ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 10, October 2013**

# The Influence of ICT Security to Academic Environment at Universities, Case Study Uganda

[1]Bogere Ayub, [2] Faruque A. Haolader, [3]Mohammad Mahbubur Rahman

[1,2,3]Department of Technical and Vocational Education, Islamic University of Technology (IUT), Organisation of Islamic Corporation (OIC) Boarbazar, Gazipur, Dhaka, Bangladesh.

***Abstract:*** ICT security has been one of the major causes of problems in the world in that billions of dollars are lost every year because of cyber terrorism that has become a way to destroy the world in just a few seconds, nevertheless Universities are not exception to this kind of terrorism, that's why they are encouraged to ensure strict ICT security within the University campus. This research study aimed at describing the critical need for ICT security in Universities and to show that ICT security can affect academic progress in Universities. The population of study comprised of ICT academic personnel (Lecturers, Technicians, and Lab-Attendants). Findings showed that there is a strong relationship between academic activities and ICT security. Therefore, without a well-secured ICT security, a University can come to a standstill.

**Keywords***:* ICT security, Universities, Academic Environment.

## I.INTRODUCTION

The coming of the submarine cables to the East African coast (Nora Mulira, et al, 2009/2010), promised greater affordability of Internet access and in turn, an increase in use of the Internet in Uganda. James Saaka, (2011) the Executive Director of the National Information Technology Authority Uganda (NITA-U) in the Interment Governance forum report revealed that, Phase one of the National Backbone Infrastructure/E-Government Infrastructure project had been completed. Phase Two was scheduled for completion by September 2011 which would cover the whole country. As it was prophesised in Nora's (2009/2010) research, by 2012 there were a huge number of internet users since the sub marine cable was finished. But before, there was an indicator that showed that even though teachers showed great interest and motivation to learn about the potential of ICTs, in practice, the use of ICT was relatively low and was focused on a narrow range of applications, with word processing being the predominant use. With the increase in internet by the end of 2011 many teachers in universities increased the utilisation of internet which now calls for security concerns. According to (Aguti& Fraser et al, 2006).There was a widespread belief among Ugandans that exposure of students to computers would increase their educational achievement and greatly enhanced their employability after school. Various technocrats are of the view that integration of ICT into their world of work will improve their own performance and commitment. This has led rapid increase in the use of ICTs in Universities which now calls for security controls to maintain the technology introduced.

The Uganda Internet Governance Forum report (2012) shows that Uganda has made progress on implementing some key Internet Governance issues. Internet Governance focuses included affordability and access to cyber security management and critical Internet resources.

On cyber security management, Uganda has operationalised cyber laws, including the Computer Misuse Act (2010), Electronic transactions Act (2011) and the Electronic Signatures Act, 2011. Attendant draft regulations for the Electronic Transactions Act and the Electronic Signatures Act have been developed. The ICT ministry together with NITA-U is developing an awareness strategy to the public.

Despite the availability of the law, Ugandans don't know how the cyber law operates and also none of the victims is ready to go public for fear of raining their integrity in business and on addition majority lack skills of protecting themselves against the criminals (The Weekly Observer, 12 October 2012).

According to Dr.Marian Quigley, (2011), Protection of information has been a major challenge since the beginning of the computer age. Given the widespread adoption of computer technology for business operations, the problem of information protection has become more urgent than ever. Computer files, databases, networking and the Internet-based applications all have gradually become part of the most critical assets of an organisation. When these assets are

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 10, October 2013**

attacked, damaged or threatened, data integrity becomes an issue and the proper operation of the business may be interrupted.

**Existing Methods of Protections in Academic Institutions**

Academic Institutions which feel vulnerable have formulated ICT policies, which among things address security concerns. Such institutions make use of Encryption System. Encrypting such files at least helps protect institutions with physical security measures, digital rights management systems which prevent unauthorised use.

Access Control Systems to control access to information and computer systems, the aim is to define a set of account management standards that will restrict access to authorised personnel and safeguard the services and information. This is done mostly by use of passwords.

Other existing protection methods are; Active Content Monitoring but the most frequent is the Antivirus, interior and exterior firewall and central backup servers.There is, however a limited number of Institutions protecting themselves to this level, this is mainly because of the costs involved. Most of the software protection available involves regular renewal of licenses and subscriptions, and these costs are considered by many (UgandaCommunications Commissionpaperon the state of cyber security in Uganda, 2005).

