Transactions on Machine
Learning and Data Mining
Vol. 13, No. 2 (2020) 61 - 81

P-ISSN: 1865-6781, E-ISSN 2509-9337
ISBN 978-3-942952-78-1

ibai Publishing
www.ibai-publishing.org

Corona Virus Global Health Transformation to Telemedicine, the Quality-of-Service Provision, and the Cybersecurity Challenges

Eduard Babulak[1], Petra Perner[2]

[1]Department of Computer Science, Liberty University, Lynchburg, VA, USA
[2]FutureLab Artificial Intelligence_IBaI_II, Germany
babulak@ieee.org, pperner@ibai-institut.de

Abstract. The telecommunications industry in last decade went through the dramatic changes motivated by mobility, wireless technologies, and miniaturization. The current advances in Internet, Information Communication Technologies (ICT), Cloud Computing and Smart Ubiquitous Computational Devices create platform for ubiquitous access to patients' medical record(s), while enabling multi-point live video supported patient care and post-discharge consultations. The continuous increase in the complexity and the heterogeneity of healthcare telecommunications infrastructures requires reliable methodology to assess the quality of service and Cybersecurity provision.

In this paper, the authors discuss the importance of provision of Quality of Service and Cybersecurity in the field of medical care and Electronic Healthcare Management. The main motivation to present our paper is to discuss the use of data communications, Internet, cloud and Smart Ubiquitous Computational Devices in medical field while presenting possible scenarios related to ubiquitous access to Patient's Electronic Health Record and remote control of Medical Surgical Robots via Internet and Smart Ubiquitous Computational Devices.

The message of the paper is to stress the importance of cyber security in the field of telemedicine to-day and tomorrow. The controlling of Smart Ubiquitous Computational Devices, Patient's Electronic Health Record and surgical robots are quite new applications in medical practice, and little is known about the possible scenarios that may be triggered by cyber security.

The data from the medical devices, control data of the robot and Patient's Electronic Health Record are transmitted via data communications networks and Internet. As such, the quality of service provision and proper cyber security solutions are essential to patient's safety and security

The paper presented the importance of Quality-of-Service and Cybersecurity provision in the emerging technologies and data sources that are essential for

providing reliable and high quality clinical care and operation of the public health care system not only in Canada and South Korea but worldwide.

Keywords: Telemedicine, Tele-Surgery, Quality-of-Service, Cybersecurity, E-Health Management, Future Hospital, Smart Ubiquitous Device, Health Economics

1 INTRODUCTION

The global community is facing greatest health challenges triggered by novel COVID-19 pandemic. Countries worldwide are affected significantly and over a long time-period by the pandemic.

In this situation many medical centers had to close. Only urgent not optionable surgeries could be carried out. Other surgeries had to be shifted. This put patients, relatives, but particularly medical doctors before an extreme challenge.

Also, a normal medical consultation became the problem. The patients could enter only individually the medical practices. Internet consultations were furnished, so that no more doctor's visit was necessary for sick notes. Applications were developed for smartphones, that informed the public about especially strongly Corona affected local one`s areas. The spatial-temporal information about the areas where the virus outbreak and the evolvement to other areas is of importance to ordinary people but much more to health authorities and politician so that seriously actions can be taken. It needs seriously data about the number of infected people that must be given by local public health authorities. The WHO seem to have failed on that and the US as one of the most affected countries took her decision to leave the organization.

The situation by Covid-19 showed exemplary how important tele-medicine is and how it can help a normal health precaution to form under extreme terms. That´s why we contributed our paper to Covid-19 and Telemedicine.

In this contribution we want to have a closer look at Telemedicine such as medical Teleconsultation [39] and Telesurgery and the problems and upcoming tasks with Tele-consultation and Telesurgery will be worked out. An important role plays here the guarantee of Cybersecurity. If this cannot be kept Telemedicine may be damaging the live of the patient.

But not only COVID-19 changed the view to telemedicine, numerous viral-infections have arisen and affected global healthcare facilities. Millions of people are at severe risk of acquiring several evolving viral infections through several factors. In [2] authors described about risk factors, chance of infection, and prevention methods of Middle East Respiratory Syndrome Coronavirus (MERS-CoV) and severe acute respiratory syndrome (SARS-CoV), human coronaviruses (CoVs) frequently cause a normal cold which is mild and self-restricting. Global health sector has learnt many lessons through the recent outbreak of MERS and SARS.

The world today is driven by information exchange providing support for the national and global cooperation. The supporting telecommunications infrastructures are becoming more complex providing the platform for the user driven real-time applications over large geographical distances. The essential decisions made concerning the

state welfare, health care systems, education, business, national security, and defense, depend on Cybersecurity and Quality-of-Service provision of the telecommunications and the data networks.

In this paper, the authors discuss the importance of Quality-of-Service provision and Cybersecurity challenges in future health communication infrastructures. The paper presents the use of ICT and smart ubiquitous computational devices in modern hospitals and medical infrastructures, while addressing the importance of Quality-of-Service and Cybersecurity provision in future hospitals, medical case, and national e-health management.

The paper is structured as follows. Section 2 gives and overview about the use of telemedicine in Canada and South Korea. In Section 3, the authors introduce the use of IT, portable miniature medical devices for different medical parameter acquisition of the patient and smart ubiquitous computational devices in medical field. Section 3 presents the telerobotic surgery scenario and work conducted in BioRobotics Lab at the University of Washington in Seattle. Section 4 discuss the application of telemedicine, electronic health record, and smart ubiquitous computational devices and health care economy. Section 5 describes the Cybersecurity challenges in the field of e-health and telemedicine. The section 6 explains the importance of Quality-of-Service provision in future health communication infrastructures. The final Section 7 presents conclusions and further research directions.

2 Telemedicine in Canada and South Korea

Figure 1 shows the smart care in Canada. Patients may have several portable medical devices at home at their body and connect via the internet to the hospital. The patient transmits the data to the hospital so that the data can get included into his medical record. The medical doctor can look at the data and make a medical consultation while sitting in his office. He can give advices for further treatment of the patient or check the condition of the patient remotely.

