IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 3, March 2016

Bank Locker Security Management

Juilee Sawant[1], Soumya Talkal[2], Priyanka Desai[3], Satendra Mane[4]

Student, Electronics and Telecommunication, Vidyalankar Institute of Technology, Mumbai, India[1, 2, 3]

Professor, Electronics and Telecommunication, Vidyalankar Institute of Technology, Mumbai, India[4]

Abstract: The main purpose of this paper is to design and implement a locker high security system based on RFID, PASSWORD and ZIG-BEE technology which can be organized in bank, secured offices and homes. In this system only authentic person can be recovered money from locker. We have implemented a locker security system based on RFID, PASSWORD and ZIG-BEE technology containing RFID card reader system which can authenticate and validate the user. Verifying all details in database of the system, the PIN of the validated user will be sent to particular Locker system via Zig-bee module. Locker system provides access to the locker only if the PIN received is matched with PIN entered by the validated user. The main advantage of using RFID, PASSWORD and ZIG-BEE is more secure than other systems. In general terms, RFID is a means of identifying a person or object using a radio frequency transmission. In other words RFID is an electronic method of exchanging data over radio frequency waves. The technology can be used to identify, track, sort or detect a wide variety of objects.

Keywords: RFID, Zig-Bee, Keyboard, Microcontroller.

I. INTRODUCTION

RFID verification is one of the most reliable user identification methods in Digital Electronics. This system consists of Microcontroller, RFID reader, Zig-Bee modem, keyboard, solenoid, buzzer and LCD display. In this system the RFID reader reads the ID number from passive tag and authenticates the user. System fetches valid user's PIN and sends it to the microcontroller of respective locker system through Zig-Bee. If these two passwords i.e the received PIN and the PIN entered by user are matched then the locker will be opened otherwise the microcontroller sends the false alarm to the Bank and Locker will remain in locked position. This system is more secure than other systems because two passwords are involved for verification. RFID is an acronym for Radio Frequency Identification. In general terms, RFID is a means of identifying a person or object using a radio frequency transmission [5].

II. RELATED WORKS

In this section some related works connected to the monitoring system using GSM services.In this section some related works connected to the monitoring system using GSM services.

Abstract Sample - (c) Ingens Tech Pvt Ltd, 2013,IEEE Reference: Blood and money, Year of Publication: 2012- In this project each locker is provided with a simple and low cost digital system that controls the lock to the locker instead of a key. This digital system comprises of a small display also mounted on the locker itself. The digital system is connected to a computer in the bank that in turn has the database of the customers, with various details of the customers. The digital system using various personal details of the customer like the date of birth and their ATM pin and the date of the particular day generates a random number that is unique to the customer. This random number is displayed on the display of the locker. When an individual wants to access the locker they have to see the random number and send this number from their registered mobile number to a certain bank number as a SMS, along with their ATM pin. A GSM receiver connected to the bank computer receives this SMS sent from the user number and verifies all the details like registered mobile number, the random number & ATM pin was correct or not. Thus this project can enhance the security of the bank lockers to a very high level, using a complex system that is hard to tamper with and at the same time easy for the users to use. This also reduces the manual work involved in the whole locker access process [1].

International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)-In this paper we proposed that fingerprint verification of ATM (Automatic Teller Machine) security system using the biometric with hybridization. The fingerprint trait is chosen, because of its availability, reliability and high accuracy. The fingerprint based biometric system can be implemented easily for secure the ATM machine. In this system the working of these ATM machine is when the customer place on the fingerprint module when it access the ATM for draw the cash then, the machine wants to fingerprint of that user's which use the machine. Using biometric, it verify/identify fingerprint and gives accurate result that if it valid or not valid. In this way we can try to control the crime circle of ATM and do secure it [2].

To get more security from hacking GSM channels information, parameters like Zig-Bee & RFID Reader Card is used. Here in this project verification of pin of locker is done twice giving better security.

III. PROPOSED METHOD

In this proposed work, the RFID reader reads the data from tag and sends the Bank PIN to the microcontroller, if the card is valid through Zig-Bee module. Then the account holder needs to enter the PIN at respective bank locker keypad. The microcontroller compares the PIN entered by keyboard and received through Zig-Bee. If

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 3, March 2016

these passwords are correct the microcontroller provides necessary control signal to open the bank locker. This method is simple and more secure than other system.