Harisinh (2008) says the purpose of information security is to protect an organisation's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organisation's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organisation by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake, they are put in place to protect important assets and thereby support the overall organisational mission.

## II. RECENT DEVELOPMENTS IN UGANDA CYBER SECURITY

Recent research on ICTs in Uganda shows rapid increase in the use of ICTs among Ugandans, estimated at rate of 50% increase every year (Uganda communication commission, 2012), despite of the increase in the use of ICTs, there has been little done to help the Ugandan Institutions in Improving their ICT security in both business and Higher Institutions of learning (National Information Security Strategy, 2011).Many Ugandan companies are increasingly struggling to deal with cybercrime through which they have lost billions and yet the police find it difficult to help because the companies prefer silence( The Weekly Observer Friday, 12 October 2012). The research by PanAfrican Research Agenda on the Pedagogical integration of ICTs in Uganda (2007 – 2009) shows that the cost of internet connection and maintenance is a big challenge that the academic institutions are facing.

A few recent ICT security incidences in 2012 about ICT security in Uganda, MTN Uganda, Warid Telecom, Standard Chartered and Stanbic Bank, Universities among others, counted huge losses in ICT security loopholes. Four employees of Gulu University lost millions of shillings through a bogus online car dealership. The conmen manning the website encouraged the lecturers to send money for buying cars, which they did but no car was shipped. When they insisted, the dealers sent a car without an engine then shut down the website. Many Universities and schools have lost sums of money, student's records, physical computer equipment in such circumstances but majority have remained silent because of fear to loose market and integrity in the public(The weekly observer, October 2012).

## III. I CT SECURITY CONCEPT

Kenneth Høstlandet al, (2010) say the term information security is related to the following basic concepts: Confidentiality, Integrity, and Availability (CIA).The confidentiality, integrity and availability of security is a general concept for a secure ICT system.

According to Tim Lane,(2007), despite the generosity of the concept research suggests that this concept is now too simple to describe more than the basic elements of security in that elements in CIA do not represent accountability and responsibility, but perhaps by the fact that the CIA concept was developed in the era of computing, when Electronic Data Processing (EDP) operations were representative of most computing environments, and information security was seen mostly as basically a technical function. The ICT environment is now substantially different to the early data processing days and hence the comprehensive techniques and methods are now needed.

According to Esharenana E. Adomi, (2010), during the last 20 years, information and communication technologies (ICTs) have greatly provided a wealth of new technological opportunities, with the rapid deployment of both the Internet and cellular telephone leading the way.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 10, October 2013**

FardzahSulaiman, (2010), says Information and Communication Technology (ICT) is an important strategic and essential functional requirement for many institutions of higher learning. In the developing world, ICT is achieving breakthrough in management and teaching through online learning, which helps to cater for the increasing student population. However, the security of the information being processed stored and exchanged is a growing concern to the management as the dependence on ICT for most of the institutions' core services functions are increasing.

Gunnar Bøe, Per Arne Enstad, et al, (2011); say that ICT security architecture for the Higher Education sector must meet the following overall requirements

- Institutions must provide adequate protection for their information assets. Security and risk levels must be well-established at the management level and based on risk assessments.
- The ICT systems must comply with the institution's information security policy.
- Consideration must be given to relevant regulatory requirements and directives, such as the government policy on ICT local legislation.
- The security architecture must comply with the institution's objectives as stipulated in [appropriate local legislation], and with any agreements the institution may have with third parties.
- The ICT systems must be equipped with appropriate capacity and adequate robustness in the event of failure (resilience).
- The ICT systems must have sufficient quality.

