

Cyberspace in the School Educational System: A Model Cyber Protocol in the Indian Context

Vijith T.K. Thekkekoodathil¹ and
Pramod K. Vijayaraghavan²

^{1 2}Department of Computer Applications,
Cochin University of Science and Technology,
Cochin 682022, Kerala, India.

vijithtk@gmail.com,
pramodkv4@gmail.com

January 13, 2018

Abstract

The presence of cyberspace is important and inevitable in the present educational system. And the ethical use of cyberspace is mandatory and an area of concern. Efforts are going on for the implementation of Information Communication Technology (ICT) in the educational system. It is evident that some potential dangers are there in the cyberspace for young people. But students and stakeholders are not fully aware of this situation. This will adversely affect the effective ICT use in the system as well as the future of the generation. Hence, for the effective and efficient use of cyberspace, there is a need of a protocol for both the students and the stakeholders of the system. In the Indian scenario, no such standard protocol is available. This paper proposes a protocol called cyber protocol that comprises rules and procedures for the use of cyberspace in school educational system by considering the factors present in the India. This will help prudent use of cyberspace especially in the school settings.

Key Words : Cyberspace, School Educational System, Information Communication Technology, Cyber Protocol

1 Introduction

Computers, associated connecting and communicating devices, and its users together are called cyberspace. Technological advancement has contributed to the proliferation of cyberspace. Now it has become unavoidable part of human life. The stakeholders, students, curriculum, building-setup and infrastructure as a whole are called educational system; in school scenario it is called school educational system. Cyberspace is also an integral part of school educational system. It can be admitted that a radical change has been brought in the school educational system by the use of cyberspace. But its use in the school educational system is indeed an area of utmost concern since its a double sided sword. The two main questions arise about the use of cyber space in the school educational system. i.e., is cyberspace used ethically in the system? Is the management of cyberspace effective in the system?

Educational system is in a transformational stage. It started to change from ordinary to smart and from offline to online. Hence integration of Information and Communication Technology (ICT) with the educational system has become necessary. This implies that cyberspace is going to stay as permanent component of the educational system. The potential benefits of using cyber space for teaching and learning will be hampered by the dangers attached to it inherently when used without caution. This fact is even more important in the school educational system. But the students and the other stake holders are not much aware about the dangers of the cyberspace. In most of the situations, cyber security is a least discussed topic in the school educational setting.

Cyber security in the education system is considered a grave issue by many countries worldwide even though no such thought has got publicity in India. A document published by Australian Government [1] and Australian education department [2] discuss various potential dangers that are affecting to young people. Victoria state government has prepared a document for safe and responsible use of digital technologies [3]. The University of Sydney

created protocols for learning and teaching in digital scenario [4]. Australian government has prepared a document to school teachers and management for managing risks in cyberspace [1]. The education network (NEN) [5] proposes a school e-security check list contain control measures and questions prepared for two categories of stake holders. One is for persons responsible for computer related activities (system administrator) and the second for school principal (management). Cisco has prepared a document, Service Ready Architecture for Schools A Framework for Education [6] It considers many factors for the secure school network system.

The ethical and effective use of cyberspace in the school educational settings should be a main agenda for the authorities. A cyber protocol is required in the school educational setting. And it should specify (i) the structure of the computer network, (ii) procedure for access and use of internet, (iii) procedure for use of mobile phones in school premises, (iv) management of the system (v) the role of various stake holders. The role of stake holders for the effective and efficient use of cyberspace in school educational system is crucial. The principal or the head of the institution should be more vigilant in emerging technological trends[7]. The protection of children from the cyberspace dangers and its ethical use is a societal responsibility [8].

2 Risks in Cyberspace for Young People

It is easy to access internet for students through computers or mobile phones. But they encounter many risks while using internet. The following are the various types of risks that are harmful to young people[1][2][9][10].

-
- **Content:** Students may be exposed to materials that are not intended for them such as pornographic, sexually explicit or offensive items. This also includes depiction of violence, smoking or drug-taking, suicide and other forms of self-harm etc. Students may access these materials from World Wide Web, via email, news groups, P2P networks or social media.