Fig. 1. Canada Smart-Care [F1]

Especially, in the situation of a pandemic this is of tremendous help. The patient does not need to go to the doctor`s office or the hospital to check with him. The pa-

tient can stay in his environment and does not risk getting in touch with other may be already infected people.

Figure 2 illustrates the e-health system in South Korea. The communication network infrastructure connects multiple departments and offices geographically located at various institutions and centers. Medical doctors with patients, access their medical records via Internet and medical communication network infrastructures daily while utilizing the Smart Ubiquitous Computational Devices.

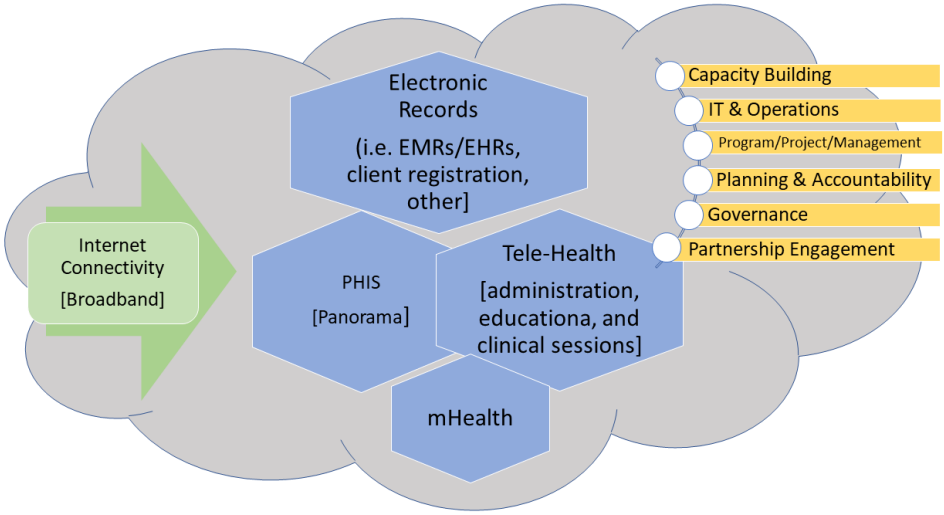

Fig. 2. Canada e-Health Infrastructure 2020-2021 [F2]

The medical communication network infrastructures supporting the patient electronic health record in hospitals are very com-plex and essential part of e-Health Management Systems worldwide. The medical doctors and staff expect secure and reliable services with best Quality-of-Service provision regardless of complexity of medical information flow(s) as an integrated part of daily operation in hospital today. For legal purposes, the patient's private data, such as medical record, insurance policies, etc. that may be transmitted via Internet and ICT networks must be safe and secure against any unauthorized or illegal use.

Technology used in hospitals and medical field today have become essential part of research for hospital management and provision of services such as medical care diagnosis and administration of medication. In medical practice today use of Smart Ubiquitous Computational Devices and ICT and future health care technology facilitates application for electronic health records.

The internet technology and electronics health record have become driving force in 21st century health care system. There are significant challenges healthcare provision in South Korea and elsewhere such as quality, safety, efficiency, and medical care accessibility to remote locations outside large cities areas.

3 Tele-Robotic Surgery Scenario

As one of the leading institutions in the field of medical robotics is the University of Washington. The telesurgery also known as remote surgery, enables a medical doctor to perform the surgery on a patient re-motely via Internet video-conference software [3].

A teleoperated surgical robotic system allows surgical procedures to be conducted across long distances while utilizing wired and wireless communication subject to proper Quality-of-Service provision that may affect the reliability and safety of the patient undergoing telesurgery.

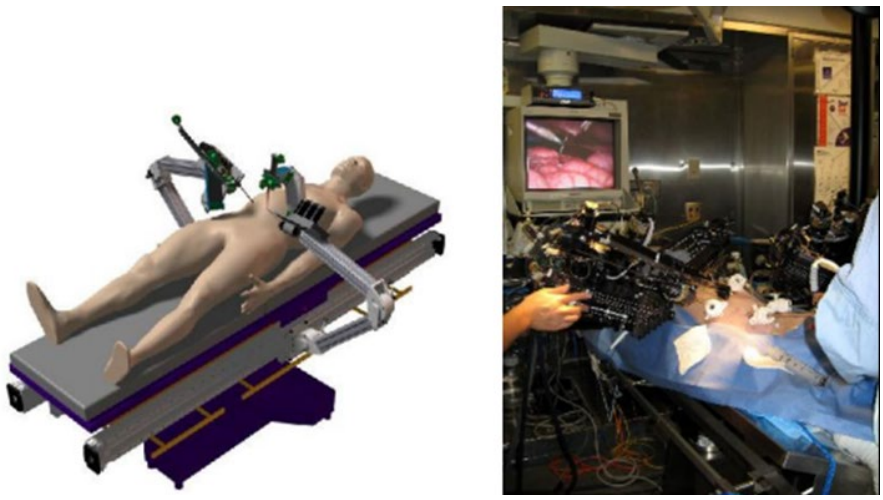

Fig. 3. Telesurgery experiment with Raven system [F2]

Figure 3 shows one example of telesurgery with an open architecture portable surgical robotic system (Raven) developed at the University of Washington. The system was developed for both open and minimally invasive surgery. It has been the subject of an intensive tele-surgical experimental protocol aimed at exploring the boundaries of the system and surgeon performance during a series of field tests under synthetic fixed time delay. One standard task of the Fundamentals of Laparoscopic Surgery (FLS) training kit was used for the experimental protocol. Network characterization indicated a typical time delay in the range of 16-172 ms in field experiments. [4]

Figure 4 shows another telesurgery robotic system called Raven-II - an advanced version of Raven. The system is a platform for collaborative research on advances in surgical robotics. There are seven universities conducting researches utilizing this platform. It has two 3-DOF (Degree in Freedom) spherical positioning mechanisms capable of attaching interchangeable four DOF instruments. Its software is based on open standards such as Linux and ROS (Robot Operating System) to facilitate software development. It is proven that the mechanism is robust enough for repeated

experiments and animal surgery experiments, however, it is not designed to sufficient safety standards for human use [5].

The surgical telerobots have become very valuable technology in the field of medical surgery, while enabling remote surgery on a patient in the environments with extreme conditions such as, battlefield, local pandemic areas or remote areas not accessible to medical doctors. Development of surgical telerobotic is one of the key research areas in surgical medical field.

