Emerging Technologies for Libraries: RFID & Biometric Smart Cards

Ajay Sharma
Chief Librarian, Institute of Management Studies, Dehraun – 248001

Abstract

Emergence of computer technologies has increased information storage capacity beyond imagination in the past decade and made it possible to access information from any part of the world easily and quickly. All this has increased the use of digital technology in all walks of life, personal and professional both. Library, being an integral and critical component of a civilized world has witnessed increasingly interesting applications of these digital technologies. Digital libraries are not single, stand-alone, repositories of digital data instead they are a heterogeneous collection of network-based repositories using a variety of protocols for user interaction, data encoding and transmission. Digital library is a logical extension of the networked environment and the development triggered therefore and provides the users with coherent access to a very rare, organized repository of information and knowledge. Through digital technology it is advantageous to access and search the information faster. There is also saving in storage space as the digital resources are compact compared to print format. Further the sharing of information helps to reduce the cost. Digital libraries can be accessed by all sections of the community over the whole world through the internet.

Smart cards are capable of storing biometrics template in the card memory itself along with other information hence template may not be stored on the central database. Also access to central database is not necessary to verify the identity. This unique advantage with this powerful combination has attracted government organization worldwide to use it as main identification card for employees, citizens and services. A Biometric - smart card protects biometric data and provides a reliable solution where there are privacy concerns. Fingerprints are an ideal credential for logical access control to computer networks and fingerprint templates never leave a smart card unprotected. Integrating a biometric sensor into a smart card reader makes sense because it is more convenient to combine a smart card reader with a fingerprint scanner in one integrated device.

This paper is an attempt to study the impact of digitization of technologies over Library management. The paper studies two prominent technologies for library management in vogue these days, viz., RFID and Smart Card-biometrics. The context, application, cost-benefit analysis, components and limitations for these libraries are also presented.

Key Words

RFID System, Smart Card, MCU, MOC, PIN.

Introduction

Invention of computers and networks (especially the Internet) are great milestones in the history and development of libraries. There has been a convergence of a number of developments in computer technology in the last few years, which has significantly affected the way computers can be used in libraries. Emergence of compact disks, digital versatile disks and high-speed processors has increased information storage capacity beyond imagination in the past decade and the Internet Technology made it possible to access information from any part of the world easily and quickly. All this has increased the use of digital technology in all walks of life, personal and professional both. This phenomenon has greatly influenced the way organizations store, retrieve and use data. Library, being an integral and critical component of a civilized world has witnessed increasingly interesting applications of these digital technologies.

Digital Library are organizations that provide

Reprint requests: Ajay Sharma
Chief Librarian
Institute of Management Studies, Dehradun – 248001
Tel:09412156058, E-mail: ajaysharma.ims@gmail.com

the resources, including the specialized staff to select, structure, offer intellectual access to, interpret, distribute, preserve the integrity of, and ensure the persistence over time of collections of digital works so that they are readily and economically available for use by a defined community or set of communities.

Radio Frequency Identification (RFID)

Generally, RFID systems have an antenna and a transceiver in a reader, and a tag (also known as a transponder). The antenna transmits a signal that activates the transceiver using radio frequency waves to the tag, which then transmits data back to the antenna. A low frequency RFID system (30 KHz to 500 KHz) has a short read range of usually less than six feet. High frequency systems of 850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz offer longer transmission ranges of more than 90 feet.

