ISSN: 2321-8169
042– 045

RFID based security system for Banks

Jyoti Jhawar
Department of Computer Science
J. D. College Of Engineering
Nagpur, India
jhawar_jyoti@rediffmail.com

Amol G. Muley
Department of Computer Science
J. D. College Of Engineering
Nagpur, India
amolmuley300@rediffmail.com

Abstract— Radio frequency identification, or RFID, is an emerging technology that wirelessly transmits an identification number from a small inexpensive device, called a tag, to devices, called readers, capable of communicating with the tag. The technology enables a single reader to inventory hundreds of tagged items per second, wirelessly and without line-of-sight; tags can remain in enclosures or packaging materials. This paper surveys the various areas where RFID has been implemented in various countries & proposes a system which can be used / implemented by Banks, for various security measures. The CCTV cameras which are used in the banks, for the security purposes do not prove much efficient to stop forgery, or robbery. There are some recent cases in India where some internal officer made duplicate locker keys and then used it for robbery, it came to notice only when these lockers were opened. The concept of this proposal is RFID embedded locker keys. These keys can be used along with personal identification of the locker holder like figure print or eye retina scan etc. The officers who enter the locker room their RFID enabled strong room keys also will be attached to their biometric authentication, so the system can restrict and buzz an alarm when anyone without authentication tries to enter. Also this could help to track the list of officers for investigation in case of robbery. The time and date of entry and exit can also be noted. Applied properly this system will help to improve the security of the Banks.

Keywords*- RFID Tag, Reader, Biometric Authentication*

*****

I. INTRODUCTION

Almost in all the nationalized banks in India; lockers are provided to the customers where they can keep their valuables. These lockers work on two keys; one key is with customer and the other is master key of the lockers which is with the bank. The 'Strong Room' lock also needs two keys, which are with Head cashier and Branch manager. There are some recent cases in India where some internal officer made duplicate locker keys and then used it for robbery, it came to notice only when these lockers were opened. In some of the robbery cases the robbers dig a tunnel and cut the lockers / ATM machine. These all cases points' to the following loop holes in the present system.

- Almost all banks have manual authentication of customers. Yet, non authorized family members can be allowed (if it suits to the conscious of the bank officer).
- The Bank officers can easily duplicate the keys for future misuse.
- If the keys are stolen the whole lockers are insecure.
- No security of lockers/ ATM is assured if robbers cut them.

This paper focuses on how to enhance security of Strong Room, Customer Lockers and ATM using Radio-frequency identification (RFID) technology along with Biometric authentication techniques. This paper proposes a system design for this add on security to the bank lockers, strong room.

RFID

An RFID system can be considered a wireless communication system since the reader communicates with the tags by using electromagnetic waves at radio frequencies. RFID systems can be categorized as active and passive systems [3]. In an active system, the tag (i.e. active RFID tag) has its own power source, which is a battery, enclosed in the transponder housing. In passive system, the tag does not have its own power source; instead, it draws power from the reader's radio signals. Passive tags are inexpensive compared to active tags [3]. Every RFID label carries a globally unique read only serial number defined at manufacture. In addition, there is a user definable read–write memory of between 64 bits and 2 kbits [4]. RFID operates in several different radio bands: 0–135 kHz, 13.56 MHz, 433 MHz, 900 MHz, and 2.4 GHz (microwaves) etc. [4].

A typical RFID system consists of three components:

1) An electronic data carrying device, called a transponder or tag;

2) Antennas and readers that facilitate tag interrogation; and

3) Software, called middleware, that controls the RFID equipment, manages the RFID data, and distributes information to other remote data-processing systems by interfacing with enterprise applications [3].

The major advantages of passive RFID tags are it is cost effective and smaller in size. Due to above advantages, it is widely use by inventory tracking technology [3, 4]. Current antenna technology makes it possible for smaller size tags [5].

II. RELATED WORKS

RFID has been widely used for security enhancing, following are some major works done in this area.

1. First work is a door locking system using passive type of RFID tag. This system can activate, authenticate, and validate the user and unlock the door in real time for secure access [1]. A centralized system manages the controlling, transaction and operation task. The door locking system functions in real time as the door open quickly when user put their tag in contact of reader. The system also creates a log containing check-in and check-out of each user along with basic information of user [1].

