ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

A REVIEW ON THE SECURITY ISSUES OF TELEMEDICINE NETWORK

Chowdhury Akram Hossain[1], Md. Saniat Rahman Zishan[2], Dr. Rabiul Ahasan[3]

Assistant Professor, American International University-Bangladesh (AIUB), Bangladesh[1, 2]

Associate Professor, Universiti Sultan Zainal Abedin (UnisZa) Malaysia[3]

Abstract: Telemedicine is currently a promising area of research as day by day the need of better medical support is increasing. There had been numerous researches done in this particular field with many aspects. In our paper we mainly focused on the review of the system and few common security threats which have a huge influence on the quality of the service. In our paper we also reviewed literatures which suggested few possible solutions to the threats.

Keywords: Telemedicine, security issues, rural health.

I. INTRODUCTION

Medical security and service is one of the most essential requirements for any human being. It is a very important aspect for any government to provide quality medical services to the citizen. In every developed country this type of assurance is served quite well to all the citizens, whereas the countries which are under developed or developing are still struggling with the problem. One of the main reasons behind this is the world of communication. It is quite obvious that if the infrastructure of a country is not well organized then the number of rural communities increases and as a result the supply of basic needs of the people living in the rural areas becomes less.

With the improvement of the communication technology in almost every part of the world now we can think of providing at least virtual support to every corner of a country. For this fact it is very important to study the availability of resources and then designing a platform which should be enough efficient from every prospect. According to the development of the technology all over the world it is now quite possible to bring the world close. Anyone living at any part of the world can be easily connected through internet to discuss about any issue. This fact has already brought a huge improvement in the world of medicine but unfortunately still in rural places especially in underdeveloped countries people are not getting the expected benefits of digital communication world.

Not only in the rural are but it is also important for any medical service provider to get connected with the modern technology and specialized suggestions from expertise on a critical or rare medical scenarios. It can bring a lot of benefit for the health of the citizen which in turn can bring a huge development in the economy of a country. In our case we are focusing on Bangladesh as an example to research on the fact of TELEMEDICINE IN RURAL AREAs. It is very suitable for our research goal as the resources available in Bangladesh is very limited hence if we can successfully complete our result then the research result can be implied on any rural city of any part of the world.

The world of telemedicine is not limited and every day it is showing promising result to save lives and every day at some corner of the world we are getting new addition to this thought. Most of the people from the medical world are now delivering promising idea to share their expertise to help people and also to train others. But for this we have a strong connection of the wireless communication world as the whole concept depends on the quality of available network. There have been several researches on this fact and very good outcomes have been found.

To implement this type of research we need a lot of focus on several facts. One of the key facts is the efficiency of the system which also focuses on the economic part. In countries like Bangladesh most of the population is living in the rural part of the country and another important fact is that the literacy rate is very low. This implies that there is a scarcity of expert doctors and medical equipment. Due to this fact most of the people who are living in the rural areas are suffering from serious basic medical needs.

There are several factors in TELEMEDICINE which should be taken into consideration. One of the key factor related to this is the security. The term security relates not only the privacy factor but also the other precautions required to deliver the service. As telemedicine completely depends on network hence security issues related to the network is a severe challenge. Whether we are using the system for rural area or urban area the security measures will always be the most key factor of the system.

Privacy protection in the fields of healthcare and nursing care requires the following in order to maintain client's dignity (1) knowing their health condition accurately and deciding service policy they can receive; (2) giving them the choice to be informed or not in case they are in serious condition; (3) confining data when clients want them to; (4) removing unreliable information that may lead to misinterpretation. Also the principle of confidentiality has been at the heart of medical ethics since the time of Hippocrates and has been developed by various codes, including the International Code of Medical Ethics which states that a doctor must preserve “absolute confidentiality in all he knows about his patient” even after the patient’s death.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

II. SECURITY CHALLENGES

Attitude. It follows that an important measure of success in implementing a security policy is that allgroups of staff are aware of, agree with and observe procedures aimed at preserving security of information. However, this is by no means easy to achieve since it requires significant change inbehaviour of staff. Indeed, many health care professionals are still reluctant to use computers at alland to be asked, for instance, to remember a new password every month only hardens their attitude.