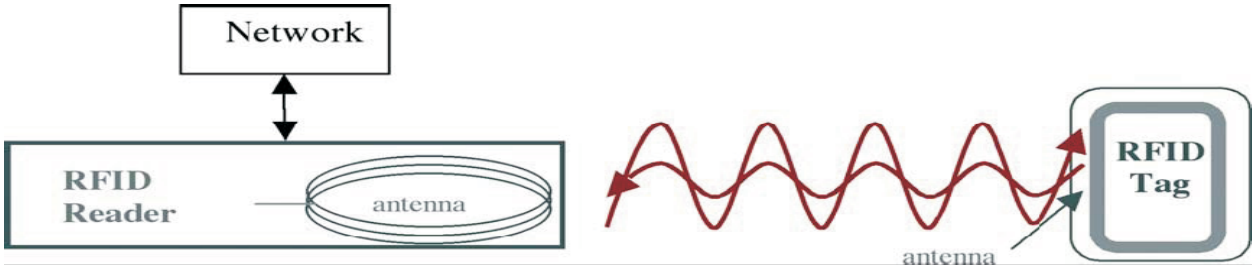
RFID is the latest technology to be used in library theft detection systems. Unlike EM (Electro-Mechanical) and RF (Radio Frequency) systems, which have been used in libraries for decades, RFID-based systems move beyond security to become tracking systems that combine security with more efficient tracking of materials throughout the library, including easier and faster charge and discharge, inventorying, and materials handling. RFID is a combination of radio -frequency-based technology and microchip technology. The information contained on microchips in the tags affixed to library materials is read using radio frequency technology regardless of item orientation or alignment (i.e., the technology does not require line-of-sight or a fixed plane to read tags as do traditional theft detection systems) and distance from the item is not a critical factor except in the case of extra-wide exit gates. The corridors at the building exit(s) can be as wide as four feet because the tags can be read at a distance of up to two feet by each of two parallel exit sensors.

Components of an RFID System

A comprehensive RFID system has four components:

1. RFID tags that are electronically programmed with unique information
2. Readers or sensors to query the tags
3. Antenna
4. Server on which the software that interfaces with the integrated library software is loaded.

The following figure shows all these components of RFID system:-



Tags

RFID tags are simple, low-cost and disposable are being used to identify animals, track goods logistically and replace printed bar codes at retailers. RFID tags include a chip that typically stores a static number (an ID) and an antenna that enables the chip to transmit the stored number to a reader. When the tag comes within range of the appropriate RF reader, the tag is powered by the reader's RF field and transmits its ID to the reader. There is little to no security on the RFID tag or during communication with the reader. Any reader using the appropriate RF signal can get the RFID tag to communicate its contents. Typical RFID tags can be easily read from distances of several inches (centimeters) to several yards (meters) to allow easy tracking of goods. RFID tags have common characteristics, including:

- Low cost, high volume manufacturing to minimize investment required in implementation
- Minimal security, with tags able to be read by any compatible reader
- Disposable or one-time use

- Minimal data storage comparable to bar code, usually a fixed format written once when the tag is manufactured
- Read range optimized to increase speed and utility.

In Indian libraries, it is a major challenge to keep the tags intact.

Retrospective conversions can be processed wherever there is a PC with barcode scanner, Programming software, and an RFID reader. The conversion procedure is straightforward and should take only a few seconds per item. The task can be performed by non-technical staff or volunteers. Some vendors also offer dedicated tagging and programming stations with touch screens, automated tag dispensing, and portability for in-stack use. Consideration must be given to the cost of dedicated stations and their space requirements.

RFID technologies have been obliged to apply and program their own tags to library items, e.g., books, periodicals, media, kits, and other assets. Now libraries may choose to have their book jobbers apply and program tags prior to shipment. While this is an increasing trend for new items, in-library application is still required for retrospective conversions of existing items and new books, media, periodicals, donated materials, and other items not procured through the book jobber. In the longer term, source tagging at item manufacture is likely.

Application

Once the reader reads the tag, the information is passed on to an "application" that makes use of the information. Examples of applications and their uses fall into at least six categories:

1. Access control (keyless entry)
2. Asset tracking (self check-in and self check-out)
3. Asset tagging and identification (inventory and shelving)
4. Authentication (counterfeit prevention)
5. Point-of-sale (POS) (Fast Trak)
6. Supply chain management (SCM) (tracking of containers, pallets or individual items from manufacturer to retailer)

Readers

RFID readers or receivers are composed of a radio frequency module, a control unit and an antenna to interrogate electronic tags via radio frequency (RF) communication (Sarma et al. 2002). The reader powers an antenna to generate an RF field. When a tag passes through the field, the information stored on the chip in the tag is interpreted by the reader and sent to the server, which, in turn, communicates with the integrated library system when the RFID system is interfaced with it Readers in RFID library are used in the following:

- Conversion station: where library data is written to the tag
- Staff workstation at circulation: used to charge and discharge library materials
- Self check-out station: used to check out library materials without staff assistance
- Self check-in station: used to check in library materials without staff assistance
- Exit sensors: to verify that all material leaving the library has been checked out
- Book-drop reader: used to automatically discharge library materials and reactivate security
- Sorter and conveyor: automated system for returning material to proper area of library.
- Hand-held reader: used for inventorying and verifying that material is shelved correctly.