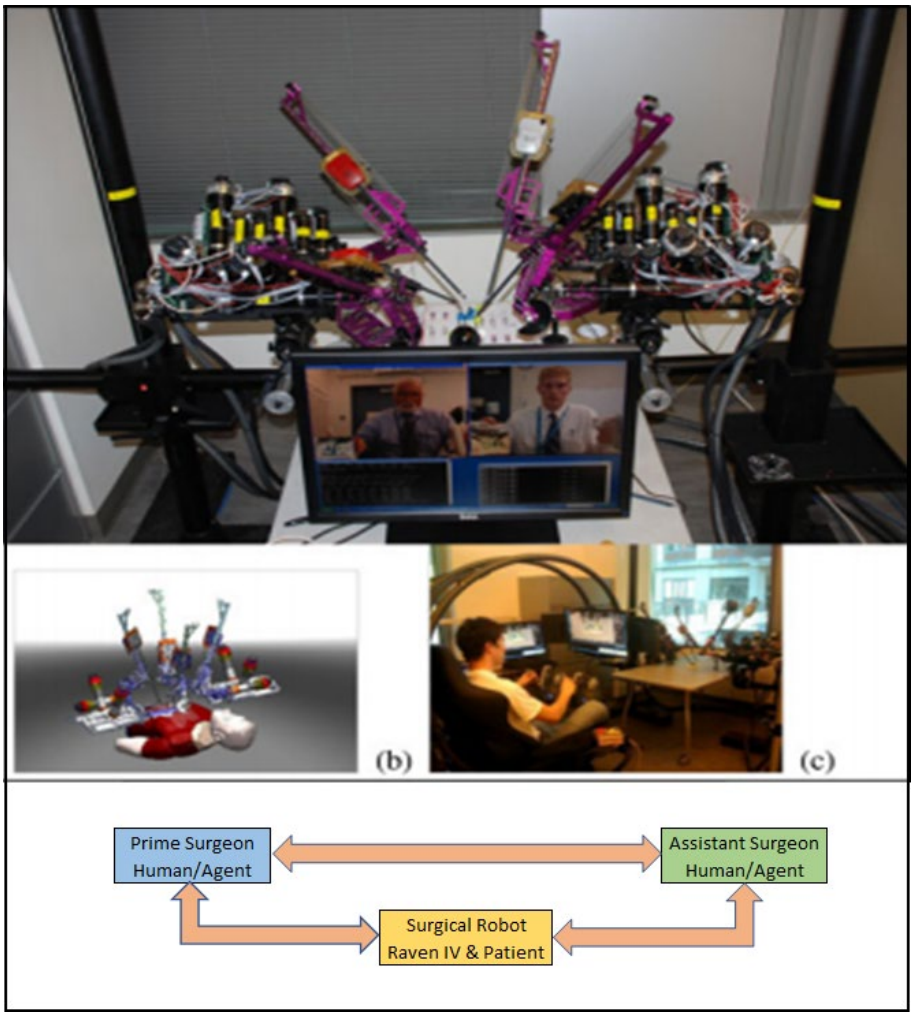

Fig. 4. System architecture of Raven II. [F3]

Currently, the surgical telerobots are still in a developing stage and are becoming more computerized in conjunction with the mechatronics and automated technologies. The remote surgery with telerobot is controlled via a microprocessor communicating

with the control center via computer network and internet cloud. Given the critical data transmission and real time control messaging over communication network, it is important to make sure that there are no malfunctions caused by poor Quality-of-Service provision such as network connection breakdown or network malfunction.

In order to provide best Quality-of-Service, security and safety, communication infrastructure and Internet technology it is essential to build proper network and communication devices with software and hardware security.

Typical network problems, such as increased communication latency or connection failures must be controlled and managed by proper network management software such as HP Open View (HPOW: http://support.openview.hp.com), Packetter (PCT: http://www.packeteer.com/), etc. To create an infrastructure required for the surgical tele-robotic, it is critical to build a medical communication network infra-structure that provide reliable services, proper Quality-of-Service provision.

To improve the Quality-of-Service provision for the surgical tele-robotic [6], researchers of BioRobotics Laboratory at University of Washington proposed a design of a portable low-cost surgical master station for teleoperated surgical robots.

The Quality-of-Service of proposed system was enhanced within following aspects:

- low cost, off-the-shelf hardware, interoperability platform for multiple surgical robots,
- use of Internet connection,
- data collection for experimental surgical tele-robotic.

3.1 Tele-Robotic Example at the Lab at the University of Washington

The proposed system consists of off-the-shelf hardware, such as low-cost hardware (i.e. laptop, omni haptic devices and USB (Universal Serial Bus) foot pedal. The kinematic mapping between the HID (Haptic Interface Devices) and the remote surgical robot in this system is entirely in Cartesian space and the motion commands are position increments, rather than absolute position under the purpose of enhancing the convenience of use of the proposed system.

Figure 5 illustrates the hardware configuration of proposed system. We can see the surgeon's Graphical User Interface (GUI) is appeared in laptop screen. The GUI allows the surgeon to execute high-level commands such as configuring the movement rate of surgical robot arm or selecting a remote IP of surgical Telerobot from a drop-down box. It is also protected with the password-based authentication. The surgical video is appeared in the LCD monitor behind the two omni haptic devices.

With this configuration, motions of HIDs in various direction causes corresponding movement in the surgical field. The reference frame for position increments is a right-handed frame, which is the x-axis pointing right, y-axis pointing up and z-axis pointing out.

The Internet protocols and specific network communication algorithms create communication and control of the proposed tele-robotic system. The communication

system and implementation of surgical tele-robotic at the University of Washington proves to be practical and cost-effective.

Fig. 5. System setup of proposed system in [4 and F4]

3.2 Interoperable Tele-Surgical Protocol (ITP) Example at the Lab of the University of Washington

Second example from University of Washington [7], is a preliminary protocol for interoperability used for multiple robots performing telesurgery at various locations. The objective of the protocol is to develop a communication platform providing support for the multiple surgeries across various interconnected heterogeneous surgical telerobotic master and slave systems.

