A VIDEO CONFRENCING SECURITY FRAMEWORK FOR SYNCHRONOUS ELEARNING

By

NATHANIEL NDEGWA KIRONGO

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MSC DATACOMMUNICATION IN THE FACULTY OF COMPUTING AND NFORMATION MANAGEMENT AT KCA UNIVERSITY

12TH NOVEMBER 2013

Declaration

I declare that this Research project is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this Research project contains no material written or published by other people except where due reference is made and author duly acknowledged.

Student Name: Nathaniel Ndegwa Kirongo Reg, No. 11/01735

Sign: _____ Date: _____

I do hereby confirm that I have examined the master's Research project of

Nathaniel Ndegwa Kirongo

AND have certified that all revisions that the Research project panel and examiners recommended have been adequately addressed.

Sign: _____ Date: _____

DR. Alice Njuguna

A VIDEO CONFRENCING SECURITY FRAMEWORK FOR SYNCHRONOUS ELEARNING

Abstract
Many higher education institutions offer educational courses online on ELearning basis with web 2.0 applications to support and conduct their coursework. One of the novel tools used in such learning platforms is video conferencing. Little has been done so far to ensure the security and integrity of information transmitted over video conferencing platforms in ELearning. Since this style of education so heavily relies on the web, threats uncommon to other forms of learning are encountered. Security measures implemented for online applications have not been very successful in securing such systems due to their unique nature.
This research sought to develop a security framework for use in securing video conferencing systems as used in synchronous ELearning in institutions of higher learning. The paper looks at the current security measures in use, their shortfalls and proposes a framework of implementing video conferencing security.
The main problem addressed is how to effectively secure a multi user learning video conferencing system that is accessible remotely but centrally hosted. The goal of the research was to provide institutions of higher learning with a framework for deploying secure video conferencing educational programs in the most secure and effective manner. The framework was developed from a study of current information security models employed in securing video conferencing and correlating them to the synchronous ELearning environment. Three relevant models were examined; The Conceptual model for Security Outsourcing (Samarasinghe et al. 2007), The Information Security Conceptual Architecture Approach (Oracle, 2011) and The Dependability model for e-learning systems (Al-Dahoud1 et al. 2010).
The developed framework was then tested by simulation and the results analysed to validate its effectiveness.
Key words: Video conferencing, Web 2.0, ELearning, Elearning 2.0, Synchronous ELearning, security and Synchronous videoconferencing.

Table of contents

Dedication

To God, my parents, siblings, friends and my wife
for their companionship, support and love.

Acknowledgements

I wish to acknowledge the worthy support received from to my supervisor Dr. Alice Njuguna, whose supervision and guidance has enabled me to produce this work.

Many thanks also go to the staff of the Faculty of Computing and Information Management that helped create an enabling environment that made it possible for me to complete this work.

Special thanks for the encouragement and support from my fellow students, most notably Amos, Cecilia, Vancy and Rogers. My friends Joseph and Rachael without whose moral support this would have been difficult. To Mr. Kiula for his valuable and timely insight.

To the Fine Media Ltd. Management, thank you for allowing me to do this and supporting my quest to advance academically.

Finally I would not be successful without the support of my most loving and supportive wife, Sylvia. Her domestic support and prayers gave me the peace and strength to go through with this; I love her more than anyone on the world.

I THANK YOU ALL

List of Figures

List of Tables

Acronyms and abbreviations

VC Video Conferencing

MCU Multipoint Control Unit

ITU-T International Telecommunications Union Standardisation

VOIP Voice Over Internet Protocol

NAT Network Address Translation

DoS Denial of Service

ISM Information Security Management.

Chapter 1

1.0 INTRODUCTION

With the increased demand for higher education and the growing number of students, institutions of higher learning are being faced with a new challenge of availing course content to students who cannot attend classes physically. In order to achieve effective remote education, training has to be approached differently from the traditional systems. This has given rise to remote learning programs (Furs-Bowe 1997), the most effective of which is synchronous ELearning **(**Kamla 2009). This mode of learning relies on synchronous video conferencing for knowledge transfer and interaction.

However this brings about a new plethora of risks not experienced by traditional education systems (SANS institute 2003). This form of knowledge transfer is heavily dependent on public communications networks and is exposed to threats that face users of public networks. The integration of different applications and interoperability pose a security challenge since access to the system is not centralized. This requires a different approach to security that ensures the data is not only secure from outsider tampering but also from insider mishandling (Bevanda et al. 2009).

1.1 Background of the study

Within higher education, one of the major teaching challenges has always been helping students to bridge knowledge with real life practice. This is especially important in applied academic disciplines including medicine, education, social science, and engineering where professional knowledge are constantly being renewed and recreated through real practice (Nicol et al. 2010). Compared to traditional methods of teaching that emphasize classroom lectures; the deployment of ELearning has increased the flexibility and effectiveness of teaching and learning by removing the restrictions of time and space in knowledge delivery and capturing (Nicol et al. 2010).

Video conferencing is one aspect of ELearning that enables students to access knowledge from experts in their fields of study without having to be physically in their presence. Students taught via video conferencing have been found to grasp concepts taught as well as students in a class (Furs-Bowe 1997).

There are several security concerns in video conferencing, namely; physical security of the endpoints, eavesdropping on the video or audio portions of a connection (meeting security), denial of service attacks, administrative security, and malicious “monkey-wrenching” of the endpoints(Furs-Bowe 1997).

Because of the diversity of the security challenges, multidimensional security approaches are required. But first understanding the motivation of possible attackers is important.

1. A business competitor or someone within your company might want to listen into an important meeting.

2. A competitor might want to launch a denial of service attack, so that an important videoconference never takes place.

3. A student that uses videoconferencing to receive instruction at a distance might want to make the system inoperable in order to avoid having class or having to take a test.

4. A thief might want to steal an endpoint in order to sell it. (SANS institute 2003)

Due to the unique nature of the design of video conferencing solutions, securing them is specific to the way the video signals are transmitted. In this paper we will be looking at desktop solutions using IP networks to communicate with a central video conferencing service provider. The designed security framework will be compatible with the International Telecommunications Union Standardisation Sector (ITU-T) H.323 umbrella of protocols for IP videoconferencing. The service will be facilitated by three elements:

- Multipoint Control Unit (MCU) that has IP-ISDN gateway capacity;
- Call routing that allows users to simply dial other users across the network the same way as making phone calls and Gatekeepers that provide call admission control which allows IP videoconferencing to be managed by user organization networks.
- A Global Dialling Scheme (GDS), a mechanism that works in tandem with the local, national and international gatekeepers in routing calls.

(Papageorgiou 2001).

In this set up, it is necessary to protect the content, services and personal data not only from the external users of a system, but also from the internal users of a system, including the development and administrative users (Bevanda et al. 2009).

1.2 Definition of key theoretical terms

To create the context of this research, this section defines the terms that will be used, among others; Synchronous ELearning, Video conferencing, Web 2.0, and ELearning2.0.

A Model

A model is a way of representing a real or conceptual complex system in a tangible form. It is designed to display the key features and characteristics of the system which is the focus of study, so as to be able to predict, modify or control the system's behavior. It therefore only includes some, but not all, aspects of the system being modeled. (Law and Kelton 2000).

A security framework

A security framework is a code of practice and principles that includes process, policy and procedures used to protect and govern information security. A comprehensive security framework boils down to three familiar basic components: people, technology, and process (Stamp et al. 2007).

ELearning

This is a learning system based on instructional packets, which are delivered to students over a network and the assignments are then evaluated by the teacher. (Grossack 2009).

Web 2.0

This refers to the social use of the internet in a way that allows people to work collaboratively, participate in an active manner in content creation, producing new knowledge and to share information online (Grossack 2009)

ELearning 2.0

This is ELearning that places increased emphasis on social learning and use of social software. (Grossack 2009)

Synchronous ELearning

This is a mode of ELearning 2.0 that is real-time, with multiple students online and led by an instructor. (Toffler 2012).

Video conferencing

A combination of communication technologies that work together in such a way that allows people in different geographical locations real time on a two-way video and audio streams (PIM toolkit 2008).

IP Video conferencing: Video conferencing done across the internet using IP.

1.2.1 Sources of problems in Synchronous ELearning Video conferencing

Video conferencing in synchronous ELearning is susceptible to challenges faced with main stream IP video conferencing. It has been seen that when a new technology is deployed on a dedicated network to which access is a connection with limited accessibility, security concerns are usually minimal. The new technology is considered secure because its access is controlled. But it has also been seen in technologies like VOIP, there are new security challenges once technology moves out into the public networks and is visible to the global Internet (Frost & Sullivan 2005).

The challenges can be looked at from two dimensions; the technical security challenges of the providers and the user related security challenges.

For the technical security aspects, the following issues are paramount as listed by Frost & Sullivan (2005):

1). Firewalls and NAT Traversal

Firewalls are a mechanism that is used to keep certain types of traffic out of a network. They are normally deployed in critical points in a network's infrastructure, mostly between the public Internet and an organization's private network or between different offices and the private network or even between segments of the same private network. In reality, it is very difficult in the connected environment that exits today to implement a firewall that completely separates networks. (Frost & Sullivan 2005).

Alot of videoconferencing systems available today use the H.323 protocol for communication. H.323 has a number of security challenges majorly because it requires the opening of a large number of ports in order to function. (Frost & Sullivan 2005).

Network Address Translation (NAT) poses another major challenge for IP videoconferencing. NAT is a preferred method for allowing a one-to-many relationship of IP addresses in a corporate network. NAT is also used to hide the digital footprint of the private network. This security feature provided by NAT causes a several security problems for videoconferencing over IP. Since many IP video conferencing systems use IP addresses for dialling, NAT makes it more complicated as a video conferencing endpoint inside the network will have a different internal IP address than it would show by the NAT to the public network (Frost & Sullivan 2005).