- **Physical Danger:** Students connect to online through chat rooms or via email. There are chances that persons may meet the students online claiming as someone but actually they are not. This risk in internet is called stranger danger. Through these meetings students may share their personal information to a stranger. These strategies are widely used by pedophiles to arrange face-to-face meeting with children (online grooming).
- **Financial:** Commercialism is increased in internet through World Wide Web, email, online advertisement, online marketing, and online gambling. Scam sites are set up to loot peoples money and opportunities. Bogus and dummy web sites have the intention of deceiving and coaxing people to pass their financial credentials. Students who fall prey to these kinds of traps will financially risk themselves or their family.
- **Cyber Bullying:** Harassment through Webpages, email, SMS, chat rooms, social media, discussion group, mobile phones are all considered as cyber bullying. Cyber bullying includes activities such as spreading rumors, teasing and being made fun of, sending unwanted messages and defamation.
- **Legal and Political:** Activities that are leading to breach of laws like copyright, privacy, IT act 2000, defamation, purchase of age restricted materials, use of dark web.
- **Privacy:** There are websites asking to students to fill online forms by entering their personal information and photo. Some of them are legitimate. But there are chances that personal information shared to online may target students for unsolicited email (spam mail), advertisement, viruses. And it may be used for illicit purposes (online recruitment).
- **Unreliable information:** Website information may misrepresent the fact, biased, or be out of date. Students need to judge the quality of material they are using or sharing.
- **Spam:** Spam is the email such as unsolicited email, junk mails or nuisance phone calls. Through these spam students may attracted to illicit activities. Filter can be used to prevent spam at certain extent.

- **Virus:** Emails are the flexible and useful mode of information sharing. But there are some risks associated with it. Sometimes emails are sent from an unknown sender containing virus infected attachment or link to virus infected website.

3 Cyber Protocol for School Educational System

The cyberspace management of school educational system is unavoidable in the present scenario. Considering the dangers of cyberspace its judicious use in educational system need a protocol. In India there is no such written and adaptable document available. Initiatives are taken by some school management towards this direction.

This paper proposes a model protocol by compiling initiatives taken by foreign countries and considering the nature of Indian school educational system. Initially a survey has been conducted among teachers and students of secondary and higher secondary school level to gather their opinions. The model protocol comprises four components. The first component describes the rules of internet access in school system. These rules are not only applicable to students but also to teachers and other stake holders of the system. The second component specifies the critical cyber security control management system. This is a proposed software system that will have the capability of handling all the cyber security software and hardware, infrastructural monitoring and management. Component three is proposed model computer network that will facilitate all the cyberspace academic activities of the school educational system. Component four describe the role of stake holders of the school educational system for the effective and efficient use of cyberspace.

3.1 Internet Accessing Rules

It is necessary to have an internet accessing rule for any institution where internet and computer facilities are available. The institution management should construct internet accessing rule that comply with the existing work policy. School educational system must have

a stringent internet accessing rule and a monitoring system that ensures its being followed. The following is a compiled form of the accessing rules framed in this direction [11][1][12].

Rule	Description	Remark
1	Access to the internet is a privilege not a right	Applicable to all
2	The purpose of the internet is to support the educational program	Applicable to all
3	The official concerned may cancel ones access at any time if the privilege is misused	Applicable to all
4	Appropriate conduct should maintain on school computers and internet access otherwise disciplinary action will enforce	Applicable to all. Immediate suspension of all access privileges
5	A declaration signed by both student and guardian stipulating that they have read these guidelines and agree to adhere to them	Applicable to students
6	Students should not use their personal devices that is being used for accessing the Internet during school hours unless approval was given by the teacher or officials concerned	Applicable to students
7	All are expected to take responsibility for his or her appropriate use of the Internet	Applicable to all
8	All student e-mail and other Internet files and records may be accessed and examined by the officer concerned for educational and administrative purposes.	Applicable to students. It ensures that these guidelines are being followed.
9	The officer concerned will coordinate and cooperate in providing access to all Internet files and records to law enforcement authorities when appropriate	Applicable to all
10	Users should not assume that their use of the school Internet will be private	Applicable to all
11	Students should promptly inform their teacher or the officer concerned about any on-line communication that the student feels is threatening, harassing, or otherwise inappropriate	Applicable to students
12	All are expected to abide by generally accepted rules of Internet etiquette as well as the rules of school decorum. These include common courtesy and the avoidance of vulgar or offensive language	Applicable to all. Appropriate disciplinary action will be enforced by authorities if anyone violates.

