2021

Electronic Security Systems (ESSs) in Academic Libraries

Rima Nath
rimanathlis2013@gmail.com

Electronic Security Systems (ESSs) in Academic Libraries

Rima Nath
Research Scholar, Department of Library & Information Science,
Gauhati University, Assam (India), E-mail: rimanathlis2013@gmail.com

Abstract:
The present paper studies the variety of Electronic Security Systems available for the library environment, including its technological components. The study also includes the positive influence of a security system to secure the library's day-to-day activities. The opportunities and challenges have also been discussed that influence the implementation of Electronic Security Systems to improve the library facilitates.

Keywords: Academic Libraries, Electronic Security Systems, Close Circuit Television (CCTV), Library Resources.

1. Introduction:

Nowadays, libraries are providing multi-dimensional information and services with the incredible application of the latest technologies. There is an urgent requirement for adequate security to control and monitor the embedded knowledge and information in this information technology environment. Edem (2010) defines security as assurance of future wellbeing and freedom from threat. Security, therefore, refers to a process designed to protect something or somebody against danger. It is an act of preventing crime. In the case of library resources, it prevents unauthorised removal or loss of materials, usually due to intruders' or thieves' interference (Ajegbomogun, 2004).

The adoption of Electronic Security Systems (ESSs) in the library has led to a manifold increase in the overall safety of its collection, services, and investments. The ESSs help the librarians act smartly for any theft, mutilation, unauthorized physical and digital access of library materials by the users. ESSs refer to any electronic equipment that could perform security operations like surveillance, access control, alarming or an intrusion control to a facility or an area that uses power from mains and a power

backup like battery, generator, etc. It also includes some of the operations such as electrical, mechanical gear. The determination of a security system is based on the area to be protected and its threats.

These days, ESSs are mostly utilized within residential operations, corporate sectors, commercial places, shopping centres, railway stations, public places, defence activities etc., to minimize any crime within the location and provide safeguards to the public. It has more beneficiary components that can be worked from remote areas too.

In libraries, the application of ESSs is very much essential as these devices provide safeguard to the library resources by involving techniques like alarm systems, access control systems, fire control systems, attendance record systems, environmental control, shelving space method, physical and chemical treatment for natural damages of bindings etc. the library has been witnessing many book theft and book loss cases since its open access systems. The security of such information resources is also a significant concern for the administration. Since, library always has a limited budget and the cost of resources keeps increasing; therefore, it is the responsibility of the library to protect the available resources from theft and other damages. So library professionals should adopt a better electronic system for their library security purposes. The security system provides security and is also used in a different way to increase and improve the efficiency of libraries. The working technology of the security systems does not interfere with the library's primary objective of providing a user-friendly environment (McComb, 2004).

2. Review of Literature:

Greenwood and Mckean (1985) reported on depending on the case study of the University of Kentucky Library that the book loss rates had been decreased after the adoption of ESSs. They also added that ESSs like electronic surveillance cameras (Closed Circuit Television-CCTV), 3M library security system (electronic gates), Radio Frequency Identification (RFID) system, perimeter alarm system, movement detectors, etc. have more usefulness to academic libraries for security purposes.

Ramana (2007) discussed various categories of CCTV cameras with their technical functions. This paper also reports that fingerprints and retina scanning process under biometric method provides the safeguard in the accession of books and other library materials.

Kumbargoudar and Kumbargoudar (2008) have analyzed the need for different kinds of information security in libraries. Further, the various 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.

Uma... et al (2010) discussed the loss of books and other reading materials due to theft. It mentions different security measures adopted in University Libraries and the need for Electronic Security systems. Finally, the focus was on the importance of the Electronic Security System in University Libraries, citing the electronic security system installed in Indira Gandhi Memorial Library, University of Hyderabad.

Roy and Basak (2011) have explained RFID and its usage in library and information centres where barcoding, electromagnetic stripes etc. have been used. RFID technology helps streamline major library processes such as stock taking, circulation, and book searches, eliminating manual labour**.**

Musa et al., (2019) discussed the effect of different library security on service delivery in the Federal University Library of Nigeria. The authors explained various electronic security systems like CCTV, RFID, Perimeter Alarm System etc., are highly adopted in the library as security measures. They have also pointed out the possible challenges of the implementation of ESSs. They suggested some strategies and recommendations overcome the challenges associated with the implementation of the security measures.

