

Security of Electronic Resources: A study of Private Engineering Colleges of Indore city

Preeti Patel

Lecturer, School of Library & Information Science, DAVV, Indore (M.P.), India
preetipatel2407@yahoo.co.in

Dr. Kishor John

Officer-on Special Duty, Additional Director of Higher Education, Motitabela, Indore (M.P.), India
john_kishor@yahoo.com

Manju Chakraverti

M.L.I.Sc. Student, School of Library & Information Science, DAVV, Indore (M.P.), India

Abstract

Internet and other computer technologies become very essential for libraries. Libraries need to have policies; protection measures and trained staff in place in order to safeguard their investments in computer and computer-related technologies, personnel and services. This paper will cover Information Security methods used in Private Engineering College libraries of Indore city. Instead of giving detailed instructions for security techniques, the emphasis here is on finding the various techniques used in library environments. Security of information is a regular process due to new techniques adopted by the libraries time to time. This article cover the security techniques used in libraries.

Key words: Network security, Information Security, Data security, Fire wall, Pass word.

1.0 Introduction

Information is one of the most important assets of libraries and Information Centers. Protection of information assets is necessary to establish and maintain trust between the library and its users, maintain compliance with the law, and protect the reputation of the library. The terms information security, computer security and information assurance are interrelated often and share the common goals of protecting the confidentiality,



integrity and availability of information; however, there are

some subtle differences between them. Security of Information is the process by which an organization protects and secures its systems, media, and facilities that process and maintains information vital to its operations. Today, almost hundred percent engineering colleges' libraries are connected to the Internet, yet frequently without proper maintains and supervision it is difficult to protect electronic resources from intrusion or tampering. Libraries need to have proper planning, protection techniques and tools and trained staff to protect E-Resources in libraries. The security of the libraries systems and information is essential to its safety and soundness and to the privacy of user's information. This article presents a general overview of information security, its core concepts and finds preference about the information security techniques used in Private Engineering colleges (PEC) libraries.

This study provides guidance to libraries to assessing and evaluating the adequacy of the organization's risk management. Security of information is an ongoing process, whereby the condition of a libraries control is just one indicator of its overall security posture. Libraries protect their information by instituting a security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks. This paper will concentrate on the topic of security of information resources like Physical security, Network security, Database security,

protection of software, preference about antivirus, tools of information security etc.

1.1 Objectives of the study

Libraries adopt new techniques and recent form of reading material for their users. Electronic information is easily handled and communicates. So there is a need to find out the security procedure for e-resources used in the Engineering College libraries. In this respect the following are main objectives of the study.

1. To know about the techniques of securing e-resources of Engineering Colleges of Indore city.
2. To observe the importance of electronic information security.
3. To identify the problems faced by the librarian in managing the E-Resources by Information Security Systems.
4. To find out the favored technique used for securing information by PEC libraries
5. This study also useful to know about the attitude of Engineering Colleges to securing Information in electronic environment.

1.2 Limitation of the study

This study is based on the 32 Private Engineering Colleges (PEC) of Indore City. Information about number of Engineering Colleges is collected from the Website of Rajiv Gandhi Technical University. Data collected from 28 libraries. Four libraries show no response. So they are not covered in this study.

1.3 Reviews of literature

Pathrose, Rathore and Dixit¹, discusses Biometric security by” Biometrics is automated method of recognizing a person based on a physiological or behavioral characteristics. Among the features measured are; hand writing, iris retinal, vein and voice Biometrics technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. **Dwivedi, Atal and Shrivastava**² discusses the data security by cryptography & steganography

as “steganography is the art of hiding information in ways that prevent its detection steganography is usually given as a synonym for cryptography but it is not normally used in that way. It is not intended to replace cryptography but supplement it though steganography is ancient craft. The onset of computer technology has given it new life. This paper explains a new algorithm which describes how steganography can be combined with cryptography to enhance security in data transfer. **Kumbargoudar and Mestri**³, analyzed the need for different kinds of information security in the libraries. Further, the different information security systems and technological trends such as RFID systems, Electromagnetic security systems and smart card security systems are studied with reference to information security in the libraries. The paper is concluded with remarks to choose the best information security system for libraries considering several factors such as cost, nature of the users, and nature of the organization etc. **Kulkarni and Powdwal**⁴, Libraries are the important institutions for human development and progress. The advancement in knowledge and technology is a vital issue for increasing the patron demands and resources in the libraries. To safeguard these resources for posterity, libraries are adopting various security measures. Unfortunately even after introducing technology driven security solutions, the problem of library security is unresolved. This study analyzes the various dimensions of existing security measures and those which may be adopted in libraries. It also provides the guidelines to handle this most sensitive but still important issue of library management.