2). End Point protection

IP Videoconferencing endpoints are also subject to growing attacks in the form of denial of service attacks and automated or unsolicited audio and video calls. Enterprises are realizing more and more the importance of protecting the endpoint not only from attacks active attacks but also from passive attack such as eavesdropping and snooping.

To increase the ease management of Video Conferencing end points, some may choose to have them logically placed outside the firewall. This practice circumvents the issues associated with H.323 opening many ort and NAT traversal problems but opens the videoconferencing endpoint to attack and misuse since it is now visible on the internet.

3. User related security issues

User related security issues, as listed by Tomas Olovsson (2001) are passive and active attacks. Some of the passive attacks include;

Unwanted guests, call snooping and recording of videoconferencing media

It is possible, albeit theoretically possible that in an H.323 set up, for a third party to snoop a session and therefore able to record or even relay the conference. Also by being able to inspect data in transit, a snooper is able to silently join a conference by simply connecting to an MCU. This is safer for an attacker as it reduces the chance of detection and being later traced (Janet 2011).
Whereas active attacks, as stated by (Gurmeet 2006.) include:

1). Masquerade Attack: This is an attack whereby one entity pretends to be another entity all together to gain unauthorized access. This attack usually includes one of the other active attacks.
2). Replay Attack: It involves the capturing of messages being transmitted and retransmitting them to produce an unwanted effect.
3). Modification of Messages: Some portion of a legitimate message is altered of messages are delayed or reordered to produce an unauthorized effect.
4). Denial of Service (DoS) Attack: DoS Attacks occur when packets are sent to flood a system or a video conferencing node .The aim being to clog the system and consume the bandwidth and

making it hard to refuse the requests of the attacker, without also refusing legitimate requests for service.

1.3 Problem Statement

Whereas there has been an influx of higher learning ELearning programs, enough has not been done in terms of securing information shared over such interactive platforms. Information on the Internet is continuously exposed to security threats. As a consequence of ELearning having to depend on the Internet or, specifically, mostly via web applications, the ELearning environment has also become affected by security threats. (Hayaati et al. 2010). Synchronous ELearning requires active online presence for the parties communicating; meaning exposure to threats is constant.

Synchronous ELearning uses video conferencing as the major tool of knowledge transfer and such a system is fully online and visible from the internet while in use. There is therefore need to secure the system to ensure the integrity of the information shared on it.

There are several security concerns in synchronous ELearning: The system's integrity, availability and confidentiality of information, which may lead to serious legal and academic consequences. The disclosure of sensitive information or the unauthorized participation in e-training activities must be prevented. (Granda et al, 2011). Securing the e-learning environment requires avoiding the four types of threats; fabrication, modification, interruption and interception. Currently, little research has been conducted to secure the e-learning environment. Researches in security mainly focus on three main areas: policy, identity (which refers to access management) and intellectual property. (Hayaati et al. 2010). This research seeks to come up with a wholesome and conclusive security framework for video conferencing in synchronous ELearning.

1.4. Problem Justification

Information Security Management measures used in other fields of information exchange is not relevantly flexible when applied to synchronous ELearning video conferencing. As observed by Hayaati et al. (2010) , due to the dynamic ELearning platforms and different user behaviors, novel ELearning media require a security management methodology which can act as a guide in helping the ELearning provider (institutions) in managing the information security within the ELearning environment. A good combination of ISM and current information security

technology can be used to provide a good security model for video conferencing in synchronous ELearning (Hayaati et al. 2010).

As observed by, Khalil et al. (2003), most e-learning innovations have focused on course development and delivery, with little or no consideration to privacy and security as required elements.

The academic integrity of information shared is susceptible to some of the common video conferencing dangers, namely; a confusing interface that makes many conferencing applications too complicated to use and the fear that private discussions shared via the public internet will be leaked. From literature reviewed, it was seen that while encryption protects the data that is on transit and that users are afraid of online listeners and watchers (Slayden et al, 2007).

Previous studies have shown that barrier to a more wide-spread adoption of online Education is the security of such systems (Hayaati et al. 2010).

There is therefore a need for a security framework for ELearning video conferencing that will boost the user confidence in the security of synchronous eLearning and positively impact online education as a whole.

1.5 Research Aim and Objectives

1.5.1 Aim

The main aim of this research is to develop a security framework for synchronous ELearning video conferencing systems that will be used by institutions to secure their synchronous ELearning systems and enable them to design relevant security models for their ELearning video conferencing systems.

1.5.2 The specific objectives of the study:

1. To evaluate the security status of video conferencing as used in synchronous ELearning by higher learning institutions.
2. To analyze the security challenges facing video conferencing in synchronous ELearning applications in higher education.
3. To design and implement a security framework for video conferencing in synchronous ELearning used higher education.
4. To simulate and validate the security framework

1.6 Scope

This paper focuses on creating a security framework for video conferencing in synchronous ELearning in higher education. This is deliberate since video conferencing in synchronous ELearning is a novel area in higher learning (Hrastinki 2008). Thus the security framework created will hopefully be replicated with equal success in other areas of video conferencing. Secondly, synchronous ELearning has been seen as the most effective form of ELearning **(**Kamla 2009) thus securing it will enhance its effectiveness.

1.7 Importance of the Research

With the advent of Web 2.0 technologies, education has become more online than ever before. A lot of learning is interactive and over a network as many services and day to day work activity are executed over networks. As the work place demands more interactivity and online collaboration, the education system needs to respond accordingly and train students on how to use such tools since they are required in the real world. As synchronous ELearning becomes more and more part of higher learning, securing it is very important and will preserve and hopefully improve the quality of education offered.

As pointed out by Hayaati et.al (2010), previous studies have shown that barrier to a more wide-spread adoption of online Education is the security of such systems. By creating a frame work of securing synchronous video conferencing (VC) systems in education, this research will promote the adoption of synchronous ELearning as the most effective means of online learning.

1.8 Significance of the Study/ Contribution

1. There is a need for security framework for applications used in ELearning, students' information and the platform's integrity need to be protected. (SANS institute 2003). The security framework developed by this research for VC in synchronous ELearning can be applied in other fields of video conferencing.

2. The results of this research will shed more light on issues surrounding synchronous VC enabling institutions providing the service to secure their VC ELearning platforms.

3. The simulated security framework will help higher learning institutions make informed security policies for synchronous ELearning and decide on the security measures to take. Since simulation can improve education effectiveness and help to develop the art of decision -making.

Simulation can be used as a facilitator of communicating ideas up and down within the organization (Greasley 2004)

4. With the validation of the security framework, it can be used as a tool to advice institutions offering ELearning VC service on how to do it securely and also expose any flaws in the systems currently in use. System Dynamics models help to understand the relationship between behavior patterns and the design of a system. Problems related to a system's behavior can therefore be resolved by altering the system design as observed by Marquez and Blanchar (2004).

5. Previous studies have shown that barrier to a more wide-spread adoption of online Education is the security concern of such systems (Hayaati et al. 2010). The success of this security framework will boost the confidence of users of such systems resulting in a more widespread adoption of online education, specifically synchronous video conferencing.

Chapter 2

2.0 LITERATURE REVIEW

2.1 Introduction

In this chapter the researcher reviewed literature on ELearning, Synchronous VC, system simulation and information security models and VC security vulnerabilities. This was of essence in developing a framework that evaluates vulnerabilities of synchronous VC security and provides a way of securing synchronous ELearning platforms.

2.2 Review of relevant video conferencing security solutions

The researcher in this section presents security models that are relevant to synchronous VC and have been used to secure VC systems.

i). Criticom's solution

a). The DI-366 Optical Dialing Isolator

This solution is tested up to a TEMPEST Level 1 and is a certified optical dial isolator that enables secure endpoint to endpoint dialling in classified environments. It provides the required isolation for a classified environment for isolation of between the red side (codec) and the black side (IMUX).The solution is considered secure because routing the dialling signals through this optical coupler, since there is no contact whatsoever between the codec and the IMUX. (Wainhouse Research, 2004).

It gives end-users the option of being able to dial both secure and non-secure videoconference calls from the user interface greatly easing the dialing of video calls. This solution is only manufactured in the US to ensure there is no compromising of security guidelines. The DI-366 can be used independently or together with other Criticom's products. (Wainhouse Research, 2004).

This is a proprietary solution, available in the US only and certified by US' standards. The cost of set up is considerably high.

(b). The ISEC-STS Secure Teleconferencing System

The ISEC-STS was the first secure/non-secure RS-530-based videoconferencing solution to be TEMPEST tested and certified. Each ISEC-STS system as listed by (Wainhouse Research 2004),include:

• A comprehensive TANDBERG codec

• A variety of display screens

• A Criticom's ISEC-320 switch

• A Criticom's DI-366 optical dialing isolator

• An Integrated multiplexor

• Special furniture for housing the equipment

This solution still requires the addition of an encryption device (KIV-7 or KIV-19), for users to videoconference. It can also be used with other IP encryptors for secure, IP-based videoconferencing (Wainhouse Research, 2004).

This was a solution targeting the US Government's agencies and was still proprietary and requiring a high investment. A cheaper and easier to implement solution is required.

(ii). One space solution

This is Hp created concept of having an integrated user friendly user interface. It enables all users in different connected locations to enjoy the same experience in terms of the user interface: the same view of and control over the user interface. The user interface is simple with no submenus and private information cannot be accessed without the necessary authorisation. All icons are pictorial and represent common objects found in and around the conference room (Slayden et al, 2007).