The secondary aim of the research work at UNIVERSITY OF WASHINGTON is to compare two master station designs side-by-side while improving their performance. The proposed protocol provides a platform for interconnecting multiple teleoperators and tele-surgical systems.

The system testing and performance analysis of the proposed interoperability protocol were conducted between Kagawa-Kawashima Group at the Tokyo Institute of Technology and the BioRobotics Lab at the University of Washington. The results showed the significant Quality-of-Service improvement of telesurgery system [9].

3.3 Surgical Telerobotic with Information Security Example at the Lab of the University of Washington

Provision of proper Quality-of-Service for tele-surgical system must be build side-by-side with proper hardware and software security to prevent any possible attacks or intrusion on remote surgery and surgeons` interaction. Any attack could cause prob-

lems such as fault movement of surgical robot arm during the surgery which could lead to severe injuries or even life risks.

System performance, reliability, availability, simplicity as well as serviceability are essential in conjunction with proper security and Quality-of-Service. The surgical telerobotic experiment at University of Washington promotes further research in area of security and Quality-of-Service. As shown in Figure 6, any possible security threats, and attacks against mobile surgical telerobotic systems could cost human lives.

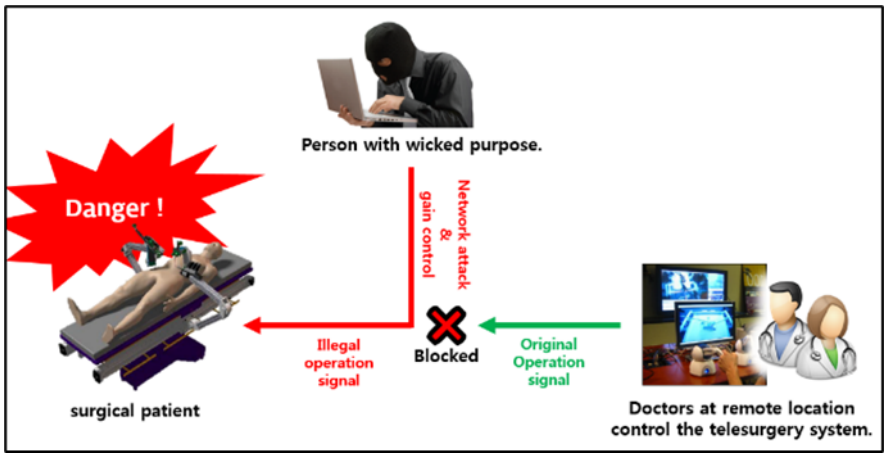

Fig. 6. Cyber Attack against medical system could lead to severe accident threatening human life

Discussion in paper [8] addresses examples of malicious signal jamming, intrusions via communication network that have significant impact on the remote surgery and surgical telerobotic systems. These could be classified in five categories:

- attacks against the wireless communication,
- attacks targeting surgeon-manipulator interaction,
- attacks on the surgeon-side software (e.g., attacks exploiting development (engineering) interfaces),
- attacks on the manipulator-side software (e.g., attacks on the programmable logical controllers (PLC)),
- physical attacks to the patient in the surgery room (that requires in the room observation systems and protection tools).

The analysis of the first category were, remote attacks targeting surgeon-manipulator interaction, such as eves dropping, Jamming and message modification (i.e. false data injection).

Typical examples in second category are simple replay, delay attack, message dropping, combined delay and drop attack, message modification and spoofing attack.

The authors discus new solution with mitigation strategies, while analyzing impact on system's performance, security and safety and suggesting further research-directions in developing telerobotic surgery systems with proper quality-of-service provision, communication security and human safety.

4 Application of Telemedicine to Psychiatric Diseases and Heart Circulatory Illnesses with Smart Ubiquitous Computational Devices

4.1 Application of Telemedicine with Voice and Video Devices to remote Psychiatric Consultation

In the South Carolina Department of Mental Health (SCDMH), the use of video telepsychiatry solution utilizing Internet, Smart Ubiquitous Computational Devices, cloud computing and video collaborative tools contributed to the patient adherence to psychiatric treatment by nearly 200%, reduced readmission, while saving $21.7 million. The telepsychiatry program, named Polycom® RealPresence® Platform [13], is powered by Polycom, Inc., a leading company in open standards-based unified communications solutions for voice and video. The Polycom system creates direct connection between medical doctors and patients via high definition video conference while eliminating the distance. It enables the doctors to observe further non-verbal cues such as lack of eye contact, abnormal movement, or enlarged pupils, which can be even more important than the cues observed with pure verbal interaction. [14].

However, the video should be trustworthy and of good quality. New methods for checking the quality of the video and the trustworthiness of the image content are requested [40].

4.2 Remote Cardiac Monitoring Example

Currently, more than one million Americans receive remote cardiac monitoring to prevent readmissions for heart failure(s), which often occur within 30days of discharge and cost Medicare $6 billion annually. The Indianapolis-based St. Vincent Health successfully conducted a pilot program that enables the nurses to consult the patients with the heart failure and chronic obstructive pulmonary disease via remote video conference. The results showed that the readmissions were reduced by an astonishing 75 percent. In addition, a Department of Veterans Affairs national home telehealth program demonstrated a 25 percent reduction in the number of days of bed care and a 19 percent reduction in hospital admissions [9].

Modern hospitals and medical centers all over the world are exploring ways of utilizing more effectively the electronic health record, smart ubiquitous computational devices, and telemedicine systems via medical communication infrastructures, cloud computing and Internet.

5 The Impact of Telemedicine to the Health Care Economy

The increased use of telemedicine services, system(s) and Smart Ubiquitous Computational Devices in the healthcare contribute to more cost-effective e-Health Management and reduction in hospital readmissions. In 2012, the American Telemedicine Association estimates that more than 10 million Americans directly benefited from telemedicine services [9].

Readmission to hospital is common, costly and may causes overcrowding at emergency department of hospitals [10]. Until recently, In Ontario, Canada, over one-third of patients discharged from hospital are readmitted within 90 days. It was estimated that these readmissions cost over $700 million per year [11].