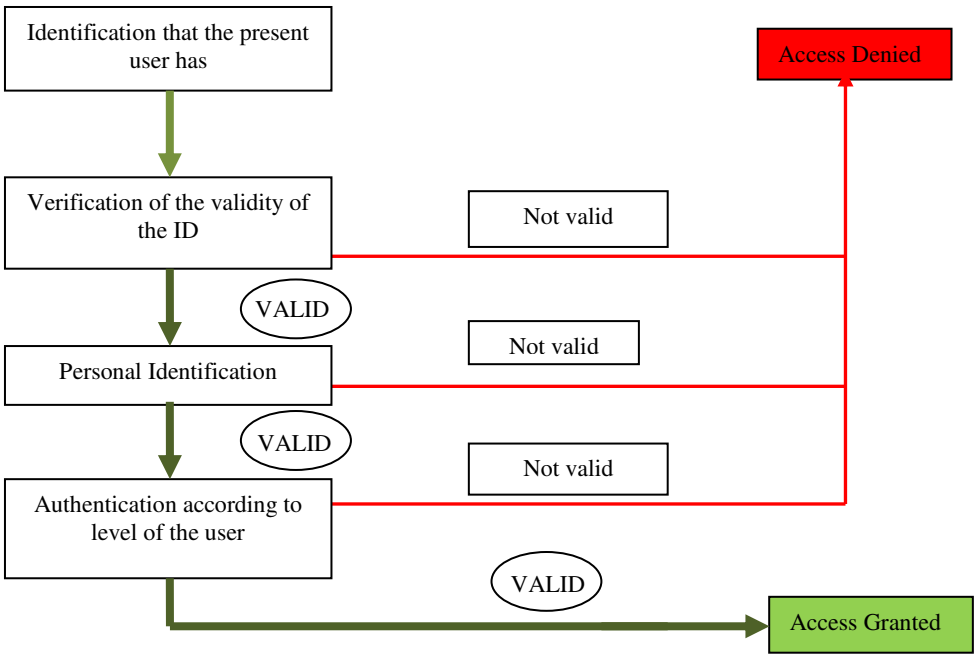
There is wide agreement by scholars like, Stephen M. Mutula, (2010); that a good information security policy is the foundation of organisations' information security. However, there is very little research into the creation of good security policies in Institution of higher learning but varieties of beliefs with respect to security policy exist. Diagram 1 illustrates the structure of a good security system for any given security system.

Richard Baskerville and MikkoSiponen, (2002), say, there are two schools of thought in existence that can be distinguished in dealing with ICT information systems, which include;

(1) Technical Security Management Control

(2) Non-Technical Security Management Control.

**Diagram: 1. Illustration of how ICT Security Systems Should Work.**




*Source: BogereAyub 2013*

Technical Controls section focuses on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 10, October 2013**

however always requires significant operational considerations and should be consistent with the management of security within the organization Parker, (1998)

Non-technical Management Controls section addresses security topics that can be characterised as managerial.They are techniques and concerns that are normally addressed by management in the organisation's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organisation.(NIST 800-12,2009).

## IV. METHODOLOGY

The Population of the study comprised of ICT academic persons, that is (ICT lecturers, ICT technicians, Lab-Attendants) of (6) six public and private Universities in Uganda, those gave their views on the study to examine ICTs security. A stratified random sampling method was used to select ICT lecturers, ICT Lab-Attendants, and ICT technicians. About sixty four academic ICT personnel were sampled out of eighty five, forty two ICT lecturers, thirteen ICT Lab-Attendants and nineICT technicians from the six Universities.
The researchers used questionnaire for gathering the opinions of selected ICT skilled persons, about the computer security management in different universities. A five point likert type scalewas used to calculate the and interpretweightedaverage.

**Analysis and Interpretation of Data**
The collected data was organised in form of frequencies. The analysis of data was done considering ICT security in relation to academic progress and management.During the analysis, quantitative approach and weighted average were used to analyse the structured data.

## V. FINDINGS

**ICT Security in Relation to Losses of Resources at the University**
Incidences of universities loosing huge sums of money were common in Ugandan universities in the year 2013, for example Kyambogo University lost shillings five billion in form of students' tuition (The New Vision Daily Apr 12, 2013) basing on this information, the opinon of respondents about "The university has experienced great resource losses due to weak security controls" were, the lecturers with a weighted average of 3.6 agreed, while the technicians with the weighted average of 3.9 also agreed but Lab-Attendants were undecided with a weighted average of 2.8. This means if the opinion of the two respondents who agreed is considered, it can be concluded by saying that, with weak ICT controls the university make great loss of resources.
**ICT Security Controls versus Financial Loss in the University**
The respondent's opinion on "Big amount of money are lost from the financial department every year due to weak ICT policies". Lecturers were undecidedwith weighted average of 3.2, technicians with 2.8 also were undecided and also the Lab-Attendants with 2.9 were undecided. Therefore the statement was not significant. This means that majority of the respondents did not take a clear stand about the statement that big amounts of money were lost from the financial department every year due to weak ICT security.
However there is much to be looked at in the issue of loss of money from the financial department because the lecturers, technicians and Lab-Attendants know less about issues of finance. Therefore there is a gap for more research.
**ICT Security in Relation to Leaking Exams**
In case the university uses the server to keep their examination online there can be possibilities that the students can hack into the system and leak exams, so on the opinion about "The University Students leak exams because of weak network security controls" the following was their responses. The lecturers with weighted average of 2.4 remained undecided; the technicians with 2.8 were undecided while the lab technicians with 2.2 disagreed. In the analysis of above results, it shown that the weighted average was very low which means that majority of the respondents disagreed with the statement.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 10, October 2013**