13	Respect the privacy of others by not posting their private or personal information	Applicable to all
14	Do not attempt to access others personal files or internet accounts (eg: e-mail)	Applicable to all
15	Do not attempt to accessing or transmitting obscene or pornographic material	Applicable to all
16	Do not attempt to post chain letters or spamming, i.e., sending unsolicited or annoying messages to large numbers of people	Applicable to all
17	Do not attempt to participate in communications that facilitate any form of criminal activity, such as, but not limited to, the illegal sale or use of drugs or alcohol, gang activity, sexual harassment, threats, or any other forms of intimidation	Applicable to all
18	Do not plagiarize any material. Due citation must be maintained if referred/used	Applicable to all
19	Do not violate copyrights, i.e., inappropriately reproducing or transmitting material protected by copyright	Applicable to all
20	Do not participate in any commercial activities that are not directly related to the educational purposes of the schools, unless specifically approved in advance by the school's officials	Applicable to all

3.2 Critical Cyber Security Control Management System

This is a conceptual software system. This software system will have the following modules and each module has specific objectives and features [5][13].

Module	Objectives	Features	Remark
Hardware Inventory	Manage all hardware devices	1) Detailed up to date list of all hardware devices 2) Keep the files related to all devices (in scanned form) 3) Details of firmware on the devices 4) Maintenance details 5) Updating/Expiration details 6) User policy	Should have a facility to manage all activities related to hardware components
Software Inventory	Manage all software	1) Detailed up to date list of all software 2) Keep the files related to all software (in scanned form) 3) Maintenance details 4) Updating/Expiration details 5) User policy	Should have a facility to manage all activities related to software
Secure Configuration	To keep secure configuration for hardware and software on laptops, mobile devices, workstations and servers	1) Standard secure configuration details for operating systems and applications used 2) Patching tools and process to update hardware and software promptly 3) Manage administrative privileges 4) Remedial measures when system becomes compromised 5) Component wise monitoring	Management of all security related activities
Vulnerability Assessment and Remediation	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities,	1) Keep abreast of new and emerging risks and issues 2) Reviewing and updating e-security process, software and hardware	Management of vulnerability assessment

	remediate, and minimize the window of opportunity for attackers	3) Monitor the updates and patches applied once vulnerabilities have been identified	
Malware Defences	Control the installation, spread and execution of malicious code at multiple points in the network	1) Procedure to prevent malware spread 2) Checking procedure for malware presence 3) Details of anti-malware software installed 4) External device(like flash drive) usage policy	Malware defence management
Wireless access Control	The process and tools used to track /control/ prevent /correct the security use of wireless local area networks (LANS), access points, wireless client systems	1) Authorized devices only can connects to network 2) Monitor security of the connected third-party devices	Network Access controls
Control of network ports, protocols and services	Mange the ongoing operational use of ports, protocols, and services on network	1) Port ,protocols, and services management	Minimize windows of vulnerability available to attackers
User Account and User privileges	The process and tools used to track/ control/ prevent/ correct the use, assignment, and configuration of user account creation and privileges on computers, networks, and applications	1) User account creation 2) Management of user privilege allocation 3) User policy 4) Monitor user activities	User accounts and privilege management

3.3 School Computer Network

The effectiveness of cyberspace in the school settings depends largely on a control and monitoring system. This requires that each and every computer should lie in a single network. To curtail bogus information which may be shared by teachers as ICT tools, a cen-

tralized censored tool repository should be setup and maintained by concerned authority and then it should be attached with the school network.

The academic and administrative monitoring and management of a school cyber space can be made easier by setting up an integrated, sophisticated and secure computer network. The following is only a model network.