3. Objectives of the Study:

i) To find out various types of ESSs available for library environment;
ii) To verify the related technological functions of ESSs;
iii) To enlist the pre-requisite areas for implementation of ESSs in the libraries;
iv) To focus on various opportunities and challenges of ESSs for adoption in the libraries.

4. Use of Electronic Security Systems in Libraries:

4.1. Closed Circuit Television (CCTV) or Surveillance System:

The libraries comprise a large area including the number of floors, reading hall, open space for recreation, lawn areas, cafeterias etc. which needs proper attention to the staff. The CCTV or

Surveillance system uses cameras at specific areas that systematically helps the team to record surveillance data of inner and outer side of the library. The CCTV surveillance system includes manly cameras, network equipments, IP cameras and monitors. Here, the cameras detect the crime and illegal activities in the protected areas and send signals through network and immediately, the alarm rings. The cameras are interconnected with the CCTV system in point-to-point or point-to-multipoint manner. The complete operation of CCTV surveillance is totally based on the internet.

The figure below is representing the CCTV Surveillance Systems.

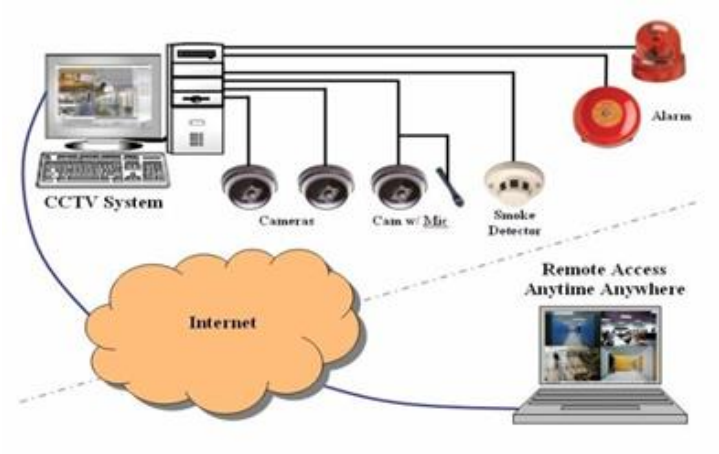

Fig 1: CCTV Surveillance system

(Source: https://www.elprocus.com/electronic-security-system/)

- **IP Surveillance System:**

The IP-Surveillance system is also designed for security purposes. Clients can control and record video/audio using an IP PC system/network through LAN or the internet. The main components of the IP-Surveillance system are Polaroid system switch, a computer for review, supervising and saving video/audio, shown in the figure below.

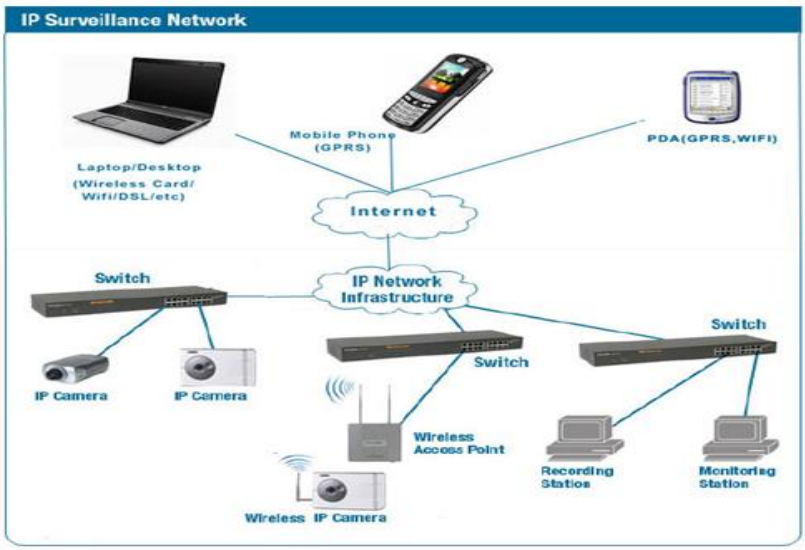

Fig 2: IP Surveillance Network

(Source: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.pinterest.com/...)

