Applied Medical Informatics
Original Research Vol. 39, No. 1-2 /2017, pp: 21-29

An Experiment to Analyze Performance of Virtual Private Network Approach to Information Exchange between Health Facilities

Siphael BETUEL[1,*], Dina MACHUVE[1], Khamis KALEGELE[2]

[1] The Nelson Mandela Institution of Science and Technology, PO Box 447 Arusha, Tanzania
[2] Tanzania Commission for Science and Technology, PO Box 4302, Dar es Salaam, Tanzania
E-mail(s): betuels@nm-aist.ac.tz; dina.machuve@nm-aist.ac.tz; khamisi.kalegele@nm-aist.ac.tz

* Author to whom correspondence should be addressed; Tel.: +255 717 766 884, +255 624006701

Received: May 18, 2017 /Accepted: June 25, 2017

Abstract
In developing countries, Tanzania in particular, studies and reports have depicted that there is a strong desire and need for seamless information exchange across health care providing facilities. A limited study conducted in few public and private hospitals has also revealed the same. On the other hand, the eHealth community has failed to effectively take advantage of the advances in technologies to make that desire come true. One potential technology is Virtual Private Network (VPN) for which it has been noticed that there is a misconception and lack of innovative initiatives that slow down its uptake in eHealth. This article presents a technical assessment of the VPN technology in Tanzanian context. Primarily, the assessment focused on practicability of the best VPN practices and the perceived user experience performance when VPN is in use. It was observed that the response time dropped significantly as expected. The increase in response time and computer memory utilization is due to security mechanisms that are involved in VPN, the stronger security is used the more performance decreases. However, the increase in response time and computer memory utilization is very small in such a way that users will not be able to notice.

Keywords: Health Information Exchange; Virtual Private Network (VPN); Care2x; IPsec

Introduction

Exchanging of health information across health centers is still a problem for many countries especially when it comes to the issue of transfer a patient from one hospital to another [1]. Different approaches have been proposed to facilitate exchange of health information between health facilities such as paper based system [2] and Electronic messaging [3]. Exchanging of patient's information among hospitals is inevitable, as many people move from one hospital to another to look for better health care [4]. Proper ways of exchanging health records are necessary to avoid problems such as delaying of information to the referred hospitals, loss or damage of the patient's records, duplication of information, and waste of resources [5]. No matter the method that is used to exchange patient's information, the information should be exchanged timely, accurately and in a secure way [6], and the performance impact should always be considered.

In the past, a paper-based system has been proven as a sufficient way of delivering health care in both developed and developing countries (including Tanzania) but currently, with rapid development in technology this system seems to be obsolete and inefficient. The performance of this system is very poor as it consumes a lot of time, for example, if a paper-based record needs to

be seen by another medical care provider, then a paper-filled file would have been physically delivered to that health care center [7].

In this study, a Virtual Private Network (VPN) technology is considered for the exchange of health records across health facilities. VPN is a secure way of connecting to a private Local Area Network at a remote location, using the internet or any unsecure public network to transport the network data packets privately, using encryption [8]. The VPN scenario fits well with the health and communication landscapes of Tanzania where health information systems are all local to health facilities and internet as the public network is increasingly becoming pervasive and accessible.

Care2x is one of the Health Information System (HIS) that improves health service delivery in some of hospitals in Tanzania [9]. The exchange of patient records between hospitals that use Care2x is still done manually, this is because Care2x does not have such functionality. The objective of this paper was to reassess the information exchange requirements and provide an initial experimental evaluation of the practicability of the VPN technology in Tanzania.

Material and Method

Evaluation of the Current Situation

This study was conducted using an experimental approach where a number of variables related to VPN were manipulated by controlling and measuring some performance indicators. Since eHealth issues are very dynamic and a lot is happening, a limited survey study was carried out to get some perspectives before the experimentation.