2.0 Meaning of Information Security

The protection of data against unauthorized access is known as information security. Digital certificates, passwords and

biometric techniques (fingerprints, eyes, voice, etc.) provide a more secure method. Security of Information is the major aspect of today's libraries because the methods of accessing information are in changing face. Security of information is always a major problem for Librarians. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

2.1 Types of Information Security

Security of information broadly divided into two major categories.

2.1.1. Information Security of Traditional reading material

A library is a social institution charged with the responsibility of disseminating knowledge to the people without any discrimination. Most of the libraries have paper based reading material in the form of books, periodicals, drawing, charts, maps, etc. the basic materials and constituents of the physical entity of these library materials are mostly organic in nature, which are susceptible to natural decay and deterioration.

2.1.2 Information Security of digital reading material

The digital material security has vast area for securing information in libraries. It includes the protection of personnel, hardware, programs, networks, and database security from physical circumstances and events that could cause serious losses or damage to institution. Protection from fire, natural disasters, burglary, theft, vandalism, and terrorism is the part of information security. Database security can begin with the process of creation and publishing of appropriate security standards for the database environment. The standards may include specific controls for the various relevant database platforms; a set of best practices that cross over the platforms; and

linkages of the standards to higher level polices and governmental regulations.³

2.1.3 Attackers in Security of Electronic Information

The e-Resources of libraries can be affected by various attackers like-

1. Computer hacker,
2. Lone criminals,
3. Malicious insiders,
4. Terrorists and Industrial espionage Information warriors.

With these type of attackers there are so many other enemies of information like viruses, worms Trojan Horses, password sniffing, IP Spoofing, Port scanning, Physical attackers, Environmental attackers, Chemical Leaks etc.

3.0 Tools and techniques of Information Security

3.1 Backups: Back up is the activity of copying files or databases, so that their additional copies may be restored in case of a data loss accident. Thus, we can emphasize first two aspects related to backup - storage media for data and depositories for backup media. Another important aspect is growing necessity in backup caused by development of computer technologies and data volumes expansion.

3.2. Antivirus Software

Antivirus software is used to scan hard disk, pen drives and CDs for viruses'. Antivirus software can also be used to scan e-mail messages and individual files downloaded from the internet. Continuously monitor memory to protect the computer from memory resident viruses

3.3 Cryptography

Few years ago cryptography used to be almost exclusively a tool for the military. However, in moving into an information society, the field of cryptography has broadened from classical encryption techniques into areas such as authentication,

data integrity, non-repudiation of data transfer.

3.4 Biometrics

Biometrics" means "life measurement" it is a method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic". A biometric system can be either an 'identification' system for verification' (authentication) system.

3.5 Honey pots

A honey pot is a tool used for detecting an intrusion attempt. It provides an additional level of security in addition to IDS .The main function of a honey pot is to fool an intruder. A honey pot simulates a vulnerable computer on a network. It contains no critical data or application but has enough data to lure an intruder.

3.6 Firewalls

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. Firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

3.7 Burglar alarm

Burglar and safety alarms are all electronic today. Sensors are connected to a control unit via a low-voltage hardwire or narrowband RF signal which is used to interact with a response device. The most common security sensors indicate the opening of a door or window or detect motion via passive infrared PIR. New construction systems are predominately hardwired for economy.

4.0 Security of Information in Libraries and Information Centers

The library is a pool of quality resources and library staff has made concerted efforts to select, shelve and promote resources to benefit library users. Traditionally library security has been a matter of devising safeguards in reaction to specific losses. Especially when we think of library security, it applies to the security of resources in all forms along with equipment. It may include security of library collections bibliographic and patron records, employees and reader as well as overall aspects of the building. Following techniques are mostly used for securing Information in libraries.

