Security Model of a Unified Communications and Integrated Collaborations System in the Health Sector Environment of Developing Countries: A Case of Uganda

Excellence Favor, Bakari M. M. Mwinyiwiwa

International Science Index 84, 2013 waset.org/publications/9996790

***Abstract*—**Access to information holds the key to the empowerment of everybody despite where they are living. This research has been carried out in respect of the people living in developing countries, considering their plight and complex geographical, demographic, social-economic conditions surrounding the areas they live, which hinder access to information and of professionals providing services such as medical workers, which has led to high death rates and development stagnation. Research on Unified Communications and Integrated Collaborations (UCIC) system in the health sector of developing countries aims at creating a possible solution of bridging the digital canyon among the communities. The system is meant to deliver services in a seamless manner to assist health workers situated anywhere to be accessed easily and access information which will enhance service delivery. The proposed UCIC provides the most immersive telepresence experience for one-to-one or many-to-many meetings. Extending to locations anywhere in the world, the transformative platform delivers Ultra-low operating costs through the use of general purpose networks and using special lenses and track systems. The essence of this study is to create a security model for the deployment of the UCIC system in the health sector of developing countries. The model approach used for building the UCIC system security carefully considers the specific requirements for the health sector environment organization such as data centre, national, regional and district hospitals, and health centers IV, III, II and I and then builds the single best possible secure network to meet their needs. The security model demonstrates on how the components of the UCIC system will be protected physically and logically in the health sector environment. The UCIC system once adopted and implemented correctly will bring enhancement to the speed and quality of services offered by health workers. The capacities of UCIC will help health workers shorten decision cycles, accelerate service delivery and save lives by speeding access to information and by making it possible for all health workers and patients to collaborate ubiquitously.

***Keywords*—**Developing Countries, Health Sector Environment, Security, Unified Communications and Integrated Collaborations.

I. Introduction

THE health sector of a developing country is a large organization that has always turned to technology to drive it's day to day activities. Now, more than ever, the health sector is asking Information Technology (IT) staff to do more, with less human and financial resources. This is due to the fact that the funds always allocated to the health sector are not sufficient to facilitate all the activities of the sector. The health sector is a hyper organization and needs to deliver real time services so it is looking to technology to help improve processes to increase the efficiency of the sector. The problems of effective service delivery is answered by unified communications and integrated collaborations (UCIC) system, the core competency of a UCIC solution is to address this need to do more with less and do it better than done before.

The health sector should be therefore able to deliver a robust infrastructure that caters for the following initiatives: Messaging – Email & Calendaring; Collaboration - Web Portal services [1], Intranet [2]; Unified Communication – Instant Messaging, Conferencing, Presence; System Management and Security [3], [4]; Change management – Training & Process [5]. UCIC is the integration of real-time communication services such as instant messaging (chat) [6], presence information [7], telephony (including IP based telephony) [8], video conferencing [9], data sharing (including web connected electronic whiteboards or Interactive white Boards) [10], call control [11] and speech recognition [12] with non-real-time communication services such as unified messaging (integrated voicemail, e-mail, SMS and fax). UCIC is not a single product, but a set of products that provides a consistent unified user interface and user experience across multiple devices and media types [13], [14].

Excellence Favor and Bakari M. M. Mwinyiwiwa are with the University of Dar es Salaam, Dar es Salaam, Tanzania (e-mail: bakari_mwinyiwiwa@yahoo.com).

II. Unified Communications and Integrated Collaboration (UCIC)

UCIC is the integration of real-time communication services such as instant messaging (chat), presence information, telephony (including IP based telephony), video conferencing, data sharing (including web connected electronic whiteboards aka IWB's or Interactive White Boards), call control and speech recognition with non-real-time communication services such as unified messaging (integrated voicemail, e-mail, SMS and fax). UCIC is therefore a set of products that provides a consistent unified user interface and user experience across multiple devices and media types [15].

UCIC allows an individual to send a message in one medium and receive the same communication on another medium. For example, one can receive a voicemail message and choose to access it through e-mail or a cell phone. If the

International Science Index 84, 2013 waset.org/publications/9996790

sender is online according to the presence information and currently accepts calls, the response can be sent immediately through text chat or video call. Otherwise, it may be sent as a non real-time message that can be accessed through a variety of media [16].

TelePresence is a combination of cutting edge audio, video and network enterprise solutions, also hardware optimized environments and a software glue that holds the elements together to make the best high definition video presence available in industry today [17].