The major weakness in this system is the door thickness request: 32mm ~ 45mm [1]; which is too small for bank locker and Strong rooms' doors. In most of the banks the door size is of 6-10 inches and these are very heavy with multiple layers of steel sheets. Second drawback is it uses only one RFID card to open the door [1]; where as in the bank's the double security is must.

2. Second work has implemented a bank locker security system based on RFID and GSM technology. This contains door locking system using RFID and GSM which can activate, authenticate, and validate the user and unlock the door in real time for bank locker secure access [2]. In this system the RFID reader reads the id number from passive tag and send to the microcontroller, if the id number is valid then microcontroller send the SMS request to the authenticated person mobile number, for the original password to open the bank locker. If the person send the password to the microcontroller, which will verify the passwords entered by the key board and received from authenticated mobile phone and if these two passwords are matched the locker will be opened otherwise it will be remain in locked position [2].

It is not practically possible to implement this system due to following reasons –

a) If there are no mobile towers, or the tower signals are too weak then system fails. (In India many remote areas don't have mobile towers.)

b) Sending the password over mobiles has its own hacking ricks involved.

c) Delay in the message sending and receiving can occur and even messages can be hacked.

3. Some other security works are on the security of shopping malls, as CCTV doesn't provide much aid to stop the shop-lifters from stealing items in the shop. In those systems a passive RFID tag is attached to each item in the shop and if these items are taken out of shop/mall without bill payment it triggers an alarm warning of the shoplifting [11,12]. The security of the cash section can also be achieved by RFID identity cards (ID) of the employees [12]. These RFID ID card restricts entry of the employees in secured zone where cash and other documents are to be kept [12].

But these systems are also insufficient for bank locker security.

III. PROPOSED SYSTEM

In this paper we propose a system for the security of 'Customer lockers', 'Strong Rooms' in banks and ATM. This system will have the RFID tagged Key for each locker, Digital Lock for the door of the Locker Room/Strong Room, Biometric Authentication Devices, Light Sensor Device for each locker and a Database which will store all the related information about the lockers as shown below.

RFID Tagged Key

Each locker holder customer will have only one physical key with the RFID tag attached to it, though some key chain like mechanism. As the RFID tag has a unique number hence duplication of the keys will not be possible. The RFID tag number entry will be done along with the Bank Locker number. Note the locker key allocated will be only one. We propose passive RFID tags which are much cheaper as compared to active tags. These are also smaller in size as compared to active tags [3]. In the cases when a customer loosed an RFID key, different key can be given with new RFID tag after proper verification and previous will be deactivated from banking database.

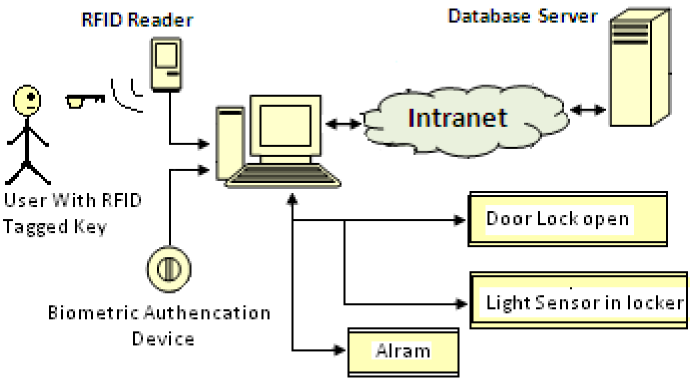

Figure 1: Proposed design of the system

BIOMETRIC AUTHENTICATION DEVICE

This can be either eye retina scan or the finger print scan device. Generally owner of the bank locker nominates two persons, who can operate the locker. Usually one is the family member and other is the customer himself/herself. Hence, it is needed to store the biometric authentication of both the operators of a particular customer locker. In State Bank of India and some other Banks figure print authentication devices for the bank employees are already installed which are basically used as a protection to access banking software. Hence for Indian Banks it can be extended for customer identification; as proposed in this paper.

DATA BASE

The Database will contain the detail information about each locker like the name of the customer, mobile number, locker number, RFID tag number and details about biometric authentication of the locker operators like figure print or eye retina scan data along with their names. The Database will also have the Log Reports every time the locker is opened. This log may contain the name of the person who operated locker, date, time and duration for which the locker was open.