Focused care after discharge can improve post-discharge outcomes [12]. Recent advances in smart ubiquitous computational devices, mobile video, cloud access enabling multi-point, live video-supported post-discharge programs in conjunction with HER and telemedicine (i.e., such as patient-care consultations or post discharge meetings) contribute to significant reduction of hospital readmissions.

6 Cybersecurity Challenges

6.1 What is Cybersecurity?

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage, or unauthorized access. [15-19] In short, we can say that Cybersecurity is a security technique to protect our networks for Cybersecurity attacks.

Cybersecurity comes from the combination of these two root-words: cyber and security. Cyber means internet, networking, and digital communication. It is all about technologies that we are having nowadays. Security is the degree of resistance to harm or protection from harm. The Figure 7 illustrates example of cybercrime motivated by money or cyber-terror.

Comparing with the traditional security concept in physical world, Cybersecurity is more complex because the intruders use Internet to attack a PC or even patient's medical record remotely.

In particular the mobile security is needed because mobile technology is proliferating in today's medical and corporate environments. While there are significant opportunities to leverage these devices to increase the effectiveness of mobile workers, there are also significant concerns about the privacy of sensitive corporate data stored on the devices that IT must handle. McAfee's Gary Davis predicts that the next hacker target will be mobile devices. "Smartphone's and tablets are at even greater risk than PCs," Davis says, since they have fewer security features and often allow access to an individual's entire network. Just in the last quarter, there was a 76 percent increase in malware on Android devices alone. [20]

Some attacks occur at the national level. Due to its massive scale and significant influence it is considered as a cyberwar or cyber warfare. In contrast with the fact that

traditional war between organizations or nations in physical world is uncommon today, cyber wars are everywhere and have never stop. Past month, the North Korea conducted a series of cyber-attacks on South Korea and United States government websites [21].

Fig. 7. Illegal cyber activity [F4]

Figure 8 illustrates cases of cyber-attacks worldwide, captured and visualized in real time by Honeynet Project [22]. The red dots on the world map represent cyber-attackers and the yellow dots represent the targets. These attacks were conducted systematically on worldwide scale across multiple countries and continents.

The Honeynet Project official website stated that these events are just small portions of cyber-attacks conducted all over the world in the past few years.

As a result, several Cybersecurity standards have been created including, the ISO/IEC 27001, IEC NERC 1300 and RFC 2196 published by IETF.

In the field of e-Health the cyber-attacks may compromise patient's safety or even put human lives in danger. In addition to cyber-attacks it is important to con-sider the errors cause by personnel. One way in which systems may fail, is through the incorrect action of the system's operators [23]. No matter how great the cyber-attack defense mechanism or algorithm of the security system is, the system can be easily exposed to security threats if the security system operator or administrator operates the system incorrectly. In order to prevent any system errors or malfunction, it is essential to implement proper Cybersecurity mechanisms and policies [24]. The inappropriate design of user interface may also misguide the operator/user and in-crease the possibility of fault operation or security breach. Other human errors and real-world computer related crimes that may compromise human safety and system security may include:

- Revealing the system password voluntary or under threats,
- Physically stealing or destroying security devices.

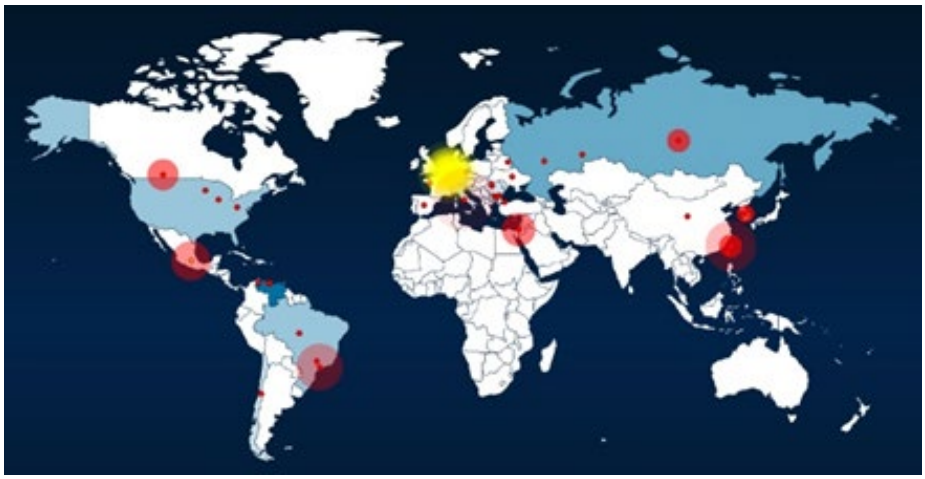

Fig. 8. Cyber-attacks around the world. [F5}

In addition to human factors in Cybersecurity, natural disasters such as fires, earthquakes, floods, and hurricanes can put the e-Health systems in great danger. Natural disasters may compromise or destroy the Cybersecurity systems and devices, as well as causes damage triggered by widespread power outage. Without electricity, the medical data communication network infrastructures, Cybersecurity systems, banks, etc., are nonoperational. From the above, we can see that Cybersecurity is extremely important and complex.

6.2 Importance of Cybersecurity

With the increasing degree of ubiquitous connectivity to support critical operations in national e-Health system, state defense, banking, telecommunication, transportation, electric power grid control, etc., the provision of proper Cybersecurity is essential to any country all over the world [25].

The cyber-attacks may be motivated by political conflict, social tension, economics, religious belief, and any form of extremism [26-27]. The cyber-attacks can occur at anytime, anywhere targeting any SCUBs or e-Health system. In Taiwan, a child at age of only 14 successfully hacked several learning websites of his school, making them unavailable for normal services [27]. Cyber-attacks could cause fatal disaster.

Nowadays, most of the nation's critical infrastructures such as power grid are operated by cyber systems, which means security incident in these cyber systems will affect the physical critical infrastructures and cause a devastating crisis in our real world. Recent findings indicate the growing threat of physical and cyber-based attacks in numbers and sophistication on electric grids and other critical infrastructure systems. [28]

Table 1. Threats to Cybersecurity. [T1]

Threat Category	Types of Threats
Errors and accidents	• Human errors • Procedural errors • Software errors • Electromechanical problems • "Dirty data" problems • Errors, damage, or disturbance of the smart ubiquitous computational devices
Natural hazards	• Power failure • Flooding
Computer crimes	• Theft of hardware • Theft of software • Theft of online music and movies • Theft of time and services • Theft of information • Internet-related fraud • Taking over your PC: zombies, botnets, and blackmail • Crimes of malice: crashing entire systems
Computer criminals	• Individuals or small groups • Employees • Outside partners and suppliers • Corporate spies • Foreign intelligence services • Organized crime Terrorists

From above, we can see that cyber-attacks are everywhere and can be conducted at any time for any purpose by any person or organization from anywhere and can lead to a severe consequence. Thus, Cybersecurity is extremely important for safety of human world.

