity of CPS systems have made it difficult to study the problem with one generalized model. In this paper, we study and systematize existing research on CPS security under a unified framework. The framework consists of three orthogonal coordinates: 1) from the security perspective, we follow the well-known taxonomy of threats, vulnerabilities, attacks and controls; 2) from the CPS components perspective, we focus on cyber, physical, and cyberphysical components; and 3) from the CPS systems perspective, we explore general CPS

features as well as representative systems (e.g., smart grids, medical CPS, and smart cars). The model can be both abstract to show general interactions of components in a CPS application, and specific to capture any details when needed. By doing so, we aim to build a model that is abstract enough to be applicable to various heterogeneous CPS applications; and to gain a modular view of the tightly coupled CPS components. Such abstract decoupling makes it possible to gain a systematic understanding of CPS security, and to highlight the potential sources of attacks and ways of protection. With this intensive literature review, we attempt to summarize the state-of-the-art on CPS security, provide researchers with a comprehensive list of references, and also encourage the audience to further explore this emerging field [8].

A Smartphone based Application to Improve the Health Care System of Bangladesh, Ahmed Imteaj, Muhammad Kamrul HossainNowadays, smartphones have reached every hand and every home. As a result, people are making use of the beneficial mobile applications to make their everyday life easier. This paper focuses on development of a mobile application(app) to help providing an effective health care system. Using this app people can get numerous benefits like finding hospital information in the city, information about cabin, cabin booking with payment, intelligent suggestion on choosing suitable hospital, finding a doctor, emergency service calling, first aid information, alarm system for medication, Body Mass Index (BMI) calculator etc. This application will be a helping hand for people who find it difficult to select hospital, book cabin, contacting doctor for appointment or seeking help in emergency situation. Besides, it will help the masses in their everyday life by providing health care information, aid and medication information, medicine reminder system, etc [9].

Future Delivery of Health Care: Cybercare, C. Everett Koop, Robyn Mosher, Luis Kun, Jim Geiling, Eliot Grigg, Sarah Long, Christian Macedonia, Ronald C. Merrell, Richard Satava, Joseph M. Rosen Health-care system reforms can change the structure of the current U.S. health-care system, from centralized large hospitals to a distributed, networked healthcare system. In our model, medical care is delivered locally in neighbourhoods and individual homes, using computer technologies like telemedicine, to link patients and primary care providers to tertiary medical providers. This decentralization could reduce costs enough to provide all citizens with medical insurance coverage; it would benefit patients and providers; and as a dual-use system, it would better protect the country's resources and citizens in an event of biological terror or natural disasters [10].

Systems Health Care the aspect of home and medical care, Hiroshi Nakajima, Toshikazu Shiga, Yutaka Hate The importance of measuring vital signs and life style activities in ordinary life besides in medical field has been realized more and more. This is because the affect of life style disease in super aging society has been strongly associated with long term nursing care. Additionally, sensing and information technology has been developed for realizing ease of use, cost reduction, and low intrusion. In this article, systems approach to health care is developed by centering home and medical care. The essence of the notion is using sensory data of vital signs and life style activities in both medical field and home by bridging between them to make medical treatment and home self-care efficient and effective. Systems Health Care mainly composes of Health Management and Knowledge Harvesting technologies. First one is designed for continuous health care and improvement by applying index, criterion, and causality. The second is for causal knowledge extraction process from sensory database, which is used in Health Management. The notion and the technologies are studied and discussed in the article. Application studies follow them by centering health care supporting system and employing both vital signal and life style activities monitoring. Blood pressure analysis program used in medical field as vital signal monitoring is employed. Regarding life style activities, active mass monitoring, non-contact sleep monitoring, and weight-loss programs are introduced [11].

Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems, Aakarsh Rao, Nadir Carreón, Roman Lysecky, and Jerzy Rozenblit Medical devices are complex cyber-physical systems exposed to numerous security risks and vulnerabilities. This article presents a dynamic risk management and automated threat mitigation approach based on a probabilistic threat estimation framework. A smart-connected pacemaker case study illustrates the approach [12].

Testing Health-care Integrated Systems with anonymized test-data extracted from Production Systems, Ali Raza, Stephen Clyde
Testing of data-centric health-care integrated systems involve numerous non-traditional testing challenges, particularly in the areas of input validation, functional testing, regression testing, and load testing. For these and other types of testing, the test-data suites typically need to be relatively large and demonstrate characteristics that are similar to real data. Generating test-data for integrated system is problematic because records from different systems need to be inter-related in realistic and less-than perfect ways. Using real-data is also not a feasible choice, because health-care data contains sensitive personal identifying information (PII). As a foundation, this paper provides a classification of testing challenges for health-care integrated systems and a comparison of anonymization techniques. It also narrates our experiences with a test-data creation tool [13] that extracts and anonymizes loosely correlated slices of data from multiple operational health-care systems while preserving those real
data characteristics, discussed under the classification scheme [13].

