CHAPTER 1
INTRODUCTION

1.1 INFORMATION SECURITY SYSTEM

Information security includes personnel security, privacy, policy and computer security. Specific personnel must be assigned security related tasks in order for any security system to be effective. Due to the continuing emergence of new security exploits, tools and techniques coupled with the constant parade of software and hardware upgrades likely in most library environments – ongoing diligence is required to keep informed of security developments.

Libraries are institutional set ups to cater to the educational, cultural, research, recreational and information needs of their users. Libraries have the main objectives of being entrusted with the selection, acquisition, organization, storage and dissemination of information to their patrons. Jama’a (1984:1) observed that academic libraries in particular, assume a focal point where users of diversified age groups, socio-political, economic backgrounds and cultural interests have to converge to utilize all the available resources that are relevant to their individual needs. As a result of this diverse use of the materials, these libraries stand vulnerable to all forms of crime and security risks not only from the users, but also from the library staff as well. Vandalism, mutilation, theft, etc are problems regularly encountered by the materials of these libraries. Books and other information materials are valuable and expensive but are likely targets for criminal activities.

The expected roles of the academic library tend to lead it to criminal activities. The more the control, safeguard and security levels, the less it resembles a library that is traditionally expected to serve as user. Theft of and
malicious damage against books are difficult to contest because the risk of getting caught is very low, while the likelihood of success is high. Criminal activities in academic libraries are not limited to library information materials alone but theft of properties such as handbags, purses, keys and notebooks are equally common. The extent, nature and rate at which these crimes occur vary from one academic library to another.

1.2 INFORMATION SECURITY POLICY

Policy formulation is an important step toward standardization of security activities in IT resources. IT security policy is generally formulated from the input of many members of an organization, including security officials, line managers, and IT specialists. Two types of policy typically needs to be developed to meet an organization’s needs: programme level and issue specific. Programme Level policy’s main function is to establish the security programme, assign programme management responsibilities, and state the wide-organization IT security goals and objectives.

1.3 POLICY FOR SECURITY

Programme level policy should have sufficient breadth of scope to include all of the organization’s IT resources, including facilities, hardware, software, information and personnel. In some instances, it may be appropriate for a policy to name specific assets, such as major sites installations, and large systems.

The three security related needs which are universally most emphasized among IT resources experts and the general computer user communities are integrity, availability, and confidentiality. These concepts should be the basis of the goals established for an organization in its IT security policy.

Integrity means assuring that information is kept intact, and not lost, damaged, or modified in an unauthorized manner. Availability means assuring
that information is accessible to authorized users when needed and that to the extent possible, IT systems are safe from accidental or intentional disablement. Confidentiality means assuring that information is accessible only to authorized personnel or via unauthorized means.

1.4 ISSUE SPECIFIC POLICIES

Issue Specific policies serve to provide guidelines for the further development of procedures and practices within the functional elements of an organization. A major challenge to IT security specialist has long been the fact that for every new technology there are also new associated problems and issues to be addressed. Many organizations today, develop and refine communications security policies in order to better address such questions as to who should have e-mail access, how will privileges be assigned and monitored, for what types of activities and information is e-mail sufficiently secure and what criteria should be used for the re-sending of messages among users.

The following are the gist of guidelines proposed by ALA

- Appointment of a Library security officer
- Forming a Security Planning Group
- Communication with the Public Relations Department
- Communication with Law Enforcement Agencies
- Work for Institutional and legislated Support.

1.5 DEFINITION: SECURITY

Merriam-Webster online dictionary defines “security as the quality or state of being secure, freedom from danger, and freedom from fear or anxiety. Security is a continuous process of protecting an object from unauthorized access. It is a state of being or feeling protected from harm”.

3
Information security as defined by the standards published by the Committee on National Security Systems (CNSS) is the protection of information and its critical elements including the systems and hardware that is used to store and transmit the information.

The following are the different threats to information (Whitman and Mattord, 2011)

Table 1.5.1 Categories of Threats

<table>
<thead>
<tr>
<th>S. No</th>
<th>Categories of Threats</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Acts of human error or failure</td>
<td>Accidents, Mistakes</td>
</tr>
<tr>
<td>2</td>
<td>Compromises to intellectual property</td>
<td>Piracy, copyright infringements</td>
</tr>
<tr>
<td>3</td>
<td>Deliberate acts of Espionage or trespass</td>
<td>Unauthorized access of information</td>
</tr>
<tr>
<td>4</td>
<td>Information extortion</td>
<td>Blackmail or information disclosure</td>
</tr>
<tr>
<td>5</td>
<td>Acts of sabotage or vandalism</td>
<td>Destruction of information or systems</td>
</tr>
<tr>
<td>6</td>
<td>Acts of thefts</td>
<td>Illegal confiscation of information</td>
</tr>
<tr>
<td>7</td>
<td>Software attacks</td>
<td>Viruses, worms, macros</td>
</tr>
<tr>
<td>8</td>
<td>Nature</td>
<td>Fire, Flood, Lightning</td>
</tr>
<tr>
<td>9</td>
<td>Deviation in quality of service</td>
<td>ISP, Power of WAN issues</td>
</tr>
<tr>
<td>10</td>
<td>Technical</td>
<td>Equipment failure</td>
</tr>
<tr>
<td>11</td>
<td>Technical software failure</td>
<td>Bugs, code problem</td>
</tr>
<tr>
<td>12</td>
<td>Technological obsolescence</td>
<td>Outdated technologies</td>
</tr>
</tbody>
</table>