User experience is defined by a standard (ISO 9241-210-2010) as a person's perceptions and responses that result from the use and/or anticipated use of a product, a system or a service. User experience explores how a person feels about using a system, i.e. the experiential, affective, meaningful and valuable aspects of a product use [10]. When comparing usability and user experience evaluation we find that usability evaluation focuses on task performance, e.g. number of errors or required number of clicks to perform a task, and user experience evaluation focuses on users' lived experience. In user experience, evaluation the focus is on how the user feels about the system he/she is using and the user's motivation and expectations play a strong role in this evaluation. User experience evaluation informed the study on the current situation on health information systems (HIS).

User experience evaluation was performed with two thematic questionnaires, one for the health professionals i.e. medical doctors and nurses and another for the health IT professionals, either represented by the health IT supplier company or by the health IT department of the hospital. In the user questionnaire, the themes under study were focused on the following: Use of health information system, user satisfaction, user's assessment of the current system in use, and suggestions, comments for further development. With this questionnaire, we wanted to collect the user's experiences on the systems they have been using in their routine health care clinical practices.

In the health IT professionals questionnaire the themes studied were the following: Technical details of the system, applied standards, database coverage, decision support options, data exchange with other systems, order-entry system, statistics and reporting, integration options, data security and confidentiality. Additionally, we wanted to find out the details of the system the users have been using, these details might provide additional information that helps interpretation of the user questionnaire results.

The user experience evaluation was conducted at both government and private hospitals in Tanzania between September and October 2016. Nine (9) hospitals in five regions of Arusha, Dar es Salaam, Manyara, Singida and Pwani regions were involved on the evaluation with a sample size of 33 people interviewed and their distribution indicated in Table 1. A small number of hospitals was selected since many hospitals appeared to use the same type of HIS, therefore there was no need of including them all. Nurses and doctors are the main users of the system, and so the interest was on how they use the system and how often they use the system.

Table 1. Distribution on user experience evaluation

User Category	Users	Frequency
Health professionals	Medical doctors	14
	Nurses	11
Health IT professionals	Health IT professionals	8
TOTAL		**33**

Design of the Experiment

It was established from the user experience evaluation that there is no exchange of health records between health facilities. The HIS are all local to health facilities. A prototype using VPN connection for exchange of health records between hospitals was designed for proof of concept on secure connectivity between health facilities using experimental approach. A number of variables related to VPN were manipulated while controlling and measuring some performance indicators.

A network of two nodes was set up in a laboratory, each of which comprised a computer and a router, to represent two hospital centres. The two nodes were configured into a VPN and were used to observe the utilization of computing resources and factors, which have potential to affect user-perceived performance as computer workload was varied.

VPN consists of two main components: a tunnel and security services. A tunnel is a logical connection between two communication parts which used to carry traffics privately. By default, the tunnel is not secured so there is a need to add some security mechanisms to make it secure. Point-to-point tunneling protocol (PPTP), Secure socket layer (SSL) and Internet Protocol security (IPsec) are examples of tunnel protocols used in VPN [11], in this study IPsec Tunnel Mode was chosen(Figure1). IPsec has different security characteristics as shown in Table 2.

Table 2. Security characteristics of VPN

VPN Characteristics	Description
Authentication Protocol	Routers R1 and R2 authenticate each other by using authentication protocol which is pre-shared key or Rivest-Shamir-Adleman (RSA)-signature
Access control list (ACL)	Traffic to be protected within the tunnel is determined by configuring ACL to both Routers R1 and R2.
Encryption algorithm	R1 encrypts the message by using an encryption algorithm i.e. Advanced encryption standard (AES). AES uses 128-bit, 192-bit or 256-bit key which makes it stronger than data encryption standard (DES) that uses 56-bit key
Encapsulation protocol	R1 uses Encapsulated Security Payload (ESP) to encapsulate a packet to form a new packet with IP address of R1 and R2
Data integrity protocol	R1 then uses data integrity protocols which are Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) to ensure consistency and accuracy of the message
Decapsulation protocol	Once R2 receives the message, it first decapsulates and then decrypts it to obtain the original message and then it forwards the message to computer PC2 where the packet was supposed to reach.

This experiment was conducted under the assumption that the patient profile is the same for all hospitals. During the experiment, an assumption was made that, computers at hospitals can be used to perform other tasks while exchanging patient records is going on, so computer workloads were varied each time and then computing resources utilization and response time were observed. Initially, the results were recorded when there was only HIS running on the computers, later on, the same computers were used to stream videos and play music while sending the patient information and then the results were recorded.