It's a very new, unique, innovated technology that creates in presence, high definition, virtual meeting possible. And also TelePresence makes these things work for your work, as well as for personal life over a health sector network. The user knows predominantly it's about productivity, getting people in front of others and in a very virtual environment, but creating that in presence experience is key. Also, TelePresence is about improved responsiveness for health workers to be able to respond to patients, to be in presence of patients, also for subject matters to get in front of the patients very easily and fast. So, TelePresence enables that, also improved communication, collaboration with coworkers, partners, and patients. The aim of this research is to create an environment with seamless flow of information in the health sector by using UCIC system, thus enabling prompt medical service delivery in the health sector which will reduce the death rate in the developing countries.

III. The Health Sector Find the Needs Evolving

National or global value chains, mobile workforces, more fast service delivery, and information overload: this is the new norm. The health sector often finds their current model and applications or systems used to support it, inadequate to meet their challenges. To address these sector activities' complexities, UCIC connects people and information seamlessly, helping to enable comprehensive and effective collaborative experiences. With UCIC the health sector can:

- Connect co-workers, doctors, nurses, patients, and support staff with the information and expertise they need.
- Access all the health sector critical communications and data from anywhere and at anytime. The office is truly where you are.
- Facilitate better and more efficient team interactions, driving workforce service delivery to simply getting things done.
- Make mobile devices true extensions of the health sector network so mobile workers can deliver services anywhere.
- Innovate the way of doing things by integrating improved collaboration and communications into Health sector processes.

IV. The Current Health Sector of Uganda ICT Infrastructure

The basic infrastructure for communication is in place at the Ministry Head Quarter, at National Referral Hospital and Regional Referral Hospitals. As we move down the health care delivery system, at districts and sub-districts levels, access to appropriate ICT becomes limited as shown in Fig. 1. What is available is mainly radio calls and mobile telephones. At these levels Internet access still remains low. Use of ICT for communication is hampered by limited human resource skills, inadequacy of funds for maintenance and operational costs [18], [19].

V. The Proposed UCIC System Model

The Health sector Information Technology optimization should begin with infrastructural and foundational elements such as Directory, Identity and Authentication services as shown in Fig. 2. The services will lay the foundation for an evolution towards a high-value IT service structure, followed by such services as Microsoft Unified Collaboration including Messaging and Unified communications, firewalls, endpoint (Forefront) security, Microsoft office applications, Active Directory Rights Management Services (AD RMS), Network Access Protection (NAP), Management infrastructure, legacy clean-up and optimization, and then on to a state of other expanded well-tuned services where as the user is in the middle as shown in Fig. 3.

VI. The Health Sector Organization UCIC System Security Model

UCIC Networks offer end-to-end security solutions that can protect all the critical elements of deployment (network infrastructure, call control platforms, IP endpoints, and UCIC applications). UCIC security solutions extend to various enterprise locations such as the data center, hospitals, and health centre's, and at the end user device level, thus providing multilayered security. The following points highlight the functionality that UCIC security solution provides:

- Dynamic and granular access control to prevent unauthorized access to UCIC services
- Threat protection for the UCIC infrastructure, such as protection against DoS or protocol fuzzing attacks.
- Network security policy enforcement to administer effective UCIC policies for applications and users, such as general whitelists, blacklists, or specific SIP Application-Level Gateways (ALGs) for dynamic firewalling.
- Service protection to help ensure maximum uptime for UCIC applications.
- Network-level encryption services that enable customers to encrypt signaling and media to prevent eavesdropping while maintaining security policies across distributed health sector locations.