IT Management [21] pointed out key threats to computers and security and divided them into 4 categories: Errors and accidents, Natural hazards, Computer crimes as well as Computer criminals. The details are shown in table 1.

6.3 Human Safety and Security in Hospitals

Originally, one of the purposes of adopting ICT to hospital and medical system is to increase the human safety by keep it from human errors. Humans tend to act on their perceptions and are emotional thus their performance is usually affected by their emotions. Therefore, human errors are inevitable and fault in hospital and med-ical operation usually result in critical danger in human safety. By assess, detecting and control with ICT human errors can be dramatically eliminated and increased safety can be assured.

However, as the hospital and medical infrastructure relies on ICT more and more heavily, human safety can be threatened by illegal access and attack in telemedicine system. Breach in Cybersecurity of hospital and medical infrastructure can lead to fault operation of critical medical facilities related with radioactivity cure, or paralysis of entire medical system. Not like in common living residence, even power outage caused by cyber-attack in hospital can cause disaster that threatens patients' life. Thus, Cybersecurity in hospital and medical infrastructure should be given enough attention.

6.4 Electronic Health Record and Cybersecurity

As adopting the ICT in hospitals, almost all kinds of information in hospital are recorded in digital format today for effective storing, sharing, searching, etc. An electronic health record is an evolving concept defined as a systematic collection of electronic health information about individual patients or populations [29]. electronic health records may include a range of data, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal stats like age and weight, and billing information [30]. The patient data is private and sensitive and should be protected from illegal access.

Typical electronic health record system must be safe from any possible computer crime, improper identification access. While the information technology crime is becoming more sophisticated and frequent, so have the people charged with preventing it and disciplining its outlaws. It includes enforcing laws, computer emergency response team and tools for fighting fraudulent & unauthorized online uses.

Identification & Access: There are three ways a computer system can verify that someone has legitimate right of access. The security system in electronic health record could authenticate users' identity by determining (1) what you have, (2) what you know, or (3) who you are. Credit cards, debit cards, and cash-machine cards all have magnetic strips or built-in computer chips that identify users to the machine.

The computer room used to access information of electronic health record may kept locked, requiring a key, or may be guarded by security officers, who may need to see an authorized signature or badge (what you have). And the computers could be locked with password (what you know). Some securities are using biometrics, the science of measuring individual body characteristics (who you are).

Protection of Software & Data: Procedures such as making backup disks, protecting against viruses can help security in electronic health record. Security procedures

for protection of software & data in electronic health record include control of access (Access to online files is restricted to those who have a legitimate right to access), audit controls (for tracking which programs and servers were used, which files opened, and so on to creates an audit trail) and people controls (people are the greatest threat to a computer system, security precautions begin with the screening of job applicants).

7 Importance of Quality-of-Service Provision in Future Health communication Infrastructure

The Quality-of-Service is one of the most elusive, confounding, and confusing topics in data networking today [31]. While research papers on Quality-of-Service hardly ever questioning raison d'etre (reason to exit) it is frequently the topic of heated debates. Why there are so many publications and even workshops on a topic which is questioned vehemently while at the same time has so little impact on current products or services [32]. The term service quality may have a different meaning to different people [33]. This is perhaps more accurately called Quality-of-Service, as opposed to service quality, which could be taken to mean the entirety of outcome and experience [34].

The great majority of users are not interested in the engineering of telecommunications networks or its Quality-of-Service specifications; instead they expect fast, reliable, and easy access to online resources, applications and Internet (i.e., online databases, banking services, e-commerce, e-mails, web servers, etc.) [35].

The most critical Quality-of-Service provision assessment is often made by the end user. The users' perception of telecommunications' network infrastructure Quality-of-Service provision is critical to the successful business management operation of any organization. As a result, it is essential to assess the Quality-of-Service provision in the light of user's perception.

The Quality-of-Service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance [36] the users' perception of telecommunications' network infrastructure Quality-of-Service provision is critical to the successful business management operation of any organization.

As a result, it is essential to assess the quality of service provision in the light of user's perception. The typical Quality-of-Service characteristics represent some aspect of the Quality-of-Service of a system, service, or resource, which can be identified and quantified. Disconfirmation model applied to assess the Quality-of-Service provision is illustrated in Fig.9.

The disconfirmation model shows that customer's satisfaction will be dependent on both the size and direction of disconfirmation, with only three possible outcomes. When "perceived" is greater than "expected", customers will be very satisfied; when "perceived" is equal to "expected", customers will be satisfied; when "perceived" is less than "expected", customers will be dissatisfied.

A typical customer is not concerned with how a particular service is provided or with any of the aspects of the network's internal design, but rather with the resulting end-to-end service quality [37]. It must be recognized that the customer's Quality-of-Service requirements are useful, although subjective.

Quality as perceived by customers from a comparison of what they feel the product should offer with their perception of the actual performance of the product.

