Enhancing Security of College Libraries by using Fingerprint along with RFID Embedded ID Cards

Deepak Thambi[1] Ankit Patil[2] Pranay Shah[3] T. Anas Ahmed[4] Prof. Manoj Mishra[5]
[1,2,3,4,5]Department of Electronics & Telecommunication Engineering
[1,2,3,4,5]Atharva College of Engineering/Mumbai University, Maharashtra, India

Abstract— As the number of libraries using Smart library management systems is increasing day by day, there needs to be proper security for protection of books from theft and misuse. Most libraries use either RFID or barcode in their backend. The login procedure to the library is mainly via RFID which can be easily tampered. Other way is through password based setup from PC. By using a combination of RFID and fingerprint, the security of the library can be increased by several levels. This paper demonstrates a way in which how the inclusion of fingerprints will make the library more secure.

Key words: Fingerprint Module, Raspberry Pi, RFID

I. INTRODUCTION

A library is basically a huge collection of books or any source of information material. Security is of utmost importance in college or university libraries as a number of confidential research papers are also kept in them. Also majority of students fail in returning the issued books. The cases of theft is also present. Therefore it is necessary to monitor the entry to the libraries. Most libraries employ a combination of barcodes for identifying books and RFID cards as student login. The use of only RFID as a way of authenticating is the major lapse in security system. Most Smart management systems employ weak security protocols in their RFID card and they can be easily skimmed to a new card, thus spoofing the identity of another user and can obtain access to the system. Even if one library does not contain any confidential research papers which are accessible only by few faculty or students, students can misuse it many other ways.

II. LITERATURE REVIEW

One type of attack which affects RFID is the relay attack. A relay attack is one of the attack which makes use of proximity assumptions in an RFID system. In the paper of Kfir and Wool [2], relay attack involves the use of two communicating devices, a leech and a ghost. The attacker positions the leech physically close to the target RFID device and places the ghost close to a target reader.

Intercommunication between the leech and ghost creates a sort of physical proximity between the target RFID device and the target reader while they may in fact lie very far apart.

P. Kocher, J. Jaffe and B. Jun proposed a paper which gives details about how RFID cards are vulnerable to Power Analysis based attacks. Low end smart-cards are highly vulnerable to Power Analysis based attacks [3] due to their simplicity. Therefore, any claim that an AES candidate is superior because it runs on a low end smart card would be hollow if, in fact, the implementation leaks away its key in a power based attack.

Molnar, Soppera and Wagner [1] proposed a privacy protection scheme using tree structures, keys which are efficient and are allowed to delegate the ability to identify tags. The keys are generated using a hash tree, which is stored in the tag. During each session, the tag generates its own output by calculating the hash tree from the root value. The calculation can be done efficiently through the tree structure

III. PROPOSED ALGORITHM

In the system that we have designed (Fig. 1), a fingerprint scanner and RFID reader is interfaced with a raspberry pi 3B. A LCD panel is also connected which shows the status of the system. The database can be the raspberry pi itself or can be a remotely located server. In that case, the raspberry pi manages the database wirelessly using the on board Wi-Fi chip.

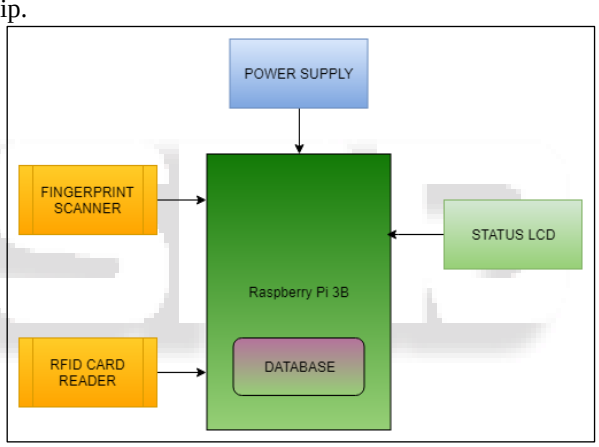

Fig. 1: Basic model

The flowchart (Fig.2) gives a basic view of how the proposed system works. When a student/user enters the library, and wants to make use of library functions like issuing or returning of book, then he/she has to go through the login process as follows (Fig. 2):