International Science Index 84, 2013 waset.org/publications/9996790

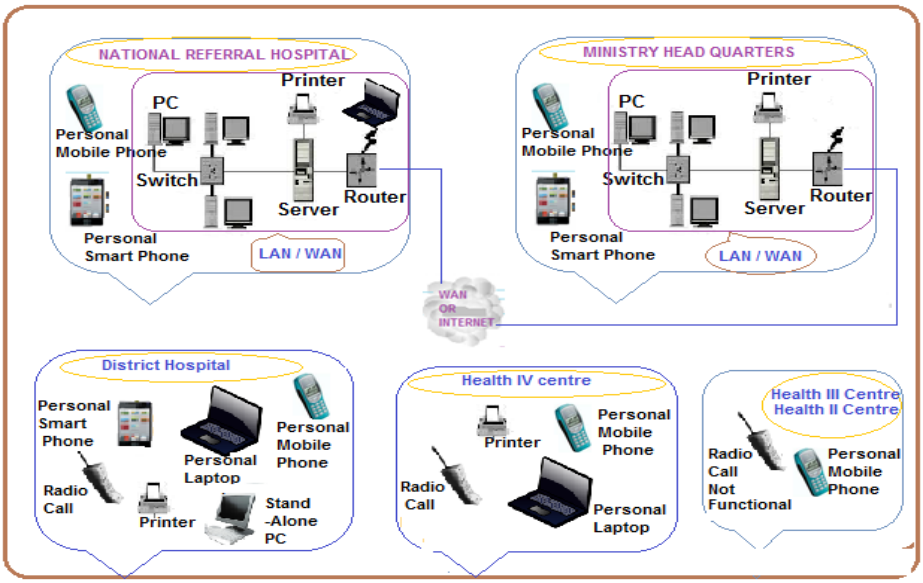


Fig. 1 Current ICT Infrastructure of the Health sector of Uganda

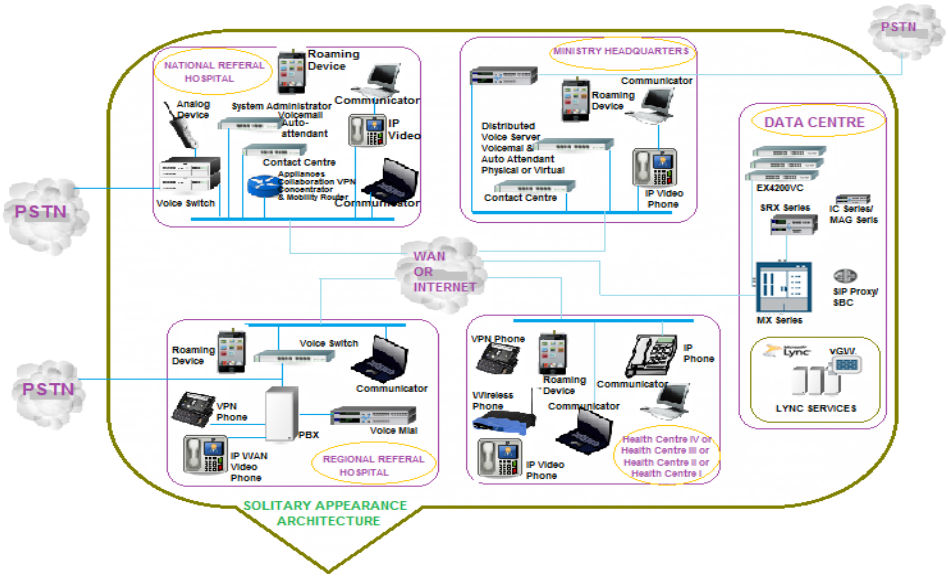


Fig. 2 The Unified Communications and Integrated Collaboration System Architecture



Fig. 3 Conceptual Diagram of UCIC Places User in the Middle

UCIC security issues are intensified by the increased mobility of network users, the Bring Your Own Devices (BYOD) phenomenon, the growing utilization of contractors, the colocation of partners on site, visiting guests, the proliferation of UCIC, and the demand for wireless access.

IT must protect valuable health sector resources from internal and external threats across large or multiple LANs with secure and ubiquitous LAN and WLAN access. Increased security threats and risks force national hospitals and health centers LANs to remain secured and controlled on all fronts while providing open and pervasive access to maintain and increase productivity. The most effective security architecture to ensure maximum protection from network and application layer threats is based on multilayered protection that is appropriate for each location on the network.

International Science Index 84, 2013 waset.org/publications/9996790

Holistic solutions that offer comprehensive security features, proven reliability, and exceptional performance are needed. IEEE 802.1X and network access control should be used to effectively handle unmanaged devices and guest users attempting network access, as well as to support unmanageable devices, post admission control, application access control, visibility, and monitoring. Firewalls and intrusion prevention systems also are needed to help ensure security across the LAN. In addition, QoS can be used as a security tool to identify, classify, and queue traffic. For example, QoS policies can protect access to departmental resources or ensure that high priority data flows are not impacted by malicious traffic. Fig. 4 shows how external and internal threats can be stopped using Intrusion Prevention System (IPS), Application level Gateway (ALG), and core security.