1.6 SECURITY MEASURES IN LIBRARIES

The preliminary security measures in libraries are stock control, marks of ownership, accessibility and use. Protecting the collection should include ensuring good security to prevent theft. Libraries are archives that must provide remote storage for overflow materials or special cold storage facilities for vulnerable materials such as microfilm, motion picture film and color negatives. Whether a library uses open access or closed access, the staff needs to observe readers from time to time to discourage deliberate mutilation or vandalism of library materials.
Both library collections and other reading materials can be secured by

- Electronic security systems
- Digital data security systems
- Physical and Environmental security systems

1.6.1 Electronic Security Systems

Today there are electronic security systems which help the libraries to control, minimize or avoid library material theft and unethical losses.

The use of electronic security equipment component typically provides alarm notification to the appropriate authority, entry control, and site surveillance. The major elements of any electronic security system include

- Burglar protection
- Collection security
- Access control
- RFID
- Bar code Technology
- Video surveillance
- Biometrics

**Burglar Protection**

A burglar protection system includes sensors to detect intrusion, alarms, and notification to appropriate authorities. There are different ways of classifying the types of sensor systems. Sensors can be active or passive, convert or visible volumetric or line detection. They can also be defined by their mode of application. Active sensors transmit some type of energy and detect a change in the received energy created by the presence or motion of the intruder. Passive sensors detect some type of energy emitted by the intruder or detect a change of some
natural field of energy caused by the intruder. Convert sensors are hidden from view and visible sensors are in plain view. Volumetric sensors detect intrusion in a volume of space where as line detection sensors detect intrusion across a line.

➢ **Collection Security**

There are many methods of ensuring that no materials leave the library without being checked out. These systems always contain a security device that is placed on the materials (including books, magazines, video cassettes, audio cassettes, CDs and DVDs) as well as detection devices which are safe for magnetic media and usually have audible or visible alarms. If desired, the audible alarm could be a voice alarm. There are two major methods currently used for detection: Electromagnetic detection and radio frequency identification (RFID)

➢ **Electronic Access Control**

Electronic access technology is the best system for controlling access to library buildings. Authorized people are allowed to enter a controlled area by automatic unlocking of the door. Plastic access cards that are inexpensive and the software can be programmed to restrict access to certain areas while recording time, date, and location of authorized and unauthorized access attempts. For extra security, access control can be used in conjunction with video surveillance to control and monitor large facilities. Access can be integrated as photo ID cards for library employees and can be used as temporary “Keys” for library clientele to have access to restricted areas. It has been proved that electronic access control systems enhance safety and protect valuable library assets.

➢ **RFID Security Technology**

RFID solutions are designed to improve library operational efficiency. This enhanced capability is provided by RFID tags which do not require line of sight to be read, so that books are actually handled less. The tag combines book
identification and book security in to one label, minimizing labeling time and cost. More than one book can be read at a time, thus speeding circulation. The tags can be placed on any type of media, including CDs, DVDs and Videocassettes. The RFID tags are read/write, providing flexibility in what is encoded. They can also be put into the patron cards, speeding up the process even more. Library staff can check out and check in several items simultaneously without having to locate and scan individual bar codes. Patron self-check-out systems are also available to libraries that incorporate RFID technology.

RFID solutions can also speed up the return process. As library items pass over the RFID check-in antenna, they are automatically checked into the central library database. With the power of the RFID tag, regular inventories can become a reality. Shelf readers allow staff to read the RFID labels easily without having to remove books from the shelves. The shelf reader can also be used to search for a single or specified group of items and alarm the user when an item has been mis-shelved.

**Use of RFID technology**

LICs use RFID tags on books and other items to provide identification during check-out, check-in, inventory, and for theft deterrence.

- **Check-out:** Check-out or charging of books is a time-consuming process. Users can check-out books on their own with the help of self-check-out station. Self-check-out station is composed of a proprietary touch-screen device along with an RFID reader plus special software for personal identification, book and other media handling and circulation. This kind of system allows the LICs to speed up book charging process i.e. checks-out several books/items simultaneously, frees staff for deploying them on other activities, reduces queuing time and provides user privacy.
- **Check-In:** It is also a time-consuming process. Manual discharging can be significantly easier, faster, and more ergonomically friendly with RFID. More books/items can be checked in at one time. The Book Drops system can be useful in this activity. In this system, the user inserts the LIC books/items into the slot. The RFID reader captures the electronic signature and sends to backend system for loan cancellation. The user’s record is updated immediately. It offers unprecedented flexibility and convenience in returning LIC items at any time of the day, even when the LIC is closed.

- **Stock verification and other inventory control:** An RFID library system would speed up finding of books and also improve the stock control of the library. It basically comprises of a portable scanner and a base station. High-speed inventory and identifying documents which are out of order can be done through proper use of RFID technology i.e. scan documents on the shelves without removing them.