1. RFID Fundamentals

Basically, an RFID system consists of an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. There are many different types of RFID systems in the market. These are categorized on the basis of their frequency ranges. Some of the most commonly used RFID kits are low-frequency (30-500 kHz), mid-frequency (900 kHz-1500MHz) and high-frequency (2.4-2.5GHz).Basically, an RFID system consists of three components: an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. An RFID reader is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data. An RFID tag is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked. "RFID" stands for Radio Frequency Identification. The tag's antenna picks up signals from an RFID reader or scanner and then returns the signal, usually with some additional data (like a unique serial number or other customized information). A passive tag is an RFID tag that does not contain a battery; the power is supplied by the reader. When radio waves from the reader are encountered by a passive RFID tag, the coiled antenna within the tag forms a magnetic field. The tag draws power from it, energizing the circuits in the tag. The tag then sends the information encoded in the tag's memory. The RX and TX pins of RFID reader connected to Tx and Rx pins of AT89C51 Microcontroller respectively. Then the reader senses the data from the Tag and transmits the sensed data to microcontroller via serial port.

2. Zig-Bee Fundamentals

It is a Technological Standard Created for Control and Sensor Network based on the IEEE 802.15.4 Standard. The main applications for 802.15.4 are aimed at control and monitoring applications where relatively low levels of data throughput are needed, and with the possibility of remote, battery powered sensors, low power consumption is a key requirement. Sensors, lighting controls, security and many more applications are all candidates for the new technology. Zig-Bee is created by the ZigBee Alliance.It operates in Unlicensed Bands – ISM2.4 GHz Global Band at 250kbps, 868 MHz European Band at 20kbps, 915 MHz North American Band at 40kbps.

It operates in Personal Area Networks (PAN's) and device-to-device networks.The distances that can be achieved transmitting from one station to the next extend up to about 70 metres, although very much greater distances may be reached by relaying data from one node to the next in a network.

General Characteristics

- Dual PHY (2.4GHz and 868/915 MHz)
- Data rates of 250 kbps (@2.4 GHz), 40 kbps (@ 915 MHz), and 20 kbps (@868 MHz)
- Optimized for low duty-cycle applications (<0.1%)
- CSMA-CA channel access - Yields high throughput and low latency for low duty cycle devices like sensors and controls
- Low power (battery life multi-month to years)
- Multiple topologies: star, peer-to-peer, mesh, Cluster Tree
- Addressing space of up to: -18,450,000,000,000,000, 000 devices (64 bit IEEE address) - 65,535 networks
- Optional guaranteed time slot for applications requiring low latency
- Fully hand-shaked protocol for transfer reliability
- Range: 50m typical (5-500m based on environment)

IV. BLOCK DIAGRAM

The block diagram of Bank locker system based on RFID and Zig-Bee technology is shown in the figure above. It comprises the power supply section, keypad, RFID Reader, AT89C51 microcontroller, Solenoid, LCD, and Zig-Bee module. The circuit is powered by regulated +12V DC.

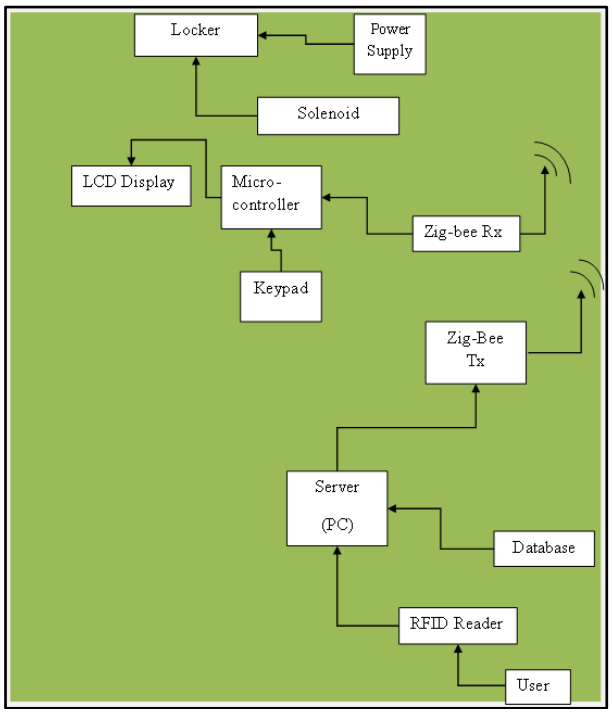

Fig.1. Block diagram of Bank Locker Security Management

V. CIRCUIT DESCRIPTION

Above figure shows the circuit of the Bank locker system based on RFID and Zig-Bee technology. The compact circuitry is built around Atmel AT89C51 microcontroller. The AT89C51 is a low-power; high performance CMOS 8-bit microcomputer with 4 KB of Flash programmable and erasable read only memory (PEROM). It has 128 bytes of RAM, 32 input/output (I/O) lines, three 16-bittimers/counters, six-vector two-level interrupt architecture, a full-duplex serial port, an on-chip oscillator and clock circuitry. The system clock also plays a significant role in operation of the microcontroller.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 3, March 2016