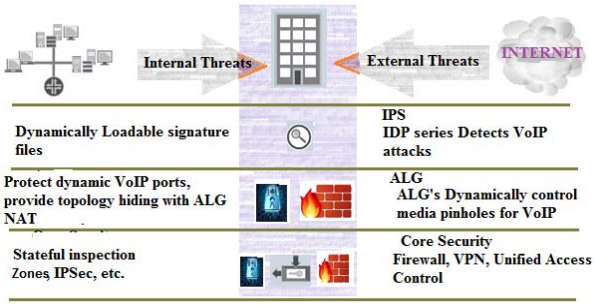


Fig. 4 UCIC System Danger Control Model

Multilayered security architecture facilitates network configuration by providing a modular model that can be rapidly and economically scale based on the number of users in an enterprise environment. It also creates a flexible network where new security services can be added easily without a total redesign. The basic idea behind multilayered security architecture is to protect the data center resources with multiple layers of defense; if one device fails, another provides crucial protection. Another important thing to remember is that not every device can be defended, so the layered defense approach should be asset-centric rather than perimeter- or technology-centric.

While focusing on an asset-centric layered defense approach is clearly important, it should not be forgotten, to protect users who access those assets as well; therefore, protecting the end users not only from external attacks but also internal ones. This means that the endpoints must be secure at all times.

A. Access Control and Segmentation

The most vulnerable and most desired targets for attack in a UCIC environment are the endpoints themselves. Therefore, an initial line of defense is required to monitor who (and what) is coming in and out of the wired/wireless network. Authentication and access control should be in place to discourage opportunistic attacks from outsiders. Authentication and authorization answers two very important questions—"who" is entering the network and "what" service is being delivered, respectively. Once the user and service is verified, the experience delivered for the application/ service can be varied per user based on user subscription and profile. Device health and location data is then determined in order to deliver granular access control. Fig. 5 shows basic network segmentation in a hospital environment.

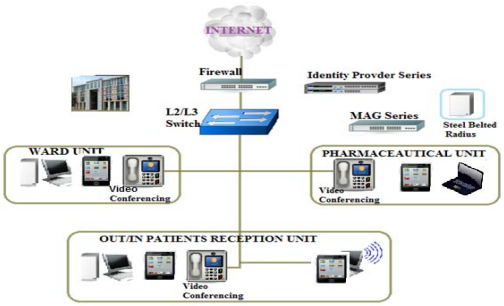


Fig. 5 Security Model in a Hospital Environment

Holistic network access control should be deployed with support for all access technologies (wired, wireless, or remote access) so that only authorized users and applications from devices that adhere to your network security policies are permitted through the first layer. Endpoints (hosts) should be authenticated when they initially connect to a LAN. Authenticating endpoints before they receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server prevents unauthorized endpoints from acquiring access to the LAN. Network access control should provide both standards-based 802.1X port-level access and Layer 2 through Layer 4 policy enforcement based on user identity. To achieve differentiated role-based access from internal networks, the hospital environment network is segmented. Also, the logical control points should be defined to control access to critical data, as well as contain any threat within the smallest segment of the network as possible. Access port security features such as dynamic Address Resolution Protocol (ARP) inspection, DHCP snooping, and Media Access Control (MAC) limiting should be leveraged to harden the access layer.

The network access control solution has combined user identity, device security state, and network location information for session-specific access policy by user and for leveraging the existing network infrastructure. The network access control delivers comprehensive control, visibility, and monitoring, as well as it is standards-based, reduces attack exposure, and decreases access control deployment costs and complexity. It is also adaptable and scalable to meet the network access control requirements for hospitals and health centers of any size.

Health sector institutions typically have a number of visiting guests and patients accessing the network from outside on a daily basis. Because of this, the network access control solution should address the common problem of how to provide appropriate access to temporary guests by using a Web interface. Guests can be granted customizable, limited time access privileges on the network during the duration of their stay. Fig. 6 shows an example of how network

administrators can enforce endpoint health policies for all types of users.

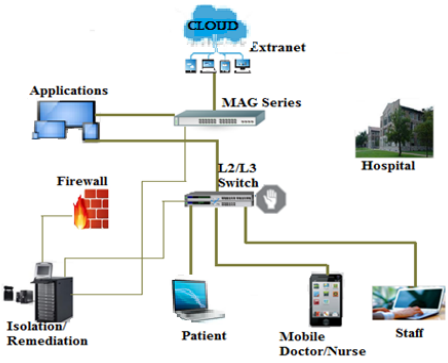


Fig. 6 Implementing Endpoint State Policy for all User Types Model

The network and security infrastructure (switches, routers, wireless access points, firewalls) integrate with inventory management and existing AAA systems, as well as network management and monitoring frameworks to gain unprecedented real-time visibility into the hospital security environment.