DIGITAL LOCK

We don't promote the system for automatic door opening; rather it opens a simple digital lock on the door of the locker room. Once this digital lock is opened, then the door can be opened manually. Looking at the developing countries and the problem of the power cut (Electricity shortage problem), it is more feasible to open digital lock than to open the door; as it will need lesser electrical power and will also work on generators or batteries. This means the door of the customers locker room will have the 'Traditional Locks' also, along with a digital lock. The 'Traditional locks' will be opened at the time when the bank opens. But the Digital lock on the door of customers' locker room will open only when an authentic customer comes with his key in which RFID tag is embedded as shown in fig.1. This digital lock will be closed again when the customer comes out of the locker room. If the door is not closed properly it will announce for the same as in case of lifts.

LIGHT SENSOR

A light sensor will be placed inside each locker. This sensor will be deactivated for a single locker at a time. When the RFID tag number matches with a locker number and the customers' biometric authentication also matches; then the light sensor in that particular locker will be deactivated. When the customer comes out of the locker room this light sensor will be activated again. This helps in two things:

1) Only one customer can be inside the locker room at a time. And only the locker (allocated to that particular customer) can be opened at that time, this enhances the security and is similar to the present system in most of the banks in India.

2) There are cases of robberies; in which the robbers dig the tunnel, reached inside the Customer Locker room, cut the lockers and looted the bank. In such a case, the small light sensors will be active for all lockers. Hence, as soon as the robbers cut any locker and even the diffused light enters into the locker, it will buzz an alarm. These light sensors are quite cheap and can be installed using electric wires.

WORKING

As explained earlier the physical locks on the door of the locker room will be opened by the bank officers when the bank opens in the morning, like traditional way. But the digital lock will still closed. Following fig. 1 explains briefly about the working logic.

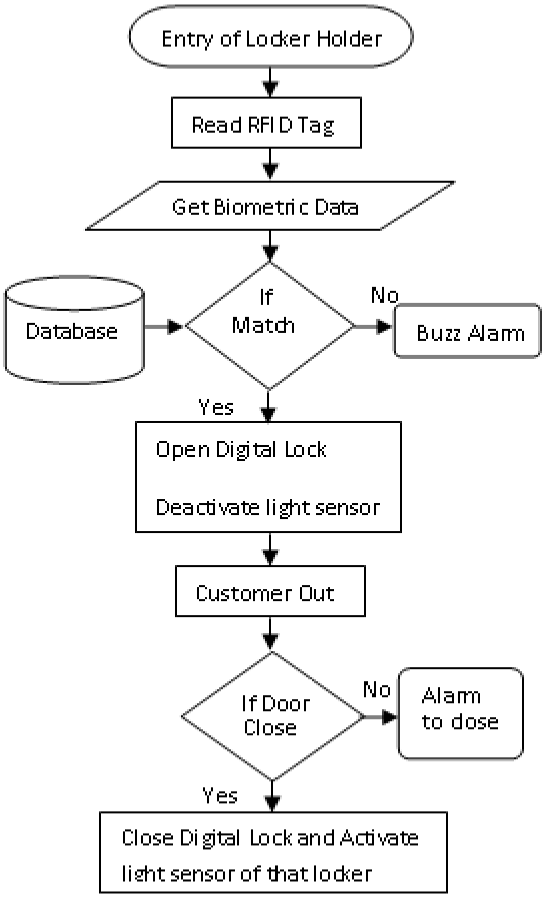

Fig. 2 Locker Operating Process

As shown in the fig.2 when a customer comes with the RFID tagged key, the card reader reads the RFID tag number, sends the data to the computer attached. The customer gives his/her figure print or eye scan on the biometric authentication device. The computer gets the details from the database server about the locker number of that RFID tag, along with other data. The customer authentication is done by matching the stored eye/figure print.

If the biometric authentication matches with the nominated person for that particular locker and RFID tag also matches for that locker number, then the digital lock on the door of the locker room opens. And customer now can walk inside the locker room. The light sensor for that particular locker is deactivate, where as the light sensors of all other lockers will be active. Hence only that locker can be opened for which the biometric and RFID tag has been matched. When customer steps out of the door, the RFID reader senses back the same RFID tag, this closes the digital lock and activates the light sensor inside that locker. If the locker room door is not closed properly, it announces to close like in case of lifts. A log report is created with details like name of person who opened locker, date, time and duration etc. The security can be enhanced if the message is sent from the bank to the customer mobile number whenever the locker is opened. If the RFID tag number on the key and the biometric authentication does not match an alarm will buzz informing the forgery. Two customers will not be allowed to operate the locker at the same time; this will be cross verified by the exit of the RFID tag of that customer.