The IP-Surveillance system provides video controlling and recording from any place through system/network access. The digital audio/video streams can be accessed from remote areas with a wired or remote IP system.

4.1.1. Uses of CCTV System in Library:

(i) To automatic capture of library activities in the form of image and video footage.

(ii) To monitor various vandalism activities like book theft, mutilation of books, hiding books, destroying library properties etc, by the students.

(iii) The library can quickly analyze the video footage of CCTV cameras installed in various places like entry gates, stake areas, stairs, circulation areas etc., to take a critical decision against any security and material-related issues.

(iv) CCTV camera recordings are helpful to use as identification proofs to solve any problem that took place in the library.

4.2. Fire Detection and Alarming Systems:

It is also referred to as detection and the alarming system as it has the facility of alarming alert to detect any suspicions that occur in a protected area. This system consists of a detector device with a sensor followed by an alarm or alerting circuit. The primary function of this system is to rapidly extinguish an advancing fire, and alarm tenants preceding impressive harm that happens by filling the secured zone with a gas or concoction smothering operator. Different sensors are available for detection, but sensor usage is purely based on application requirements, like home automation, warehouse fire detection, intrusion alert, etc.

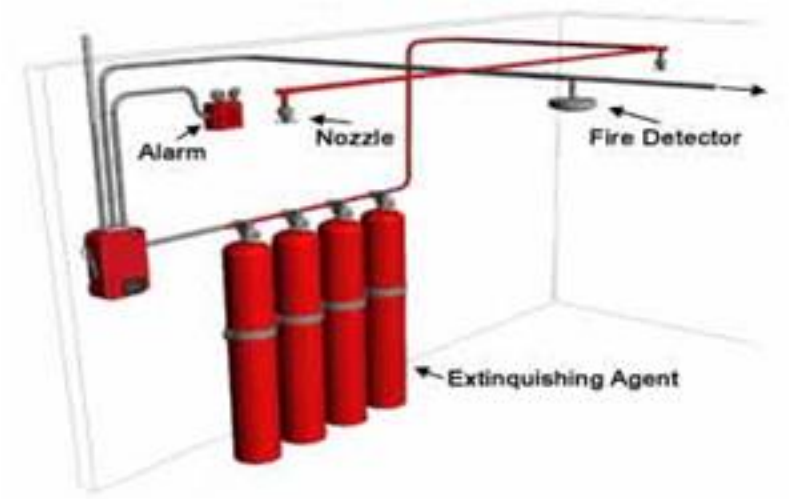

Fig 3: Fire Detection and Alarming system

(Source: https://www.google.com/search?q=fire+detection+system&tbm/..)

4.2.1. Use of Fire Detection and Alarming Systems in Library:

i) Using a fire detection and alarm system, the library can get a quick alert for any fire emergency inside the library.

ii) It helps the library safely the essential resources from any harmful burn by releasing the gases rapidly.

iii) Without human intervention, everything can be kept under control in such an emergency and safety from significant loss.

4.3. Access Control Systems:

An access control system provides secured access to a facility or another approach to enter or control the entrance. It is also acting as a controlling attendance system which implies very effective for security purposes. This access system is classified according to user credentials and possessions; what users use for access makes the system different. Users can provide different credentials like pin, biometrics or smart card etc., to control the access. In contrast, the system can even use all possessions from a user, which further involvement of multiple access controls become possible.

4.3.1. Components of Access Control System:

a. **Access Cards**: In an access control system, access cards are used as entering keys to the building or specific areas. Each access card contains its unique code, allowing the user control access for each individual, quickly turning access on and off at different times or different areas of the building. Access cards are typically the size of a credit card, making them portable and easily fit inside a wallet.

b. **Card Reader**: The card reader is the device that will read access cards to grant access. There are different types of card readers, some requiring card insertion, some requiring swipes, and some only needing cards to pass in proximity to the reader. Card readers are typically mounted on the door or next to the door they control, so the number of card readers an access control system contains will depend on the number of doorways in restricted access.

c. **Keypads**: Access control keypads are another method of entry. Instead of scanning an access card, the user can punch the passcode on a numeric keypad. Keypads are sometimes used instead of card readers and sometimes in conjunction with card readers. For an extra layer of security, a door might have a card reader and a keypad, requiring an access card and a correct passcode in order to gain entry.

