ACCESS CONTROL MANAGEMENT SECURITY SYSTEMS USING NFC TECHNOLOGY

Anand Vasudevan[1], Varun.C[2], Vijay Krishnan[3], Renita Rexy[4]

[1, 2, 3] UG Student, [4] Asst. Professor,

Dept. of Electronics and Communication Engineering, Bharath University, (India)

ABSTRACT

The use of keys are outdated and not safe. It is tedious to carry keys in our pockets. Though we have advanced technologically in various aspects, the usage of keys still exists. We need keys for safety, yet it would be easy and cool if the replacement for a key would be something that can be easily carried and still remain safe. The main concept of this project is to eliminate the use of keys, replacing it with a smart device that can remain undetectable. A NFC sensor attached to the PIC microcontroller detects the passive device worn or carried by the authenticated person, thereby enabling them to access the door by simply using the device.

Keywords: NFC watch, NFC sensor, unique ID, home safety, security systems, NFC locks

I. INTRODUCTION

The usage of RFID cards to access doors in companies are prevalent throughout the world. But RFID cards can be tampered with, stolen or otherwise cease to work as the card gets old. This is where a NFC device can be used as an able alternative to eliminate the shortcomings found in RFID cards. Moreover RFID cards are cards. They have to be either worn using a card holder or kept in a wallet. This can be tedious and we might tend to misplace it. A NFC device (namely: watch or ring) can be worn i.e., it would be more secure than a card that we carry usually thereby enhancing the safety issues that arises with the usage of either keys or cards.

II. PROPOSED SYSTEM

In this proposed system, we have replaced the keys with a NFC enabled watch. This watch acts as a passive device which will contain an unique ID (UID).

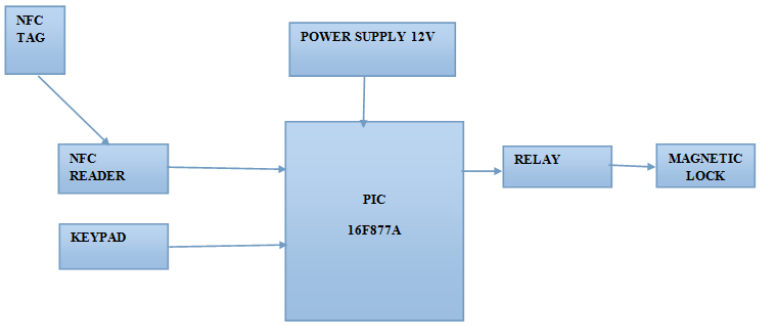


Figure 1 Block Diagram of the Proposed System

When the watch comes in contact with the lock system, an active NFC sensor will generate electromagnetic waves and read the UID from the passive device. This NFC sensor will be a part of a PIC microcontroller in

which prior information regarding the unique ID will be fed. Should the unique ID match, the microcontroller will instruct the motor to run, thereby unlocking or locking the door.

2.1 Working of Proposed System

This system works on a 12V power supply, The voltage regulator (7805) which has a range between (12V - 5V) regulates the supplied 12V between the components o the system. The PIC Microcontroller(16F877A) has a 5V supply and the voltage controller is used to regulate the power supply to the desired components. MAX 232 is used for serial communication between the ports and is also used for the level conversion. The crystal oscillator generates a clock pulse of 20 Mhz.

The RC6 port acts as a transmitter while the RC 7 port acts as the receiver. When the NFC tag is brought in contact to the sensor, it detects the unique ID thereby passing command via the PIC microcontroller to the relay system. This relay system then enables the lock to open using the RC6 and RC7 ports.

2.1.1 Pic Microcontroller

PIC 16F877 is one of the most advanced micro controller from Microchip. This controller is widely used for experimental and modern applications because of its low price, wide range of applications, high quality and ease of availability. It is ideal for applications such as machine control applications, measurement devices, study purpose, and so on.