Antenna

The antenna produces radio signals to activate the tag and read and write data to it. Antennas are the channels between the tag and the reader, which controls the system's data acquisitions and communication. The electromagnetic field produced by an antenna can be constantly present when multiple tags are expected continually. Antennas can be built into a doorframe to receive tag data from person's things passing through the door.

Server

The server is the heart of some comprehensive RFID systems. It is the communications gateway among the various components .It receives the information from one or more of the readers and

exchanges information with the circulation database. Its software includes the SIP/SIP2 (Session Initiation Protocol), APIs (Applications Programming Interface) NCIP (National Circulation Interchange Protocol) or SLNP necessary to interface it with the integrated library software but no library vendor has yet fully implemented NCIP approved by NISO (Koppel, 2004). The server typically includes a transaction database so that reports can be produced.

Using Process in RFID Systems

A RFID system will consist of two basic parts – a reader and the tags. The reader performs several functions, one of which is to produce a radio frequency magnetic field by means of an antenna. This field provides the power necessary to activate the RFID tag. In the case of passive tags (without an internal battery) the inbuilt antenna gathers the energy present in the magnetic field and converts it to the electrical energy which powers the embedded integrated circuit. Thus, the memory contents of the circuit (the tag information) are transmitted by the tag's antenna. The electromagnetic signal from the tag is picked up by an antenna within the reader and then converted back into an electrical form. The reader's electronics further process the tag's signal, demodulating the original data stored in the tag memory. Once this data has been demodulated, a microcomputer within the reader can perform error checking and data validation, along with further decoding and restructuring for transmission in the format required by the host computer system. In case of active RFID tags, a miniature battery provides the power supply for the integrated circuit. When interrogated by the reader, this circuit broadcasts a signal that identifies itself to sensitive reader detection and data transmission circuits. This allows the active tag to broadcast its data at a considerably greater distance than its passive counterpart Potential applications for RFID may be identified in virtually every sector where data are collected. Over the past few years, RFID has begun to move from its early, experimental phase into a mature and proven technology; its inclusion in major consumer applications underlines this. RFID systems may be roughly divided into four groups, according to their applications:

- EAS (Electronic Article Surveillance) systems;
- Portable Data Capture systems;
-Networked systems;
- Positioning systems.

Electronic Article Surveillance systems are typically single-bit systems used to sense the presence or absence of an item. The basic use for this technology is in retail stores, where separate items are tagged and large antenna readers are located at each exit of the store to detect unauthorized removal of the item as in the case of a theft, for instance.

Portable data capture systems typically contain portable data terminals with an embedded RFID reader, and are used in applications where a high degree of variability in sourcing required data from tagged items may be exhibited.

Networked systems applications can generally be characterized by fixed-position readers deployed within a given site and connected directly to a networked information management System. The tags are usually positioned on moving or moveable items.

Positioning systems use tags to enable automated location and navigation support for guided vehicles. RFID technology is a good example of a technology which assists in the logistical tracing of items.

RFID technology works at the forefront of data circulation within an organization. In this respect, a decision to use it will inevitably influence data management practices within the organization.

Libraries use RFID tags on books and other items to provide identification during check-out, check-in, inventory, and for theft deterrence. Benefits of adoption may include:

- Reduction of staff manual processes and errors;
- Reduction of staff and patron time spent in finding items;
- increased customer satisfaction and access to more items as the fast RFID check-in process quickly clears their accounts; and
- enhanced customer experience through fast and private self check-outs.

While costs continue to decrease due to mass adoption, current RFID implementations require a considerable initial investment and ongoing expense. While there is a dearth of both anecdotal and published reports on return on investment, the rationale for implementation today is based on the following criteria, including:

1) Percentage of staff time spent on check-out,
2) Percentage of staff time spent on check-in,
3) volume/percentage of check-outs handled by staff versus patrons,
4) increase in check-outs handled without additional staff,
5) Speed and accuracy of inventory,
6) Accuracy of check-in,
7) Worker's compensation costs from repetitive strain injuries, and
8) Customer satisfaction with check-out and check-in processes.