**ICT Security versus Academic Activities at the University**

The opinion on, "A weak network security leads to low academic activities in the university" the following were the responses.The lecturers with 3.7 weighted average agreed with the statement, technicians with 3.3 remained undecided but the weighted average is moderate, the Lab-Attendants with weighted average of 4.1 agreed. It can be concluded that the majority of the respondents agreed with the statement, which means the hypothesis is significant that a weak network security leads to low academic activities in the University.

However it should be noted this only can be possible in a university whose activities are automated using ICTs, in universities where most activities are Manual, ICT security is not a serious problem to them.

**The Perception on ICT Security whether it is A Hard Task to Achieve in the University**

The respondent's view on whether ICT security is a hard task to achieve or not was that,the Lectures with 3.1 were undecided whether managing ICT security is a hard task, the technicians also were undecided with 2.8 and also the Lab-Attendants were undecided with 3.2. The above results show that the statement was not significant because majority of the respondents did not take a clear stand about the statement.

**Many ICT Security Tasks are Left Unattended to in Universities**

The respondent's view on whether many ICT security tasks are left unattended to because of lack of skilled man power and security tools were as follows; the lecturers agreed with the statement with 3.8, and the technicians also agreed with 4.1, but the Lab-Attendants were undecided with 2.9 weighted average but this weighted average was moderate. Basing on this, the researcher concluded that majority of the respondents agreed with the statement that manyICT security tasks of the Universities are left unattended because of lack of skilled man power and security tools.

**Influence of ICT Security on Electronic Learning**

The opinion of the respondents about the Issue of the Universities failing to implement electronic learning systems partly because of network security problems experienced was as follows; the lecturers with a weighted average response of 3.6 agreed with the statement, technicians with 4.0 weighted average responses also agreed, the Lab-Attendants with 4.1 agreed with the statement also. Therefore the hypothesis is significant, this means that majority of the respondents agreed with the statement that the universities failed to implement electronic learning systems because of network security problems experienced.

## VI. DISCUSSION OF THE FINDINGS

The study shows that a weak ICT controls in Universities can make great loss of resources, however when respondents were asked a related question, whether big amounts of money were lost from the financial department every year due to weak ICT security, majority of the respondents disagreed with the statement.

It can be noted therefore that considerations can be made for universities whose activities are majorly manual, there may be no any resource loss due to ICT security, but for a University like Kyambogo that lost 5.5 billion (2012) in form of student (Daily Monitor 24th April 2013)they have to improve on their ICT security. Therefore, Universities should implement an advanced ICT security based on the research by Harisinh (2008) where he said that the purpose of information security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

Majority of the students disagreed with the issue of University Students leaking exams because of weak network security controls, however there can be possibilities of leaking exams when examination are kept on the computer which is online, students can hack through the network and have access to such examinations, therefore all Universities are advised always to keep their examinations on computers that are offline for security purposes.

Majority of the respondents agreed with the statement that a weak network security leads to low academic activities in the Universities. This is because there would be less research conducted, the loss of study materials, computers could not work because they are infected with viruses, and hence leads to low academic activities. However, it should be noted that much as ICT security can affect academic activities in a University, the early universities used to operate without ICTs which means, still the can operate manually, but with the modern world of today it's a very hard task to

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 10, October 2013**

operate in a University without computers. Therefore there is critical need to take proper care of ICT equipments to ensure proper running of Universities.

The respondents agreed with the statement that the universities failed to implement electronic learning systems because of ICT and network security problems experienced. It should be noted that electronic learning is done on computers and without ensuring their security, it's hard to realise a proper teaching and learning environment on computers.

## VII. CONCLUSIONS AND RECOMMENDATIONS

The research findings showed that ICT security and education within Universities are closely related, and that if the administration ignores the security of the ICTs it can even lead to the closure of a university particularlyincases when most activities in a university are automated and manned by computers. Therefore making ICT security at a critical consideration by the management of the university would make academics progress well. This would be through allocating enough resources to maintain ICT security, employing ICT security experienced personnel, creating awareness about ICT security among the academic staff, procuring the latest hardware and software that suit the security needs of a university, and lastly all the above can successfully contribute in maintaining ICT security when integrated as one system in university.