Health care organisations have knowingly compromised information security through less thansatisfactory access controls simply in order to encourage all staff to use the computer systems. Oncesuch compromise has been adopted, it is subsequently very difficult to convince users of the need to strengthen access control.

Reluctance to change working practices in order to make information more secure is widespreadamongst health care professionals. Despite their general acceptance of the principle of patientconfidentiality, health care professionals tend not to accept responsibility for information security.

Ignorance. This reluctance is due in part to a poor understanding of the measures necessary toachieve security (many of which are very simple and easy to observe). Doctors are a particularlydifficult group to teach about information security since they often believe they know all aboutconfidentiality (through the Hippocratic Oath) and those other aspects of security are not theirproblem. Unfortunately, whilst they know about the principle of confidentiality, doctors' knowledgeof the potential threats to computer systems and how they can best be prevented may be poor.

Information security, data protection and human rights should be a prominent part of medical informatics courses during undergraduate training and in postgraduate education.

Conflicting demands. It is not only in the medical curriculum that information security has been suppressed. The attitude that protection of patient information is less important than direct patient care pervades planning and provision of clinical services in general. Obtaining adequate funding forinformation security in an environment of limited resources, therefore, becomes a significantchallenge. Indeed, the expense of installation and maintenance of additional security controls isoften cited as a reason for failure to adopt them. In addition to financial constraints, there are increasing demands for access to personal health caredata for the purposes of monitoring, regulation, audit and research. Managed care organisations, insurance companies and health authorities contracting services are seeking access to patient records to substantiate claims or detect fraud. Surveillance, epidemiology and research programmessystematically gather the patient clinical data to monitor health care practices and understanddistribution, spread and control of diseases. The police seek information from medical sources thatmay lead to the identification of criminals or to the prevention of crime. It is the ready availabilityof large quantities of clinical information on computer systems that has made such investigations possible and of appeal to regulators and the public. The laudable aims of greater efficiency,accountability, liability and knowledge achieved through such systematic data processing are,however, putting at risk the fundamental principle of patient confidentiality (Applebaum 2000). Thebalance between openness and confidentiality is the subject of much debate, which, while it remainsunresolved, prevents application of a consistent approach to the protection of clinical information.

Inadequate systems. Given the availability of many good technical solutions to achieving securesystems, it is disappointing that few of the commercial health care computer systems currently onthe market have more than the most basic security features. Either there is no commercial gain inincorporating more stringent controls, or the purchasers have been unwilling to pay for, or to implement, more secure systems. Poorly designed security controls often impose constraints or impediments to access that are unacceptable to clinical staff. Even passwords are considered by many to be awkward and unnecessary, particularly when enforced expiry is imposed. Re-establishing network connectionscan take so long that busy clinical staff avoid logging off between transactions on networkworkstations. Security measures must be practical, acceptable to staff and cause minimal disruptionto the processes of care. Few commercial systems at present achieve these ideals. However, onceappropriate access control and auditing is installed, staff scepticism soon turns to acceptance as theycome to realise their importance and benefit (Denley, Smith 1999).

Inconsistent policies. The extent, to which individual health care facilities apply security controls totheir own computer systems, can vary markedly. Inconsistent policies and procedures can lead tofrustration, confusion and potentially even harm to patients. This is exemplified by differences inorganisation's policy towards transmission of patient information by facsimile. Whereas bestpractice is to send patient-identifiable information by facsimile machine only in emergencies andaccording to agreed protocols, the convenience of such means of communication has led manyorganisations to allow their routine and uncontrolled use. An organisation attempting to apply morerestricted use of facsimile transmissions is then faced with complaints from other organisations withmore lenient policies whose staff are frustrated that they cannot send or receive patient informationby that means.