- **Security at the gate:** When a user leaves the LIC with the issued document, these are checked at the exit gate. For this purpose, RFID technology can be efficiently used and a terminal/lane installed at the gate. Theft detection is an integral feature of the chip/circuit within the RFID tag. It is a stand-alone technology. Each lane is able to track items of about 1 meter. When an unissued document passes through the gate, the terminal/lane sounds an alarm. In this way RFID system can minimize theft of LIC items. In addition to the above application, RFID technology can play an important role in case of retrospective conversion process and inter-library loan process.
Advantages of RFID technology at LICs

The use of RFID technology increases efficiency and eliminates human error due to fatigue and psychological reasons. The major advantages can be summarized as follows:

- Improves efficiency of the staff and quality of services
- Increases the speed of operations i.e. reduces the amount of time required to perform circulation operation, stock-verification, etc.
- Enhances accuracy
- Increases user satisfaction and hence improves the image of the LICs
- Provides reliable statistics for management information system (MIS) and management control
- Saves time of the users
- Improves information availability

➤ Bar-code Technology

Bar-code Technology plays an important role in automating the functions of the library, especially circulation. Its application increases the speed and accuracy in operations. Bar-code Technology provides a simple and
inexpensive method of encoding text information that is easily read by inexpensive electronic readers. Bar-coding also allows data to be collected rapidly and with extreme accuracy. A bar-code consists of a series of parallel, adjacent bars and spaces. Predefined bar and space patterns or “symbologies” are used to encode small strings of character data into a printed symbol. Bar-codes can be thought of as a printed type of the Morse code with narrow bars and spaces representing dots and wide bars representing dashes. A bar-code reader decodes a bar-code by scanning a light source across the bar-code and measuring the intensity of light reflected back by the white spaces. The pattern of reflected light is detected with a photodiode which produces an electronic signal that exactly matches the printed bar-code pattern. This signal is then decoded back to the original data by inexpensive electronic circuits.

The basic structure of a bar-code consists of a leading and trailing quit zone, a start pattern, one or more data characters, optional one or two check characters and a stop pattern.

Features of bar-code technology

▷ It is an automatic identification technology
▷ Barcode is a predefined format of dark bars and white spaces
▷ Structured to contain a specific piece of information
▷ It allows real-time data to be collected accurately and rapidly
▷ Combination of bar-code technology with computer and application software improves performance, productivity and profitability

Advantages of bar-code technology

▷ Distinctive identity of a product
▷ Error-free data entry
▷ Efficient management of resources and inventories
Functions and applications of bar-code technology for library systems:

- **Checking system at the Gate**

  This is a checking system when a user leaves the library with the issued document. For this purpose, bar-code technology can be effectively used and a terminal can be installed at the gate. Since charging and discharging is done online, the whole database is automatically updated. When a borrower leaves the library, the accession number of the document carried by the user will again be scanned at the gate. In case of issued document, the computer will approve the exit. But, if in case, someone carries a document that has not been issued, the computer will give an alarm and a message with immediate effect.

- **Identification of membership**

  One knows very well that in libraries, entry is restricted to their members only. Thus a person is deputed at the gate as gateman or security guard to check identity cards of each person entering the library. If the members are provided with bar-coded identity cards, then this checking becomes very easy. A bar-code scanner is installed at the gate of the library and every person entering the library has to place his/her identity card on the scanner. If the person is not a member of the library, the computer will give the alarm and thus restrict the entry and the identification of unauthorized entry will be made.
• **User statistics**

Under the manual system, most of the libraries maintain gate register wherein members are requested to enter his/her details and mark their signature as a proof of their visit to the library. It is time-consuming and users show indifference towards entering their particulars. With the help of this register, time series and classified statistics cannot be given instantly. When users are provided with bar-coded identity cards, it is possible to overcome all these difficulties. Thus user statistics are useful for various purposes, particularly for improvement in library services and control.

• **Charging and discharging of books**

Due to normal distribution system, charging and discharging of books becomes a time-consuming process, as stamping of due dates and other data entry work have to be carried out. But in bar-coded environment, when a user goes to the circulation counter, the counter staff scans his/her identity cards and activates the borrowing status. If the computer permits the borrowing facility, the document is scanned for accession number and is issued to the user without delay.

![Fig 1.2 Book Issue](image1) ![Fig 1.3 Barcode Printer](image2) ![Fig 1.4 Scanner](image3)
• **Issue of no dues certificate**

No dues certificate is issued when any member leaves the organization/institution and his/her membership is cancelled. This process is time-consuming and error prone in a manual system. In an automated system using bar-code technology, the member surrenders his/her identity card and the counter staff scan it. The automation package searches the database for any document issued in his/her name. If nothing is due, no dues certificate will be printed. Otherwise, the related list of documents is issued in the name of the member.

• **Stock verification and cross checking**

Stock verification and cross checking is a very tedious and time-consuming job in libraries and during stock verification and cross checking, the users are restricted to use the library facility. Here bar-code technology is used very effectively and it is quicker and error-free. Under this process, all the documents in the library are scanned and the data is gathered in the hand-held terminal. Once all the documents in the library are scanned, it is compared with the database of the total documents. If it does not tally, it gives the details of documents of which accession number has not been scanned.

➢ **Video Surveillance or CCTV (Closed Circuit Television System)**

Video surveillance and closed-circuit television (CCTV) systems serve as a way to watch and record security and ensure safety. Advances in CCTV technology and reduction in costs have also made video surveillance a cost-effective management device for library services.

Libraries can use CCTV to identify visitors and staff monitor work areas, prevent theft, and make sure the security of the location and other facilities. The system can also be used to monitor and record evidence on clientele and employee misconduct.
CCTV systems are quickly becoming one of the most important and economical security and protection tools available to libraries.