4.1 Radio Frequency Identification (RFID)

It is the latest technology introduced in 1990s. It is radio frequency based technology is combined with microchip technology and used as library theft detection system. The gates that are placed at the entrance or exits are known as exit sensor or antennas and they create security corridor for the library. The sensors read the information on the tags of the material passing by with the reader, and communicate this information to the server .If the material is not properly issued out; the server activates the alarm after checking with the circulation database. The latest technology called chip less RFID allow for secrete identification of tags without an integrated circuit, thereby allowing tags printed directly onto library martial at lower cost than traditional tags. RFID tags come in

three varieties: passive, active, or semi-passive (also known as battery –assisted) passive tags require no internal power source, thus being pure passive devices (they are only active when a reader is nearby to power them) whereas semi-passive and active tags require a power source, usually a small battery.

4.2 Closed Circuit television (CCTV)

It is the use of video cameras to transmit signal to a specific, limited set of monitors. It is often used for surveillance in areas which need monitoring. This system works by linking the control of the cameras to a computer, and tracking semi-automatically. The overall control of the system is monitored by the chief of the library. It is well suited in modular architecture of the building and the material stacked area if it is in single floor. If the collection of the library is spread on different floor, then multiple monitoring station are required.

4.3 Electro-magnetic surveillance system (ESS)

It is used to check the theft and vandalism. It is based on the electro-magnetic devices to ensure the security of library materials by sensitization and desensitization of tattle tapes. Tattle-tape is the magnetic metallic strip inserted in the books. It is easily applied be been the pages or the spines of books or any other library materials. The strip is completely concealed and impossible to detect and remove once inserted within the library materials. It can be desensitized and re sensitized repeatedly without losing effectiveness. There are sensors in this system and the magnetic power of the strip is negated while the reader gets the book issued. When the library books are returned, they are again re sensitized by the library staff. If the library material is taken with out desensitizing it, an alarm starts sounding unauthorized issue of library material.

4.4 Video cameras

Video cameras are used in machine vision, quality monitoring, security, and remote monitoring for industrial and commercial operations. Choices for imaging technologies for video cameras include CCD, CMOS, tube, and film. Charge Coupled Devices (CCD) use a light-sensitive material on a silicon chip to detect electrons excited by incoming light. CMOS image sensors operate at lower voltages than CCDs, reducing power consumption for portable applications. In a tube camera, the image is formed on a fluorescent screen. Image is exposed onto photosensitive film, which is then developed to be played or stored.

5.0 Tables and figures

5.1: Preference of security used in P.E.C. Libraries

Information Security is essential for aspect of today’s library and Information Centers. There are different types of information security available. Through this study we able to find the preference of security in Library and Information centers use in PEC

Types of security	No. of response	Percentage
Physical security	8	29%
Network security	12	43%
Database security	5	18%
Others	3	11%
Total response	28	100%

libraries.

Table – 1

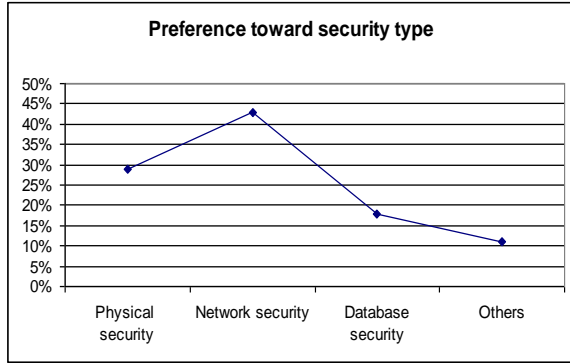


Fig-1

Information security is a very important work of library. The table shows that, 12(43%) library use of network security, 8(29%) library use of physical security, 5(18%) library use of database security and 3 (11%) library use other security.

