

Smart Library System

Khan Ziya ¹, Mujibur Rehman G.R. ², Shaikh Swaleha ³, Najibullah Shaikh ⁴

^{1,2,3}B.E Students, Department of Information Technology, M.H.Saboo Siddik College of Engineering, Mumbai University, Mumbai, India.

⁴Assistant Professor, Department of Information Technology, M.H.Saboo Siddik College of Engineering, Mumbai University, Mumbai, India

Abstract— Library management system is an aspect or branch of information management system that keeps the records of both the library users, books in the library and the activities that is going on in the library, activities like borrowing books and returning books.

Information management in general is the collection and management of information from one or more source and distribution of the information to one or more audience. This sometimes involves those who a stake in or right to that information. Management means the organization of and control over the structure, processing, and delivery of information. In short information management entails organizing retrieving acquiring and maintaining information. It is closely related to and overlapping with the practice of data management.

I. INTRODUCTION

The Library Management System is designed to provide one systematic System for user to search the available booklist in library and he/she can also reserve the book. And user would be able to download the e-books .Basically the system will be created using Android SDK. The LMS provides different application methods for different users i.e. regular user and the administrative user. Regular user can be any student or registered person and the administrative user is the librarian or staff of library who are responsible for issuing the books and managing user's Account. Only Administrative user's are allow to access the restricted data. The LMS will store all the books and members information that consist book no, Book title, book

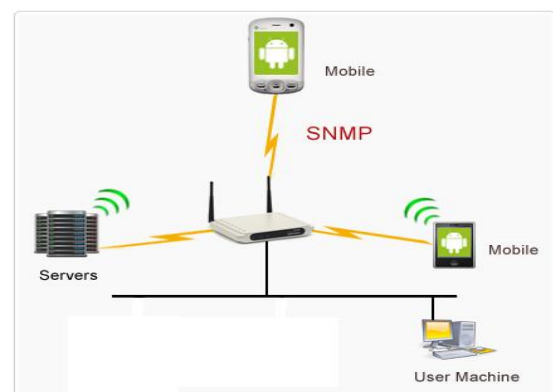
author and racks of the system Database. The LMS also provide search function to help users to find the books by book title. Search function will search through the books Database to look for the book and view where the book is situated. For the Administrator user, only librarians have access to view or edit data from the system database. Admin user will handle Administrative functions such as create new LMS user account and also manage it.Admin can also perform the function of issuing the books and updating database. To perform all the functions Admin has to enter valid id and password.

Regular user should first get registered to the database of library through the LMS application(Smart Library System).

II. SLS & ITS COMPONENTS

A. SLS Data Transactions

SLS is defined as exchange data which take place over the Internet primarily use digital technology. These data transaction including searching, reserving, downloading e-books, registering, user



information. In earlier LMS there was no use of Mobile Applications which uses database of LMS through network. The LMS will provide information from the database through the SLS via network. This can be done through the access of HTTP communication. For HTTP communication we need to create one web page. This web page will act as the communication medium for the LMS and SLS.

With the help of HTTP communication the SLS will be available 24x7 online and much more convenient and cheaper.

B. SLS System Components

There are four major components of SLS, the User Account, Security System, Buffer, Communication Gateway and the Database.

User account: Library authorized account users will be allowed to perform the functions on the SLS. This application first need to get registered the user's Mobile number to the database of LMS. Once the Mobile number is registered then the LMS will notify each event to the SLS. After registration the can be able to perform the searching of books, reserving of books, and checking the status and the history of the user.

Secure server connection: 'https://' connects to a special computer which encrypts confidential ordering data for clients protection. The "s" on the end of https in the URLs or the lock in the lower part of a browser which will look something like this are signs that shows that the page is secured if ordering information is not sent through a secure server it can be intercepted by computer hackers.

Buffers: Software which facilitate reserving books if user reserve the books then the book will be reserve for that user for 4 hours. So within 4 hours user have to visit library and issue that book. If he/she fails to do it the reservation for the book of the user will be cancelled after the 4 hours. Between 4 hours the books will be in the buffer state means those books will not be shown available for other users.

Database: Database is required to store the data in the system. Database consist of different tables like books table having details about the books book-id book-name, book-authors, book-reference number. Table of students having details about the students like student-name, Mobile No, Student id, Address, Branch, year.

Database of Books is for both SLS (Smart Library System) and LMS (Library Management System).

III. E-SECURITY ISSUES AND TRUST

"A security threat has been known as a situation, or event with the potential to effect economic adversity to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse Security, then, is the protection against these threats. With regard to the security of SLS applications, it is useful to distinguish between client-side security issues, server-side security issues, and transaction security issues.

A. Client-side Security Issues

From the user's point of view, client-side security is typically the major concern. In general, client-side security requires the use of traditional computer security technologies, such as proper user authentication and authorization, access control, and anti-virus protection. With regard to communication services, the client may additionally require server authentication and non-repudiation of receipt.

A.1 Application Side Security Issues:

The application of SLS should provide a security such that unauthorized user should not have access to the application. User should not give the access to use his/her SLS application to another users.

B. Server-side Security Issues

Contrary to that, server-side security is typically the major concern from the service provider's point of view. Server-side security requires proper client authentication and authorization, non-repudiation of origin as well as reliability and availability.

C. Transaction Security Issues

Transaction security is equally important for both the client and the server side. Transaction security requires various security services, such as data authentication, access control, data confidentiality, data integrity, and non-repudiation services.