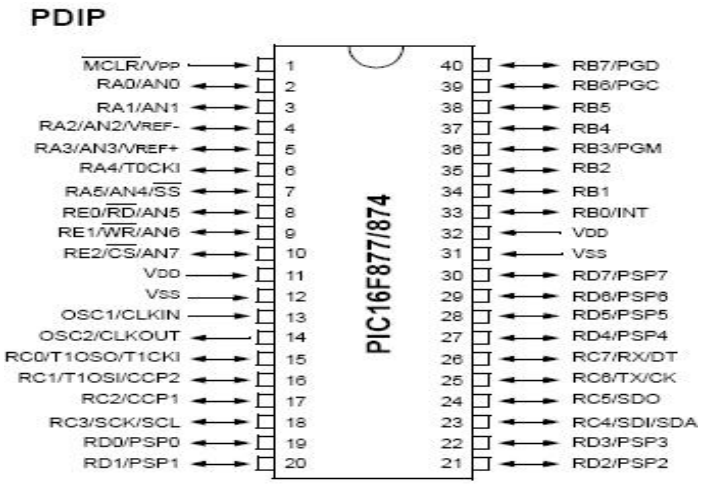
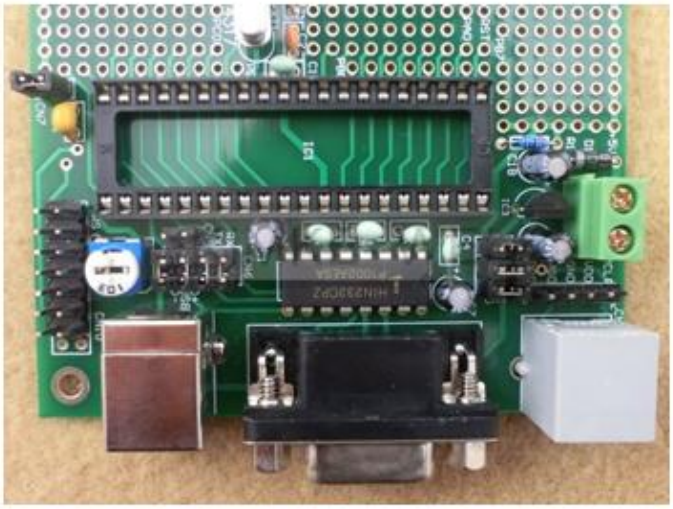


Figure 2 Pin Diagram of Pic Microcontroller

2.1.2 Key Features

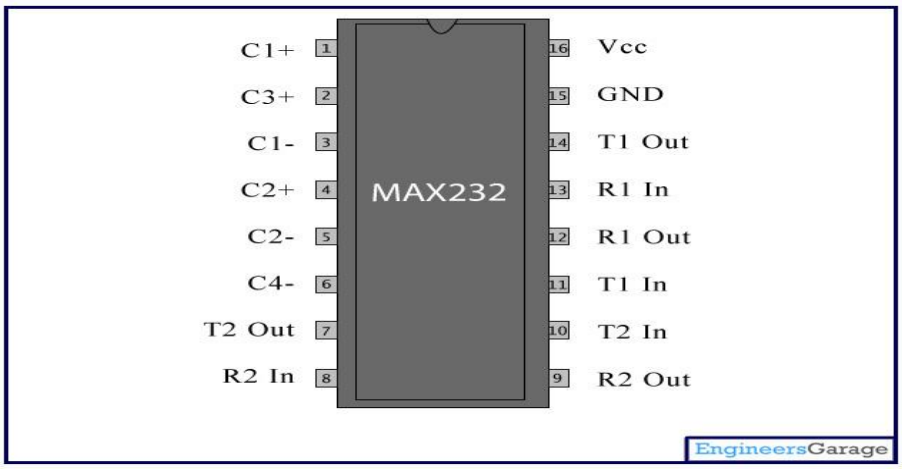
- Maximum operating frequency is 20MHz.
- Flash program memory (14 bit words), 8KB.
- Data memory (bytes) is 368.
- EEPROM data memory (bytes) is 256.
- 5 input/output ports.
- 3 timers.
- 2 CCP modules.
- 2 serial communication ports (MSSP, USART).
- PSP parallel communication port
- 10bit A/D module (8 channels)