5.2: Security used in Library Software packages

There are various kinds of library Software packages available for Library and Information Centers. They provide different security techniques for security of information. By this question we enable to find the preference toward security techniques using in PEC libraries of Indore

Types of Security	No. of response	Percentage
Password security	24	86%
Licensed security	3	11%
Web based security	1	4%
Total Response	28	100%

Table – 2

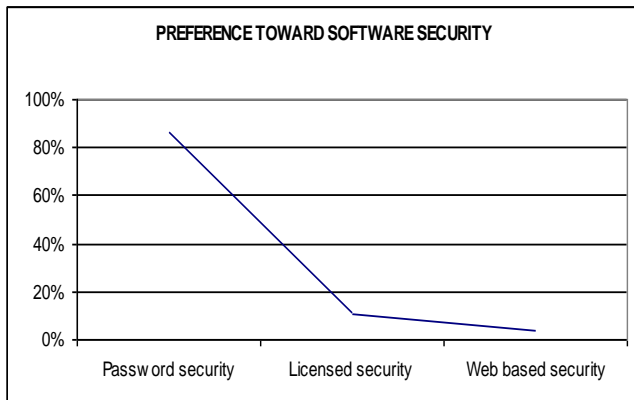


Fig -2

Fig.-2

To observe the graph and table it is clear that password security [24/28(86%)] is the favorite technique used for library software security. Only 3/28 (11%) library provide licensed security and 1(4%) library provide web based security for library software package.

5.3:Types of Attackers in Information Security

Attackers can create so many problems in the E-Resources of the libraries. Attackers always disturbed library system especially in automated library system. There are a lot of varieties of attackers. Through this observation we find the most problematic attacker who influences the library work.

Types of Attackers	No. of response	Percentage
Thieves and Hackers	3	11%
Unauthorized users and websites	2	7%
Viruses	18	64%
Others	5	18%
Total response	28	100%

Table – 3

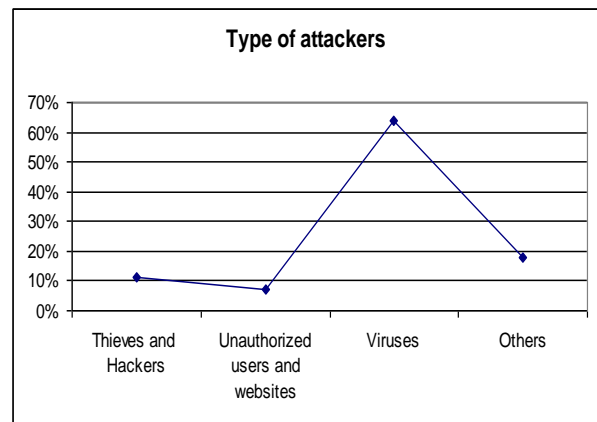


Fig – 3

The data available in the tables representing that 18 (64%) are affected by the viruses, 5(18%) are affected by the others attackers, 3(11%) are affected by the Thieves& Hackers and 2(7%) are affected by the Unauthorized users. Viruses are the most problematic form of attackers which destroy library system in today's library.

5.4: Preference toward techniques for securing E- Resources from attackers

Whenever attackers destroy systems there are various techniques used by LIS

Preference toward techniques	No. of response	Percentage
Password	12	43%
Firewall	1	4%
Antivirus	8	29%
Backups	5	18%
Web cameras	2	7%
Total Response	28	100%

professional for protecting their information. This question helps to obtain the preferable technique used by PEC libraries.

Table -4

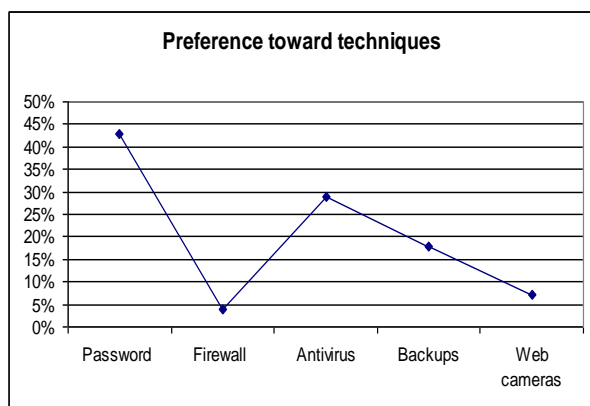


Fig -4

Data shows that 12(43%) by Password Protection, 8(29%) by Antivirus, 5(18%) by backups, 2(7%) by Web cameras and 1(4%)

by Firewall Protection. It is clear from the graph that Password protection, Antivirus, backups etc. are the more preferable security techniques used by PEC libraries

5.5: Preference for security tools used by PEC libraries

There are many tools available for securing information in library and Information Centers. This question helps to find the preference of tool used by the PEC libraries. The table shows that how much the Security devices connected in libraries can be secured

Preference toward security methods	No. of response	Percentage
Closed-Circuit Television(CCTV)	5	18%
Electro-Magnetic surveillance system(ESS)	3	11%
Radio-Frequency identification(RFID)	4	14%
Others	2	7%
No response	14	50%
Total response	28	100%

the e-Resources and the computer systems.