An 11.0592MHz quartz crystal connected to pins 18 and 19 provides basic clock to the microcontroller. Power-on reset is provided by the combination of electrolytic capacitor C3 and resistor R1. Port pins P2.0 through P2.7 of the microcontroller are connected to data port pins D0 through D7 of the LCD, respectively. Port pins P3.7 and P3.6 of the microcontroller are connected to register-select (RS) and enable (E) pins of the LCD, respectively. Read/write R/W pin of the LCD is grounded to enable for write operation. All the data is sent to the LCD in ASCII format for display. Only the commands are sent in hex form. Register-select (RS) signal is used to distinguish between data (RS=1) and command (RS=0). Preset RV1 is used to control the contrast of the LCD. Resistor 10k limits the current through the backlight of the LCD. Port pins P3.0 (RXD) and P3.1 (TXD) of the microcontroller are used to interface with the RFID reader through Max232(1) and GSM Modem are used to interface through Max232(2).

When an allowed person having the tag enters the RF field generated by the RFID reader, RF signal is generated by the RFID reader to transmit energy to the tag and retrieve data from the tag. Then the RFID Reader communicates through RXD and TXD pins of the microcontroller for further processing. Thus on identifying the authorized person, the authorized person enters the password through keyboard and send to the microcontroller. If the password is correct then the microcontroller send the SMS to the account holder person, account holder again send the password through SMS to the microcontroller. The microcontroller verifies the password and received password through GSM mobile. If this password is correct, the microcontroller provides high signal to port pin P3.2, transistor Q2 drives into saturation, and relay RL1 energizes to open the bank locker. Simultaneously, the LCD shows "access granted" message and send to and port pin P1.7 drives piezo buzzer PZ1 via transistor T1 for aural indication. If the password is not valid, the LCD shows "access denied" and the bank locker doesn't open.