The interest was in two metrics: the computer memory utilization and the response time. This information is necessary for the hospitals to be aware of the resources that are going to be used i.e. computer memory and also how long they should expect for information to be transmitted to

another hospital i.e. Response time. In analyzing the results, a simple average method was used i.e. the average of the memory utilization and response time with and without VPN were taken. Finally, a comparison of the averages of a Network that use VPN and the one without VPN were made.

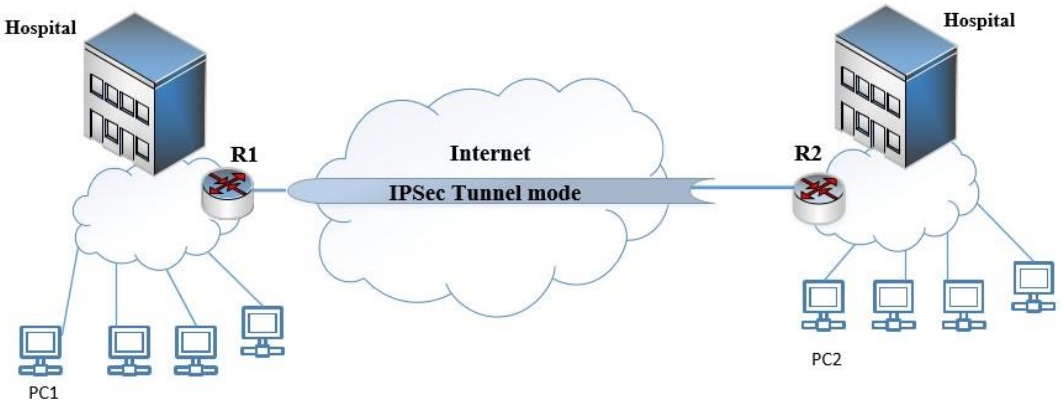

Figure 1. Site-to-site IPsec VPN

Experimental Setup

Experiments were conducted as presented in the above subsection. The aim was to compare the performance of patient information exchange when VPN was used and when VPN was not used.

For experimental purposes, a general HIS was used with dummy data which composed of ID, full name, age, sex, religion of a patient and region of residence. Different hardware and software were used during the experiment as shown in Table 3.

Table 3. Hard wares and Soft wares used in Experiment.

Hard ware Devices	Software
Two computers	Windows operating systems
Two Cisco VPN routers	Telerik Fiddler Web Debugger
One console cable	Browser's task manager
Two unshielded twisted pair cables (UTP-Cat 6)	
Four registered jack (RJ-45) connectors	

The experimental setup was divided into two parts, part A involves the exchange of information without VPN while part B involves VPN configuration. The setup of the experiment was as seen in Figure 2 and 3.