Fig 1.5 CCTV Camera

The key steps of designing a CCTV security system

- Find out the Primary Application of the CCTV system
- Identify the layout and characteristics of the controlled area(s)
- Decide on camera type and features
- Determine the best location for viewing monitors
- Determine the best method of signal transmission
- Decide on the type of recording/archival equipment for the system

When used for video surveillance and monitoring, the primary purposes of a CCTV system are detection, assessment, and identification. In all applications, a CCTV system must provide the ability to visually observe, monitor and record. Observation provides real-time information for detection and identification. Recording provides after the fact material for assessment, analysis, and review, usually with overlaid time, date, and location information.

Biometrics

The term biometrics refers to a science involving the standard analysis of biological characteristics. A biometric is a unique measurable characteristics
or trait of a human being in automatically recognizing or verifying identity. Biometric system takes into account the unique characteristics of person’s body which include fingerprints, head geometry, retinal and iris seeing, hand and finger geometry, voice pattern, facial recognition and other related techniques. Use of biometrics has not so far entered in the library field. However, it is possible to use biometrics in face of smart cards or other identification cards, since; it facilitates not to be misused by unauthorized persons. It avoids misuse by the other person as a proxy.

It is very crucial that how acceptable a security system is to the user and how effective it is in maintaining the security. The biometric systems are highly reliable and effective. The implementation of biometric system is vital in creating a security system by a professional. The biometric system ranks top in terms of effectiveness and acceptance. The following are the effective biometric control to be included in modern control system:

- Fingerprint recognition
- Handprint recognition
- Voice pattern recognition
- Signature recognition
- Retina recognition
- Facial geometry

1.6.2 Digital Data Security

Information security system

Maintenance of the security system is very crucial in a changing environment. The information security system needs constant monitoring and testing to know its effectiveness. The system should be able to upgrade to meet the over changing threats. The information security system should be stable and
reliable to face the emerging new threats. The system should undergo constant vigilance and security that can be compared so that the threats from outside can be managed. Information security system should have the following characteristics to cope with the needs mentioned below:

- Supporting and modifying the system
- Testing periodically for compliance
- Upgrading the system
- Updating and repairing to meet the changing technology

➢ **Intrusion Detection System**

Intrusion Detection Systems are commercially available and it mostly works like a burglar alarm. It detects the violation of configuration and activates the alarm. This alarm can be audible or visual and silent. The silent alarm gives email alert to the user to notice the violation. The Intrusion Detection Systems can be customized to provide detection and response to the administrator when threat is found. The Intrusion Detection Systems are used to detect the following type of threats

- To detect attacks and violation of security systems
- To detect and deal the preambles to attacks
- To document the existing threats
- To provide instruction about the intrusion.

➢ **Anti-Virus Security**

Anti-Virus Security is the unending quest and solution to virus attacks. The computer virus is a computer program that usually makes copies of itself in the computer’s memory storage or over a network without permission of knowledge of the user, and is intended to cause harm to the system on which it
resides. Cure to viruses lie in the anti-viruses which are the only antidote for the threatening viruses. That is the reason why anti-virus industry today is thriving relentlessly at a faster pace than ever before. Some of the Anti-Virus softwares are Norton Antivirus, The Shield Pro, Kaspersky Antivirus, McAfee Virus Scan Plus and PC-killing Internet Security.

**Network Security**

In this age of cyber world today, if there is a single word for ensuring security in Internet, the magic word is Network Security. Network Security forms the backbone or fundamental block for Internet Security. Network Security cannot be ignored since information transfer network becomes the lifeblood of the present century. Therefore, Network Security Products are emerging to meet the challenges. Some of the security products are firewalls, Antivirus, intrusion detection system, smart systems and intrusion management system.

**Barriers in adopting library security**

The major barriers in adopting the library security in libraries are given below.

- Lack of Information Facilities.
- Lack of National / State Policy for Preservation.
- Lack of Interest and Concern from Working Librarians.
- Lack of Financial Support.
- Lack of Initiative from Employees and Institutions.
- Lack of Manpower, both Professional and Non-Professional.
- Lack of Interest by Regional and National Professional Association.
- Lack of Technical Knowledge.
- Lack of proper planning by librarians towards preservation.
- Lack of adequate training in the schools of library information Science in theoretical, technical and practical aspects of preservation and conservation.
Data Security

Libraries face security problems and a varying degree of personal and professional risks since their earliest beginnings. One could even look at attempts for security as an exercise in futility because all attempts to make any library completely crime-proof have met with failure. Modern technology does not merely promise to create or improve better sensors and alarms to protect library collections. Emergent technology may actually slam the door on potential criminals, rendering them incapable of achieving their goals while helping publicize thefts and alerting other libraries that do not talk to one another or exchange information about missing material or thieves caught in the act, and methodologies used by those who steal.

Advances in technology may actually serve to make both theft and mutilation of materials and violence in library buildings things of the past by a simple expedient of removing the building from the equation. But even if one can never hope for a perfect library security in existing buildings, one can at least work conscientiously towards the goal. In the coming age of virtual libraries, the era of the smash-and-grab thief will be over for libraries and the day of the clever, resourceful electronic thief will be present, supplanting one problem with a potentially greater one. But even in this imperfect age of library vulnerability, one gets better at catching crooks, or at least in making their nefarious tasks far more difficult.