**Recommendations to Universities**

1) Institutions need to confront the reality to protect sensitive data which is much sensitive in the progress of academics. Institutions should enact reforms that honor their core values and remain conscious of the way a university works while aiming for systemic changes to ensure confidentiality and integrity of information within the university and all the university outside businesses.
2) The researcher recommend E-Campus software like the one that was developed by Kyambogo students together with administration that captures the data of all students and their financial standing in the university and also alerts students on logging in the due date for payment of tuition fees. This would help in controlling the financial losses of the university due to weak information security.
3) ICT security should be included in the university budget, this would help in allocating a specific amount of the university funds to maintain ICT security within the university.
4) Formalised ICT security policies should be designed to govern all Connors of loop holes within the security within the ICT security system of the university.

## BIBLIOGRAPHY

[1] Adomi, E. E. &Kpangban, E. (2010).*Application of ICTs in Nigerian secondary schools. Library Philosophy and Practice.* Available at: http://www.webpages.uidaho.edu/~mbolin/adomi-

[2] Adebiyi,JohnnesArreymbi, et al, (2012).Vol. 1, No. 4, 2012. 1 | Page www.ijacsa.thesai.org. Security Assessment of Software Design using Neural. Network.

[3] Alisha Cecil *"A Summary of Network Traffic Monitoring and Analysis Techniques"* found At:http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index. html

[4] Aguti, J. N., & Fraser, W. J. (2006). *Integration of information communication technologies (ICTs) in the distance education Bachelor of Education Programm*e, Makerere University, Uganda,TurkishOnline Journal of Distance Education, 7(3), 89-104.

[5] Brendan Guenther Ayers, Cynthia (September 2009). *"The Worst is yet to come"*. Cyber Laws Available at: http://www.nita.go.ug/index.php/policies-and- laws/cyber laws/104-cyber-laws-passed-in-uganda.

[6] Bruce Schneier (1998) President Counterpane Systems, A free monthly newsletter providing summaries, analyses, insights, and commentaries on cryptography and computer security.found at: http://www.counterpane.com.

[7] Baldridge, J. V., Curtis, D. V., Ecker, G. P., & Riley, G. L. (1999) Alternative Models of Governance in Higher Education. In J. L. Bess & D. S. Webster (Eds.), Foundations of American Higher Education (pp. 483-498). Boston: Pearson Custom Publishing.

[8] Cate, F. H. (2006). The Privacy and Security Policy Vacuum in Higher Education. EDUCAUSE Review, 41(5), 19-28.

[9] [Cisco] *Safe Reference Guide Revised:* July 8, 2010, OL-19523-01, found at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf" Crime in the 21st Century: The New Field of Computer Forensics." *InfoWorld,* December 14, 1998.

[10] Desouza, K.C. and Hensgen, T. (2003), *"Semiotic emergent framework to address the reality of cyberterrorism",* Technological Forecasting and Social Change., Vol. 70 No. 4, pp. 385-96.

[11] Daily Monitor 24th April 2013 found at: http://www.monitor.co.ug/News/National/More+rot+unearthed+at+Kyambogo/- 688334/1756544/-/5iqhra/-/index.html.

[12] Embar-Seddon, A. (2002*), "Cyberterrorism: are we under siege?", American Behavioral Scientist*, Vol. 45 No. 6, pp. 1033-44.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 10, October 2013**