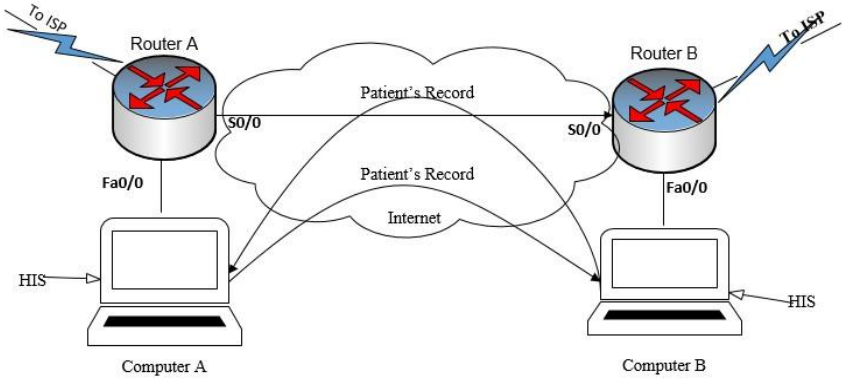

Figure 2. Without VPN configuration

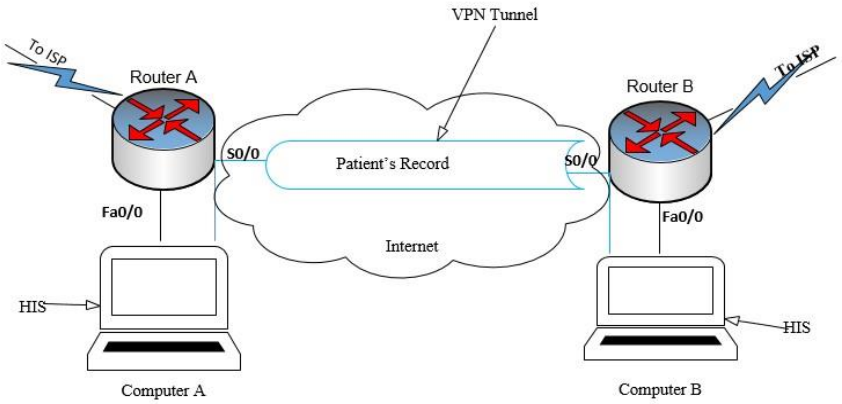

Figure 3. With VPN Configuration

Part A

Initially, a general HIS was deployed to both computers, the interface of HIS was as seen in Figure 4. The setup of the experiment was as in Figure 2, RJ 45 with the cable was used to connect computer A to Router A, computer A then got the IP address together with the default gateway.

ID	Firstname	Lastname	Surname	Age	Sex	Religion	Region	Action
40	xx	xx	xx	10	Male	Christian	Arusha	SEND
41	yy	yy	yy	20	Femal	Muslim	Dar es salaam	SEND

Figure 4. HIS interface

The IP address of computer B was configured to the HIS within computer A and the IP address of computer A was configured to the HIS within computer B. Next from both computers, HIS, Telerik Fiddler Web Debugger and browser's task manager were started. The information to be shared was then selected in computer A and then '**send**' button was clicked to allow the information to move to computer B. The format of the shared information was text; no images were involved as seen in Figure 4.

After sending the information, the response time and the memory utilization were captured by using Telerik Fiddler Web Debugger and browser's task manager respectively. To be able to see the browser's task manager you have to press SHIFT+ ESC. The complete procedures were repeated five times and later on the average response time and memory utilization were taken.

Part B

The setup of the experiment with VPN was as in Figure 3, an IPsec VPN was configured to both routers as shown in Table 4.

The same configurations were repeated on Router B and finally, the same procedures followed before VPN were repeated to get the response time and memory utilization.

Results

Based on the evaluation it was observed that all hospitals use HIS, but patient records are still exchanged manually as shown in Table 5. Among nine (9) hospitals, which were visited five (5) systems are in use as shown in Table 5.

Table 4. IPsec VPN configuration between the two Routers

Steps	Activity	Procedures
1	Internet security association and key management protocol (ISAKMP) parameters (Phase 1) and a pre-shared key were configured on both routers to make a security negotiation between the two routers.	Crypto isakmp policy 1 Authentication pre-share Hash sha Encryption aes 128 Group 2 Lifetime 86400 Crypto isakmp key <cisco2017> address (IP address of Router B)
2	Parameters that will be used for Internet key exchange (IKE) phase 2 tunnel were configured	Crypto IPsec transform-set myset esp-aes esp-sha
3	Access list to identify traffics to be encrypted was created	Access-list 101 permit <source ip address> <destination ip address>
4	A crypto map was created and applied to the appropriate interface	Crypto map Router A_to_Router B 10 IPsec-isakmp Set peer <IP address of Router 2> Match address 101 Transform-set myset Interface S0/0 Crypto map Router A_to_Router

Table 5. Summary of the Evaluation of HIS

SN	Hospital Name	Region	HIS in use	Mode of exchange information with another health facility
1	Arusha Lutheran Medical Center (ALMC)	Arusha	Care2x	Manual/paper based
2	St. Elizabeth	Arusha	Care2x	Manual/paper based
3	Hydom Lutheran Hospital (HLH)	Manyara	Care2x	Manual/paper based
4	Makiyungu Hospital	Singida	Care2x	Manual/paper based
5	Muhimbili National Hospital (MNH)	Dar Es Salaam	Jeeva	Manual/paper based
6	Muhimbili Orthopaedic Institute (MOI)	Dar Es Salaam	MediPro	Manual/paper based
7	Kairuki Hospital	Dar Es Salaam	EHMS	Manual/paper based
8	Sanitas Hospital	Dar Es Salaam	EHMS	Manual/paper based
9	Tumbi Hospital	Pwani	GOT(HMIS)	Manual/paper based