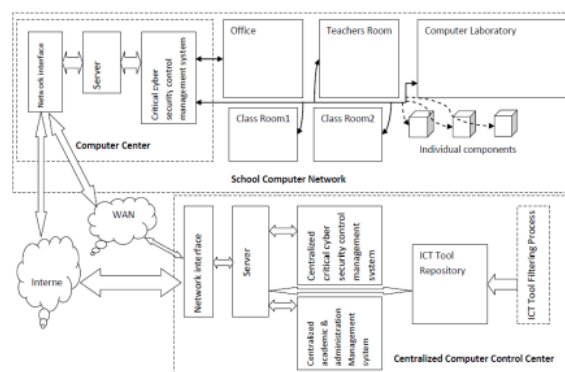


Fig.1.1. Model of School Computer Network

3.4 The Role of Stake Holders

Stake holders of the school education system in India are Government, school management, teachers, and parents. Each of the stakeholders has their own role and responsibility for the functioning of a school. For the cyberspace management stakeholders have the following roles.

- Government:
 1. Leading role for the effective implementation of ICT
 2. Introduce cyberspace training to various student categories and teachers
 3. Revamp curriculum for making adaptive to ICT and cyberspace
 4. Setup centralized monitoring for risks in cyberspace

5. Setup central repository for ICT tools
 6. Develop a customized web browser and search engine for school students
 7. Setup a regular cyber security alert system to students and schools
 8. Develop a customized mobile phones for students
- School Management
 1. Create a post for managing cyberspace in schools
 2. Create and implement cyberspace policy
 3. Construct a committee for monitoring cyberspace activities
 4. Conduct regular training programs for relating cyberspace to students, teachers, and parents
 5. Take Initiative to implement cyber protocol
 - Teachers
 1. Should be a role model in cyberspace use
 2. Update knowledge by participating in cyberspace training programs conducted by government and management
 3. Guide students to use cyberspace ethically and effectively
 - Parents
 1. Participate in cyberspace training programs conducted by government and school management
 2. Share their apprehensions about cyberspace use of their children to school officials
 3. Regularly monitor the gadgets used by their children
 4. Consult with school official before buying any software or hardware for children

4 Discussion and Conclusion

School educational system is a very sensitive area. Any paradigm shift in the system will affect the future of the nation. Due diligence is required for any action in this area. Hence the use of cyber space in the educational setting needs to be carefully maintained by the authorities. Otherwise there will be more adverse effects than the positive effects. Many factors inbuilt in the cyber space itself are posing threats to the students. This fact necessitates the use of a controlling and monitoring system for the school cyber space. Students and teachers need to be information literate in order to manage information ethically which in turn helps in effective use of cyberspace. The model protocol proposed here will be a guideline in this direction. Students, teachers and other stakeholders are responsible for the effective use of cyber space.

References

- [1] A. G. Australia's Internet safety advisory body, *NetAlert*, A Teach. Guid. to Internet Saf., 2004.
- [2] *Keeping students safe online at Out - of - School - Hours Learning Support Programs*, pp. 14, 2014.
- [3] Department of Education and Training, *Safe and Responsible Use of Digital Technologies*, State Government of Victoria. pp. 37, 2015.
- [4] B. Ford, *School of education and social work*, in The idea of a new university: An experiment in Sussex, 1964, pp. 135-152.
- [5] T. S. Group, *NEN The Education Network*, no. November, 2014.
- [6] CISCO, *Cisco Service Ready Architecture for Schools Design Guide*, 2010.
- [7] V. E. Garland, *Emerging technology trends and ethical practices for the school principal*, J. Educ. Technol. Syst., vol. 38, no. 1, pp. 39-50, 2009.

- [8] R. Von Solms and J. Van Niekerk, *From information security to cyber security*, Comput. Secur., vol. 38, pp. 97102, 2013.
- [9] J. M. Kizza, *Ethical and Social Issues in the Information Age*, Fifth. Springer, 2013.
- [10] I. Resource and L. Taylor, *Cyberbullying among Students**, no. 310, pp. 17.
- [11] Milton Public Schools, *POLICY AND GUIDELINES FOR INTERNET USE*. [Online]. Available: <http://www.miltonps.org/documents/AUP.pdf>.
- [12] Y. Q. Government and F. Queenslanders, *Program for primary school students*, pp. 1820, 2017.
- [13] J. W. McMahon, R. P. Mills, W. E. Bennett, and J. W. Tuffey, *BEST PRACTICES FOR SCHOOL SAFETY AND SECURITY*, 2004.