This solution is focused on a centralized system where participants to the meeting are in known geographical locations such as different offices. Although it addresses the user's need to be

confident of the system's security, the security solution needed for synchronous video conferencing needs to be decentralized due to the nature of its implementation.

a). State of the art of video conferencing security in Synchronous ELearning

The adoption of e-learning technologies in higher education has shown a commendable increase in the use of technology. A research was done to examine the status of e-learning in African Universities, based on 358 responses from 25 African countries. It showed that 174 respondents (49%) had used a learning management system (LMS) for teaching in the previous 12 months while 185 respondents (52%) had interracted with an LMS in a learning environment (Unwin et al., 2010). This shows the uptake of ELearning in Africa is at encouraging levels, thus there is therefore need to create a way of securing such systems and consequently encouraging more uptakes.

In tertiary education, one of the biggest challenges in teaching for a long time has always been how to help students connect the knowledge acquired in class with real life practice. This is especially important in many applied academic disciplines including medicine, education, social science and engineering where there is a constant change in the knowledge base as a result of practice and innovation (Nicol et al. 2010).

New web 2.o applications have been seen to provide an avenue to facilitate e-learning, but this has been with new security risks that were not being experienced earlier. Mainstream research has for long only focused on technical solutions, and—increasingly—pedagogical issues but privacy and security have not yet been adequately addressed, as observed by Weippl and Eber in 2008. They put forth several valid concerns, stating that there are three potential risks: First the complexity of the applications can result in vulnerabilities in design and coding errors. Secondly plagiarism is hard to detect since there can be so many sources not acknowledged and finally publicly owned ELearning platforms may risk students, privacy by exposing their personal information and privacy to the public.

The exposure is not just to the student, but also to the tutor and the institution offering the e-learning course and the platform being used.

Effective teaching needs constant feedback from the student and numerous interaction opportunities (Ebner, 2007). Since conducting such a class requires the tutor to be online, exposure to security risks is inevitable.

For the institutions offering ELearning courses, the initial infrastructural investment may be quite high and outsourcing the service can be seen as a viable option as a survey by the Columbia University (2010) noted. This means that the data transferred, stored and processed on such platforms are not controlled by the institution offering the ELearning course. The main risk comes from the fact that students and teachers may not be entirely aware that their institution does not control these services. The can servers are located in a different countries and therefore privacy laws may differ.

In addition, as most Web applications are mostly built as three-tier architecture and this results in typical security weaknesses such as invalid input, a lack of server side checks, and excessive privileges. These can expose an institution to major security risks.

It is notable therefore that there is a need to address the security of synchronous ELearning. This is primarily because the security challenges faced by such programs are unique and different from the mainstream security threats. Research is needed to explore security and privacy of information issues in new learning media in education (Maleko, 2011).

Sadly, although new teaching technologies have been adopted in ELearning, such as synchronous VC, much has not been done to ensure the security of such systems.

There are several security concerns in synchronous ELearning: The system's integrity, availability and confidentiality of information, which may lead to serious legal and academic consequences. The disclosure of sensitive information or the unauthorized participation in e-training activities must be prevented. (Granda et al. 2011).

b). State of Practice of synchronous video conferencing security in ELearning.

Today, e-learning mainly takes the form of online courses offered by colleges and universities. As a consequence, the dominant learning technology employed today is a type of system that organizes and delivers online courses; the learning management system (LMS), Downes , (2005). In general, content is traditionally in this model and availed either exclusively online or together with normal teaching classes to cohorts of students, led by a lecturer, following a specific teaching plan to be completed at an already set pace also known as asynchronous ELearning (Toffler, 2012).

VC is a promising state of art technology that enriches the synchronous distance learning experience. Synchronous VC is seen as the most effective and practical way of delivering ELearning 2.0 courses, because it allows face to-face interaction. Information is richest when it

is delivered face-to-face because you see the speaker's body language, hear the tone of voice and natural language is used (Kamla, 2009).
Although the effectiveness of synchronous videoconferencing in ELearning 2.0 is undeniable, security issues such as authentication, fast symmetric encryption and secure key exchange are almost completely neglected, this is risky since security is very important in ensuring private sessions are confidential, and billing. (Geyer and Weis, 1998).

While a lot of effort in the e-learning domain has been put into modern infrastructure and content delivery, major security issues have not been sufficiently addressed (Webber et al. 2007).

The recent terrorist activities and the global focus on security have increased the interest in secure videoconferencing. The market has been dominated by legacy videoconferencing security solutions were inconvenient, complex and quite expensive, requiring dedicated networks and heavy infrastructural investments, such as Criticom's ISEC. (Waine house research, 2004).
The proprietary solutions cannot serve well in an ELearning setting because of the inflexibility and high infrastructural investment required.
Other solutions involving SIP and H.323 protocol have been seen to be more appropriate for synchronous VC for ELearning due to their flexibility. The two solutions still have their shortfalls. Without any security provisions, the messages in both protocols face the risk of being intercepted, modified, dropped or duplicated. The obvious solution is to apply security mechanisms to ensure integrity, privacy and non-inference of the messages (Papageorgiou, 2001).
Video conferencing can be shown to offer several advantages in the delivery of distance education, it is equally clear that the chance of realizing the potential is greatly enhanced if the implementation process is preceded by very careful design, paying due attention to ensuring selection of optimal systems, as these relate to both equipment and transmission media (Dallas,2010). There is need for a framework to ensure careful implementation of video conferencing security.
This research seeks to develop a security framework that will address these issues.

Chapter 3

METHODOLOGY

3.0 Introduction

This section focuses on the methods that will be used to design the security framework, and ways collect and analyze data to validate it. Research methodology is defined as the general approach to the research process, beginning from the hypothetical groundwork of the research approach to the gathering and analysis of data (Collis, 2003). The methodological approach selected for this research is literature review, data analysis and simulation. This research shall rely on the following guidelines;

- Review and analysis of current synchronous VC security literature, including vulnerability models, ISM models and security practices.
- Conduct an analysis of the effectiveness of each methodology, vis-à-vis the ideal framework.
- Design a security framework covering all the most vulnerable areas of synchronous VC security in education.
- Simulate the functionality of the developed framework and provide the results.
- Provide recommendations and implications of the developed framework on synchronous video conferencing security in education.

3.1 Review of recent research methodologies used in eLearning

Several researchers have done work in the field of e-learning using different approaches. Mixed methods have been applied in designing a model for adoption of social networked learning, comprising of survey and interviews was adopted in the collection of data for building the model (Maleko et al. 2011).

Another approach used a combination of content analysis and semi-structured interviews to collect data (Lwonga 2012).

In the above cases, a quantitative approach led to the goals of the research being achieved with valid data acquired.

For this research, qualitative methods will be used. *Much more research needs to be undertaken to accomplish best practices in the implementation of security by using a combination qualitative and quantitative research* (Dr. Malik 2011)

Three qualitative models will be examined; the Information Security Conceptual Architecture Approach (Oracle, 2011), The Conceptual model for Security Outsourcing (Samarasinghe et.al. 2007) and The Dependability model for e-learning systems (Al-Dahoud et.al. 2010). These methods and others will be analyzed to come up with a security framework for VC in synchronous ELearning.

The developed framework will also theoretically be informed by the Technology Acceptance theory (Venkatesh et al, 2003) and the information security maturity model (Dr. Malik 2011).

A simulation of the developed framework will be done to establish its effectiveness and verify its attributes.

3.1.1 ELearning Video conferencing security models

At present, information security technology, hardware and software have been used in order to secure the e-learning environment (Najwa et al. 2010). This section will examine the information technology approaches used in securing eLearning environments such as synchronous video conferencing.

3.1.2 The Information Security Conceptual Architecture Approach

The Information Security Conceptual Architecture Approach (Oracle, 2011) lists several access control areas of consideration when designing information security control architectures;

- Confidentiality
- Integrity
- Availability
- User Management
- Network Security
- Key Management
- Security Management
- Governance
- Risk
- Regulation