Table-5

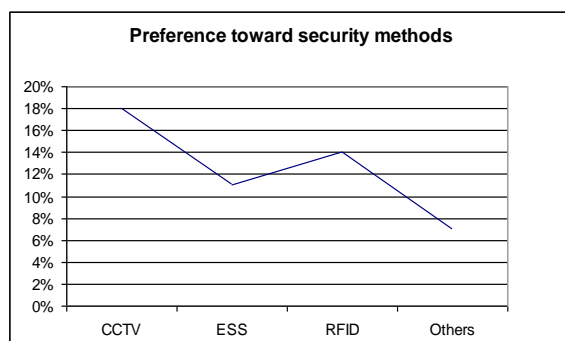


Fig-5

Data available in the tables representing that 14(50%) giving No response, 5(18%) by Using Closed-Circuit television (CCTV), 4(14%) by Radio-Frequency identification (RFID), 3(11%) by Electro-Magnetic

surveillance system (ESS) and 2(7%) by other techniques. It is clear from the figure that there are a large number of libraries who doesn't use advance tools for Information Security in their libraries and Information Centers.

5.6: Preference toward Antivirus software used in PEC Libraries

Antivirus are the Computer program used for security of computer systems. In the age of electronic form of material it is necessary to the Library and Information Centers to protect their material by using antivirus software packages.

Pref. toward Antivirus software	No. of response	Percentage
AVG	7	25%
Norton	13	46%
Trend micro	5	18%
Others	3	11%
Total Response	28	100%

Table-6

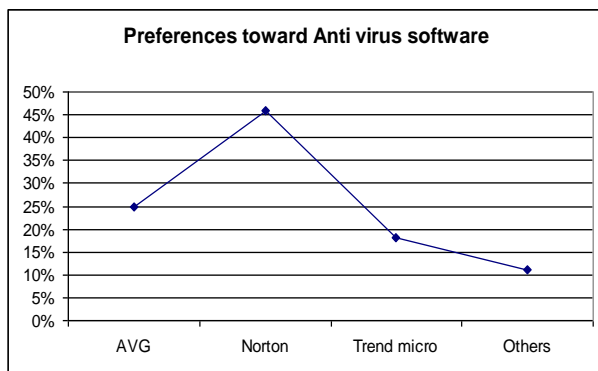


Fig.6

The above figure shows that Norton antivirus is most prominent antivirus used by the libraries. Data available in the tables representing that 13(46%) by Norton, 7(25%) by AVG, 5(18%) by Radio Trend micro and 3(11%) by Using other techniques.

5.7: Criteria of selection antivirus for PEC libraries

Feature criteria for selection antivirus	No. of response	Percentage
Speed removing	12	43%
In-expensive	9	32%
Easily usable	5	8%
Work efficiency for a long period	2	7%
Total response	28	100%

There are a large variety of anti viruses available for commercial use. By this question we find the preferable criteria for Anti virus selection used by PEC libraries .

Table-7

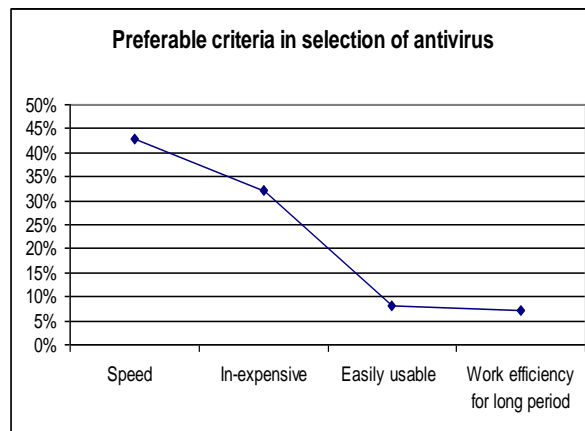


Fig.-7

The above table shows the speed is the main reason to use an antivirus in the libraries. Most of the libraries used antivirus for their speedily removing capacity. The tables representing that 12(43%) for Speed removing, 9(32%) for In-expensive reason, 5(8%) due to easily usable and 2(7%) due to Work for a long period.