d. **Electric Lock Hardware**: The hardware that locks and unlocks the doors is also part of the access control system. Electric lock hardware will electronically open the door after a keycard swipe or keypad code entry and electronically lock the door again when it closes. There are many different types of electric lock hardware, such as electric locks, electric strikes, electromagnetic locks, and more. The type of hardware used will depend on the construction of the door. In addition to electronically locking and unlocking the entry doors, electric lock

hardware ensures that doors can be freely opened whenever someone wishes to exit in order to comply with building and fire codes.

e. **Field Panels**: Field panels are the control panels that connect all other parts of the access control system, such as card readers, keypads, hardware, and more. Field panels are used to process access control activity for the whole building. The number of panels will be determined by the size of the building, the size of the system, and the extent to which the system is used. Field panels are typically installed in telephone, electrical, or communication closets.

f. **Access Control Software:** Access control software is the brain of the entire system. It is the central database and file manager for the system. It records system activity and distributes information to and from the field panels in the building. This software runs on a traditional computer. It requires one computer to load this software and it will be dedicated for full-time use of the software.

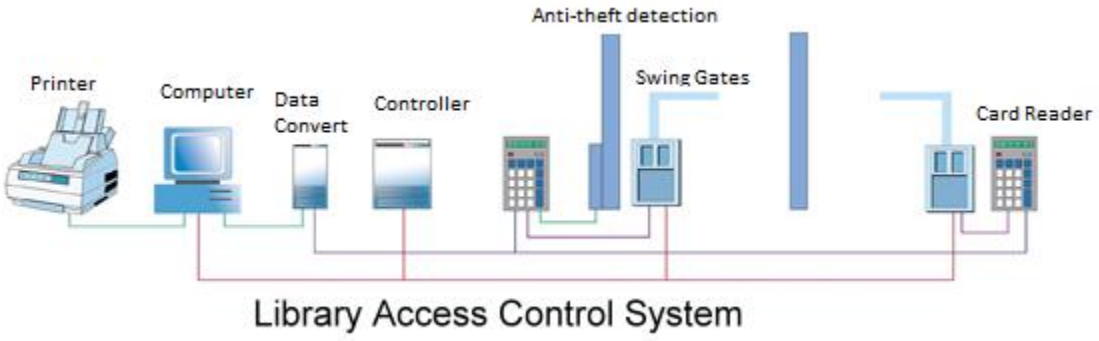

Fig 4: Library Access Control System

(Source: https://www.google.com/search?q=library+access+control+system&tbm/..)

4.3.2. Use of Access Control System in Libraries:

i) It is used in libraries to restrict access to the library to authorized users only and help prevent theft of books from there.
ii) Helps librarian centralize monitoring and control of multiple devices and locations.
iii) Librarian can send messages to Interactive Control Unit for the patron. The patron will need to acknowledge the message, and then they can enter library. (library 2.0)

iv) Helps the Counter computer monitor the entrance status and support remote access status data by using the browser.
v) By using this access system, the notification of the system operation can be collected in real-time.
vi) It can be easily installed in any library and also have the features of integration with firefighting, biometrics and other technical security systems.

4.4. Intruder Alarms and Detector:

An intruder or burglar alarm system is a set of interconnected devices aimed to protect an object, usually a facility, against intruders and notify the owner or/and the monitoring station/center of any violation of the protected zones. More advanced alarm systems can perform functions like access control (motorized gates, electric strikes in wickets/doors), lighting and heating control, and many other home/building automation tasks.

A basic intruder alarm system consists of a control panel with rechargeable battery power backup and internal or external keypads, several interiors and perimeter intrusion detectors, and one external sounder, at least. The interface devices contain modern keypads and touch panels, which beyond the aesthetic appearance and intuitive operation, can store maps of the facility on memory cards for easier control of the entire system, as well as (optionally) mobile phones or handhelds and PCs with dedicated applications and Internet connection.

4.4.1. Components of Intruder Alarm Systems:

Alarm control unit/panel (switchboard): this is the primary unit that contains a dedicated housing/box together with a backup/buffer battery along with power supply, the sensors, keypads, anti-tamper circuits, line connection for data transfer and also detects any faults in the wiring. The control panel monitors the proper operation of all the equipment installed in the system. It collects information from, and in the event of an irregularity, switches on optical and acoustic signalling.