Security Management in Health Care Information Systems, Berglind Fjola Smaradottir Health care information systems play an important role for communication across the organizational borders of health care services. The electronic health record represents the main entity in the management, exchange and storage of medical information. Health care organizations must adopt strategies for security and privacy risks associated with access to health care information systems, but on the other hand, the information needs to be accessible and readable for authorized health care professionals carrying out patient treatment. This paper

presents a literature review on security management in health care information systems. The aim was to analyze descriptions and definitions of information security policy, access control management and the usability of security solutions [14].

OpenEHR aware multi agent system for interinstitutional health data integration, Vieira-Marques P., Bacelar-Silva G., Patriarca-Almeida J., Robles S., Frade S., Cruz-Correia R.Most patients receive care from many health care providers, and consequently their health data is dispersed over many institutions' paper and EHR-based record systems. This reality leads to a fragmented system of storing and retrieving essential patient data that impedes optimal care leading to the coexistence of somewhat autistic systems. Providing means for scattered clinical information to be congregated where and when needed may have a strong impact on healthcare quality. Interoperability is a major requisite for effectively sharing information between systems. Standards like openEHR play an important role on achieving interoperability. Agents are software entities, which can embody different perspectives of the surrounding environment and act accordingly. They can perceive the dynamic character of the environment and update their knowledge, enabling pro-activeness regarding actions that are better suited according to a particular user and a given set of goals. In this work we extend our previous work of building a VEPR for inter-institutional data integration with the inclusion of openEHR usage for querying and storing data in order to pursuit the efforts towards Health Information Systems semantic interoperability [15].

Smart Grid Information Security – A Research on Standards, WANG YuFei, ZHANG Bo, Lin WeiMin, ZHANG TaoSmart Grid has received tremendous development momentum over the last years. Information and cyber security of smart grid faces severe challenges and has gained considerable importance. First, the characters of smart grid are analyzed and discussed. Then a hierarchical information and communication model is abstracted. Based on the proposed model, the information security risks and information security protection demands of smart grid are studied and summarized. According to the model and security risks, this paper surveys, collects, and study's different smart grid and common information and cyber security standards and guidelines from three dimensions. The dimensions are different domains of smart grid, different hierarchies of the proposed information and communication model, different stages of the information system life cycle. Also, a comparison of these standards is made. After discussed, studied and analyzed, an information security standard architecture is designed and described to guide the electric power utilities in their smart grid information security efforts [16].

Information Security Protection in Software Testing, Yubin Wang, Jinyu Yao, Xiaoxue YuAt the present, information security protection for software testing is faced with serious situation. There are risks of software information interaction and transmission throughout the life cycle in software testing process. Lack of information security protection and technical support will result in important information leakage, such as the source code leakage, etc. By analyzing the leakage way of software information, a method in accordance with the information security requirements is elaborated which composed by technology framework, Controlled library, and test data security etc. The method is throughout the life cycle of software testing process in order to ensure the security of software testing [17].

Seamless Personal Health Information System in Cloud Computing, Wan-Young Chung Noncontact ECG measurement has gained popularity these days due to its non-invasive and conveniences to be applied on daily life. This approach does not require any direct contact between patient's skin and sensor for physiological signal measurement. The noncontact ECG measurement is integrated with mobile healthcare system for health status monitoring. Mobile phone acts as the personal health information system displaying health status and body mass index (BMI) tracking. Besides that, it plays an important role being the medical guidance providing medical knowledge database including symptom checker and health fitness guidance. At the same time, the system also features some unique medical functions that cater to the living demand of the patients or users, including regular medication reminders, alert alarm, medical guidance, appointment scheduling. Lastly, we demonstrate mobile healthcare system with web application for extended uses, thus health data are clouded into web server system and web database storage. This allows remote health status monitoring easily and so forth it promotes a cost-effective personal healthcare system [18].