5.8 Continuous steps for securing Information

The continuous security measures are necessary for securing information in electronic age. The table shows that libraries use backup of information, continuous update antivirus and ban on unauthorized access to securing information.

Methodology	No. of response	Percentage
Regularly update antivirus	15	53%
Store backup of data	10	36%
Stop unauthorized accessing	2	7%
Others	1	4%
Total response	28	100%

Table - 8

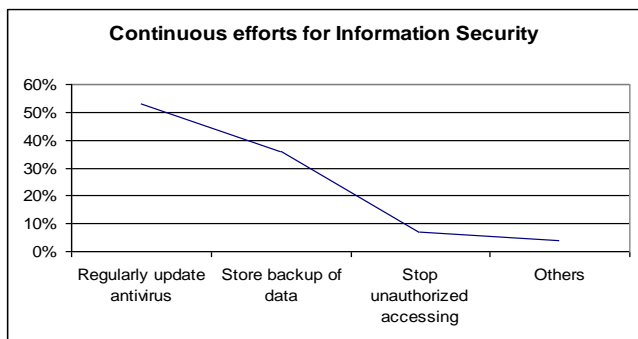


Fig. 8

The figure signify that 15(53%) are regularly updated antivirus, 10(36%) are Store backup of data, 2(7%) are in Stop unauthorized accessing and 1(4%) are using some other techniques.

5.9: Use of Bio metric security methods used in P.E.C. Libraries

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyzes human body characteristics, Iris / Retina, Fingerprint (including nail), Hand (including

knuckle, palm, vascular) Face and Voice recognition etc.

Preference toward method	No. of response	Percentage
Thumb impression	14	50%
Any Others	3	11%
No. response	11	39%
Total response	28	100%

Table -9

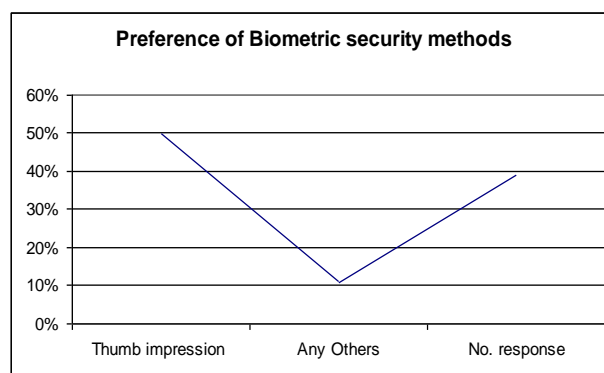


Fig. 9

The above figure shows that which types of firewall software are used by the libraries. Data available in the tables epitomize that 12(42%) are using Licensed, 8(28%) are using Licensed for limited system, 6(21%) are using Free ware and 2(7%) are giving No Response.

5.10: Budget for security of E- Resources granted to P.E.C.

Budget is the most important of library. Budget helps to collect and dissemination information for users. Security of Information is an important part of library and Information centers. Changing form of information create so many problems for information security.

Amount in Rs.	No. of response	Percentage
10,000-50,000	20	71.43%
50,000-1,00,000	5	17.86%
1,00,000-5,00,000	3	10.71%
Total response	28	100%

Table – 10

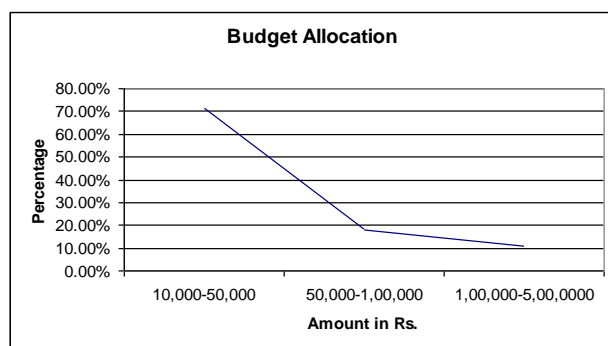


Fig – 10

Graph shows that 20(71%) library security budget have 10,000-50,000, 5 (17%) library security budget have 50,000-1,00,000 only 3(11%) library budget have 1,00,000-5,00,000 for their security development. This is found by the study that collage management takes less interest in security of Information in Libraries.

