



## **Torry Harris Business Solutions**

### **Biometric Fingerprints Based Radio Frequency Identification**

**Author: Senthilkumar Chandramohan**

[www.thbs.com](http://www.thbs.com)

**Further Inquiries and Feedback:** [torry\\_harris@thbs.com](mailto:torry_harris@thbs.com)

**Notices:**

The contents of this paper are protected by copyright. No part of this paper may be reproduced or used in any form by any means without the prior written authorization of Torry Harris Business Solutions, Inc.

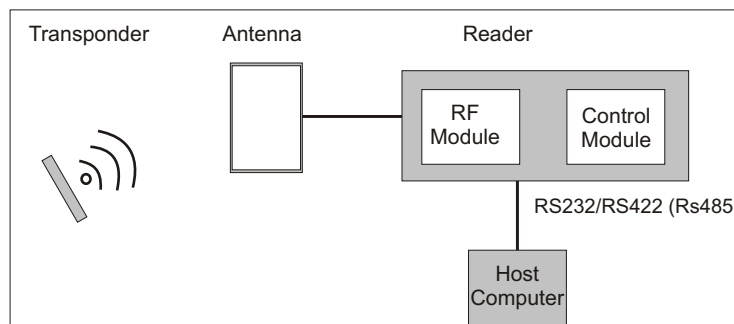
## 1. Introduction

In recent years, Radio Frequency Identification procedures have become very popular in various aspects of life. Radio frequency identification, or RFID, is a generic term for technologies that use radio waves to automatically identify people or objects. There are several methods of identification, but the most common is to store a serial number that identifies a person or object. In most of the cases the serial number is usually the roll number of the person or the serial number of the associated object. The most notable disadvantage of such an automated identification system is their inability to avoid the miss use of RFID tags.

In this write-up we propose a method to incorporate the Biometric Fingerprint Authentication technology with the existing Radio Frequency Identification systems. The goal of our work is to develop a more reliable Radio Frequency Identification system, which can prevent the misuse of tags. In the proposed system we replace the serial number with codes similar to EPC. We use the data obtained by processing the user fingerprint for generating the mentioned codes.

## 2. Radio Frequency Identification

**At its most basic level, RFID is a short-range radio communication to uniquely identify objects or people. RFID systems include electronic devices called transponders or tags, and reader electronics to communicate with the tags.**



**Fig. 1.** Radio Frequency Identification System. This figure shows the various RFID system components. An RFID tag consists of a microchip attached to an antenna. Tags are either active or passive. An RFID reader serves the same purpose as a barcode scanner. The reader captures the RF waves from tags and converts them into digital data. The RFID reader handles the communication between the Information System and the RFID tag. An RFID antenna activates the RFID tag and transfers data by emitting wireless pulses.

## 3. Biometric Fingerprint Authentication

Ridges and valleys form fingerprints. These ridges and valleys take unique form one person to another. Fingerprint authentication systems use features like ridge endings, ridge bifurcation, islands, enclosures etc. These features of the fingerprint are called as the fingerprint minutiae. Biometric authentication system on scanning and processing the fingerprint extracts the minutiae features from the fingerprint. Minutiae extracted are stored as templates in the database. Whenever authentication is required minutiae are extracted from the scanned fingerprint and compared with the stored templates in the database. The notable disadvantage in this highly effective and secured authentication system is the storage space required for storing the templates. In the proposed system the fingerprint minutiae templates are converted into unique integers and these integers are stored in the database instead of fingerprint minutiae templates. During authentication the same algorithm is used to process the scanned fingerprint and the unique integer representing the scanned fingerprint is compared with those in the database with an allowed margin of deviation. For converting the minutiae templates to unique integers we plot the minutiae position in a two dimensional plane and generate a relative common reference point, which remains same irrespective of rotation of the fingerprint. The distance between this reference point and all the minutiae points are obtained and summed up. This summed up value, on scaling linearly results in unique integers to represent fingerprints.

#### **4. Proposed EPC format for Biometric RFID**

Biometric RFID tags stores data obtained using the unique integers generated by fingerprint authentication system. Proposed data format to be used in biometric RFID system environment is similar to the EPC format. The data to be stored in the RFID tag to represent a human is proposed to have continent code, country code, state code and scaled unique integer from fingerprint processing. The scaling can be reader specific giving way for encryption and privacy for the user. This system by using the unique integers obtained from fingerprint processing incorporates the reliability of fingerprint authentication with the RFID technology.

#### **5. Is Biometric RFID a more reliable option?**

Biometric RFID system proposed above is more reliable compared to the existing RFID technology. This greatly avoids the misuse of Radio Frequency Identification Tags. Automated entry points to highly restricted environments can use both the RFID and fingerprint authentication for authentication where as the other access points in same the environment can use RFID technology. By using Biometric RFID we avoid misuse of RFID tags and also enjoy using the contact less RFID authentication system at most of the access points. Since tags store data with specific scaling, privacy is ensured for the users. This makes RFID technology a more reliable one to be used and extends usage of RFID technology at highly secured environments and for human tracking.

#### **6. Enhanced Applications**

This approach introduces a fingerprint authentication, which uses fingerprint templates in integer formats rather than collection of minutiae points. This drastically reduces the memory needed to store a fingerprint template and also results in a faster fingerprint authentication algorithm. Apart from contributing to the biometric fingerprint authentication by incorporating the results from fingerprint processing in RFID technology, RFID system is made a more reliable technology. Applications involving human such as human tracking and monitoring systems are made more secured increasing the privacy of the user.