The advent of the virtual library may be the most significant change in the nature of the library. Libraries without walls, containing books without pages are now broadly available on the internet, and more paperless books come all the time. Such a capability makes it possible for users to consult a library’s catalogue and use or purchase books without ever setting foot in the building or even travelling to the host city. Digital books in virtual libraries, in fact, may be vulnerable to destruction or alteration intentional or accidental from a power surge, a lightning strike, or acts of sabotage.
The fragility of digital files, in fact, is of great concern to libraries, since more and more of them rely on silicon storage to hold and archive their materials and to make them more accessible without the risk of loss. Loss and the problem of paper deterioration make computer storage attractive as a medium of retention and distribution. The promise of electronic libraries is alluring and seductive for librarians up to their necks in crumbling print and hard copy information.

The dilemma of how to preserve and protect electronic documents while carefully observing all provisions of the copyright law continues, and will continue in the discernible future. Keeping their heads up and their eyes open may well, in fact, be the best way librarians can keep a responsible level of security in library buildings. Security forces help, too, especially trained professionals who know their jobs well. And developing technology has provided and will continue to provide ways that one can safeguard the collections and assure the safety of people in library buildings.

Imagine a virtual library in which the library’s holdings are electronic, consisting of magnetized documents available to users by means of telecommunications and computer equipment. The risk of losing materials in the customary way—things lost to mildew, wear, vandalism or walking out the door concealed on the persons or in the belongings of patrons becomes a non-factor. The archival copy of each document could be held in a secure, remote location, unvisited and untouchable by users and preferably backed up by additional copies held in other sites, safe against the possibility of fire, damage, lightning strikes, or other catastrophes. Under these circumstances, the matter of library theft becomes a non-issue because users never really hold original copies in their hands.
Need for digital data security

Digital data in any form in an organization is an asset to that organization. As the data is available on World Wide Web and can be accessed by number of users over networks, where anyone can accidentally or intentionally damage the data. The data could be confidential in nature and only authorized person should get access to it so that confidentially and accuracy of the data can be maintained. Some of the security issues related to digital data are classified into three categories:

- **Environmental Risks:** There are always some environmental threats to the data, it may be due to natural disasters like floods, fire, cyclones, earthquakes etc. These types of threats can totally swab out the data which cannot be recovered if proper security steps are not organized.

- **Physical Threats:** User can be the main factor as it depends upon the intention of the users, if the intentions are wrong then there is always a threat to data getting damaged, corrupted, modified or may be stolen. Possibility of physically damaging the media can also exist. There are some threats which may arise due to interrupted power supply and improper cooling of devices.

- **Technical Threats:** These are the threats related to data security over network, like hacking of data over unsecure transmission media, corruption of data with viruses/Trojans, stealing of data with spywares etc., and alteration of data by some un-authorized access. Vulnerability of systems hosting data, disk failures are also threats to data accuracy, integrity and availability. Accuracy, confidentiality, integrity and high availability of the digital data, necessitate perfect security.
Advantages of digital data security

- **Easy to access:** The data is easily and faster accessible by user from anywhere over network. The only thing required is internet connection. There is no need for the users to go to the library physically.

- **Easy to accumulate:** The data can be easily stored in physical medium e.g. Hard Disk, CD Rom, Tape drives etc.

- **Multiple accesses:** Multiple users can access the same information simultaneously as compared to the restriction of consulting the resource by single user at a time in traditional library system.

- **High availability of data:** The data is available round the clock and can be available at different locations for disaster recovery.

- **Easy Tracking:** In digital library, data can easily be indexed and tracked by a user.

- **Easy to preserve:** The huge amount of data can easily be preserved in the form of data sets and databases.

- **Ease of data retrieval:** The user is able to use any search term (word, phrase, title, name, and subject) to search the entire collection in few seconds. Digital libraries can provide very user-friendly interfaces, giving clickable access to its resources.

- **Less space requirement:** As compared to traditional library physical space requirements, digital library requires very less physical space. Digital data can be hosted on a single server which requires very small physical space.
1.6.3  Physical and Environmental Security

Physical Security

The library security should be planned during the time of construction of the building through architectural considerations which includes side design and building design.

The security personnel should be employed to undertake patrol within the library and to enforce appropriate library access at the main lobby. Inspection of bags and other belongings of library users while entering and leaving the library, by security or library staff is being followed in almost all libraries. Most of the libraries do not allow the users with notebooks, records notes, etc. and insist depositing such things in the property counters provided exclusively for this purpose. They permit the users to take loose sheets or small scribbling pads inside the library.

Visual inspection by library staff through floor walks is another manual method followed by librarians to overcome unethical practice viz., malicious writings, injuries, cuts, mutilations and destruction of library materials within the library premises.

Mutilation and theft of library materials are major problems throughout the library world. Accurate figures on losses of books by theft are difficult to obtain as the libraries, nowadays have neglected to take physical inventories of their collections. The problem of writing down on library books by students and mutilating them by removing a single page or an entire section has become common experience of almost every librarian. Loss of books from libraries has become a topic of research today. Open access system in the
Libraries also facilitates and provides a medium for misplacement, mutilation and theft of books from libraries. In this digital era, there are many possible advantages to invent technologies to catching book thieves at the exit.