STRONG ROOM AND ATM

For security of the ' Strong Room', the Chief Cashier and Branch Manager, both officers will have two separate keys with RFID tags attached to it like a key chain. And they both have to record their biometric attendance along with the RFID keys, then only the digital lock will open for the strong room. Even if one of the RFID or biometric authentication doesn't match the digital lock will not open. Here also due to RFID tag the keys cannot be duplicated.

This has an advantage that even if the duplicate keys are made their RFID numbers cannot be duplicated increasing security. Also, usually bank officers hand over their keys to some other officer and keep themselves absent to open the door lock, but due to biometric authentication both the offices have to be present in person with the authentic keys.

Inside the ATM machines, where the cash tray rests a light sensor can be installed. When some robbers cut this machine to take out the cash trays, light will enter inside the cash tray and the light sensor will buzz an alarm. Also an RFID tag can be installed inside an ATM so whenever the machine is taken out of the room it will buzz an alarm. These small equipments can make the ATMs robbery free.

IV. CONCLUSION

Proposed system can give a strong add on security for the Customer Lockers, Strong Rooms and ATM machines' cash box. The proposed system needs lesser power (electricity) and it is cheaper as compared to the other systems developed. The passive RFID tags are recommended with light sensors and a digital lock which minimizes the cost. The system can be enhanced by attaching the existing GSM system for sending the messages to the customers' or Bank Officers mobiles when the customer lockers, ATMs/Strong Rooms are opened respectively.

REFERENCES

[1] Gyanendra K Verma, Pawan Tripathi, "A Digital Security System with Door Lock System Using RFID Technology", International Journal of Computer Applications (0975 – 8887), Volume 5 – No.11, August 2010, pp. 6 – 8.

[2] R.Ramani, S.Valarmathy, S. Selvaraju, P.Niranjan, " Bank Locker Security System based on RFID and GSM Technology", International Journal of Computer Applications (0975 – 8887) Volume 57– No.18 November 2012, PP. 15 – 20.

[3] Can Saygin and Balaji Natarajan, "RFID-based baggage-handling system design", *q* Emerald Group Publishing Limited [ISSN 0260-2288], Sensor Review, Vol. 30, No. 4, 2010, pp. 324-335.

[4] Sven Peets, C. P. Gasparin, D. W. K. Blackburn, R. J. Godwin, "RFID tags for identifying and verifying agrochemicals in food traceability systems", Springer Science + Business Media, Precision Agric (2009) 10, DOI 10.1007/s11119-009-9106-4, pp. 382-394.

[5] Axel Decourtye, James Devillers, Pierrick Aupinel, Franc¸ois Brun, "Honeybee tracking with microchips: a new methodology to measure the effects of pesticides", Springer Science + Business Media, Ecotoxicology (2011) 20:429–437, DOI 10.1007/s10646-011-0594-4, pp. 429 – 437.

Article in a journal:

[6] Brandt, David, "The aloha tracker", ProQuest Science Journals, May 2008, 40, pp. 50–52.

[7] Cross, Candi S, " Olympian Logistics", ProQuest Science Journals, Jun 2008; 40, pp. 24 – 28.

[8] Higgins, Kevin T, " Eye You Know", Dec 2004; 76, 12; ProQuest Science Journals, pp. 37 – 44.

[9] Claire Swedberg, "RFID Is the Ticket at Washington Nationals' Park ", RFID Journal(online), http://www.rfidjournal.com/article/view/9489, White Paper, Security Access control & retail, 4th May 2012.

[10] Edson Perin, "VGB Group to Deploy RFID at Its 120 Siberian and Crawford Stores", http://www.rfidjournal.com/article/view/9432, white paper 13th April 2012.

[11] Claire Swedberg, "RFID Has Shoppers Running to New Balance's Store in Boston", http://www.rfidjournal.com/article/view/9459

Article in a conference proceedings:

[12] Jyoti Jhawar, "RFID : A technology for the maintenance & security of the shops/malls against thievery", Proceedings of Transilience-2012, International Conference on Technology Enabled Oraganisational Transformation.