Intelligent Security System with Wireless Sensors

R.Shrikeerthana
PG Student
Computer Science and Engineering
Sri Krishna College of Technology

A.Balamurugan
Professor
Information Technology
Sri Krishna College of Technology

ABSTRACT

Wireless sensor networks emphasize in most of the real world applications such as military applications, medical field and home appliances and so on. Sensors used in such applications do not provide any confidentiality, however it is been used in almost all the areas in our day-to-day life. Usually sensors were used in buildings after the construction. This work presents a solution which ensures security using sensors in building constructions. In particular, this work proposes an intelligent method that provides security for banking purpose.

Keywords

Wireless sensors, security, temperature sensor, heart beat sensor.

1. INTRODUCTION

In building environmental management (BEM) applications area, the demand for wireless sensor network (WSN) technology has increased in recent years. Wireless sensors contribute high security and confidentiality in many areas, for banking sectors in particular. This paper focuses on ensuring security with wireless sensors for vault in banking purpose. In this system, the sensors that are placed in the vault room are more complex to be breached and highly sensitive to temperature changes.

Wireless sensors provide high security and confidentiality for banking sectors. The sensors that are placed in the vault room are more complex to be breached and highly sensitive to temperature changes. Finger prints provides more reliability to enter the vaults once the temperature sensor is valid. The security details are maintained in a standalone system that is maintained by the high authorities who preserve the security details of the bank.

Only if the temperature sensor permits, the security system allows for the higher level processes that includes finger print sensor and eyeball sensor. The finger prints provide more reliability to enter vaults once the temperature sensor is authenticated. The security details are maintained by a standalone system that is maintained by the authorities of the bank. The standalone system is supported with security using heartbeat sensors. The higher functional complexity of the wireless sensor nodes may enable WSN systems replace most of the current wired sensor systems in the foreseeable future.

2. RELATED WORKS

The Tyndall mote and an indoor light powered wireless sensor node are the methods used in [1].The analysis of energy consumption of the wireless sensor node and its energy consumption pattern is based on the experimental results of the Tyndall mote. Main constraints of the wireless devices are lack of an everlasting and maintenance free power supply. Relatively few indoor light powered harvesters have been presented and much research remains to be carried out on a variety of related design considerations and trade-offs.

The method used in [2] is "the matching algorithm" that plays a key role in a fingerprint recognition system and "a novel fingerprint matching algorithm" is proposed. The performance of even state-of-the-art matchers is still much lower than the expectations of people and theory estimation. Therefore, much effort is still needed to improve both the performance and the speed of fingerprint recognition systems.

The method used in [3] is fingerprint recognition using minutia score matching method (frmsm). The images are subjected to matching process and matching score is computed. The use of this system sometimes requires not just the fingerprint of the user but also a valid pin, which can be more difficult to use than traditional systems.

This kind of system requires the use of modern computer hardware and software, which can be very expensive. In [4] ridge image is an effective representation of the fingerprint image. The synthesized image is generated using the following steps:

→To compute the distance transform of a ridge image

→To replace the intensity value greater than a threshold

The image quality of the finger prints are reduced due to dry or wet skin, dirty or injured fingers, and non uniform pressures. In such a case, it is difficult to make a reliable decision whether two fingerprints are from the same finger.

3. PROPOSED METHOD

Temperature sensor is placed in the vault at the time of construction. The security system accepts the vault to be accessed only at a particular temperature, set by the authorized person in the bank. Confidentiality is further provided by the fingerprint sensors and eyeball sensors that are placed in the vault that allows for high level security. The confidential data for the security system is maintained in a standalone system and security for the system is accommodated with heartbeat sensor. The system is proposed using a microcontroller that controls the entire system. The RF transmitter and receiver of the proposed system are shown in Figure 1 and Figure 2 respectively.

3.1 Temperature Sensing

- Temperature sensor that is placed in vault senses the temperature of the vault room continuously.
- The temperature is sensed and continuously displayed in the LCD.

- The buzzer starts to beep if the temperature exceeds the threshold value which is set for the security purpose, indicating the breach of the vault.
- In this system the threshold value for temperature sensor is set from 25-60 degree Celsius
- When the temperature decreases below 25 degree Celsius or increases above 60 degree Celsius, the buzzer starts beeping indicating breach in the system

3.2 Heartbeat Sensing

- Heart beat sensor is placed at the receiver. It senses the heart pulse rate of the authorized person of the vault
- Heart beat sensor gives the digital output of the authorized person's pulse rate and only if it is authorized the system allows to access the vault
- The digital output is directly connected to the microcontroller
- The buzzer starts to beep when the pulse rate value vary and access to vault is denied