Typical library processes where the technology can be applied are considered:

- Check in
- Check out
- Security (anti-theft)
- Inventory management, including assets management

For the initiation of the project the management of the library decides to cover the first three of these, with a view to incorporating inventory management in the future. The library has to choose between a numbers of available systems. This process is easier now than in the past, as the library management can consult peers. The experience of other libraries shows that tagging of similarly sized collections can be achieved without a need for additional employees.

The library organizes its new system as follows:

1. A sensor is located at the entrance/exit. It registers immediately any books which are not checked out. If an attempt is made to steal a book, the information system reports immediately details of the offending item, as the tags combine security bits with identification data.
2. A staff service station is placed at the lending desk. It is connected to the library database which is used for book check-outs and returns. This station is used by visitors of the library who are not yet familiar with the new system. In the long-term it will be considered whether this workplace should be used only for these purposes, or whether the staff member will have to take on additional duties. Such a staff service station is also extensively used when applying RFID tags to books.
3. There is also a self-check-out station for visitors who would prefer to use the new system. This consists of a computer terminal with a touch screen and an RFID reader which can read the visitors' ID cards and check their books out. A facility to print receipts is also included.
4. Finally, the staff service station is used for the initial tagging.

The library management also has to decide on procedures for work in the new environment.

A procedure for placing RFID tag on a library book which already has a barcode might be organized as follows:

1. Put tag in tag programmer machine;
2. Read barcode label with scanner;
3. Verify correct barcode using the computer system;
4. Remove backing from tag and put tag in book;
5. Put cover label over tag.

The setting up of each stage of implementation may involve a significant amount of work, but several factors may ease this burden, including:

- There are people in a number of libraries who have the practical experience how to organize it;
- The tasks which have to be performed are routine, and easily described in formal procedures;
- Quality control and performance criteria can be formulated relatively easily.

For all these reasons, the library management

considers that the benefits more than compensate the required effort.

Limitations of RFID Technology

The following technological limitations have been proposed as reasons why consumers should not be concerned about RFID deployment at this time.

1. Read-range distances are not sufficient to allow for consumer surveillance.

RFID tags have varying read ranges depending on their antenna size, transmission frequency, and whether they are passive or active. Some passive RFID tags have read ranges of less than one inch. Other RFID tags can be read at distances of 20 feet or more. Active RFID tags theoretically have very long ranges. Currently, most RFID tags envisioned for consumer products are passive with read ranges of under 5 feet.

2. Reader devices not prevalent enough to enable seamless human tracking.

The developers of RFID technology envision a world where RFID readers form a "pervasive global network" It does not take a ubiquitous reader network to track objects or the people associated with them. For example, automobiles traveling up and down Interstate 95 can be tracked without placing RFID readers every few feet. They need only be positioned at the entrance and exit ramps.

3. Limited information contained on tags.

Some RFID proponents defend the technology by pointing out that the tags associated with most consumer products will contain only a serial number. However, the number can actually be used as a reference number that corresponds to information contained on one or more Internet-connected databases. This means that the data associated with that number is theoretically unlimited, and can be augmented as new information is collected.

4. Passive tags cannot be tracked by satellite.

The passive RFID tags envisioned for most consumer products do not have their own power, meaning they must be activated and queried by nearby reader devices. Thus, by themselves, passive tags do not have the ability to communicate via satellites. In addition, active RFID tags with their own power source can be enabled with direct satellite transmitting capability. At the present time such tags are far too expensive to be used on most consumer products, but this use is not inconceivable as technology advances and prices fall.

5. High cost of tags makes them prohibitive for wide-scale deployment.

RFID developers point to the "high cost" of RFID tags as a way to assuage consumer fears about the power of such tags. However, as technology improves and prices fall, it is predicted that more and more consumer products will carry tags and that those tags will become smaller and more sophisticated. It is predicted that the trend will follow the trends of other technical products like computers and calculators.

Cost of RFID

The cost of RFID technology, a small library of 40,000 items should plan on a minimum budget of Rs. 20, 70,000/- for an RFID system without book drop readers, or patron self-charge/discharge.