Environmental Security

- **Fire**

  New technical advances have given automatic sprinklers to get over the fire problem. These are fitted in buildings and when on account of fire the temperature rises to a certain degree, the sprinklers start working automatically.

- **Sunlight**

  Exposing books to sunlight is a danger to the life of books. The ultraviolet rays cause much harm to both the paper as well as the binding.
The ultraviolet rays loom over molecular structure of paper and leather which may be experienced through the fading of dyes or the browning of the paper. Where direct sunlight is unavoidable, it should be filtered through thick green glasses, thus screening out the harmful ways.

- **Darkness**

To protect books from the effect of direct sunlight, one may go to the extremity of darkness. Darkness when associated with humidity involves germination of molds and insects. Excessive humidity is one of the factors of deterioration. The cure consists in removing humidity either by artificial heating, circulation of dry air, or by the use of electrical dehumidifiers or handy wire containers which are specially designed for this purpose, may be used to absorb moisture.

- **Polluted Air**

The site of the Library should be away from laundry or power plant or any other lethal instruments developed by various companies. Care should also be taken to select dust free surroundings for a library.

- **Air Conditioning**

Temperature and rate of deterioration of book materials have an identical relationship. The warmer the books, the faster the deterioration. This warrants these books should be kept as cool as possible. 60% F is probably the lower limit at which books should be stored.

    Heating and air conditioning systems should thus be operated in such a manner that temperature and humidity are kept constant 24 hours a day. Adequate ventilation and circulation of air is important to prevent pockets of stagnant air which can create conditions prone to growth of mildew.
1.7 PROPOSED RESEARCH / NEED FOR THE STUDY

Due to multifold increase in library resources, libraries need to be equipped with modern technologies to safeguard library collections. Maintenance of library collection is a responsibility of the library personal. Books are often found on library shelves with all their pages torn from the spine. Sometimes, books have been damaged beyond repair and need to be replaced. Unfortunately, some books cannot be replaced because they are out of print. Library collection is a real wealth to the academic community and one cannot afford to lose this wealth. This alarming situation has initiated the authority to find out the means for safeguarding the library collection.

Today in the era of information and communication technology (ICT), the need is to maintain and manage information resources in the digital format and make the resources sharable for multiple accesses. The data in the digital format in an organization is an asset to that organization. The transmission of digital data requires protection of data, security of contents, its authorized utilization and user privacy. The survey was undertaken to find out the application of security measures in University Libraries of Tamil Nadu for minimizing such a heavy loss of library resources.

A study on the applications of information security systems in University libraries of Tamil Nadu is very meager. On review of the literature, it was found that no comprehensive study on the applications of information security systems in the University Libraries of Tamil Nadu has been analyzed. Hence the present study has been proposed and conducted.

1.8 STATEMENT OF THE PROBLEM

Diverse use of library materials and diverse group of libraries stand vulnerable to all forms of crime and security risks from not only the users, but also the library staff. Vandalism, mutilation, theft etc. are problems
regularly encountered by the materials of these libraries. Hence for the present research, an analytical study, on Information security systems in University Libraries of Tamil Nadu: An analytical study was undertaken.

1.9 SCOPE OF THE STUDY

The present study tries to bring to limelight, the realization of the effectiveness of the information security systems. Compared to other States in India, large number of universities such as Universities of Social and Humanities, Medical, Agricultural and Technical, Engineering, Law and other professional function in Tamil Nadu. Among these Universities, the researcher has selected forty University Libraries for the study.

State Universities

1. Alagappa University, Alagappa Nagar, Karaikudi-630 003.
2. Anna University, Guindy, Chennai-600 025.
3. Annamalai University, Annamalainagar- 608 002.
4. Bharathiar University, Coimbatore-641 046.
5. Bharathidasan University, Tiruchirappalli - 620 024.
6. Madras University, Chennai-600 005.
7. Madurai Kamaraj University, Madurai-625 021.
8. Manonmaniam Sundarnar University, Thirunelveli-627 012.
9. Mother Teresa Women's University, Kodaikanal-624 102.
10. Periyar University, Salem-636 011.
11. Tamil University, Thanjavur-613 005.
12. Tamil Nadu Agricultural University, Combatore-641 003.
13. Tamil Nadu Dr. Ambedkar Law University, Chennai-600 028.
14. Tamil Nadu Physical Education and Sports University, Chennai.
15. Tamil Nadu Veterinary & Animal Sciences University, Chennai-600 051.
16. Thiruvalluvar University, Fort, Vellore- 632 004.
Deemed Universities