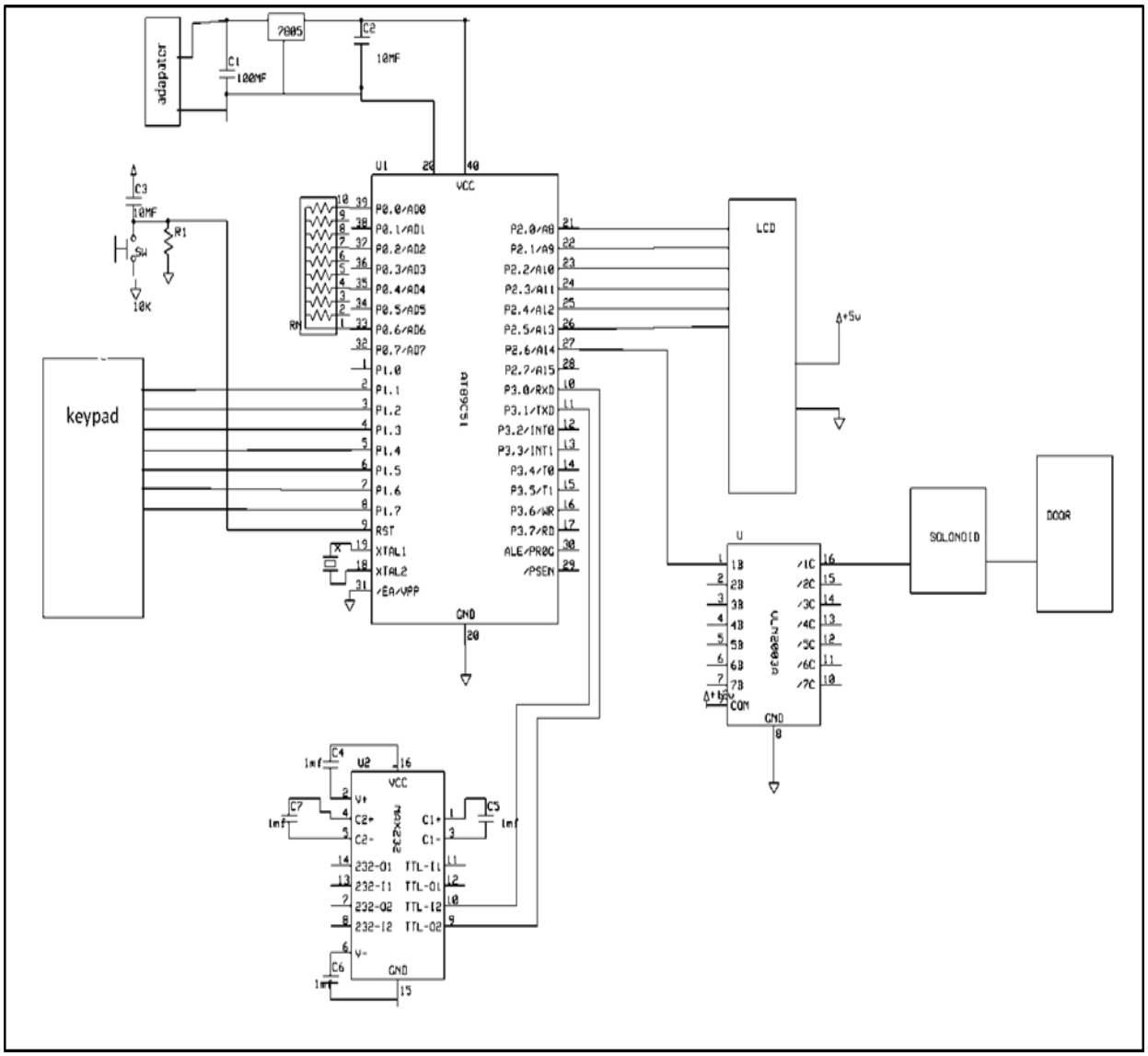

Fig.2. Microcontroller subsystem

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 3, March 2016

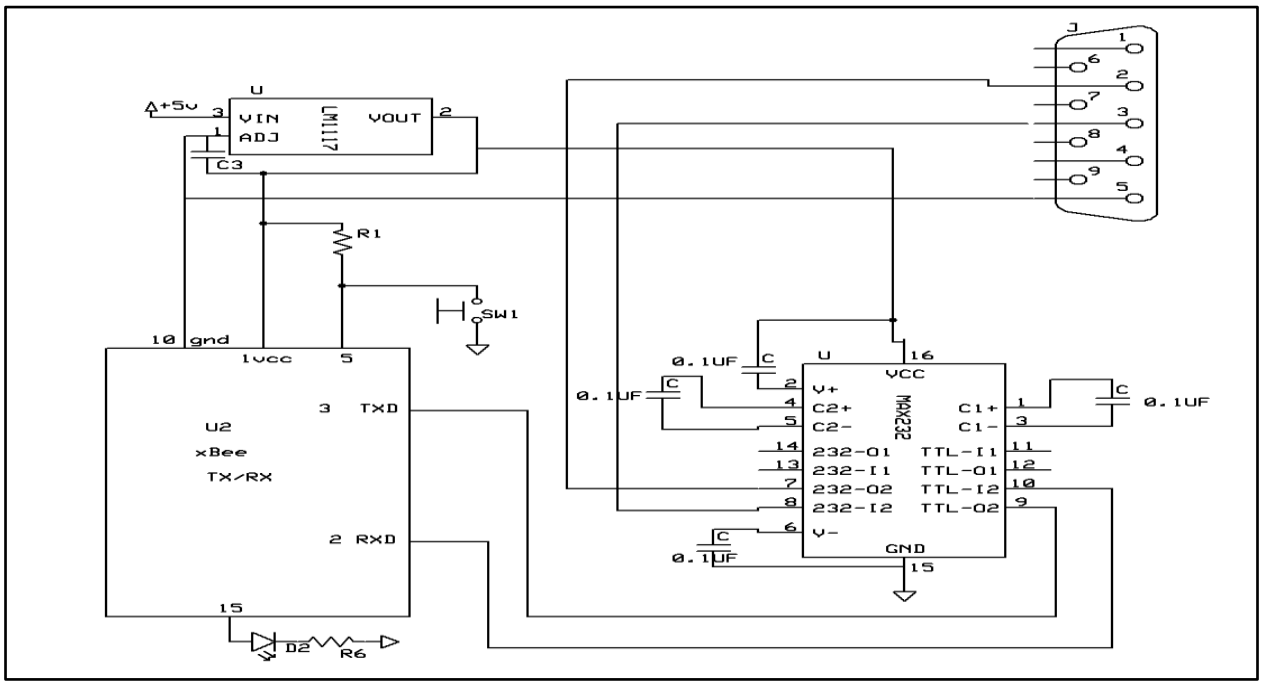

Fig.3.Zig-Bee subsystem

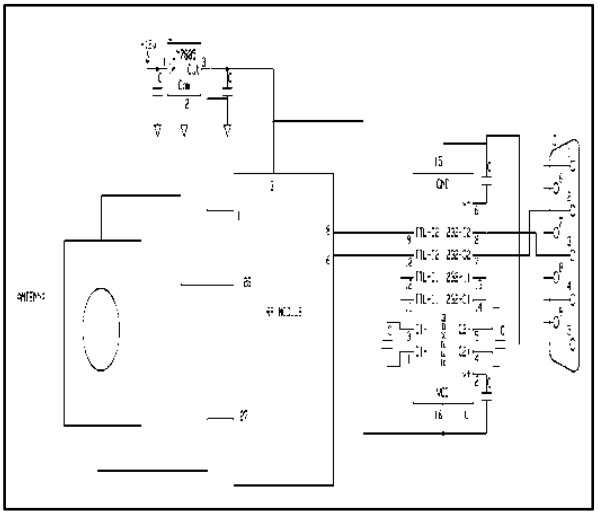

Fig.4. RFID subsystem

VI. RESULTS

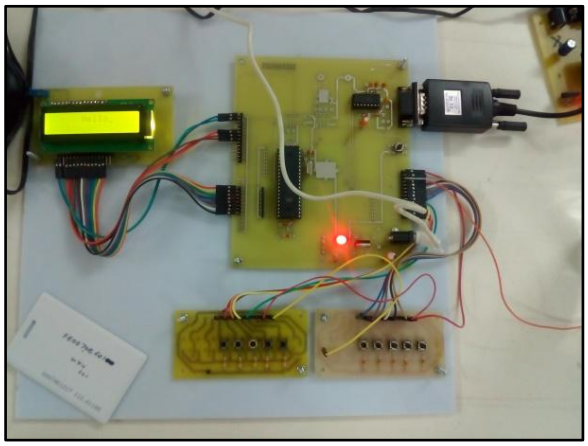

Fig.5. Implementation with Hardware Result

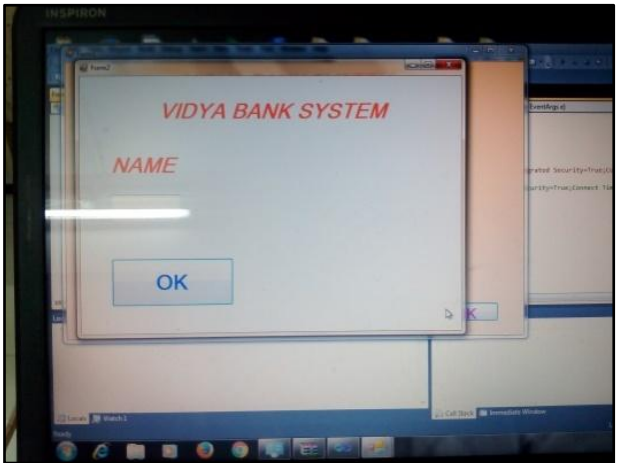

Fig.6. Software Result

VII. COMPARATIVE STUDY OF EXISTING AND PROPOSED LOCKER SYSTEM

Table1 Comparison of earlier and proposed system

Existing system	Proposed system
Key & signature is verified	RFID Technology is used for user verification
Duplication of key is possible	RFID tag code is unique. Hence duplication not possible
Manual work is required	System is digitized
If any bank person is corrupted, security is endangered.	RFID code and PIN of locker is unique and hence system is fault proof

V. CONCLUSION

We have implemented a Bank locker security system using passive RFID and Zig-Bee module. It is a low cost, low in power conception, compact in size and standalone system. The microcontroller compares the passwords entered by keyboard and received through Zig-Bee receiver. If these passwords are correct the microcontroller provides necessary control signal to open the bank locker. Alarm will be turn on whenever PIN match is not found.

ACKNOWLEDGMENT

We take this opportunity to express our profound gratitude and deep regards to our guide **Prof. Satendra Mane** for his exemplary guidance, monitoring and constant encouragement throughout the course of this project work.
We also take this opportunity to express a deep sense of gratitude to **Dr. Saurabh Mehta,** HOD of E.X.T.C. Dept. for his cordial support, valuable information and guidance, which helped us in completing this task through various stages.
We are obliged to staff members of Vidyalankar Institute of Technology, for the valuable information provided by them in their respective fields. We are grateful for their cooperation during the period of our project work.
Lastly, we thank almighty, our parents, our family and friends for their constant encouragement.

REFERENCES

[1] www.ingenstech.com.
[2] www.ijettcs.org
[3] www.atmel.com
[4] automatic identification manufacturers -- aim
[5] www.godrej.com