 Audit

 Access Control

 Standards for Interoperability

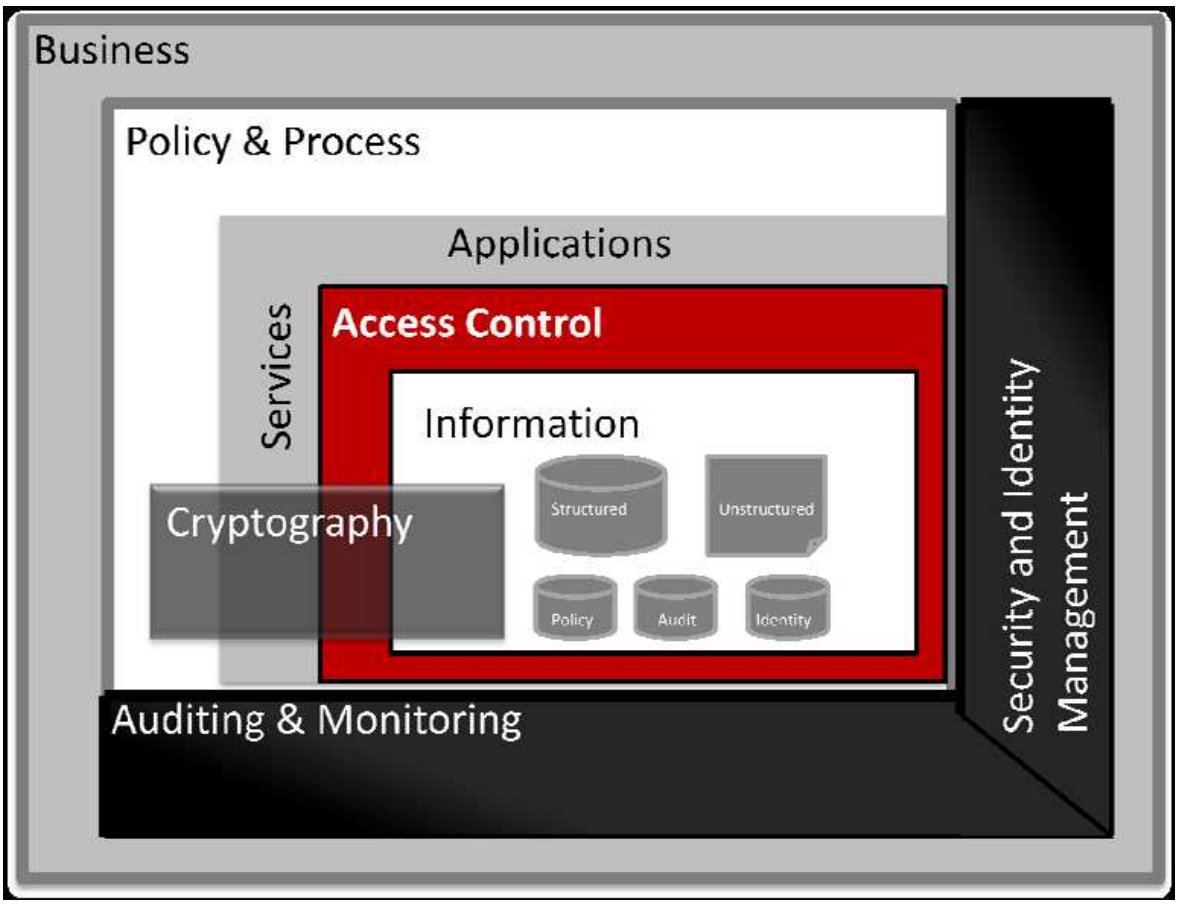

Figure 1: Oracle Information Security Conceptual Architecture, 2008

The model is positioned as an outline of the building blocks required when considering the topic of Information Security, but is by no means an exhaustive list of the controls, frameworks or challenges related to Information Security in general and specifically in synchronous ELearning video conferencing.

It discusses the importance of providing an end-to-end, deep defence across an organization's Information Security architecture with practical points to check ensuring business and IT requirements for control as well as enabling the organisation to meet their desired goals.

This is a good security model for a standalone system in a dedicated network that is only accessed through the fixed terminals; it does not put into consideration remote access across a public network, outsourcing or hosted services.

3.1.3 The Conceptual model for Security Outsourcing

The Conceptual model for Security Outsourcing by Samarasinghe et al., 2007, is a model that can be used in making security management and outsourcing decisions. It outlines several considerations;

The first step is to decide whether there is really a need to outsource IT security or not, the second steps is to select a chosen Security Service Provider (SSP) that meets the required specifications. The third step is to prepare a Service Level Agreement (SLA) that covers areas of performance and expected levels performance. The fourth step is to implement the security outsourcing and finally the last step is to monitor the Security Service Provider's (SSP) delivery of service.

This model provides a concise overview of the step by step process involved in outsourcing IT security and identifiable key steps. The model can be used to guide an organisation through the process of outsourcing IT security. It gives the rationale of security outsourcing by dividing the key steps into sub processes and explains how the conceptual model addresses each.

Since the security of VC in synchronous ELearning, may require the services of an external security service provider, a good security framework for the system should also consider the option of outsourcing. An effective security framework for synchronous VC must have both aspects of a self-hosted and outsourced security.

3.1.4 E-learning Dependability model

Another model of interest, The Dependability model for e-learning systems (Al-Dahoud et al. 2010) was also examined. This model presents dependability aspects of an e-learning system as the availability, interoperability, usability, stability, scalability and security of software and hardware components of e-learning systems. Its authors propose the business continuity of an e-

learning system as a major dependability factor. A hardware high availability approach was presented and ways of monitoring the underlying services were outlined.

The authors presented an inexpensive yet interactive ELearning platform for reliable online lectures creation, which assures lectures delivery in a timely manner as would be desired by students to make ELearning more convenient and more efficient.

Dependability is a crucial aspect of any novel learning system, and the developed framework must ensure dependability.

3.2 The proposed framework for synchronous VC security in ELearning

The developed framework considers that the institution offering the VC service can either host the service and students access it remotely or the institution can provide the information/content and outsource the service.

3.3 Characteristics of the developed framework

The developed ELearning video conferencing security framework will cover the following security areas of a video conferencing system;

Security area	Control areas	Factors affecting security
Policies and procedures	Access control	• Authentication and Authorization of onsite users • Remote access for off-site users – Passwords and digital certificates. • Physical access security control • High level IT security e.g. Firewalls and database security systems.
	User management	Differentiated users and access rights: • System access for information use • System access for Information Production • System access for information management
	Identity management	• Policies : Managed by the ACL • Identity classification • ACL management • Security policy actualization
	Cryptography	• Maintaining the confidentiality of information through encryption. • Maintaining the integrity of Information by digital signing
	a. Availability b. Usability c. Scalability	• Legal and regulatory requirements. • External commercial relationships(interoperability)

Dependability	d. Interoperability e. Stability f. Security.	• Internal organizational factors • SLA agreements and checks • System capacity
Risk Management	Outsourcing Decision	• Decision: outsource or not o Decide the services to outsource • Select appropriate SSP. • Create an SLA for the SSP • Roll out the service • SSP performance monitoring.
	Auditing and Monitoring	• Information Access • Policy Administration • User Administration • Information storage

Table 1: Characteristics of the Framework

3.4 How the specific objectives were achieved

The specific objectives are listed below and techniques that were used to achieve them are laid out as follows:-

- To Identify shortcomings with the current models used in securing ELearning systems
- To identify key variables for inclusion in the developed security framework
- To develop a synchronous ELearning security framework for use as a decision support tool by service providers.
- To validate the model by simulation
- To make recommendations to the vulnerable users and service providers

3.5 The developed framework

Existing literature was reviewed including technical papers, electronic journals, and reports to establish how VC systems are secured and the vulnerabilities associated with the methods used. After examination of the key areas of concern, a simple framework was developed that addressed the major security concerns of synchronous ELearning VC, namely;

1. Security of the users – Identity, information shared/generated, privacy of the sessions and encryption of their passwords

2. System security – Endpoint security; Access passwords, user right management, data encryption, simple user interface and capacity to host a big number of simultaneous users.

3. Security of data – Encryption of transmitted data and encryption of stored data.

3.5.1 Identifying Variables

The variables used in the simulated framework were gotten from reviewing of literature on VC security and focused by the researcher to serve the area of synchronous eLearning. They include;

1. Ease of use for the user interface and simplicity
2. Passwords for the users and the strength of those passwords, storage of the passwords (hashing).

3. Encryption of user data, both during generation, transmission and storage

4. Number of ports required to be open through the firewall.

3.5.2 Validation

The variables were then weighted and simulated using MATLAB R2009a neural networks module. The researcher believes the simulation results were valid, as asserted by Law and Kelton (1991). Law and Kelton stated that a model is valid if the decisions made with the model are similar to those that would be made by physically experimenting with the system it models. They also asserted that a model is credible when its simulation and results are accepted by the relevant body and the system's users as being valid, and is then used as a tool in decision making.

The simulated framework will able to show the most secure of several VC solutions that will be analyzed by it.

Chapter 4

THE CONCEPTUAL FRAMEWORK

4.1 Scope

The research focused on the analysis of Synchronous VC security mechanisms and the efficient ways to dynamically determine the security of a VC system. Open source VC solutions were examined using a software simulation tool due to the constraints of time, unavailability of local educational video conferencing implementations and cost. It also examined the various factors that can be used to determine how secure a VC solution is.

All the above findings were used to derive VC security variables which were then tested and validated through simulation. The period of study considered is 2011 to 2013.

4.2 Definition of Data Types

The primary data used in this research was sourced from technical data of the open source software's examined. A number of key variables were examined, from encryption, password hashing, number of open ports required, and simplicity of the user interface among others. All these variables were derived from relevant literature review.

4.3 Conceptual Framework

A conceptual Framework in form of a diagram is represented below in a way that explains the set up and operation of a secure VC solution for a synchronous ELearning scenario. The conceptual framework depicts a synchronous VC system implemented using the developed security framework. Showing how the different aspects interact.