Many similar inconsistencies in security policies are becoming evident the more that patientidentifiableinformation is being communicated across organisational boundaries. There is agrowing need for commonality in security policies and negotiated agreements between agencies thatare sharing patient information. Without a clear framework of responsibility and accountability,such agreements will be difficult to achieve. Previous studies of telemedicine information

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

security have generally discussed vulnerabilities in terms of risk.Several studies simply list threats and categorized them in a risk matrix by likelihood and consequence. Thoughuseful for risk analysis purposes, this approach does not provide an understanding of the types of threats and potential counter measures for specific threats to a given vulnerability.

III. CONCLUSION

The telemedicine network is a very sensible network as it deals with data with full privacy of a patient. Hence the network architecture of the system should be highly secured and always updated with latest protocols. It should also be mentioned that this type of network needs continuous monitoring and maintenance which should follow an automatic system. The equipments connected to this network always require precise data processing and accurate result. In our future work we are currently working do analysis the current protocols and systems that have been used for this type of service to propose the most efficient network protocol. It should also be noticed that the security concerns are not only limited to the network but also to the physical presence of the person who are involved with the system. Hence a better training and more awareness is also required to get the best result.

REFERENCES

[1] Parker, D. B. (2002) Toward a new framework for information security, in, S. Bosworth and M. E. Kabay (Eds.)Computer Security Handbook. New York: John Wiley & Sons.

[2] Morris, T. J., Pajak, J., Havlik, F., Kenyon, J., and Calcagni, D. (2006). Battlefield Medical Information System–Tactical (BMIST): The Application of Mobile Computing Technologies to Support Health Surveillance.Telemedicine Journal and e-Health, 12(4), 409-416.

[3] Zhang. Y., Lee. W. and Huang.Y. (2003)"Intrusion Detection Techniques forMobile Wireless Networks". WirelessNetworks Journal (ACM WINET), Vol. 9,No. 5, pp. 545-556.

[4] TACHAKRA, S., MULLETT, S.T.H., FREIJ, R. and SIVAKUMAR, A., 1996.Confidentiality and ethics in telemedicine.Journal of Telemedicine and Telecare, 1(2), pp. 68-71.

[5] Solaiman. B., Cauvin. J.M., Puentes. J.,Le Guillou. C., Brunet. G., Debon. R. andRoux.C. (2001) "Enabling Technologyfor Telemedicine and Telehealth". Proceedings of the 23rd Annual InternationalConference on Engineering in Medicine andBiology Society.

BIOGRAPHIES

Chowdhury Akram Hossain is an Assistant Professor at the Department of EEE in American International University-Bangladesh (AIUB). He was enrolled for PhD degree at the Department of Energy in *Politecnico Di Milano*, Italy. He also worked with Alstom for his PhD research. He completed his M.Engg. in Telecommunication and B.Sc. in Electrical and Electronic engineering both from AIUB. His research interests are in the field of power engineering,wireless communication,Telemedicine, MatLab, smart grid, Adhoc Network etc.

Md. Saniat Rahman Zishan joined AIUB as a faculty member in September 2009. He is currently working as an Assistant Professor in EEE Department. Since December, 2012, he is working as Special Assistant of OSA(Office of Student Affairs). He completed his M.Engg. in Telecommunication and B.Sc. in Electrical and Electronic engineering both from AIUB in 2011 and 2008 respectively. His current research interests are in the field of signal processing, tele-medicine, wireless communication, smart grid, Adhoc Network.

Dr. Rabiul Ahasan is an Associate Professor of Universiti Sultan Zainal Abidin located in the state of Terengganu, Malaysia. He teaches semester courses in the area of biomedical sciences and conduct research on WMSD, TSD & CTS. Dr Ahasan is also interested in military ergonomics, medical dance, and music therapy. He has presented research findings at numerous scientific conferences and authored over 70 research papers on diverse facets of occupational and environmental medicine. He is also involved in many editorial activities in many scientific journals. Dr. Ahasan research interests focus on carpal tunnel syndrome, traumatic stress disorders, synchronization process, telemedicine etc.