1. Amrita Vishwa Vidyapeetham, Coimbatore-641 105
3. Bharath Institute of Higher Education & Research, Chennai-600 073
4. Chennai Mathematical Institute, Chennai -603 103
5. Gandhigram Rural University Gandhigram, Dindigul -624 302
6. Hindustan Institute of Technology and Science (HITS), Kelambakkam, Kancheepuram District.
7. Kalasalingam Academy of Research and Higher Education, Virudhunagar-626 190, via Srivilliputhur
8. Karunya Institute of Technology and Sciences, Coimbatore-641 114
9. M.G.R. Educational and Research Institute, Maduravoyal, Chennai-600 095
10. Periyar Maniammai Institute of Science & Technology (PMIST), Vallam, Thanjavur -613 403
11. Ponnaiyah Ramajayam Institute of Science & Technology (PRIST), Thanjavur-614 904
12. S.R.M Institute of Science and Technology, West Mambalam, Chennai-600 033
13. Sathyabama Institute of Science and Technology Jappiaar Nagar, Chennai-600119
15. Sri Chandra sekharendra Saraswathi Vishwa Maha vidyalaya Sri Jayendra Saraswathi Street, Kancheepuram-631 561
16. St. Peter's Institute of Higher Education and Research Chennai
17. Vel's Institute of Science, Technology & Advanced Studies (VISTAS) Pallavaram, Chennai
18. Vellore Institute of Technology, Vellore-632 014
19. Vinayaka Mission - Research Foundation, Ariyanoor, Salem-636 308
20. Karpagam Academy of Higher Education, Coimbatore
22. Rajiv Gandhi National Institute of Youth Development, Sriperumbudur - 602 105
23. Vel Tech Rangrajan Dr. Sagunthala R&D Institute of Science & Technology, Chennai
24. B.S. Abdul Rahman Institute of Science & Technology, Vandalur, Kanchipuram Distt., Chennai

1.10 OBJECTIVES OF THE STUDY

The present study aims to investigate the application of information security systems in the University Libraries of Tamil Nadu with the following objectives:

1. To study the operational status and facilities available at the State and Deemed University Libraries in Tamil Nadu.

2. To analyze the nature of manual and digital preservation techniques practised in University Libraries.

3. To evaluate the status of the State and Deemed University Libraries in adoption of Barcode Technology, Radio Frequency Identification Technology (RFID) and CCTV.

4. To measure the librarians’ perception towards benefits of information security systems.

5. To examine the librarians’ perception towards hindrance faced by them in implementation of effective ISS (Information Security Systems).
6. To identify the prevention measures taken by the librarians towards effective management of ISS and their satisfaction towards the same.

7. To offer constructive suggestions for the improvement of library security systems both at State and Deemed University Libraries in Tamil Nadu.

1.11 HYPOTHESES

The following are the major hypotheses of the study: The implementation of the information security systems at University Libraries in Tamil Nadu is far from satisfactory.

- There exists no uniformity in the library facilities available at State and Deemed Universities in Tamil Nadu.

- There exists no association between nature of damages incurred by the libraries and the manual information protection systems adopted by them.

- Challenges faced by the librarians in the management of digital preservation system significantly hinder their digital and electronic data preservation practices.

- Frequency of RFID systems available in the libraries significantly affects the barriers faced by the librarians in the usage of RFID systems.

- State and Deemed Universities operating in Tamil Nadu have been significantly benefitted from the adoption of information systems in the libraries.

- There exists no association between the level of benefits and satisfaction derived by the librarians in implementing information security systems.
1.12 METHODOLOGY

Study Area

The study area refers to State and Deemed University Libraries, Tamil Nadu.

Data Collection

The present study is on “Information Security Systems in University Libraries of Tamil Nadu: An Analytical Study”. The researcher has selected forty University Libraries of Tamil Nadu. For this purpose, review of literature has been collected to find out the contribution in these subjects. The data and information collected were examined with special reference to the impact of information security systems in libraries. Survey method was adopted to collect the data. The collection of data is a first-hand study made by the investigator. In order to achieve the objectives of the study, the following methods have been adopted

- **Questionnaire Survey**

   Well-structured questionnaires were prepared and distributed to the Chief Librarians of the Universities. The main purpose of distributing the questionnaires to the Librarians was to obtain data regarding information security systems and its advantages, the different kinds of electronic security systems, various methods involved in safeguarding the library resources, protecting the digital data from virus, macros, bugs, code problems, avoiding theft and mutilation, preserving library materials from insects, book worms and to investigate Librarians’ technical knowledge and assess Librarians’ interest in the implementation of security systems in libraries. These questionnaires were distributed to the Chief Librarians of the Universities with a covering letter indicating the significance of the study and intended plans for the results.
Semi-Structured Interviews

The method of collecting information through personal interviews is usually carried out in a structured way. This is called structured interviews. Such interviews involve the use of a set of predetermined questions of highly standardized techniques of recording information. For the present study, both telephone and face-to-face interviews were conducted with the Chief Librarians of the Universities using a semi-structure interview schedule. The purpose of interviews was to complement the quantitative information obtained by the questionnaire with more detailed qualitative information. This method provided the interviewer, the opportunity to clarify certain questions which was unclear to the respondent. The interviews directly addressed the implementation of information security systems in University Libraries of Tamil Nadu where there was more personal response when compared to the questionnaire.

Observation of Libraries

Observation becomes a scientific tool and method of data collection for research. It is systematically planned and recorded and is subjected to check its validity and reliability. For the present study, observation visits were conducted in libraries to collect data about information security systems such as electronic security systems, digital data security systems, computer hardware and software security systems, physical and environmental security systems and examine its advantages and effective utilization of security measures.

Sample Size

The main focus of the present study was to analyze the information security systems in the University Libraries of Tamil Nadu. All State and Deemed Universities of Tamil Nadu were selected for the present study. The researcher took
a sample of 48 University libraries for analysis. After strenuous effort, it was found that 3 State Universities do not have a proper library system, and 5 Deemed University Librarians showed no interest to respond.