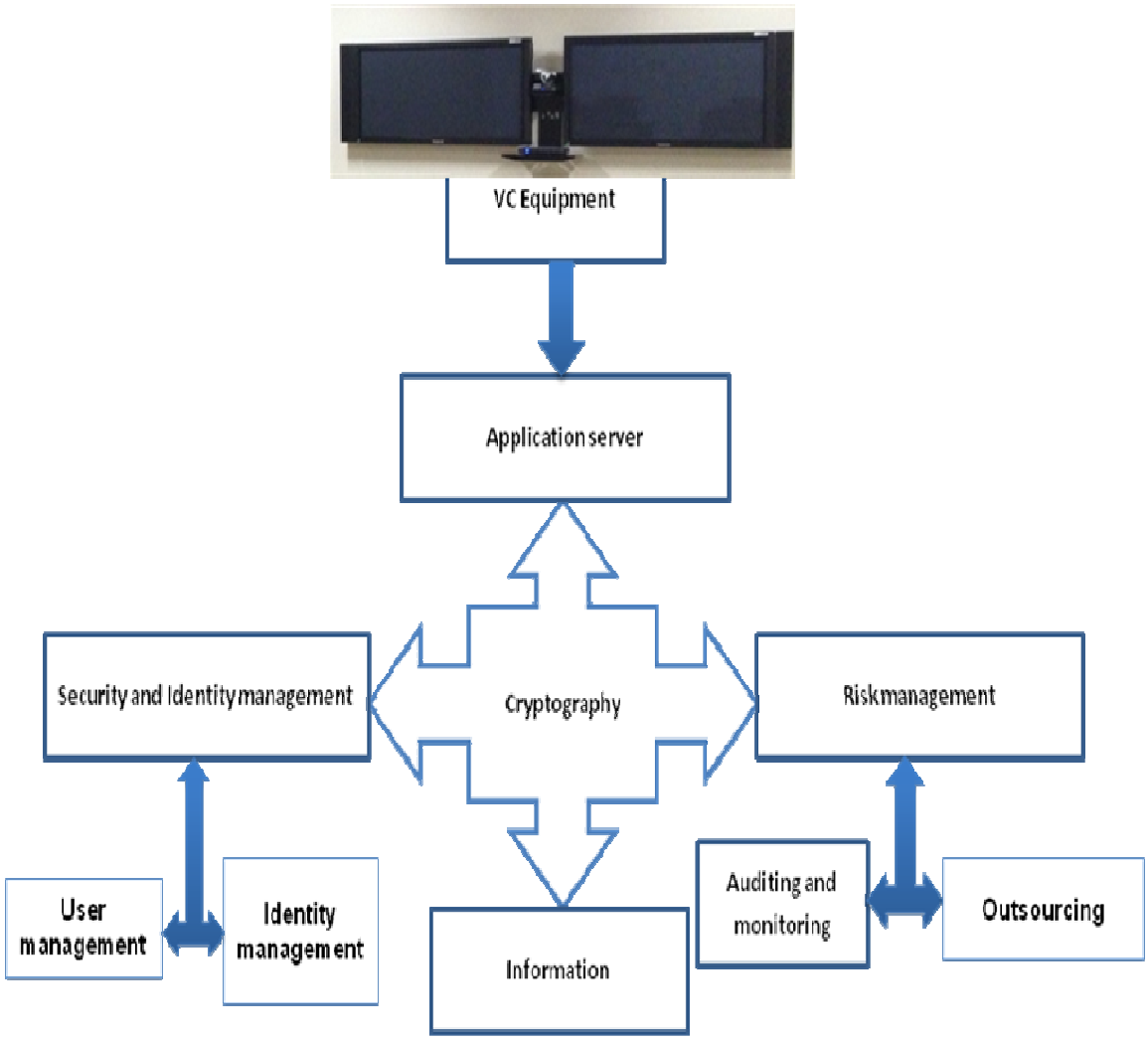

Figure 2: The conceptual Model

The above conceptual framework depicts four main components; with encryption being at the center of the whole system. The VC's system security is determined by the following steps as depicted in the above diagram:

1. The VC endpoint is accessed through an application server, and the data is encrypted.
2. Access to the data is only allowed to users whose identity has been verified.
3. There is a user identity management system that verifies the identity of users allowed on the system and a mechanism of securely storing user data.
4. There is a provision to outsource this service, and away of managing the security service provider through SLA agreements and auditing.
5. Stored information is encrypted and access regulated.

The conceptual model presented a useful foundation for developing a simulation model of the synchronous VC framework created. Variables of each of the components, weighed and correlated to the required level of functionality were used for the simulation.

The most key variables were selected for the secure standard framework design. The variables were then ranked and weighted as per their relative importance and effect on a VC system's security.

Below is the list of key variables;

	Variables
1	User log in Passwords :Allowed characters
2	Passwords :Required to Join a Conference
3	User interface : Simplicity in design
4	User interface : Ease of use
5	Secure Key exchange
6	P/w hashing
7	SSL traffic
8	Varying IP for different calls
9	Video and audio encryption
10	Number of open ports

Table 2: Secure VC Variables

Chapter 5

IMPLIMENTATION

5.0 Introduction

Although detailed implementation of a synchronous VC system are inherently determined by the developer or the institutions offering the synchronous VC ELearning learning, the security considerations can be examined by checking on some specific variables.

5.1 How the specific objectives were achieved

The specific objectives are listed below and techniques that were used to achieve them are laid out as follows:-

1. To evaluate the security status of VC as used in synchronous ELearning in higher learning institutions.

Literature was reviewed on the current security solutions used in synchronous VC by institutions of higher learning. It was realized that the solutions were specific to the specifications of the mode of VC used.

2. To analyze the security challenges facing video conferencing in synchronous ELearning applications in higher education.

Again literature was reviewed on the security techniques used in securing synchronous VC solutions and the key challenges and variables noted.

3. To design and implement a security framework for VC in synchronous ELearning used higher education.

A security framework was designed from literature review and evaluation of current IS models used in securing synchronous VC solutions.

4. To simulate the security framework

Using variables derived from literature review, a simulation was done for the developed security framework.

5.1 Shortcomings with the current approaches

Throughout the reviewed literature, the researcher did not come across a comprehensive security framework for VC in synchronous ELearning. The existing models and approaches were

evaluated by the researcher to come up with a security framework for VC in synchronous ELearning.

Most of the research reviewed by the researcher in the area of synchronous ELearning had been done primarily through qualitative approaches; this research however, chose a quantitative approach. This was deliberate as and as mentioned by Dr. Malik F., (2011) who stated that; Much more research needs to be undertaken to accomplish best practices in the implementation of security by using a combination qualitative and quantitative research (Dr. Malik F. 2011).

5.2 Proposed approach

The researcher proposed a focused approach to VC security in synchronous ELearning, starting with identifying areas of risk and dealing with the risk by either accepting , transferring it (by outsourcing) or reducing the risk.

The researcher identified variables in synchronous VC in ELearning security and developed a weighted matrix of analyzing them in a system. He proceeded to use the developed weighting framework to analyze the security of existing open source VC solutions using MATLAB's R2009a neural networks module.

The results of the simulation were then discussed.

5.3 Identified Variables

Several variables were identified. Since most VC platforms are commercial, the cost of an institution developing its own system was high compared to using commercial or open source solutions. For this reason, several open source solutions were examined, and their security levels evaluated.

The variables were picked from the different areas of interest in the VC security considering the way their interact and affect each other.

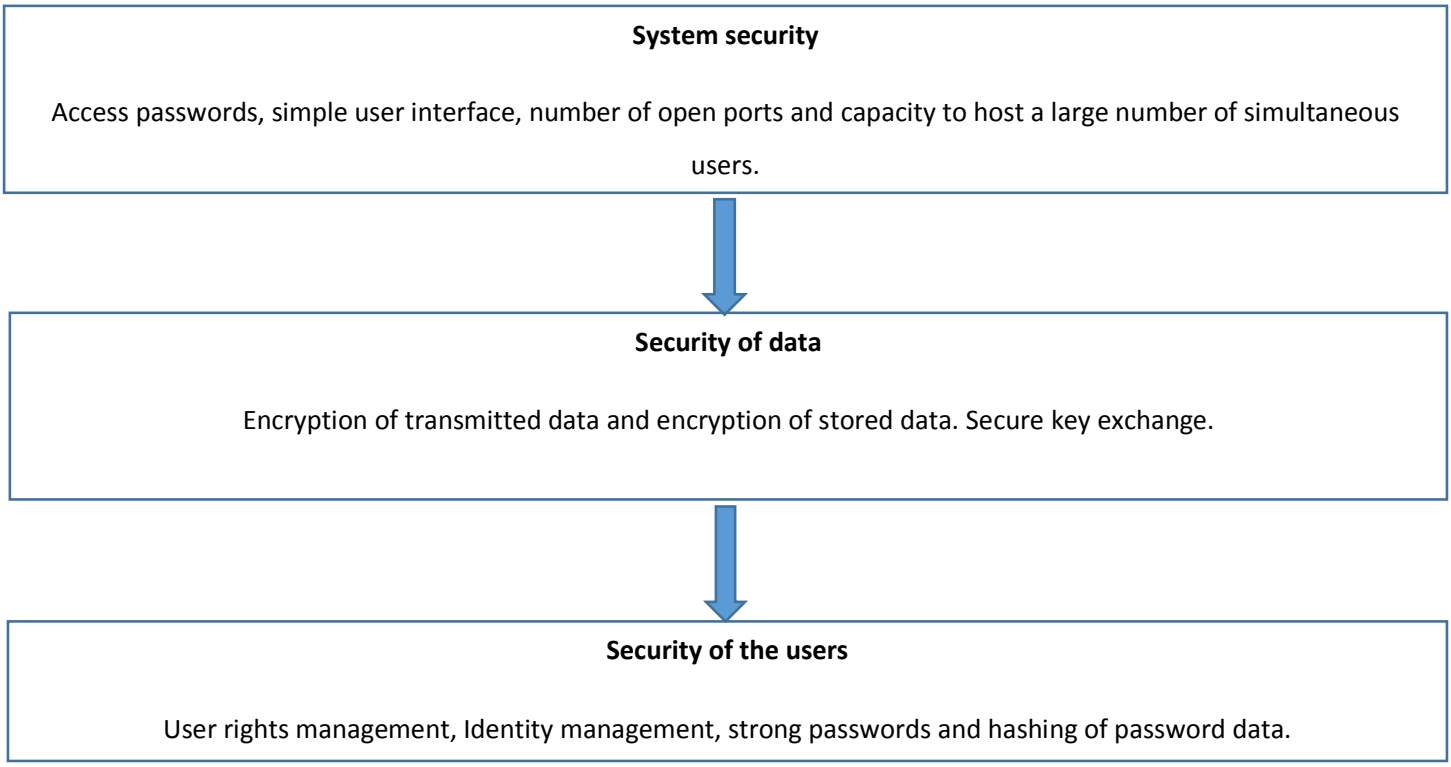

Figure 3: Identification of variables

5.3.1 Definition of Variables

Through literature review, it was noted that a good security frame work for a given system depended on three main factors; people, policies and procedures and technology (Khalid et.al 2007).

Policies and procedures dictate the usage of the system, access parameters and controls. The different kinds of users are a factor, whereby strict categorization and access rights regulation are required. The technology used, dictates the vulnerabilities, either inherent of the standard it is based on or product/provider specific.