6.0 Findings: -

1. Password security is the favorite form of security used by Private Engineering colleges' libraries of Indore city.
2. Attackers generate the problems in information security. The study finds that viruses (86%) are the most common type of attacker which effected libraries collection development.
3. Electronic resources mostly protected by pass word protection (43%) is the favorite form, anti virus (29%) is second choice to protect information. Very few libraries used

back up camera (7%) and Fire wall (4%) protection for their collection.

4. Almost all the libraries well connected by computer systems. 50% libraries used security guard, 36% used monitoring software, 18% using CCTV, 14% used RFID, and 11% used ESS for securing information in libraries.

5. The continuous security measures are necessary for securing information in electronic age. 53% are continuously up date antivirus 36% used backups of data for secure information in libraries.

6. Changing form of information create so many problems for security of information in Library and Information Centers. Most of the librarians feel that they have lack budget for securing information in cut electronic age.

7.0 Conclusions:-

Continuing emergence of new security exploits, tools and techniques coupled with the constant parade of software and hardware up grades likely in most library environments ongoing diligence is required to keep informed of security development. The study concludes that the libraries are using latest antivirus, licensed software, licenses firewall for their security of library and software and computer system. Some of the libraries used advanced security techniques like CCTV. Most of the institutions are satisfied with their security techniques but they also want to use latest technologies. They are putting separate budget for the security. Information security of information resources is the major priority of all the Private Engineering Collages of Indore city.

References:

1. Pathrose, Joshua, Rathore, Maya and Dixit, Ashish (2008). "Biometrics: Technological Revolution in Security". *National conference on Information Technology: Issues & Challenges*: 41-51
2. Dwivedi, Kaushal Kishor, Atal, Maya and Shrivastava, Amit. (2008). "Data Security by cryptography and steganography. *National conference on Information Technology: Issues and Challenges*": 331-338.
3. Kumbargoudar, Praveen Kumar and Mestri, Mamta (2008). "Biometric security technology for library". *SRELS* Vol. 45(1):37-44
4. Kulkarni, Shobha and Powdwal, Sushma. (2008) "Library security system: Matamorphism"; *Library Herald*. Vol. 46(2):81-90
5. Joseph, JVM. (2003). "Network Administration and security in a Digital library environment". *First International Convention on Mapping Technology on libraries and People, Caliber, 2003, in Ahmedabad: INFLIBNET Ahmedabad pp.* 422-427
6. Upadhyay, V.V., Upadhyay, Rituja and Upadhyaya, M.M. (2003). "Network security to a Digital library". *First International Convention on Mapping Technology on libraries and People, Caliber, 2003, in Ahmedabad: INFLIBNET Ahmedabad pp.* 429-437
7. Panday, Shweta and Shroff, Bhaumik. 2003. Network security policy: A key to successful network management. *First International Convention on Mapping Technology on libraries and People, Caliber, 2003, in Ahmedabad: INFLIBNET Ahmedabad pp.* 456-466
8. Arifa, K. (2003). Ethical issue in Cryptography and Information security: Concerns for Digital libraries. *First International Convention on Mapping Technology on libraries and People, Caliber, 2003, in Ahmedabad: INFLIBNET Ahmedabad pp.* 467-490
9. Kanaujia, Shiva and Satyanarayana, N. R. (2004). "Information security measures in networked library and information center". *IASLIC Bulletin* Vol. 49(1):45-50
10. Kalyankar, N.V. and Khamitkar, S.D. (2003). "Security threat to digital data: computer viruses". *Library Progress*. Vol. 23(1):73-77
11. Jadhav, M.N. and Kulkarni, Shobh. (2003). "Electronic security: A case study of IIT Bombay Central library. *First International Caliber 2003, 13-15 February, 2003 in Ahmadabad (India)*: 134-139

Follow us on:

[IRJLIS](#)

[Facebook](#)

[Twitter](#)