Among the forty libraries selected, 16 libraries are State University Libraries, 24 are Deemed University Libraries. A pilot study was conducted in seven universities in Coimbatore District. Data was collected from the Librarians of all the selected University Libraries through completely structured questionnaires comprising of ten sections. The data collection commenced in December 2012 and was completed by the end of October 2013. The information obtained from questionnaire survey was updated through an observational visit to the libraries.

The collected data are analyzed using Excel sheet and MS-Word to generate tables, figures, charts, etc. SPSS package is also used wherever necessary.

1.13 STATISTICAL TOOLS AND TECHNIQUES

To assess the implementation of Information security systems in University Libraries of Tamil Nadu, the collected data was classified and tabulated according to the objectives of the study and analyzed using statistical tools such as Percentage Analysis, Weighted Arithmetic Mean, Independent ‘z’ test, ANOVA, Rotation Factor Analysis, and Multiple Regression Analysis.

- The frequency distribution of the variables has helped the researcher to calculate the distribution value of the variables tested.

- Weighted arithmetic means and Likert’s Summated scales helped in calculation of sum and mean values for: implementation of computerized services in the library, librarians’ opinion on preservation methods adopted in the library, computer security measures taken in the libraries, digital and electronic preservation of information adopted in the library, type of object
scanned using bar-code reader, librarians’ opinion on benefit of digitalization in operation security measures, librarians’ perception towards benefits of bar-code technology, librarians’ perception towards benefits of RFID, barriers faced by the librarians in preservation of information materials, barriers faced by the librarians in adopting RFID systems, challenges faced by the libraries in digital preservation, librarians’ opinion towards the measures implemented in libraries to prevent valuable properties, measures taken in the libraries for physical and environmental security, measures taken in the libraries for the safety of users, type of network used in the library, computer software used in the libraries to preserve the digital materials, measures taken in the libraries to protect the database of the user, measures taken in the libraries for network security, measures taken in the libraries for software security and measures taken in the libraries for hardware and server security, collection security measures adopted in the libraries.

- Independent ‘z’ test was applied to measure whether uniformity exists in the library facilities available at State and Deemed Universities in Tamil Nadu

- ANOVA test was applied to measure whether there exists association between the nature of damages incurred by the libraries and the manual information protection systems adopted by them. The same test is used for measuring the significant usage of RFID systems available in the libraries and the barriers faced by the librarians in the usage of RFID systems.

- Rotation Factor Analysis was applied to group into five factors the benefits derived State and Deemed Universities operation in Tamil Nadu due to adoption of information security systems in the libraries.

- Multiple Regression analysis was performed to measure the association that exists between level of benefits and satisfaction derived by the librarians in implementation of information security systems.
1.14 LIMITATIONS OF THE STUDY

Though this study provides useful information about the adoption of information security measures in effective library management, few limitations must be acknowledged. The process of collection of data was a real challenge as the respondents consumed more time to respond. Further, there was reluctance on the part of the respondents to provide data and few Universities have no proper library system. However, adequate care has been exercised in the collection of data.

1.15 CONCLUSION

Information Management covers a whole spectrum of information handling activities, technology, covering methods of inputting, storing, retrieving and distributing information. Its function incorporates a wide range of disparate activities including records management, library management, printing, reprography and micrography. The present day Information Society has witnessed the widespread transition of knowledge from print format to electronic format, which has also given rise to the problem of its preservation in digital form. The problem of preservation is further complicated by the rapid obsolescence of the hardware and software requirements interpreting and presenting digital documents. Ensuring continued access to digital information necessarily involves copying or transforming digital documents to run on current media, software, hardware and operating systems.

Globalization of information, the emergence of Internet and other global communications, networks and web resources have transformed the role of Information Organization and Management. In this context, Digitization is a major issue for preservation managers in library and information centers and archives. There is a big task ahead of them as to how they could cope with the current trends in the task of managing information. Keeping in view the recent
developments in this information handling and management, the benefits of digital preservation and digitization could not be overlooked and augmented effectively in order to preserve and disseminate for the future generations to come. Therefore, the information professionals are to be trained in the area of digital preservation and digitization techniques.

1.16 CHAPTER SCHEME

Chapter 1: Introduction

Chapter one presents the basic information about the Information security systems in the University Libraries of Tamil Nadu, need for study, statement of the problem, scope of the study, objectives of the study, hypotheses, research design and methodology, analysis and interpretation, limitation of the study, statistical tools and techniques etc.

Chapter 2: Review of Literature

In chapter two the review of literature has been presented. Review of literature, a part of the thesis describes all the recent knowledge related to Information security systems implemented in various Universities both at National and International level. It deals with the concept of application of security systems such as electronic security measures, digital data security methods, computer security systems, network security methods, collection security methods, physical and environmental security systems and Information related review of literature, information security technologies in libraries, security measures adopted by the library authorities.
Chapter 3: Description of the Area of Study

Chapter three focuses on the investigations of forty University Libraries of Tamil Nadu. It states the background information about Universities, library resources and services and information security systems in University Libraries of Tamil Nadu.

Chapter 4: Analysis and Interpretations

Chapter four presents the analysis and the interpretations relating to the data collected from the forty State and Deemed University Libraries of Tamil Nadu.

Chapter 5: Major Findings, Suggestions, and Conclusions

Chapter five deals with the summary of the findings and concludes with suitable suggestions and recommendations for future development in safeguarding library resources in the University Libraries.

Review of Literature is presented in the next chapter.