Smart Card – Biometrics

A smart card is typically a device containing an embedded integrated circuit that can either be a micro-controller (MCU) with internal memory or a memory chip on its own. They can have a contact interface, a contact less interface or a combination of both on one card. Smart cards have the unique ability to store large amounts of data, carry out their own on-card functions and interact intelligently with a smart card reader. Smart card technology conforms to international standards.

A biometric - smart card protects biometric data and provides a reliable solution where there are privacy concerns. Fingerprints are an ideal credential for logical access control to computer networks and fingerprint templates never leave a smart card unprotected.

Integrating a biometric sensor into a smart card reader makes sense because it is more convenient to combine a smart card reader with a fingerprint scanner in one integrated device. Fingerprint sensors in smart card readers

enhance security by bringing the biometric sensor physically closer to the smart card system. In case of a "match on a card" (MOC) system, they stay inside the card from the time of first enrollment.

There are three factors in this authentication process: smart cards provide the "something you have" factor; the "something you know" is usually a PIN that must be entered to access a card; and, integrating a fingerprint scanner into a smart card reader increases security by adding "something you are" to the authentication process.

Smartcards are ideal to store templates, make them portable and validate the identity of the card holder. Those templates can either be matched on the host system, on an intelligent smart card reader, or on the card its self via match on card (MOC).

Use of Smart Card

Smart card technology is used in applications that need to protect personal information or deliver secure transactions. Contact smart card technology provides similar capabilities but does not have the RF interface that allows contact less smart cards to be conveniently read at a short distance from the reading mechanism. There is an increasing number of contact less smart card technology implementations that capitalize on its ability to enable fast, convenient transactions and its availability in form factors other than plastic cards – for example inside of a watch, key fob or document. Current and emerging applications using contact less smart card technology include transit fare payment cards, government and corporate identification cards, documents such as electronic passports and visas, and contact less financial payment cards. The contact less device includes a smart card secure microcontroller, or equivalent intelligence, and internal memory and has the unique ability to securely manage, store and provide access to data on the card, perform complex functions and interact intelligently via RF with a contact less reader. Applications that require the highest degree of information and communications security use contact less smart card technology based on an international standard that limits the ability to read the contact less device to approximately 4 inches (10 centimeters). Applications that need longer reading distances can use other forms of contact less technologies that can be read at longer distances. Smartcards have finally entered the public domain and our used in a variety of applications, sometimes without the use of being aware that they are actually using a smartcard. The smartcard itself is simply a plastic card with an integral embedded chip. This provides a degree of tamper resistance and security for the information held within the card. Smartcards may be categorized into two primary types, memory cards or microprocessor cards. Memory cards simply store data and allow that data to be subsequently read from the card. Microprocessor cards on the other hand, allow for additions and deletions to the data, as well as various manipulations and processing of the data. The smartcards may be further categorized into contact or contact less cards. Contact cards required the card to be physically inserted into a smartcard reader. Contact less cards enable the card to be read without physical contact via a radio frequency link with an antenna embedded into the card. There is in fact another type of card called a combination card which combines both contact and contact less technology. This allows for the card to be read by either type of card reader, alternatively, to be read by both techniques at the same time, enabling a higher degree of security. Applications using contact less smart cards support many security features that ensure the integrity, confidentiality and privacy of information stored or transmitted, including the following:

- Mutual authentication. For applications requiring secure card access, the contactless smart card-based device can verify that the reader is authentic and can prove its own authenticity to the reader before starting a secure transaction.
- Strong information security. For applications requiring complete data protection, information stored on cards or documents using contactless smart card technology can be encrypted and communication between the contactless smart card-based device and the reader can be encrypted to prevent

eavesdropping. Additional security technologies may also be used to ensure information integrity.

- Strong contactless device security. Like contact smart cards, contactless smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance.

  Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks.

- Authenticated and authorized information access. The contactless smart card's ability to process information and react to its environment allows it to uniquely provide authenticated information access and protect the privacy of personal information. The contactless smart card can verify the authority of the information requestor and then allow access only to the information required. Access to stored information can also be further protected by a personal identification number (PIN) or biometric to protect privacy and counter unauthorized access.

- Strong support for information privacy. The use of smart card technology strengthens the ability of a system to protect individual privacy. Unlike other technologies, smart card-based devices can implement a personal firewall for an individual, releasing only the information required and only when it is required. The ability to support authenticated and authorized information access and the strong contactless device and data security make contactless smart cards excellent guardians of personal information and individual privacy.