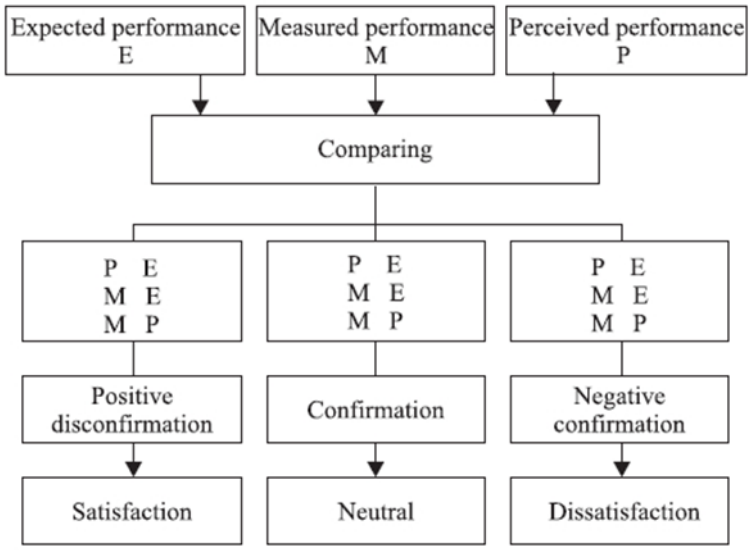

Fig. 9. The disconfirmation model of customer satisfaction. [F6]

When customers register with the network, they already have expectations of how network should perform, and this will cover a whole host of criteria [35] including:

- conformance to specification (user accounts and privileges, accessibility,
- performance (primary network characteristics, such as utilization and error rate),
- reliability (probability of the network malfunction-free performance),
- availability (probability of the network being available),
- simplicity (ease of use),
- serviceability (speed, courtesy, and competence of repair),
- signal and image quality check of the devices.

Thus, to provide users a satisfactory service with ICT, Quality-of-Service provision in future health communication infrastructure is very important.

In support of best Quality-of-Service the provision of Cybersecurity become an essential to electronic health record management at modern hospitals and medical communication network infrastructures worldwide.

Most doctors and medical staff today (i.e., clients) use daily the SUDCs and expect to have immediate access to patients medical record via various communications technologies (i.e., wireless, mobile, fiber optics, Ethernet, etc.) while using almost any

software application, following the banking principle of anywhere, anytime, and anyhow [38].

8 Conclusions and Further Research Directions

The current technological evolution in the electronic health record presents new challenges and research problems to community of experts working in the field of medicine and information technology. However, despite of technological and medical research advancements it is essential that the computerized electronic health record systems will be available to all community of doctors, medical staff and patients worldwide as a tool that ultimately contributes towards the process of humanization of all aspect related to medicine. In the current climate of business-driven hospital and medical service with a focus on the user's satisfaction it is essential that the net-works of hospital infrastructure provide support for a large number of software applications running reliably over very complex interconnection hardware with fast system-response and high security. This requires a great deal of quality of service and Cyber-security within the networks. The paper presented the importance of Quality-of-Service and Cybersecurity provision in the emerging technologies and data sources that are essential for providing reliable and high quality clinical care and operation of the public health care system not only in South Korea but worldwide.

Acknowledgement

This paper was supported by the Sungkyunkwan University and Korea Tech research grants. The authors are grateful for the support received from the Telerobotics Laboratory at University of Washington.

References

1. Riyanti Djalante and Jonatan Lassa and Davin Setiamarga and Aruminingsih Sudjatma and Mochamad Indrawan and Budi Haryanto and Choirul Mahfud and Muhammad Sabaruddin Sinapoy and Susanti Djalante and Irina Rafliana and Lalu Adi Gunawan and Gusti Ayu Ketut Surtiari and Henny Warsilah, Review and analysis of current responses to COVID-19 in Indonesia: Period of January to March 2020, volume = "6", pages = "100091", year = "2020", issn = "2590-0617", doi = https://doi.org/10.1016/j.pdisas.2020.100091
2. Ali Al-Hazmi, Challenges presented by MERS corona virus, and SARS corona virus to global health, Saudi Journal of Biological Sciences, Volume 23, Issue 4, 2016, Pages 507-511, ISSN 1319-562X, https://doi.org/10.1016/j.sjbs.2016.02.019.
3. Wikipedia [Internet]. Wikimedia Foundation, Inc [cited 2013 Jun 11]. Available from: http://en.wikipedia.org/wiki/Remote_surgery.
4. M.J. Lum, J. Rosen, H. King, D.C. Friedman, T.S. Lendvay, A.S. Wright, et al., Teleopera-tion in Surgical Robotics Network Latency Effects on Surgical Performance, in: Conf Proc IEEE Eng Med Biol Soc, USA, Sep 2-6, 2009.

5. B. Hannaford, J. Rosen, D.W. Friedman, H. King, P. Roan, L. Cheng, et al., Raven-II: An Open Platform for Surgical Robotics Research, IEEE Trans Biomed Eng 60 (4) (2013) 954-959.
6. G. Sankaranarayanan, H. King, S.Y. Ko, M.J.H Lum, D.C.W. Friedman, J. Rosen, B. Hannaford, Portable surgery master station for mobile robotic telesurgery, in: Proceedings of the 1st international conference on Robot communication and coordination, Greece, Oct. 15-17, IEEE, 2007.
7. H.H. King, K. Tadano, R. Donlin, D. Friedman, M.J.H Lum, V. Asch, et al., Preliminary protocol for interoperable telesurgery, in: International Conference on Advanced Robotics Advanced Robotics, Germany, Jun. 22-26, 2009, pp. 1-6.
8. T. Bonaci, H.J. Chizeck, Surgical Telerobotics Meets Information Security, in: 21st Usenix Security Symposium, USA, Aug. 8-10, 2012.
9. G. Slabodkin, Problem of hospital readmissions, benefits of telemedicine hit home [Internet]. Fierce Mobile Healthcare. [cited 2013 Jun 13]. Available from: http://www.fiercemobilehealthcare.com/story/problem-hospital-readmissions-benefits-telemedicine-hit-home/2013-02-01
10. 1CADTH [Internet]. Canadian Agency for Drugs and Technologies in Health; c2013 [cited 2013 Jun 13]. Available: http://www.cadth.ca/products/environmental-scanning/environmental-scans/environmental-scan-27
11. CARP [Internet], [updated 2011 Oct 31; cited 2013 Jun 13]. Available: http://www.carp.ca/advocacy/advarticle-display.cfm?documentID=6061
12. C.W. Van, I.A. Dhalla, C. Bell, E. Etchells, I.G. Stiell, K. Zarnke, et al., Derivation and Val-idation of an index to predict early death or unplanned readmission after discharge from hos-pital to the community, CMAJ 182 (6) (2010) 551-557.
13. Polycom. [Internet]. POLYCOM, Inc; c2013 [cited 2013 Jun 13]. Available from: http://www.polycom.com/products-services/realpresence-platform.html
14. Polycom. [Internet]. POLYCOM, Inc; c2013 [cited 2013 Jun 13]. Available from: http://www.polycom.com/company/news/press-releases/2012/201209100.html (Visited on 11 Jun. 2013)
15. L. Wilbanks, Cybersecurity: Welcome to My World, IT Professional 9 (2) (2007) 61-64.
16. L. Hoffman, Exploring a national cybersecurity exercise for universities, Security & Privacy 3 (5) (2005) 27-33.
17. W. Chou, Cybersecurity Costs: Balancing Blanket Security with Real-World Practicality, IT Professional 9 (2) (2007) 16-20.
18. 18. S. Ghemouti-Helie S, A National Strategy for an Effective Cybersecurity Approach and Cul-ture, in: Proc Int Conf Availab Reliab Secur, Poland, Feb. 15-18, IEEE, 2010, pp. 370-373.
19. J.D. Howard, T.A. Longstaff, 1998. A common language for computer security incidents, Technical report, Sandia National Laboratories.
20. Dimensional Research. The Impact of Mobile Devices on Information Security: A Survey of IT Professionals [Internet] Dimensional Research. 2012 Jan [cited 2013 Jun 11]. Available from: http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf
21. IT Management, WILEY, 2011
22. HoneyMap [Internet] Honeynet Project [cited 2013 Jun 13]. Available from: http://map.honeynet.org
23. M.G. Lee, Securing the human to protect the system: Human factors in Cybersecurity, in: in-corporating the Cyber Security Conference, UK, Oct. 15-18, IET, 2012, pp. 1-5.