Poster Abstract: Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices, Yanchen Xu, Daniel Tran, Yuan Tian, Homa Alemzadeh With advances in sensing, networking, and computing, smart medical devices have been widely deployed in various clinical settings. However, cyber attacks on hospital networks and critical medical devices are serious threats to patient safety, security, and privacy. This paper studies the cyber-security attacks that target hospital networks and other interconnected clinical environments. Our goal is to characterize threat models in such environments by studying the public data from vulnerability databases on medical devices and reports on real attacks targeted at hospitalnetworks. We use a keyword-based approach to identify security reports on medical devices. We summarize our observations from the analysis of the vulnerability reports and provide insights into the types and impacts of vulnerabilities [19].

Investigating the Security Threats on Networked Medical Devices, David Zaldivar, Lo'ai A. Tawalbeh, Fadi MuheidatThis paper explores the cyber security threat of Implanted Medical Devices. The widely use of Internet of Thing capable devices in healthcare like pacemakers, infusion pumps, and insulin pumps support patients, at the same time they are considered a point of security threats. All of these devices are susceptible to hacking and exploitation, which has been demonstrated at various cyber security conventions for nearly the past decade. Although some progress in security measures seems to have been made, recent discoveries and interviews with researchers show a battle is still being fought with some manufacturers. Through pressure applied by some of these researchers, The Food and

Drug Administration (FDA) has taken notice and issued safety warnings for some of these devices. We will begin by defining what these devices are and explore why people need them. Next, we will briefly give a history of the Internet of Things, explore prior security issues, and then introduce the security researchers and groups involved with finding the exploits of healthcare devices [20].

From WannaCry to WannaDie: Security Trade-offs and Design for Implantable Medical Devices, Guanglou Zheng, Guanghe Zhang, Wencheng Yang, Craig Valli, Rajan Shankaran and Mehmet A. Orgun Healthcare sectors are increasingly facing cyber security challenges and threats from adversaries due to numerous security flaws and the lack of security safeguards in medical devices. Among these medical devices and systems, security issues that concern implantable medical devices (IMDs) have attracted attention from both academia and the industry. In this paper, we discuss security vulnerabilities in current IMD products by presenting security tests and demonstrations performed by researchers. Based on this, three critical trade-offs in the IMD security design are analyzed, namely security vs. accessibility in medical emergencies, emergency access vs. checkup access and strong security requirements vs. limited IMD resources. Biometrics based security solutions can provide support for emergency access and thus are surveyed, including those using electrocardiogram signals, iris and fingerprints. During the design, we propose to adopt the concept of decoupled design and usable security in order to develop a viable security solution for the IMDs [21].

Information system integrated security, Milena TvrdíkováSecurity is an important part of information system design and development. The security of information system (IS) cannot be solved only by management of information technologies security because information technologies constitute only a part of IS. A comprehensive and integrated view of the security of IS considering all its parts (hardware, software, human factor, data, and the impact of real world), is presented in the paper. The design of well-implemented information security management system is the reliable way towards the safety of information in a company or in an institution [22].

III. CONCLUSION

Today, due to automation, there is a huge amount of data that has been produced. The healthcare organisations are not able to fully manipulate the data as the data is in huge amount. Including manipulation, security of this data is also become an important aspect. Space is not the issue but to secure the data in the given span of time might be the major factor affecting the authentication of the data. As we all know that huge amounts of data can be stored in the cloud storage but to secure the cloud storage is the challenging part. IoT-based devices used in healthcare also needed to be secured as the sensors of the IoT based devices produce large amount of data.

As the data includes the personal information of the patients, it needs to be secured and prevent from getting the data into the hands of the unauthorized person. The databases that include the medical information should be secured because the exploiters can inject the vulnerable content in the database as well. There are various mechanisms used to secure the medical information from getting exploited by the unauthorized users. So, here was the deep literature survey about how Cybersecurity might be improved in Health care.

REFERENCES

[1] Chiuchisan, Iuliana, Doru-Gabriel Balan, Oana Geman, Iulian Chiuchisan, and Ionel Gordin. "A security approach for health care information systems." In *2017 E-Health and Bioengineering Conference (EHB)*, pp. 721-724. IEEE, 2017.

[2] Chaudhry, Junaid, Craig Valli, Michael Crowley, Jon Haass, and Peter Roberts. "POStCODE Middleware for Post-Market Surveillance of Medical Devices for Cyber Security in Medical and Healthcare Sector in Australia." In *2018 12th International Symposium on Medical Information and Communication Technology (ISMICT)*, pp. 1-10. IEEE, 2018.

[3] Androuchko, Leonid, and Isao Nakajima. "Developing countries and e-health services." In Proceedings. 6th International Workshop on Enterprise Networking and Computing in Healthcare Industry-Healthcom 2004 (IEEE Cat. No. 04EX842), pp. 211-214. IEEE, 2004.