B. Stateful Firewalls and Router-Based Security

In this ever-changing attack setting, smarter and more sophisticated attacks have the ability to penetrate the previously mentioned lines of defense. Thus, as an added layer, a robust firewall with stateful inspection is necessary. These firewalls provide stateful inspection of traffic traversing different network segments. In addition, they should be able to create VPNs using internet protocol security (IPsec) for authenticating and encrypting IP packets to provide critical protection against DoS, Distributed Denial of Service (DDoS), and other types of attacks deployed at the perimeter. Firewalls must be scalable to handle increasing volumes of traffic when deployed at the network perimeter or at the core, so the network's performance is not negatively impacted during spikes. Firewall security consists of several distinct features as listed hereunder:

Scalable performance - leverages new services with appropriate processing capabilities without sacrificing overall system performance.

System and network resiliency - provides carrier-class reliability.

Interface flexibility - supports highly flexible I/O configuration and independent I/O scalability.

Network segmentation - offers security zones, VLANs and virtual routers which allow administrators to tailor security and networking policies for various internal, external and Demilitarized Zones (DMZ) subgroups.

Robust routing engines - provides physical and logical separation of data and control planes to allow deployment of consolidated routing and security devices and to ensure security of routing infrastructures.

Comprehensive threat protection - provides integrated security features and services that include a multi-gigabit firewall, IPS, DoS/DDoS detection and mitigation, Network Address Translation (NAT), and QoS. In both wireless and wired hospital networks, intelligent routers should be deployed to prevent IP spoofing. On the data plane, routers should perform anti-spoofing by implementing Access Control Lists (ACLs) and IP fragment filtering to drop all inbound traffic with suspicious source IP addresses or IP address ranges. Networks SRX Series Services Gateways are designed to meet the network and security requirements for hospital LAN consolidation, rapid services deployment, and aggregation of security services.

C. Application Layer Security

The most sophisticated network attacks require another logical layer of defense, namely an Intrusion Protection Services (IPS). The IPS detects unusual or suspicious behavior on the application layer by using customizable signatures based on stateful protocol inspection, attack patterns, and behavioral learning. This capability is vital for hospitals to protect their networks against penetration and proliferation of worms and other malware including trojans, spyware, keyloggers, and adware. These systems should be designed to detect the presence of attacks within permitted traffic flow to the network by using stateful signatures that scan for attacks based on known patterns. Stateful signatures should be easily customizable in order to fit into different provider requirements and specific concerns.

Networks AppSecure™ is a suite of next-generation security capabilities for the SRX Series Services Gateways that uses advanced application identification and classification to deliver greater visibility, enforcement, control, and protection over the network. Working in conjunction with the other security services of the SRX Series, AppSecure provides a deep understanding of application behaviors and weaknesses to prevent application borne attacks that are difficult to detect and stop. As an integrated service, AppSecure provides the scalability to meet the requirements of the most demanding environments.

D. Mobile Device Security

Today's health sectors are challenged with deploying mobile security and granular access control for a growing number of diverse mobile platforms, including Apple iOS, Google Android, Nokia Symbian, Microsoft Windows Mobile, and BlackBerry. With increasing choices of smartphones and other types of mobile devices, employees often bring their personal devices into the enterprise and use them to access corporate resources. When these devices are lost or stolen, enterprises risk losing sensitive corporate data such as e-mail and confidential documents.

The Networks UCIC system devices operating system mobile security suite creates a comprehensive solution comprising mobile device security and secure mobile access control. With this solution, enterprises can overcome the challenges of a heterogeneous mobile environment, as well as secure mobile devices from malicious attacks.

International Science Index 84, 2013 waset.org/publications/9996790

International Science Index 84, 2013 waset.org/publications/9996790

E. Comprehensive Protection

In today's environment of constantly evolving threats, providers require solutions that can protect against unknown and known attacks. Many of the most significant attacks involve "zero-day" attacks or unknown pattern attacks that leverage vulnerabilities where there is no signature or software patch. Furthermore, while external threats such as trojans, viruses, worms, buffer overflows, and SQL injections are the most publicized, internal threats are often overlooked and may be more common than external threats. Implementing multilayered security helps to protect against both external and internal threats.

If one of the components of a comprehensive, multilayer security approach is missing, Health sector networks are easily vulnerable to a loss of network integrity, revenue, and even corporate reputation. Networks end-to-end security solutions, supported by its integrated products, provide this high level of comprehensive protection to enterprise campus networks.