Keypads or touch panels: These manipulators allow the installer to set up the control panel and program all the functions of the alarm system. They also are the user interface for communication with the alarm system, which provides information on the system status and enables appropriate codes for activating and deactivating operations. An alarm system usually contains one master keypad and zone

manipulators. The master device consists of LCD display and numeric keys, or touch screen and is responsible for the complete control of the entire alarm. The partition keypads have numeric keypads and simple optical signalling in the form of LEDs.

Sensors: The correct deployment of sensors determines the actual usability of the entire intruder system.

The employed sensors are motion detectors like Passive Infra-Red (PIR), MicroWave (MW), peripheral sensors like reed switch mounted on the door/window frames, and other sensors like glass break and vibration water, smoke etc. These sensors activate the alarm when someone tries to break into the library or on its premises.

Input/output (I/O) expansion modules: I/O modules expand the capabilities of alarm control units with additional inputs and outputs. The type of the outputs depends on the needs. In addition to increasing the number of inputs/outputs, the expanders are often used for wired connections of detectors located in more distant locations. As a result, there is no need to lay cables from each detector to the control panel. The communication between the sensors and control panels is performed via the expanders using the system bus.

Wireless controllers: The controllers enable the expansion of the system with additional wireless devices, e.g. detectors. They are connected to the control panel via the system bus. The control panel controls the wireless programming using a keypad with dedicated software. In battery-operated wireless, the battery life depends on the transmission power and the transmission time.

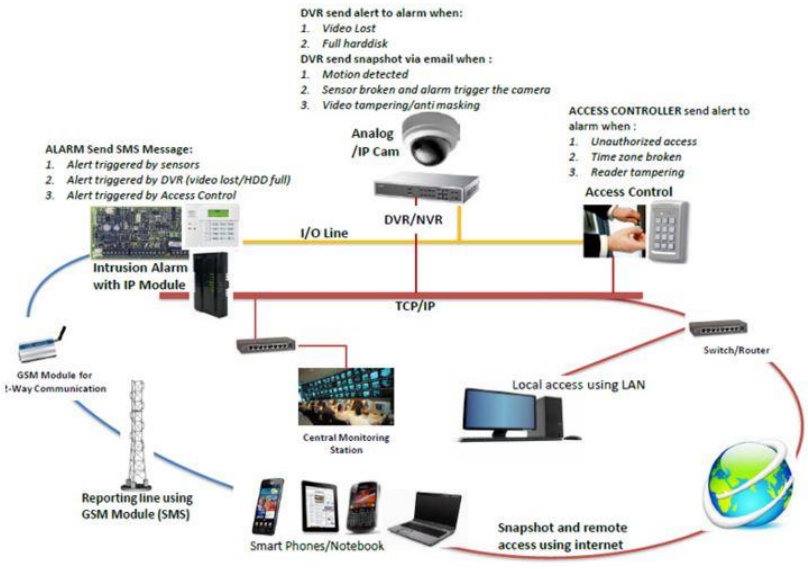

Fig 5: Intruder Alarm and Detection System

(Source: https://www.google.com/search?q=intrusion+detection+system&tbm/...)

4.4.2. Uses of Intruder Alarm and Detector Systems in Libraries:

In any library, numbers of valuable resources are available for exploitation and genuine use. The library must critically observe unauthorized access to protect the resources from miscreants. Intruder Alarm security systems trigger the alarm and detect anything wrong, and ultimately brings security to the library.

4.5. Recent Developments in Electronic Security Systems (ESS) in Libraries:

In recent times, ESSs have played a vital role in libraries. Libraries also use different ESSs like RFID System, Barcode System, 3M Exit Detection, Moisture Sensor, Glass Break Sensor, Fire /Smoke Sensor, Flood Detector, Biometrics, Smart Card etc. In this 21st century's information age, libraries are more responsible for evolving to protect internet safety and security. Therefore, these libraries are very much concerned about the adoption of physical and other security measures like Data/Information Security, Computer Security, Hardware/ Software Security, Network Security etc.