Each time computer workloads were varied and then, results were recorded as shown in Table 6. In analyzing the results, a simple average method was used i.e. the average of the memory utilization and response time with and without VPN. In addition, a standard deviation was calculated for both computer memory utilization and response time.

Tabel 6. Results

Computer Memory utilization in Kilo Bytes (KB)						Response Time in Seconds(sec)				
With VPN	15,112	14,804	14,600	14,508	16,664	0.056	0.092	0.079	0.056	0.074
Without VPN	14,116	15,204	14,516	14,556	14,326	0.008	0.009	0.008	0.008	0.008

Finally, a comparison of the averages of response time and computer memory utilization for a

Network that uses VPN and the one without VPN was made. On conclusion, it was observed that response time and memory utilization before VPN was 0.0082 seconds and 14,543.6KB respectively. With VPN it was observed that the response time and memory utilization was 0.0714sec and 15,137.6KB respectively. In addition, standard deviation before VPN was 408.42KB and 0.0045sec respectively while with VPN the standard deviation was 884.16KB and 0.0155sec respectively.

Discussion

The survey results did not influence the outcome of the experiments in any way, but rather the results served to justify the need to improve information exchange between hospitals.The experimental results indicated that response time and memory utilization for a network that uses VPN was higher than the network without VPN. Users care a lot about response time especially in hospitals, as users are very busy, patients have little time to wait, so web pages that respond very quickly seem to be more popular among users than slow ones. The increase in response time and memory utilization is due to security mechanisms involved in VPN, the stronger security mechanisms are used the more performance decreases [12]. However, this increase in time i.e. 0.0714_seconds after VPN configuration is very small for users to notice. According to [13], the maximum waiting time for users to start noticing that the system is misbehaving is 10_seconds. A research conducted by [14] on system response time also shows that users will start to notice that the system is misbehaving after 10 seconds. Similarly, the increase in memory utilization after VPN configuration has no effect for computers that are dedicated on health information systems. HIS computers usually have average speed, large storage capacity and reasonable Random Access Memory (RAM) [15]. The values of the standard deviation indicate that, individual data before VPN are close to average computer memory utilization and average response time. This is also true for the case of VPN.

Security is very important in health care systems as everybody cares about protecting the privacy of his/her medical data. Since VPN has been used in this experiment, it is quite clear that patient information will remain private and exchanged in a very secure way[16]. VPN also allows someone to prioritize traffics, so it's easy to dedicate bandwidth to the applications which are very critical. Through VPN it's easy to transfer multimedia applications[16], which is very useful in health facilities as sometimes they may need to exchange information like texts, images, audios and videos.

However, these results are based on dummy data and the general HIS that was used; next plan is to repeat the experiment by using Care2x and actual data. A new module is going to be added in Care 2x that will assist sharing of patient's records between hospitals that are using the same health information system, for this case is Care 2x. The actual data that are going to be used in the next experiment includes demographic data of a patient, Diagnosis report, Lab results, Radiology results and medical reasons for transfer. The aim is to check further performance issues such as page load time and rate of occurring of error after integrating the new module with Care2x.

Care2x is an open source web-based Integrated Healthcare Environment (IHE) that is used in some hospitals in Tanzania including Arusha Lutheran Medical Hospital (ALMC), St. Elizabeth Hospital in Arusha, Hydom Lutheran Hospital in Mbulu and Kilimanjaro Christian Medical Centre (KCMC) [17].

Conclusion

The results of our study shows that there is a strong need for data exchange in such a way that data can be communicated at all levels of health facilities. The solution proposed in this study, which is VPN, ensures a high level of security to the information to be exchanged which is very important to ensure the privacy of patient data. Once VPN is in use, response time and computer memory utilization seems to increase but the increase in these parameters is very small in such a way that users cannot observe.