2.1.3 MAX 232

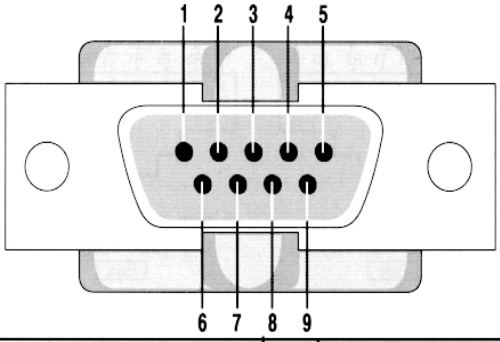
The MAX232 is an integrated circuit that converts signals from an RS-232 serial port to signals suitable for use in TTL compatible digital logic circuits. The MAX232 is a dual driver/receiver and typically converts the RX, TX, CTS and RTS signals. The drivers provide RS-232 voltage level outputs (approx. ± 7.5 V) from a single + 5 V supply via on-chip charge pumps and external capacitors. This makes it useful for implementing RS-232 in devices that otherwise do not need any voltages outside the 0 V to + 5 V range, as power supply design does not need to be made more complicated just for driving the RS-232 in this case.

The receivers reduce RS-232 inputs (which may be as high as ± 25 V), to standard 5 V TTL levels. These receivers have a typical threshold of 1.3 V, and a typical hysteresis of 0.5 V.The later MAX232A is backwards compatible with the original MAX232 but may operate at higher baud rates and can use smaller external capacitors – 0.1 µF in place of the 1.0 µF capacitors used with theoriginal device.



2.1.4 RS-232

Communication as defined in the RS232 standard is an asynchronous serial communication method. The word serial means, that the information is sent one bit at a time. Asynchronous tells us that the information is not sent in predefined time slots. Data transfer can start at any given time and it is the task of the receiver to detect when a message starts and ends. Asynchronous communication has some advantages and disadvantages which are both discussed in the next paragraph.



Pin	Signal	Pin	Signal
1	Data Carrier Detect	6	Data Set Ready
2	Received Data	7	Request to Send
3	Transmitted Data	8	Clear to Send
4	Data Terminal Ready	9	Ring Indicator
5	Signal Ground		

2.1.5 NFC

Near Field Communication or the NFC is the latest technology that has very short range frequency. It enables the transfer of data between two systems that has this technology. NFC has developed a lot in recent times with it being used in mobile transactions, bill payments etc. It operates at a speed of 13.56 MHz and can transfer data up to 424 kilo bytes per second.

III. CONCLUSION

When compared to other security systems, this is much better owing to the fact that this NFC device can be fitted in any accessory as desired. For example, we can set it in a ring, chain etc. This makes the key to remain out of sight and safe. This paper helps us in the enhanced usage of a developing technology like NFC thereby enhancing home security systems. The highlight of this concept is that it is cheap and easy to install.

REFERENCES

[1] Gerald, Josef,Christian and Josef Scharinger, “NFC Devices: Security and Privacy, ARES 08 proceedings of the 2008 Third International Conference on Availability, Reliability and Security, IEEE Computing Society, Washington, DC, USA, 2008.

[2] Gauthier Van Damme and KarelWouters, “Practical Experiences with NFC Security on Mobile Phones, Belgium, 2008

[3] Ernst Haselsteiner and KlemensBreitfu, “Security in Near Field Communication (NFC) - Strengths and Weaknesse”,Philips Semiconductors, Mikronweg , Gratkorn, Austria, 2006.

[4] PäiviJaring, ViliTörmänen, ErkkiSiira, and TapioMatinmikko, ”Improving Mobile Solution Workflows and Usability Using Near Field Communication Technology”, Technical Research Center of Finland Oulu, Finland, Springer-Verlag Berlin Heidelberg, pp. 358–373, 2007.

[5] Near Field Communications Handbook by Syed A. Ahson and Mohammed Ilyas