24. A. Beautement, M.A. Sasse, M. Wonham, The compliance budget: managing security behavior in organizations, in: Proceedings of 2008 Workshop on New Security Paradigms, USA, Sep. 22-25, ACM, 2008, pp. 47-58.
25. N. Ye, Y. Zhang, C.M. Borror, Robustness of the Markov-chain model for cyber-attack de-tection, Reliability 53 (1) (2004) 116-123.
26. R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Z. Qiuming, P. Laplante, Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political, Technology and Society Magazine 30 (1) (2011) 28-38.
27. SINA [Internet]. SINA Corporation, c1996-2013 [updated 2012 Jul 04; cited 2013 Jun 11]. Available from: http://tech.sina.com.cn/it/2012-07-04/09317346411.shtml
28. C.W. Ten, G. Manimaran, C.C. Liu, Cybersecurity for Critical Infrastructures: Attack and Defense Modeling, Systems, Man and Cybernetics, Part A: Systems and Humans 40 (4) (2010) 853-865.
29. T.D. Gunter, N.P. Terry, The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions, Journal of Medical Inter-net Research 7 (1) (2005) e3.
30. Wikipedia [Internet]. Wikimedia Foundation, Inc. [cited 2013 Jun 11]. Available from: http://en.wikipedia.org/wiki/Electronic_health_record#cite_note-1
31. P. Ferguson, G. Huston, Quality of Service, Wiley, 1998.
32. M. Ott, 1998, What is wrong with Quality-of-Service research?, NEC Internal Report, C&C Research Laboratories.
33. E. Babulak, Trader's quality of service specifications and effects on system performance for video-on-demand, in: International Conference of Multimedia and Expo, New York, USA, Jul. 30-Aug. 02, IEEE, 2000, pp. 837-842.
34. R. Johnston, G. Clark, Service Operations Management, Financial Times, Prentice Hall, 2001.
35. E. Babulak, R.A. Carrasco, The university network model for the quality of service provision analysis, International Journal of Mathematics 2 (7) 2002 pp. 651-661
36. Wikipedia [Internet]. Wikimedia Foundation, Inc. [cited 2013 Jun 11]. Available from: http://en.wikipedia.org/wiki/Quality_of_service
37. D.J. Wright, Assessment of alternative transport options for video distribution and retrieval over ATM in residential broadband, IEEE Communication Magazine 35 (12) (1997) pp. 78-87.
38. E. Babulak, R.A. Carrasco. The IT quality of service provision analysis in light of user's perception and expectations, in: International Symposium of CSNDSP, Staffordshire, UK, 2002.
39. Petra Perner, B2ML – E-Business to Manufactoring and LifeSciences, Business Plan of B2ML Company, Leipzig Germany 2013
40. Petra Perner, Novel Methods for Forensic, Multimedia Data Analysis: Part I, Digital Forensic Science, Book Chapter, Intechopen in progress, online available since June 2020 https://www.intechopen.com/online-first/novel-methods-for-forensic-multimedia-data-analysis-part-i. in print

Figure Sources

[F1] Collaborative Video Solution in Healthcare, Center for Digital Government, May 2013 issue, Canada.

[F2] B. Hannaford, D.C. Friedman, H. King, M. Lum, J. Rosen, G. Sankaranarayanan, 2009, Evaluation of RAVEN surgical Telerobot during the NASA Extreme Environ-ment Mission Operations (NEEMO) 12 Mission, Technical Report, Deptment of Elec-trical Engineering, University of Washington.
[F3] B. Hannaford, J. Rosen, D.W. Friedman, H. King, P. Roan, L. Cheng, et al., Raven-II: An Open Platform for Surgical Robotics Research, IEEE Trans Biomed Eng 60 (4) (2013) 954-959.
[F4] G. Sankaranarayanan, H. King, S.Y. Ko, M.J.H Lum, D.C.W. Friedman, J. Rosen, B. Hannaford, Portable surgery master station for mobile robotic telesurgery, in: Pro-ceedings of the 1st international conference on Robot communication and coordina-tion, Greece, Oct. 15-17, IEEE, 2007.
[F5] Honeynet Project. http://map.honeynet.org (Visited on 11 Jun. 2013)
[F6] E. Babulak, Methodology to measure the quality of service in healthcare information and telecommunications infrastructures, Journal of Telecommunications and Information Technology (2005) pp.133-138.

Table Sources

[T1] IT Management, WILEY, 2011.

Acronym List

ISO: International Organization for Standardization
IEC: International Electrotechnical Commission
NERC: North American Electric Reliability Corporation
RFC: Request for Comments
IETF: Internet Engineering Task Force