Considering that policies and procedures are organizational factors, this research sought to focus exclusively on the security variables that are product or provider specific, since these are the major concerns in securing a VC system in synchronous ELearning.

The key identified variables, as pointed out by Rudiger et al. (1998) are;

1. Secure key exchange
2. Symmetric encryption
3. Authentication.

Weippl and Eber (2008) put forth several valid concerns; among them the complexity of the applications can result in vulnerabilities in design and coding errors. Therefore another factor to consider is the simplicity of the VC solution.

In a synchronous VC this set up, it is necessary to protect the, services, content and personal data not only from the users who access the system from outside, but also from internal users of a system such as the development and administrative personnel (Bevanda et al. 2009). The use of passwords and hashing the password data can be used to do this.

These control areas could be broken down to some measurable variable, such as the password strength, encryption type, password hashing, simplicity of the user interface etc.

The scale was from 0 to 5, 5 being most secure the ideal scale.

(i) Target variables

	Variables	**Secure standard weighted value**
1	User log in Passwords :Allowed characters	5
2	Passwords :Required to Join a Conference	5
3	User interface : Simplicity in design	5
4	User interface : Ease of use	5
5	Secure Key exchange	5
6	P/w hashing	5
7	SSl traffic	5
8	Varying IP for different calls	5
9	Video and audio encryption	5
10	Number of open ports	5

Table 3: Target Variables

The target variables are the weighted from literature review and a standard established for the developed framework. The variables for the evaluated open source VC solutions were measured against the developed framework's standard.

(ii)Input variables

	Variables	Skype	Tynychat	Hear Me	oovoo
1	User log in Passwords :Types characters	4	2	1	1
2	Passwords :Required to Join a Conference	0	5	0	0
3	User interface : Simplicity in design	3	4	3	3
4	User interface : Ease of use	3	4	3	2
5	Secure Key exchange	5	5	5	0
6	P/w hashing	5	5	5	0
7	SSl traffic	5	5	5	0
8	Varying IP for different calls	0	0	1	0
9	Video and audio encryption	4	5	4	0
10	Number of open ports	1	3	2	2

Table 4: Input variables

The input variables were derived from the technical data of the open source VC solutions being evaluated and weighted against rating of a secure VC using the target standard of the developed framework.

Data on the number of open ports was acquired from the port scan website.

5.3.2 Simulation of the Model

The variables were modeled and simulated with MATLAB R2009A, using its neural networks module. MATLAB was selected because of its useful modules for computer technical data analysis and simulation. The neural networks toolbox was selected because of the ability of neural networks to be trained to compare an input to a given target until the network matches the target. The neural network can be trained to behave in a certain way consistently.

In this case, our target is the developed security framework and the variables being fed in to the neural network are the weighted values from the synchronous VC systems being evaluated. The neural network was effectively trained and was able to model the security framework.

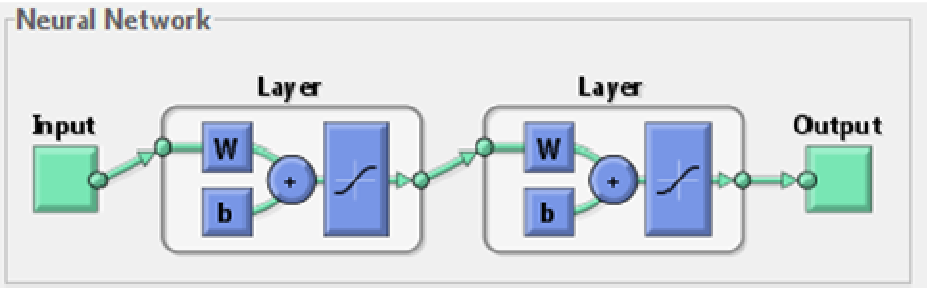

Figure 4: A neural network

The neural network was able to effectively match the input variables to the target framework for all the variables for each open source Video Conferencing solution. The result was out put on a chart that was easy to interpret and thus make a choice on the most secure open source synchronous VC solution.

5.3.4 Simulation Model Development

The simulation tool of choice used in the implementation of this thesis is Artificial Neural Networks (ANN). MATLAB R2009a was selected as the simulation software of choice because it has been widely used develop valid electronic models. In MATLAB, one of the toolboxes ANN was used. This was because ANN provides an easy to use interface that effectively displays complex interaction of variables in an easy to understand manner. One is able to observe from the interactive graphical user interface the quantitative interaction of variables within a system (Hagan and Demuth 2013). The graphical user interface can be used to describe and analyze very complex mathematical systems.

ANN was the best suitable simulation module because of the following reasons;

(i) It expresses all the variables into cause and effect relationship. This is necessary because we are examining several variables that affect the security of a VC system.

(ii) ANN gives a solution to the vulnerabilities by analyzing each VC solution by identifying the origin of the vulnerability, and how it relates with the other variables.

(iii) ANN enables the vulnerabilities of different VC systems to be examined against a set standard, the developed framework, thus determining their security.

5.4 Validation

The researcher was able to develop a framework that was successfully used to analyze a number VC software and rank them in terms of security. This was done using the individual system's technical data. The ranking was plotted graphically.

According to Law and Kelton (1991), a model is valid when decisions made with the model should are the same as those that would be made by physically experimenting with the system being modeled.

The developed framework can be said to be valid since it gave the correct ranking that could have been obtained by analyzing security data of each system.

Chapter 6

DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

6.0 Overview

In this chapter the researcher looks at how the objectives of the research satisfied through modeling and simulation. The findings and the final contributions of the thesis to synchronous VC in ELearning are examined. Conclusions and recommendations are also given.

6.1 ANN Modelling and training.

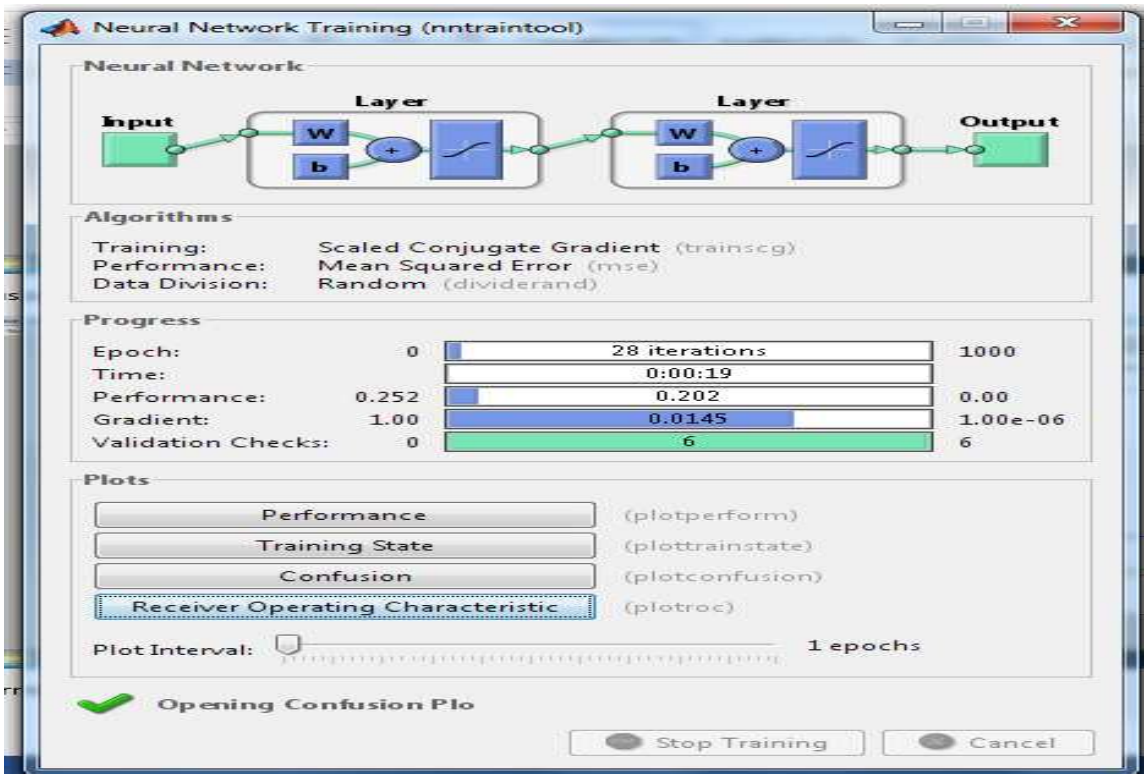

Figure 5: Training of ANN with input variables.

The ANN was trained to correctly model the input variables. After 28 iterations and 6 validation checks, the ANN was able to match the input variables to the target variables.

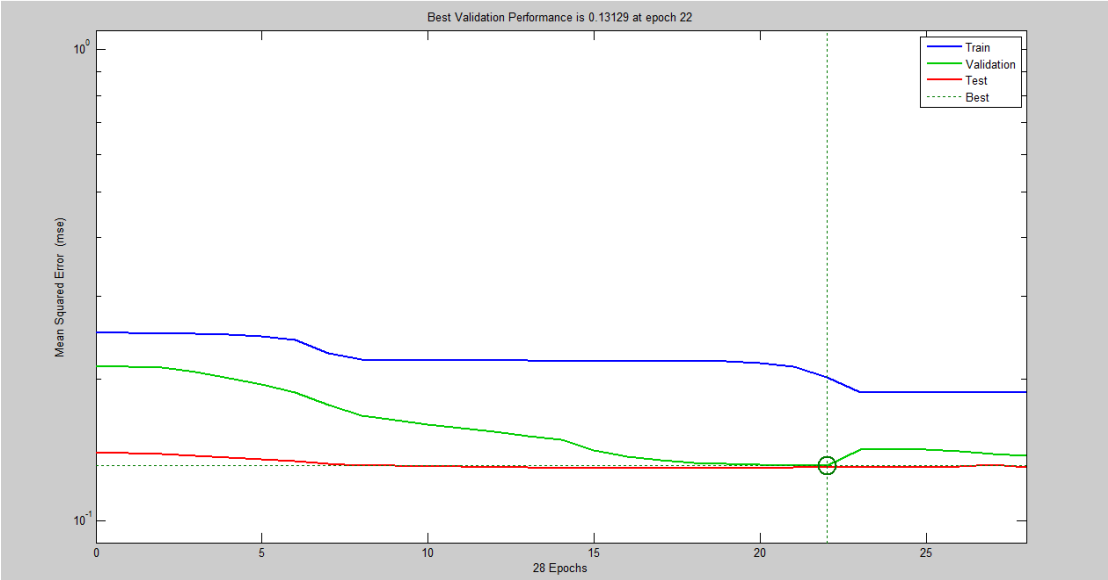

Figure 6: Best Validation Performance for the ANN.