[4] Dhanaliya, Unnati, and Anupam Devani. "Implementation of e-health care system using web services and cloud computing." In *2016 International Conference on Communication and Signal Processing (ICCSP)*, pp. 1034-1036. IEEE, 2016

(ICCSP), pp. 1034-1036. IEEE, 2016.

[5] Dienna, Amir, and Diamel Eddine Saïdouni. "Cyber attacks classification in IoT-based-healthcare infrastructure." In *2018 2nd Cyber Security in Networking Conference (CSNet)*, pp. 1-4. IEEE, 2018.

[6] Dogaru, Delia Ioana, and Ioan Dumitrache. "Cyber-physical systems in healthcare networks." In *2015 E-Health and Bioengineering Conference (EHB)*, pp. 1-4. IEEE, 2015.

[7] Garcia, Saulo José Argenta, Rubia Alves da Luz Santos, Priscila Sousa de Avelar, Renato Zaniboni, and Renato Garcia. "Health care technology management applied to public primary care health." In *2011 Pan American Health Care Exchanges*, pp. 250-253. IEEE, 2011.

[8] Humayed, Abdulmalik, Jingqiang Lin, Fengjun Li, and Bo Luo. "Cyber-physical systems security—A survey." *IEEE Internet of Things Journal* 4, no. 6 (2017): 1802-1831.

[9] Imteaj, Ahmed, and Muhammad Kamrul Hossain. "A smartphone based application to improve the health care system of Bangladesh." In *2016 International Conference on Medical Engineering, Health Informatics and Technology (MediTec)*, pp. 1-6. IEEE, 2016

[10] Koop, C. Everett, Robyn Mosher, Luis Kun, Jim Geiling, Eliot Grigg, Sarah Long, Christian Macedonia, Ronald C. Merrell, Richard Satava, and Joseph M. Rosen. "Future delivery of health care: Cybercare." *IEEE Engineering in Medicine and Biology Magazine* 27, no. 6 (2008): 29-38.

[11] Nakajima, Hiroshi, Toshikazu Shiga, and Yutaka Hata. "Systems Health Care the aspect of home and medical care." In *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2616-2621. IEEE, 2012.

[12] Rao, Aakarsh, Nadir Carreon, Roman Lysecky, and Jerzy Rozenblit. "Probabilistic threat detection for risk management in cyber-physical medical systems." *IEEE Software* 35, no. 1 (2017): 38-43.

[13] Raza, Ali, and Stephen Clyde. "Testing Health-care Integrated Systems with anonymized test-data extracted from Production Systems." In *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 457-464. IEEE, 2012.

[14] Smaradottir, Berglind Fiola. "Security Management in Health Care Information Systems—A Literature

Review." In *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 1742-1746. IEEE, 2017.

[15] Vieira-Marques, P., J. Patriarca-Almeida, S. Frade, G. Bacelar-Silva, S. Robles, and R. Cruz-Correia. "OpenEHR aware multi agent system for inter-institutional health data integration." In *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-6. IEEE, 2014.

[16] Wang, Yufei, Bo Zhang, WeiMin Lin, and Tao Zhang. "Smart grid information security-a research on standards." In *2011 International Conference on Advanced Power System Automation and Protection*, vol. 2, pp. 1188-1194. IEEE, 2011.

[17] Wang, Yubin, Jinyu Yao, and Xiaoxue Yu. "Information Security Protection in Software Testing." In *2018 14th International Conference on Computational Intelligence and Security (CIS)*, pp. 449-452. IEEE, 2018.

[18] Chung, Wan-Young, and Ee May Fong. "Seamless personal health information system in cloud computing." In *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 3658-3661. IEEE, 2014.

[19] Xu, Yanchen, Daniel Tran, Yuan Tian, and Homa Alemzadeh. "Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices." In *2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pp. 23-24. IEEE, 2019.

[20] Zaldivar, David, A. Tawalbeh Lo'ai, and Fadi Muheidat. "Investigating the Security Threats on Networked Medical Devices." In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0488-0493. IEEE, 2020.

[21] Zheng, Guanglou, Guanghe Zhang, Wencheng Yang, Craig Valli, Rajan Shankaran, and Mehmet A. Orgun. "From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices." In *2017 17th International Symposium on Communications and Information Technologies (ISCIT)*, pp. 1-5. IEEE, 2017.

[22] Tvrdíková, Milena. "Information system integrated security." In Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions, pp. 158-169. IGI Global, 2012.