Data/ Information Security measures help libraries store data back-up in hard drives, CDs/DVDs, disks, tapes, etc. To control the access user identification and password, biometric systems use address verification systems can be used properly. Likewise, Computer Security measures have the facilities like data encryption, password, computer virus, computer locks, system back-up, off-site storage, card access, printer fax security, diskette security etc. Software/ Hardware security includes anti-virus software, anti-spyware security, cleanup software, ID management software, multi-user operating systems, user entrance log, web filtering software, systems, regular backups for the data, The server environmental control, library server's operating systems etc. And Network Security includes Firewall, Local Area Network, server segregation, wireless security etc. These different security measures now become very protective beneficial to control the information safety in any kind of libraries.

Recent developments in ESSs describe its transformation in response to the profound changes in technology, research and information services. Library in a digital age it becomes even more critical that importance of the protecting our information assets and consolidated data. The British library has adopted and established a high-level Information Security policy which is also a part of Information security management system with ISO /IEC 27001:2013 for creating and managing ISMS. Adopting the

standard assists us in identifying, managing and minimizing the range of threats to which information can be subjected. The framework of controls, policies and standards, as laid out in the Information Security Management System, protects the confidentiality, integrity and availability of all the information held and owned by the British Library. Clemson University Library and Mugar Memorial Library at Boston University also established some guidelines and security policies in using ESSs. The American College Research Library (ACRL), a division of the American Library Association, has also published guidelines regarding library collection, user, staff, and library building etc., security. Likewise, in India, the IITs, IIMs and Higher Educational Institutional libraries have emphasized more importance in implementing ESSs like CCTV, RFID, Biometrics, and other measures of Information Security Systems. Moreover, the institutions have followed various Security Management Models like COBIT, ISMMM, SSE-MME, IA-CMM etc., along with ISO standards like 27001, ISO/IEC 17799:2005, BS 15000 etc. which further help the institutions to design a practical framework for the libraries.

5. Pre-requisites for Implementation of Security Systems in Libraries:

An academic library must be concerned about the strategic plan before implementing appropriate electronic security systems and its pros and cons. Following are some important aspects which need to be taken under consideration before initiating the security systems-

- Total library collections.
- Total library users.
- Type of access in the library- Open or Restricted Access system
- Whether the Library is performing automated House-keeping operations
- Practice and Procedure for proper stock verification.
- To look into the approximate loss of books by theft, unauthorized access or misplacement of books.
- To intensely observe the library hours when loss of documents could be more.
- Security system adopted by the library is working properly or not.
- The monitoring of staffs for circulation, reading room, security areas are sufficient.
- The library materials are Bar-coded or not.
- Availability of Library Budget.

6. Opportunities:

6.1. Assets Protection:

Electronic Security System is very effective security measures which give full protection to the valuable assets from both internal and external theft. It provides safe gourds to intellectual properties even if they are under strict non-disclosure conditions.

6.2. Safe work place:

Having CCTV, alarm system, intruder system in work place provides reassurance to the employees that they are safe during their day and night shifts. It will give them support to control emergency situation related to intrusion on property and also give stress less mind to concentrate in the work.

6.3. Instant Security updates:

The modern ESSs are very user friendly and can be manageable and accessible through different electronic devices such as computers, tablets or mobile phones etc. it includes novel technology and cloud system which enable remote access facilities. The security alerts can find out from anywhere within seconds.

6.4. Conflict resolution:

Integrated security system including CCTV security cameras, access control system, security alarms and security officers can provide vital evidence to solve any critical problem arises in the workplaces.

6.5. Value for money:

ESSs are very cost-effective for an institution. Though the primary stages of ESSs implementation are a challenging task, it has effective value addition in terms of money and peaceful mind in the long run.

6.6. Monitoring High-Risk areas:

ESSs are very effective for high-risk areas. It can be installed in places that are vulnerable to vandalism, theft or break-in. It uses an automation system and analytical reports, representing a refined use of resources, making it easier for humans to control any emergency.

7. Challenges:

i) **Technological Challenge**:

Technological challenge refers to sufficient computers, proper hardware and software requirements, internet connectivity, etc. These factors are very much essential for implementing electronic security systems in libraries.

ii) **Personnel Challenge:**

The library staff should have intensive and extensive knowledge and practical experiences about electronic security systems to effectively implement electronic security systems.

iii) **Financial Challenge:**

The major challenge for implementing various kinds of electronic security systems is the financial or budgetary constraints. For any library, adopting new technology is very challenging because it involves the monetary factor.

iv) **Organizational Challenge:**

One of the important challenges for adoption of electronic security systems is the organizational or management challenge. The authority must be convinced of the positive side of these security systems.