The network performance improved after 10 epochs, the network training performed best at the 22nd epoch. This indicates that after training the network it was able to give the correct feedback following the repeated iterations during the training.

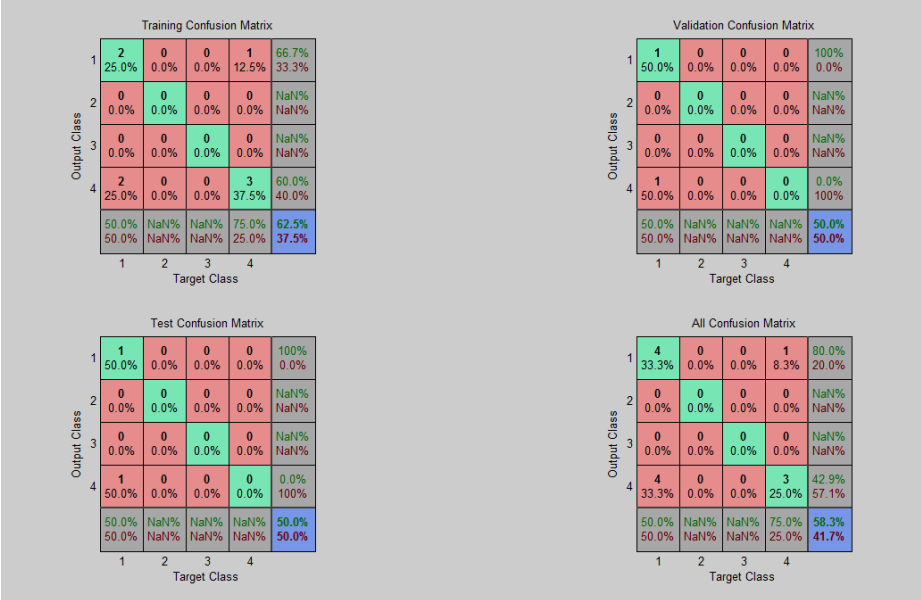

Figure 7: Confusion Matrix for the performance of the ANN

The network produced the right output at 62.5% given the target from the input as opposed to the 37.5% tendency of producing the wrong output. This shows that with training the ANN is able to predict whether a VC synchronous solution is secured or not secured.
The ANN produced the correct output after the given iterations and allowed the researcher to infer that with a given number of iterations, given the right input and correct variables it is possible analyze and even develop a secure Synchronous VC solution for ELearning.

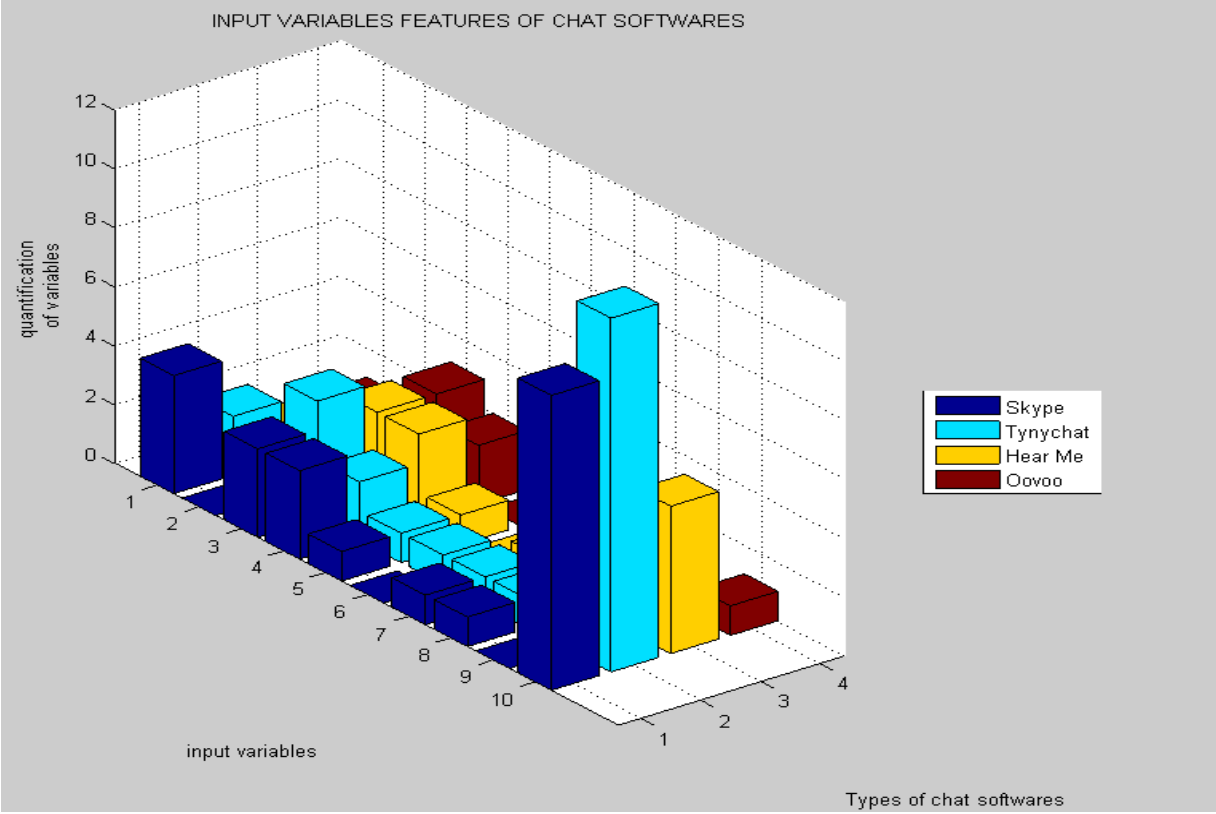

Figure 3: Modeled VC software solutions ranking

The developed model was able to effectively evaluate different open source VC platforms' vulnerabilities. The technical data of four VC solutions were examined. The result of the simulation was an easy to understand 3D ranking graphic.

The security ranking of the four showed Tinychat as the most secure solution, followed by Skype, Hear Me and finally Oovoo.

6.2 Discussion

The researcher achieved the objectives of the study using a number of techniques. Identification of vulnerabilities with the current VC security measures in ELearning and open source video conferencing software were examined and the variables used in the simulation model.

Three security models were investigated, taking in to account the accuracy, focus, non-bias, inclusiveness, and ease of use. The strength and focus of each model was reconciled to synchronous VC in ELearning and a framework developed.

Through the developed framework, the problem statement was overcome by results of the simulated model.

The developed framework was able to effectively evaluate the security aspects of several VC open source solutions and yield a simple mechanism of choosing a synchronous VC software solution for an institution.

6.2.1 Limitations

The research was done primarily on technical data obtained from literature review of the evaluated open source software. There is need to further examine the performance of the developed framework on proprietary and commercial synchronous VC solutions.

6.3 Conclusion

The framework was able to effectively identify the most secure synchronous VC solution through simulation. It can therefore serve decision tool to help institutions in selecting or developing secure synchronous Video conferencing ELearning programs.

6.3.1 Recommendations for policy makers

With the simulations' results, it was notable that this solution was primarily technical and for it to be effectively used by an institution, it would require several policy considerations to be made;

- Develop comprehensive policy on the access and use of the VC platform. This is because security of any system is not merely technical but a holistic view of a system. Policies define parameters and interactions of key players in a system. A good security framework

for a given system depends on three main factors; people, policies and procedures and technology (Khalid et.al 2007).

- Perform comprehensive security assessments periodically (regular/random intervals). As with many matters security, loop holes are discovered even in systems that were initially seen as impregnable. Regular checks are important since it is important to protect the system and the data on it from both external users of a system and the internal users, including the development and administrative personnel (Bevanda et al. 2009).

- Train users in computer security awareness and risks associated with online applications. From literature review, it was seen that one of the major security breaches were caused by improper use of the synchronous VC systems.

- Establish a security and technical approval process prior to deploying VC program. Video conferencing is a technology use in education may require approval from regulators of the education sector.

- Establish a strong SLA with the choice provider of the service if it is outsourced, and if an open source solution is opted for, a proper assessment of the required security features must be evaluated for the best suited solution to be selected.

6.3.2 Technical Considerations

- The solution requiring the least number of ports open is best. The fewer the number of ports, the harder it is to exploit the system.(Sullivan Whitepaper, 2005)

- Encryption of passwords and the streaming media is necessary. Transmitted data and stored information should always be encrypted to prevent unauthorized access. Encryption protects the data being transmitted, (Slayden et al. 2007).

- Turn off VC endpoints when not in use. Leaving endpoints on after use provides an easy loophole for security breaches. Endpoints access should also be regulated by passwords.

- Ensure all default passwords for the endpoints are changed and auto answer is disabled. Failure to change default passwords can result to exploitation by malicious parties and unauthorized access to a synchronous VC systems.