F. Network Management

Network management usually consists of a wide variety of tools, applications, and products to assist network system administrators, who face many challenges when provisioning, configuring, maintaining, and monitoring an enterprise network that consists of routers, switches, and firewalls. Network management systems help network administrators with various device management tasks, including Fault-management, Configuration, Accounting, Performance, and Security (FCAPS) management, and they also provide programmable interfaces that developers can leverage to automate repeated tasks.

VII. Conclusions

With today's ever increasing demands on global communications and collaboration, combined with a myriad of communication tools and end user types and devices, health sector must deploy a suite of services that enable these communications tools to operate seamlessly over an IP-based network with high performance and a good user experience that is still cost-effective. Major trends as unified communications, bandwidth-hungry applications, BYOD, and WAN/LAN security are forcing the health sector to consider a solution that addresses all of these challenges. The critical points include the access, aggregation core, security, WAN edge tiers, and most importantly, hospitals where security is critically important, as is the network administrator's ability to maintain high performance and an enhanced user experience. The UCIC system is the right system to be deployed to address the above mentioned concerns for the health sector as described in details in this paper.

UCIC delivers a high quality, highly secure experience across any workspace. This helps the health sector to: Shorten service delivery cycles, reduce response times, encourage innovation. reduces lag with better real time tools, deliver a streamlined and better user experience, increase workforce agility, reduce support and administrative overhead and save money.

References

[1] M. Denny, "Active voice to integrate nuance speech recognition into it's unified communications solutions" voice access to messages makes it easy to manage daily communications. www.avst.com/pr-archive/active_voice. As per July 12, 2012.

[2] M. Rouse, "Unified communications" multimedia services include messages of mixed media types. http://searchunifiedcommunications.techtarget as per July 12, 2012.

[3] Bhat and Norquist, "Telepresence Technology Overview. Cisco Telepresnce Cisco on Cisco.www.cisco.com/go/offices as per October 26, 2011.

[4] C. Jackson," Net Defense - The Unified communications security testing suite" www.networld.com/community as per July 13, 2012.

[5] Cisco, 2013, "How Cisco Achieved Environmental sustainability in a connected workplace". Cisco Connected workplace aspires towards a green work environment. http://www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/TelePre. As per July 14, 2013.

[6] F. Baglioni, "Unified communications solutions" Learn how unified communications from Microsoft can reduce costs improve and instant messaging systems with an integrated windows-based platform. www.microsoft.com/uc/ as per July 12, 2012.

[7] R. Grigonis, "Inseparable: presence and unified communications" www.tmcnet.com/channels/calls-center as per July 12, 2012.

[8] A. Anoshin, "The connected enterprise" Unleash the true potential of your enterprise VoIP; IP-telephony-VoIP unified communications sorting out the definitions. http://bsc.it.com/books/connected-enterprise as per July 10 2012.

[9] J. Barlett, "Video Conferencing integration considerations" Integrating Video Conferencing with unified communications. http://searchunified_communications.techtarget as per July 12, 2012.

[10] S. J. Campbell, "Mobile unified communications featured", http://www.tmcnet.com_channels/mobile_unified_communications as per July 12, 2012.

[11] J. Farla, "Unified communications" How remote call control powers. http://unified-communications.blogspot.com as per July 12, 2012.

[12] Teliris, 2012 "The magic of TelirisTelepresence is that you forget about the telepresence technology and focus on your meeting" www.necunifiedsolutions.com as per August 21, 2011.

[13] J. Scarpati, "Intranet strategy with collaboration products ensure fresh content" http://searchunifiedcommunications.techtarget as per July 13, 2012.

[14] M. Rouse, "Unified communications-Multimedia services include messages of mixed media types" http://searchunifiedcommunications.techtarget as per July 12, 2012.

[15] J. Parlas, "Unified Messaging and Unified Communications" http://www.viewer.media.bitpipe.com/1078177630_94711 as per October 26, 2011.

[16] J. Pirkola, "Unified communication and Collaboration" http://www.tieto.com/what-we-offer as per July 13, 2012.

[17] D. Don van and M. Parker, "Achieving cost and resource savings with unified communications" How unified communications provides proactive responses to the harsh economic environment and how Microsoft unified communications solutions can enable those responses for your enterprise. www.microsoft.com/uc as per July 13, 2012.

[18] MoH "Health Strategic Plan III 2010/11 – 2014/15" www.health.go.ug/docs/HSSP_III_2010.pdf.

[19] HSA, Uganda health system assessment 2011. http://health.go.ug/docs/hsa.pdf as per January 7, 2013.