[13] Gordon, S. and Ford, R. (2002), *"Cyberterrorism?", Computers &Security*, Vol. 21 No. 7, pp. 636-47.
[14 FardzahSulaiman, T. Ramayah and Azizah Omar, (2010), *ICT Security Policy in a HigherEducation Institution in Malaysia*, found at:www.igi-global.com/chapter/ict-security-policy-higher.../45395
[15] Fites, P., and M. Kratz. Information Systems Security: A Practitioner's Reference.York: Van Nostrand Reinhold, 1993, (especially Chapter 12, pp. 331 - 350).
[16] Fletcher, Charlie. "ID Thievery is On the Rise." *Catalog Age.* June 2000.Gantz, John. "Take a Bite Out of Crime on the Web." *Computerworld.* February 19, 2001.
[17] Gittlen, Sandra. "World Organisations Urge Sharing of Security Info." *Network World.*October 23, 2000.
[18] Harper, Jim. "There's no such thing as cyber terrorism". RT. Retrieved 5 November 2012.
[19] Ian Goldberg and David Wagner (January 1996) "Randomness and the Netscape Browser," Dr. Dobbs Journal, no. 243, January 1996, pp. 66–70.
[20] Jahidul Arafat, Md. WaliullahGolam and MoktaderDaiyan (2010), Information Technology Security, Strategies and Practices in Higher Education
[21] James Saaka (2012) *Uganda National Internet Governance Forum 2012*, found at: http://www.intgovforum.org/cms/2012/Regional%20National%20IGF/upload/2012%20National%20%20IGF%20report-1%20copy.pdf
[22] James Saaka (2011) *Uganda National Internet Governance Forum 2011*, found at:http://www.intgovforum.org/cms/2011/NationalregionalIGFreports/UgandaIGFREPORT2011.pdf
[23] Jim Harper (2011). "*The Underwhelming Threat of Cyberterroris"* Junaid Ahmed Zubairi&AtharMahboob (August, 2011)*"Cyber Security Standards, Practices and Industrial Applications"*
[24] Kim, G., and E. Spafford, "Monitoring File System Integrity on UNIX Platforms." *Infosecurity News*. 4(4), 1993. pp. 21-22.
[25] Munro, Neil. "Cybercrime Treaty on Trial."*National Journal.* March 10, 2001.
[26] Neeley, DeQuendre. "Justice Department Report Arouses Concerns." *Security Management.* May, 2000.
[27] [NIST 800-12, 2009].An Introduction to Computer Security: The NIST Handbook. NIST SP 800-92 Special Publication 800-92. *Guide to Computer Security. Log Management. Recommendations of the National Institute of Standards and Technology*.found at:http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
[28] Nora Mulira, ApoloKyeyuneand Ali Ndiwalana (2009/2010) *Uganda ICT Sector Performance Review*
[29] Peter Mell&TimothyGrance Peter (September 2011)The*NIST* Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.
[30] Radcliff, Deborah. "A Case of Cyberstalking."*Network World.* May 29, 2000.
[31] Rapaport, Richard. *"Cyberwars: The Feds Strike Back."Forbes.* August 23, 1999.
[32] ReachardBejtlick (2010), Richard Bejtlich's blog on digital security, concentrating on global challenges posed by China and other targeted adversaries. Saturday, January 16, 2010.
[34] Stephen M. Mutula (2010)International Review of Information Ethics. Vol. 14 (12/2010). (Sufferkvacik&Voloudkis, 2003)

## BIOGRAPHY

BogereAyub holds a Master of Science in Technical Education (M.Sc.T.E.) with Specialization in Computer Science and Engineering (CSE) from Islamic University of Technology (IUT), Dhaka Bangladesh. He also holds a Bachelor of Information Technology from Islamic University In Uganda (IUIU), He worked as the District IT officer for Busia Uganda, from April 2010- June 2011 Uganda.E-mail bogerea@yahoo.com.

Dr. Faruque A. Haolader has a Doctoral degree in Technical and Vocational Education from Stuttgart University, Germany. He has a Master"s degree in Vocational and Adult Education for International Development Work from Dresden University of Technology, Germany, a master's degree in Engineering (Electronics and Information Technology) from the University of Birmingham, England, and a bachelor"s degree in Electrical and Electronic Engineering from Dhaka University of Engineering and Technology (DUET), Bangladesh. He has more than 30 years of working experience of which 6 years as TVET teacher trainer at the Department of Technical and Vocational Education (TVE) of Islamic University of Technology (IUT) and at Technical Teachers Training College (TTTC). His

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 10, October 2013**

industrial and research experiences include 1 year as Programmer at the Ministry of Planning, Govt. of Bangladesh and 10 years of applied research & industrial experience as Research Fellow at Fraunhofer Institute & Stuttgart University, and as Engineer in the field of Technical and Vocational Education, Automation & Information Technology, and Electronic Systems Design & Development in Germany. He has published numerous journal and conference articles and 2 text books. Moreover, for his excellent academic and workplace performance he was awarded UNESCOFellowship, German DAAD Scholarship, British ODA Scholarship and Bangladesh Govt. Scholarship

Mohammad Mahbubur Rahman. M.Sc.T.E (Student of Final Semester), Department of TVE, Islamic University of Technology (IUT), B.Sc.T.E (First Class First), Dhaka University (DU).Dhaka, Bangladesh. He is interesting as a teacher or a trainer in a University or in a Training Center related to Technical and Vocational Education (TVE) and interesting to develop teaching method with technology. mmrahmanmollah@gmail.com