List of abbreviations

ACL= Access Control List
AES= Advanced Encryption Standard
DES= Data Encryption Standard
ESP= Encapsulated Security Payload
HIS= Health Information System
IHE= Integrated Healthcare Environment
IKE= Internet Key Exchange
IP= Internet Protocol
IPsec= Internet Protocol Security
ISAKMP= Internet Security Association and key Management Protocol
MD5= Message Digest 5
PPTP= Point-to-Point Tunnelling Protocol
RJ-45= Registered Jack
RSA= Rivest-Shamir-Adleman
SHA= Secure Hash Algorithm
SSL= Secure Socket Layer
UTP-Cat 6= Unshielded Twisted Pair Cables
VPN=Virtual Private Network

Conflict of Interest

The authors declare that they have no conflict of interest.

References

1. Puustjarvi J, Puustjarvi L. The role of medicinal ontologies in querying and exchanging pharmaceutical information. Int J Electron Heal. 2009;5(1):1-13.
2. Haskew J, Ro G, Saito K, Turner K, Odhiambo G, Wamae A, et al. Implementation of a cloud-based electronic medical record for maternal and child health in rural Kenya. Int J Med Inform. 2015;84(5):349-54.
3. Moorman PW, Branger PJ, van der Kam WJ, van der Lei J. Electronic messaging between primary and secondary care: a four-year case report. J Am Med Inform Assoc. 2001;8(4):372-8.
4. Kaelber DC, Bates DW. Health information exchange and patient safety. J Biomed Inform. 2007;40(6 SUPPL.):40-5.
5. Johnson KB, Unertl KM, Chen Q, Lorenzi NM, Nian H, Bailey J, et al. Health information exchange usage in emergency departments and clinics : the who, what, and why. J Am Med Informatics Assoc. 2011;18(5):690-7.
6. Everson J, Kocher KE, Adler-milstein J. Health information exchange associated with improved emergency department care through faster accessing of patient information from outside organizations. J Am Med Informatics Assoc. 2017;24(e1):e103-e110.
7. Kalogriopoulos NA, Baran J, Nimunkar AJ, Webster JG. Electronic medical record systems for developing countries: review. Conf Proc IEEE Eng Med Biol Soc. 2009;2009:1730-3.
8. Sharma T. Security in Virtual private network. Int J Innov Adv Comput Sci. 2015;4:669-75.
9. Ishabakaki P, Kaijage S. RFID-based Drug Management and Monitoring System, Case of Public Hospitals in Tanzania, A Review Paper. Comput Eng Appl. 2015;4(3):165-71.
10. Vermeeren APOS, Law EL-C, Roto V, Obrist M, Hoonhout J, Väänänen-Vainio-Mattila, K. User experience evaluation methods: Current state and development needs. Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries 2010, pp. 521-30.

11. Malik A. Performance Analysis of Virtual Private Network for Securing Voice and Video Traffic. Int J Comput Appl. 2012;46(16):25-30.
12. Lin X, Wong JW, Kou W. Performance Analysis of Secure Web Server Based on SSL. International Workshop on Information Security 2000, pp. 249-61.
13. Nah FF-H. A study on tolerable waiting time: how long are Web users willing to wait? Behav Inf Technol. 2004;23(3):153-63.
14. Schaik P Van, Ling J, Schaik P Van, Ling J. The effect of system response time on visual search in Web pages. The Electronic Library, 2004;22(3):264-8.
15. Grace RK. Medical Image Retrieval System in Grid using Hadoop Framework. IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), 2015, pp. 73-77.
16. Gamundani AM, Nambili JN, Bere M. A VPN Security Solution for Connectivity over Insecure Network Channels : A novel study. SSRG Int J Comput Sci Eng. 2014;1:1-8.
17. Kimollo P, Lenoir M, Niemi M. Health Management Information System for Hospitals Lessons learned from a Tanzanian experience. 2010, Availble from: https://iicd.org/documents/health-management-information-system-for-hospitals-lessons-learned-from-a-tanzanian-experience/