- Applications with the ability to be embedded onto the provider's website are more secure. Ease of use being one of the factors that make a VC platform more secure, embedding it to a website, without having the requirement of downloading the application, ensures control of the system remains only with the synchronous VC service provider.

- Users to ensure the use of secure passwords and chartroom access to be controlled by pre-shared passwords. Virtual class attendance should be regulated by unique pre-shared passwords to lock out intruders.

- Stored data of conference record should be encrypted and access password regulated. All data on a VC system should be encrypted to protect it from exploitation even if it is intercepted on an unauthorized access is done. Access to the data must be controlled centrally.

- The best solution must have a secure way of key exchange and digital certificates for authentication of users. To ensure information shared on a synchronous VC platform is secure, the initial connection must be tamper proof by ensuring secure key exchange (Rudiger et al. 1998).

This research only sampled open source solutions, therefore further research can be conducted in institutionally approved ELearning VC solutions and proprietary solutions to further test and develop the security framework. There is still much more to be done in this novel area, including developing a comprehensive security model for synchronous ELearning VC.

References

1. Woda Marek , Ali Al-dahoud and Tomasz Walkowiak, 2010. Dependable Elearning systems.

2. Alvin Toffler ,2004, http://www.cognitivedesignsolutions.com/ELearning/E-Learning1.htm , Accessed 12/12/12

3. Oracle Paper, 2011, Information Security: A Conceptual Architecture Approach.

4. Australian Learning and Teaching Council Priority Project. Paper for National Roundtable, 2009. Web 2.0 Authoring Tools in Higher Education Learning and Teaching: New Directions for Assessment and Academic Integrity.

5. Bevanda, V. Azemovic, J. Music, 2009, Privacy preserving in ELearning Environment (Case of Modelling Hippocratic Database Structure.

6. Cross and Borgatti , 2003 , A relational view of information seeking and learning in social networks, Management Science.

7. Maria de Fatima, Carine G. Webber, Alexandre M. Ribeiro, Marcos E. Casa, 2007, Towards a secure Elearning applications, a multiagent platform.

8. Carole A. Barone , Mark A. Luker, 2000, The role of advanced networks in the education of the future.

9. Columbia University School of arts and sciences teaching center, 2010. Elearning ; Higher education ina web 2.o world.

10. Compendium of good practice cases of eLearning selected by members of the ICT cluster Danish Technological Institute, 2008.

11. Dr. F. Malik , 2011, Information Security Maturity model, International journal od computer science and security, Volume 5, Issue 3.

12. Lwonga Edda, 2011, Making learning and web 2.0 technologies work for higher learning institutions in Africa, Muhimbili University of Health and Allied sciences, Dar es salaam, Tanzania.

13. Martin Ebner, Edgar Weipl, 2008, Security and Privacy in Elearning 2.0 . Graz University of Technology Austria.

14. World report of an independent committee of inquiry into the impact on higher education of students' wide spread use of web 2.0 technologies, 2009, Education in the Web 2.0.

15. 7th International conference on ICT for development, education and training ,ELearning Africa, , 2009, Accessed 6/15/2012, http://www.ELearning-africa.com/review_2009_themes.php#2.

16. ELearning Magazine 2006, ELearning 2.0 , Accessed 11/10/2012, http://www.elearnmag.org/subpage.cfm?section=articles&article=29-1

17. K.Korbra, L., Xu, Y., El-Khatib and Yee, G. 2003. Privacy and Security in E-Learning.

18. Frost and Sullivan White paper, 2005, Solving the challenges created by firewalls and network address translation in videoconferencing environment.

19. Furse-Bowe, J.A , 1997, Comparison of student reactions in traditional and videoconferencing courses in training and development. International of instructional Media.

20. Gabriela Grosseck , 2009, World conference on education sciences. To use or not to use web 2.0 in higher education? Page 478-483.

21. Paul Birevu Muvinda, Godfrey Maleko Muguatosha, Jude Thaddeus Lubega, 2011, A social networked learning adoption model for higher education institutions in developing countries.

22. Greasley A. , 2004, A redesign of road traffic accident reporting system using business process simulation.

23. Gurmeet Singh, 2006, Secure Video Conferencing for web based security surveillance system.

24. Hurley C. , 2004, Wardriving : Drive , Detect, Defend: A guide to wireless security . Rockland , MA, USA Syngress publishing.

25. IAVSIT Press, Singapore , 2011, Platforms to support eLearning in higher education institutions, 2nd International Conference on Education and Management Technology IPEDR Vol. 13.

26. ISO/IEC 27034,2011, Information technology – Security techniques – Application security , last accessed 04/01/2012, ttp://www.iso27001security.com/html/27034.html.

27. Security guide for H.323, 2011, accessed in Dec 2012, Janet website ,https://community.ja.net/library/videoconferencing-booking-service/security-guide-h323.

28. Jeff Fissel , Accessed 12/12/12, http://streamingvideoplatform.com/4-ways-to-secure-your-online-video/.

29. Francisca J. Surez, Juan C. Granda, Pelayo Nuno, Daniel F.Gracia, 2011. Security Issues in synchronous e-training platform.

30. M. Warren, G.Pye, K. Samarasinghe, 2007, A conceptual Model for Security Outsourcing, Deakin University

31. Kamla Ali Al-Busaidi , 2009, The Pros and cons of video conferencing cyber course; Learning from a pilot project in the Omani University.

32. Paul Stamp, Khalid Kark, , Jonathan Penn, laura Koetzle, Jennifer albornoz Mulligan, 2007, Defining A High Level security framework.

33. Kelton, Law, A.M, W.D, 2000, Simulation Modelling and Analysis. McGraw-Hill, New York.

34. Linda J. CCastenada, 2008, ELearning in higher education; Searching for a model of curriculum analysis.

35. T. Hagan, Howard B. Demuth, Mark Hudson, Baele Martin , 2013, Neural network toolbox user's guide R2013a.

36. Rodney Petersen, Mark Luker, 2003. Educause , Computer and network Security in higher education.

37. Martin Ebner, 2007, ELearning 2.0=e-learning 1.0 + Web 2.0 ?, Submission to ARES , IEEE.

38. Davis , F.D. ,1989, MIS Quarterly, Percieved usefulness, perceived ease of use and user acceptance of information technology.

39. Ip-Shing Fan, Najwa Hayaati Mohd, 2010, eLearning and information security management , Cranfield University, UK.

40. Winnie Lai , Nicol Pan, Henry Lau, 2010, Sharing ELearning innovation across disciplines : an encounter between engineering and teaching education, university of Hong Hong.

41. Patrick S. Dallas, 2010, Video Conferencing Application to distance education with particular reference to small states.

42. Pavlos Papegeorgiou, 2001, A comparison of H.323 vs SIP , university of Maryland.

43. Paul Anderson, 2007, what is web 2.0? Ideas, technologies and implications for education. JISC Technology and standards.

44. PIM toolkit, 2008, Video conferencing privacy and security guide lines.

45. Port scanning website, last accessed 7/16/13, http://www.port-scan.e-dns.org.

46. Daniel Spikol , Marcelo Mildrad, 2007, Anytime, Anywhere Learning supported by smart phones; Eperiences and results from the MUSIS project. Journal of education technology and society.

47. Augar N.,Raitman R., Ngo L., 2005, Security in the online Elearning environment , Advanced Learning technologies, Fifth IEEE International conference on advanced learning technologies.

48. Peter Aubusson, Sandy Schuck , Matthew, 2010, Web 2.0 in the Classroom? Dilemmas and Opportunities Inherent in Adolescent Web 2.0 Engagement, Kearney University of Technology, Sydney.

49. SANS Institute, 2003, Polycom Videoconferencing Endpoint Security and Configuration.

50. Kaur Probhjot, Sarika Malhortra, 2011, comparison of call signaling protocols fo Ad-hoc networks.

51. Sanga C., Sife , A.S., Lwonga, E.T. , 2007. New technologies for teaching and learning ; challenges for higher learning institutions in developing countries'. Interntional Journal of Education and development using information and communication technology (IJEDICT).

52. Alan H. Karp, Slayden Mitchell, 2007, Improving usability by adding security to video conferencing systems, Hewlett-Packard Laboratories.

53. Stefan Hratinki , 2008, Asynchronous and Synchronous ELearning, Educause .

54. Stephen Downes, October 2005, ELearning 2.0 .

55. The E-Learning frameworks website. Accessed 13th Oct 2012, http://www.elframework.org .

56. The Janet website 2011, call snooping, recording and unwanted guests, accessed 25/04/2013. https://www.community.ja.net/library/janet-services-documentation/call-snooping-recording-and-unwanted-guests.

57. Tomas Olovsson, 2012, A Structured Approach to Computer Security, Department of Computer Engineering Chalmers University of Technology S-412 96.

58. Trèek, D. 2003, An integral framework for information systems security management, Computers and Security, Volume 22.

59. Unwin T., Oloo, L.M., Alwala, J., Kleessen B., Hollow D., Williams, J.B., , et al. 2010, Digital learning management systems in Africa: Myths and realities, Open Learning, Volume 25.

60. Viswanath Venkatesh, 2003, User Acceptance of information technology: Toward a unified view.

61. Waine house research, 2004, Security for Video conferencing: A guide to understanding, planning, and implementing secure compliant ISDN & IP videoconferencing solutions.

62. Rudiger Weis, Werner Geyer, Praktische Informatik IV, 1998, A Secure, Accountable, and Collaborative Whiteboard. University of Mannheim, Germany.

63. Yong, J. 2007, Digital Identity Design and Privacy Preservation for ELearning, Proceeding of the 2007 11th International Conference on Computer Supported Cooperative Work in Design, pp. 858-86.