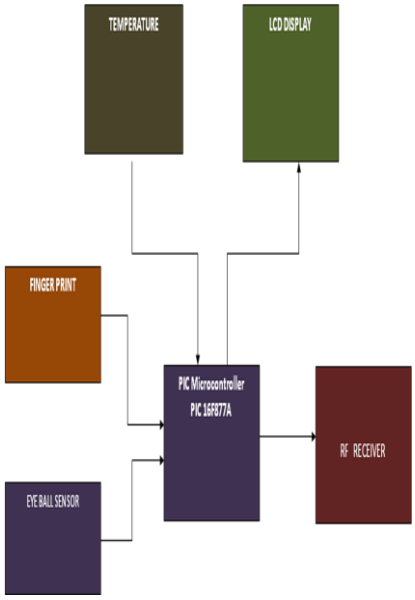

Figure 1: Block Diagram of Proposed Method-Transmitter

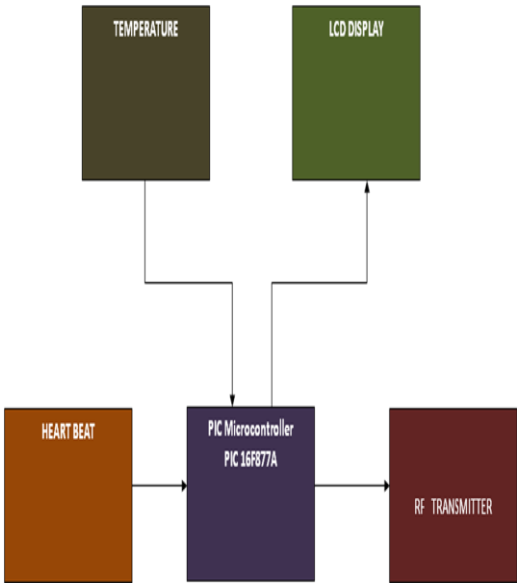

Figure 2: Block Diagram of Proposed Method-Receiver

3.3 Temperature Sensor

Temperature sensor that is placed in vault senses the temperature of the vault room continuously. The temperature is sensed and continuously displayed in the LCD. The buzzer starts to beep if the temperature exceeds the threshold value which is set for the security purpose, indicating the breach of the vault.

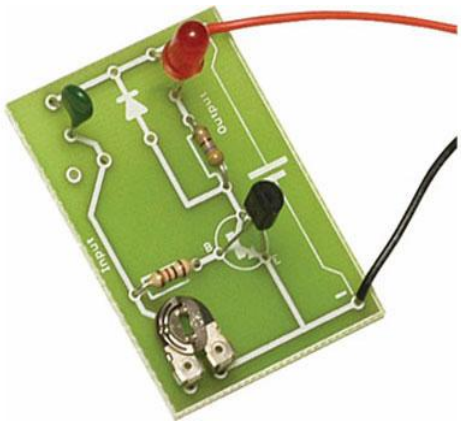

Figure 3: Temperature sensor

3.4 HEARTBEAT SENSOR

Heart beat sensor is designed to give digital output of heart beat when a finger is placed on it. When the heart beat detector is working, the beat LED flashes in unison with each heart beat. This digital output can be connected to microcontroller directly to measure the Beats per Minute (BPM) rate. It works on the principle of light modulation by blood flow through finger at each pulse.

When an unauthorized person tries to access the stand alone system in which confidential data of the bank are stored, the heart beat sensor detects the pulse rate. The buzzer starts beeping when the sensor detects indicating the breach in the system.

Figure 4: Heartbeat sensor

4. CONCLUSION

In this paper, security is ensured using sensors in building constructions and the work proposes an intelligent method that provides security for banking purpose. Wireless sensors contribute high security and confidentiality in banking sectors. The wireless sensors that are deployed not only provide security but it also supports confidentiality providing high security. Thus the proposed system provides secured and confidential access of the bank vault. This reduces security breaches and threats that are evolving.

5. REFERENCES

[1] W. S. Wang, T. O'Donnell, L. Ribetto , B. O'Flynn , M. Hayes , C. O'Mathuna "Energy Harvesting Embedded Wireless Sensor System for Building Environment Applications" 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, pp. 36 – 41, May 2009.

[2] M. Tico and P. Kuosmanen, "Fingerprint Matching Using an Orientation-Based Minutia Descriptor," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 25, no. 8, pp. 1009-1014, Aug. 2003.

[3] J. Gu, J. Zhou, and C. Yang, "Fingerprint Recognition by Combining Global Structure and Local Cues," IEEE Trans. Image Processing, vol. 15, no. 7, pp. 1952-1964, July 2006.

[4] P. Lo and G. Yu, "Print Matching Method and System Using Direction Images," US Patent Application Publication No. 2008/0273769A1, 2008.

[5] J. Feng, "Combining Minutiae Descriptors for Fingerprint Matching," Pattern Recognition, vol. 41, no. 1, pp. 342-352, 2008.