A "smart" card, which is an RFID card with additional encryption, is an alternative to merely adding an RFID tag to a patron card. That would make it possible to make it into a "debit" card, with value added upon pre-payment to the library and value subtracted when a patron used a photocopier, printer, or other fee-based device, or wished to pay fines or fees.

Limitations of Smart Card Technology

Smart Cards are prone to security risks at the user level. If Smart Card is to be held at every library in the security risk will be present at each of these libraries and such risks will be both technical and manpower based. It is also a myth to consider that Smart Cards are hacker proof. The limitations of Smart Cards would be largely academic and un productive if a proper alternative was not available.

As a smart card application development is a costly undertaking, typically performed by the large corporations that stand to profit from the sale of millions of smart cards. History has shown that in order for a new technology to blossom, "grass roots" application development is required. That is, a technology will not truly become a pervasive technology unless and until it is infused with the vitality and creativity of individual programmers and small development companies.

Costs and Benefits of Smart Card

There are varieties of Smart Cards from 1 Kb simple storage cards to 4 MB communicating and processing cards. The reader and writer costs also vary according to the type of cards. Current smart cards, made by Gem Plus, and Bull CP8, among others, range in price from less than Rs. 45/- to about Rs. 900/-. This cost includes the silicon, OS, module (the chip package providing the connections to the outside world), and plastic card.

A stored-value card is attractive because it reduces the amount of change the shopper carries and can be used in small-value transactions where credit cards or checks are less desirable. Retailers prefer stored value because it increases small cash transactions, which financial institutions currently avoid because the overhead on credit cards or checks are too high for profit.

Comparing RFID Tags and Smart Card Technology

Radio frequency identification (RFID) tag technology is used in applications that identify or track objects and smart card technology is used in applications that identify people or store financial or personal information. Applications

most often have differing requirements in their use of RF technology, with RFID tag and smart card technologies providing very different capabilities.

Conclusion

Here in this paper, a glimpse of the major aspects related to RFID technology and Smart Card use in a library is presented. RFID system is a comprehensive system that addresses both the security and materials tracking needs of a library. RFID in the library is boon if guidelines and benchmark practices are followed religiously in that it scales up effectiveness and efficiency by speeding up book borrowing and inventories and frees staff to do more user-service tasks. Smart card technology is used in applications that need to protect personal information or deliver secure transactions. Current and emerging applications using contactless smart card technology include transit fare payment cards, government and corporate identification cards, documents such as electronic passports and visas, and contactless financial payment cards these technologies save money and quickly give a return on investment.

Library professionals face many challenges in digitization of libraries like resource crunch, resistance to change, apathy of higher management etc. However, of late things have started to change and for better. With growing awareness and increasing technological advancements it is aptly observed that the future belongs to digital libraries.