The LCD screen shows status "Place card on scanner", the user taps his RFID card on the RFID reader. The data is sent to the raspberry pi, which in turn forwards it to the database. Now the LCD screen shows status as 'scan finger'. The user has to scan his finger which was registered with the system. The data obtained from the RFID card reader and fingerprint scanner is compared and if both are present in the database and if they match, the user is granted access to the library. Now the question arises why RFID is to be used, when fingerprint alone is sufficient for security. The reason is that the RFID chip will be embedded in patrons ID card itself which will be used for other purposes like contactless food vouchers, security doors etc. The card since can be used by anyone, the librarian or the IT department can update the cards without every time requiring the fingerprint of the user.

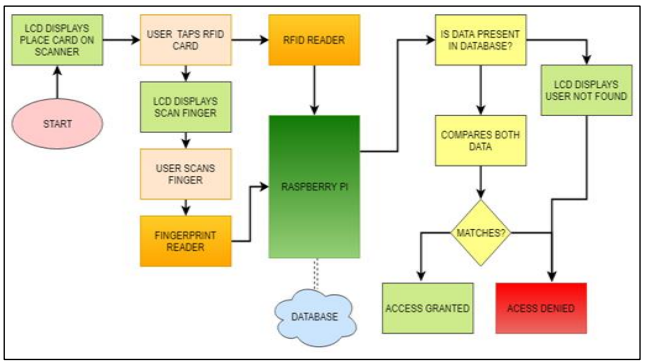

Fig. 2: Flowchart

IV. Related Technology

A. *Raspberry Pi 3B*

The Raspberry Pi Model 3B is a small card sized computing device that in this system is used manage or optionally hold the database.

The need of using this particular board is its more than average computing power which is capable of handling larger database and at about 35 dollars is also economical and can also be used in nonprofit libraries.

B. *Fingerprint module*

Fingerprint module R305 is used as an additional security layer here for user authentication. It is one of the most secure forms of the biometric authentication system and is now commonly used in smartphones the world over. It offers a unique biometric identity key to each user as well as provides additional security to the library.

C. *RFID module*

Key Specification:
Model: RS-232
Power requirements: 7V – 9V DC
Current requirements: <110mA
Communication: RS-232 Serial at 9600 baud (8N1)
Dimensions: 63mm x 98mm x 5mm
Operating temp range: -40° C - +185° C

V. Advantages

- The system overhauls the security of libraries by a great extent in an economical way
- Possibility of implementing in existing libraries and can be used as an add-on in existing smart library systems
- Unique identity to each user which in majority of cases cannot be copied.

VI. Applications and Future Scope

- It can be used in local public libraries also.
- Apart from books, this system can also be implemented in other places like in warehouse management, employee management etc.
- Surveillance camera and IR sensor can be added to further ramp up the security.

VII. Conclusion

Thus in this setup, addition of fingerprint is done by adding fingerprint authentication apart from RFID. This increases the security of system multifold. The system also is implemented in an economical way by using commonly available and cheap development board, in this proposed system we are using a raspberry pi.

References

[1] Molnar, D., Soppera, A., Wagner, D.: A scalable, delegatable pseudonym protocol enabling ownership transfer of rfid tags. Cryptology ePrint Archive, Report 2005/315 (2005)
[2] Z. Kfir, A. Wool, Picking virtual pockets using relay attacks on contactless smartcard systems, 2005, [online].
[3] P. Kocher, J. Jaffe and B. Jun. \Introduction to Differential Power Analysis and Related Attacks". http://www.cryptography.com/dpa/technical/index.html