8. Conclusion:

From the beginning, the library is playing a very significant role in delivering knowledge and information as per users demands. The resources contain valuable contents which need to be secured and preserve integrity and confidentiality. Compare to the traditional security system, the modern ESSs has ample beneficiary aspects which help the library professionals to maintain the integrity and dignity of library. The practice of surveillance cameras, biometrics, RFID systems, Smart cards and different types of alarms bring down malpractices against library resources. Meanwhile, it is also considered that the security issues will not disappear overnight or forever, but the adoption of ESSs may reduce the massive loss of library assets.

The proper installation of ESSs is nothing more than a booster to the security system of an academic library. This system will help prevent unauthorized removal of collections and feasible monitoring and detection of user traffic in general reading and reference rooms and shelves areas (Ameen and Haider, 2007). All the staff should see the general security of the library as a collective responsibility. The security of the library should not be left alone to an individual or management. This will make the staff be security conscious at all times.

References:

American Library Association (2003). *Guidelines regarding thefts in libraries.* Retrieved from http://www.ala.org/ala/mgrps/divs/acrl/standards/guidelinesregardingthefts.cf.

Brown, K. E., & Parkus, B. L.(2007). Collections security: planning and prevention for libraries and archives. Retrieved from http://www.nedcc.org/resources/introduction.php

Dawes, T. A. (2004). Is RFID right for your library? *Journal of Access Services*, 2(4), 63-70.

Gautam, V., Behera, P. K. & Singh, M. (2011) . Issues of digital data security in the library environment. *International Journal of Information Dissemination and Technology*, October- December 2011, 1 (4), 127-140.

Godbole, N. (2009). *Information systems security*. USA: Wiley. Pp. 419-435.

Greenwood, L. & Mckean, H. (1985). Effective measurement and reduction of book loss in an academic library. *The Journal of Academic Librarianship.* Retrieved from https://www.sciencedirect.com/journal/the-journal-of-academiclibrarianship/issues?page=2

Gupta, P. & Madhusudhan, M. (2017). Use of multifaceted electronic security systems in a library environment. *Journal of Knowledge & Communication Management*. 7 (2), 116-130. DOI: 10.5958/2277-7946.2017.00010.9

Jadhav, M. N. & Shobha, K. (2004) . Electronic security: a case study of IIT Bombay central library. Retrieved from file:///C|/CALIBER_Files/Caliber_2003_CD/LA/12.html

Kulkami, S. & Powdwal, S. (2007). Library security systems: metamorphism. *Library Herald*. 46 (2), 81-90.

Kumbhar, K.N. & Veer, D.K. (2016). Study of security system used in college libraries. *International Journal of Research in Library Science*. 2 (1).

Kumbargoudar, P. & Kumbargoudar, M. (2008). Biometric security technology for libraries. *SRELS Journal of Information Management*, 45 (1). 37-44.

Musa, S., Faga, A. & Ejeh, D. M. (2019). The effect of library security on service delivery in federal university Lafia, library- Nigeria. *Journal of Library and Information Sciences*. 7 (1), 63-69. DOI: 10.15640/jlis.v7n1a6

Osayande, O. (2011). Electronic security systems in academic libraries: a case study of three university libraries in South-West Nigeria. *Chinese Librarianship: an International Electronic Journal. 32.* Retrieved from http://www.iclc.us/cliej/cl32osayande.pdf

Ramana. Y.V. (2007). Security in libraries need surveillance and biometric. 498-507. Retrieved from https://ir.inflibnet.ac.in:8443/ir/bitstream/1944/1427/1/498-507.pdf

Roy, M. & Basak, K. (2011). The thief in our midst. *Library and Archival Security*. 9 (3/4), 77-81.

Uma, V., et al. (2010). Electronic security system in university libraries with special reference to IGM Library, University of Hyderabad. *Pearl: A Journal of Library and Information Science Year: 2010*, 4 (1), 13-20.