References

1. Ashim A Patil, I-TEK RFID Based Library Management Suite. White Paper Series, Infotek Software & Systems P Ltd, Pune, India. 02, April, 2004.
2. American Library Association. Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles. Adopted by the ALA Council. http://www.ala.org/ala/oif/statementspols/ifresolutions/rfidresolution.htm (January 19, 2005).
3. Ayre, Lori Bowen, The Galecia Group. Position paper: RFID and Libraries, 2004.
4. Bednarz, A. (2004, May 3). RFID everywhere: From amusement parks to blood supplies. Network World Fusion. Available at August 4, 2004 http://www.nwfusion.com/news/2004/0503widernetrfid.html. (August 4, 2004).
5. Berkeley Public Library. (n.d.). Berkeley Public Library: Best practices for RFID technology. Available at August 5, 2004 http://berkeleypubliclibrary.org/BESTPRAC.pdf. (August 5, 2004).
6. BIBLIOTHECA RFID Library Systems AG (2003) RFID Technology Overview.Available at www.bibliotheca-rfid.com, 2003.
7. Boss. R. W. (2003). RFID technology for libraries [Monograph]. Library Technology Reports. November-December 2003.
8. Garfinkel, S. (2002, October). An RFID bill of rights. MIT Technology Review. http://www.simson.net/clips/2002.TR.10.RFID_Bill_Of_Rights.html. (July 8, 2004).
9. Givens, B. RFID implementation in libraries: Some recommendations for "Best Practices." Summary of presentation to the ALA Intellectual Freedom Committee of the American Library Association at ALA Mid-Winter, San Diego, California. Available at http://www.privacyrights.org/ar/RFID-ALA.html. (January 10, 2004).
10. Garfinkel, S. (2002, October). An RFID bill of rights. MIT Technology Review. http://www.simson.net/clips/2002.TR.10.RFID_Bill_Of_Rights.htm. (July 8, 2004)
11. Hesseldahl, A. (2004, July 29). A hacker's guide to RFID. Forbes.com. http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html. (August 6, 2004).
12. Kirschenbaum, et. al. "How to Build a Low-Cost, Extended-Range RFID Skimmer", e-print archive 2006: 054.
13. Koppel, T. (2004, March). Standards in Libraries: What's Ahead: A Guide for Library Professionals About the Library Standards of Today and the Future. The Library Corporation. http://www.tlcdelivers.com/tlc/pdf/standardswp.pdf. (August 5, 2004).
14. Molnar, D., Wagner, D. A. Privacy and security in library RFID: Issues, practices and architectures. Available at www.cs.berkeley.edu~dmolnar/library: 2004.
15. P.K. Kumbargoudar & Mamata Mestri (May 2-12 2002). Digital Libraries : Indian Scenario; 2002: May 2-12.
16. "RFID for Libraries" at URL: http://www.biblio-tech.com/html/rfid.html as on 01-03-2008
17. "RFID Survival". http://www.rfidsurvival.com/contact.html. (February 25, 2008).
18. "RFID Technology". http://www.bartronicsindia.com/rfidtech.htm (February 25, 2008).
19. "RFID 2.0" available at http://www.dqindia.com/content/top_stories/2006/106040501.asp (February 25, 2008).
20. Sarma, E. S. Weis, S. A., Engels, D.W. White paper: RFID systems, security & privacy implications. Cambridge, MA: Massachusetts Institute of Technology, AUTO-ID Center: 2002
21. Schatz, B., et al. (1999). "Federated Search of Scientific Literature: A Retrospective on the Illinois Digital

Library Project." IEEE Computer, 32(2), 51-59. Also: Arms, WilliamY. , et al. (1999). "The DLib Test Suite: Testbeds for Digital Libraries Research," D-Lib Magazine, 5(2) [online]. http://www.dlib.org/dlib/february99/arms/02overview.html. March 13, 2000).

22. Sudarshan S. Chawathe ,et al, "Managing RFID Data" in the Proceedings of the 30th VLDB Conference, Toronto, Canada: 2004.

Scholarship for Females for Professional Courses

The **Samarpan Trust** (Regd.) proudly announces **Shri Subedar Memorail Scholarship** for females. Apply with Rs.100/- Demand draft favouring **Samarpan Trust** payable at Delhi as a registration charges. Terms and conditions to apply for the scholarship are as given below:

1. Four scholarships are available and each will be Rs.2500. Only female students are eligible to apply.
2. Scholarships are available only for professional courses.
3. Scholars will be selected on the basis of the percentage of marks, position in competition for the respective course, family income and age of the candidate.
4. Applicant should submit a copy of all the certificates those submitted to the respective institution at the time of admission.
5. The application should be forwarded through your principal/head of the Department along with a letter certifying that the applicant is not being supported by any other source.
6. Applicant should submit an article, matter must not exceed 10 printed pages about why the scholarship to be granted only female candidates along with two full size and two passport size photographs. Your article will be published with photographs in all 12 journals (see our website: www.ijfmp.org) of World Information Syndicate, Delhi if you selected for scholarship.
7. The scholarship committee reserves all the rights to accept, alter or reject the application/ scholarship without assigning any reason and prior notice. The committee accepts no responsibility of the statements and opinion expressed by the contributors. No payments are made to the contributors.
8. All legal disputes subject to Delhi jurisdiction.

For further information Please write to

The Chairman
Samarpan Trust (Regd.)
1/50, Sector-II, Rajendra Nagar
Sahibabad - 201 005, Ghaziabad, U.P. (India)
Phone: 91-120-4153490, 9212471261, Fax: 91-11-48042168
E-mail: samarpantrust@vsnl.net, Website: www.samarpantrust.org