The enormous increase in the uptake of ecommerce has led to a new generation of related

security threats, but SLS must meet four integral requirements as defined below–

Confidentiality: Data is protected and cannot be accessed during transition.

Integrity: The system does not corrupt information or allow accidental changes to information except by an authorized agent.

Availability: The computer system's hardware and software maintain to work efficiently and the system is able to recover quickly and completely if a disaster happen.

IV. THREATS CATEGORIZATION AND SOLUTION STRATEGIES

Threats	Motives/Goals	Methods	Security Policies
<ul style="list-style-type: none"> • Employees • Malicious • Ignorant • Non-employees • Outside attackers • Natural disasters • Floods • Earthquakes • Hurricanes • Riots and wars 	<ul style="list-style-type: none"> • Deny services • Steal information • Alter information • Damage information • Delete information • Make a joke • Show off 	<ul style="list-style-type: none"> • Social engineering • Viruses, Trojan horses, worms • Packet replay • Packet modification • IP spoofing • Mail bombing • Various hacking tools • Password cracking 	<ul style="list-style-type: none"> • Vulnerabilities • Assets • Information and data • Productivity • Hardware • Personnel

A. Threats Categorization

A hacker can target different points during an Data transferring through the http communication such as:

- Trick an online
- Sniff the network connection between an ecommerce website server and a shopper
- Attack a website's server

Tricking an online: Hackers will often get access to sensitive information. They try to access the information during login session by hacking the system. The data they usually steal includes the user's usernames and their passwords, hijacking into user databases of System, and using confidential and personal information belonging to the user.

Phishing is a common method to trick a user; the attacker sends an e-mail message pretending it is from a trusted web. The message connects the recipient to another website, which is "spoofed" and looks like original web but is not genuine. It asks the user to update his/her login and personal

data such as details of the user's personal details. By doing this, malicious people are able to steal personal information.

Denial of service (DoS) attacks and Distributed Denial of Service (DDoS) attacks is an example of impact site availability. It is a well-known strategy attacker's use in SLS with a malicious intent. Use of a few machines 'spoofing' where many computer systems are hacked with software known as "bot" which is in a robot form. The software simultaneously connects to a server website. The number of concurrent connections is so

numerous that it overloads the SLS servers making it hard for them to cope and finally they fail.

C. SLS Security Solutions

A company-wide understanding of SLS security features, methods and threats will enable both users and security administrators to trust the system that they are working with. If accurate methods are utilized to secure and use a system, it is almost impossible for an unauthorized user to gain access. At the same time, the multitude of hacking and cracking applications available can cause a serious threat to SLS applications. Hence it is essential to understand security risks and find the best solutions to minimize the threats they impose. Fig. 1 shows available defenses against attacks.

Education: It is important to raise the awareness of web security. Educate people of how to choose strong password and keep their password confidential, is an easy way to minimize the risk of hacking attack. Users need to use good judgment when giving out information, and have

knowledge about possible phishing schemes and other social engineering attacks.

Secure Socket Layer (SSL): This is the most common security method, public key encryption; it ensures confidentiality, authentication, data integrity, and non repudiation of origin and return. The technology used encloses transactions into encrypted envelopes and electronically seals where only people with the encryption key can view the contents of the envelopes that are sent securely over the internet. However, partners must install the same software and coordinate their upgrade of their systems. Electronic Data Interchange(EDI) are used as wrappers to alter conventional EDI software into secure formats, such as Secure socket layer (SSL) encryption protocol which are good in protecting online data transfer. Sensitive data, such as login details, books details, etc, should be in encrypting form before transmission across the open internet via email or the web. A 128-bit encryption protects the data from decryption by hackers easily in case they intercept it along the network. Digital certificates can be used here to encrypt email or establish a secure HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.

the main advantage of this application is its Mobility. So this application will help a user a lot

REFERENCES

1. "Open Source Library Managemnt System Software." Sangsuree Vasupongayya, Patt Emmawat.
2. "Management of AJAX-based Digital Library System" Suraj Subrun
3. "The Beginning of Automation in the University of Toronto Library" Calvin Gotileb, Carole Moore
4. "Evaluating functionalities of eCommerce websites for emigrants Célia Ferreira, Ramiro Gonçalves
5. "A History of computer Application in Libraries: Prolegomena" W. Boyd Rayward

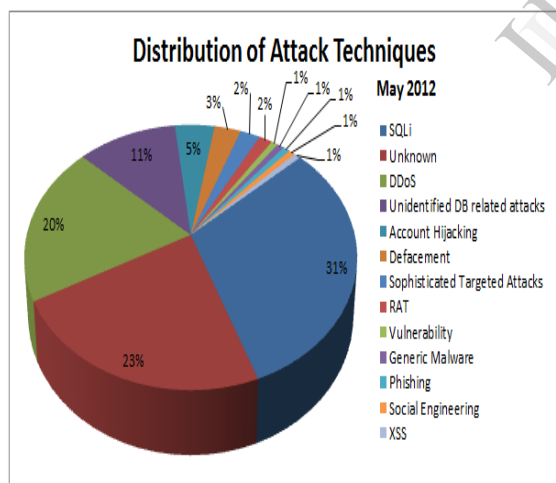


Fig 1: Different types of Attacks.

VI. CONCLUSION

As we all know that today's world is an Smart Phone Era and Online environment, So we are developing application considering all this in mind. This SLS (Smart Library System) application will help on click access of Library System. One of