INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 6.078

(Volume 6, Issue 5)

Available online at: www.ijariit.com

Biometric fingerprint enabled secure communication using Arduino and RF technology

Rahul Anil Gaikwad
rahulgaik97@gmail.com

Akash Mishra
mishra.akash.15et3004@gmail.com

ABSTRACT

The undertaking is intended to send verified messages by utilizing an encryption from a PC console utilizing biometric scanner associated with the transmitting unit by means of RF technology. The message is recovered at the recipient end only when the approved personnel's fingerprint matches with the database utilized by the transmitter. In this manner, complete privacy is kept up in this correspondence procedure. The message composed in by the client is transmitted to the receiving end through RF transmitter. At the less than desirable end the RF beneficiary is coordinated with a fingerprint scanner and show framework. Client at accepting end can just view the message if the fingerprint matches. For instance, in military tasks, security is of foremost significance. So, when there is a requirement for sending any private message, one can type the message through a keypad/PC console interfaced with the framework including a fingerprint authentication, an Arduino NANO and a RF transmitting module.

***Keywords**: Arduino NANO, RF Transmitting Module, Fingerprint and Privacy, Etc.*

1. INTRODUCTION

Secure communication is when two elements/individuals are communicating and don't need a third unwanted party to tune in. For that, we have to impart the message in a manner not vulnerable to interference. While standard encryption techniques, for example, cryptography secure the data of the message from being gotten to by unapproved clients, undercover communication disguises the presence of the communication to avoid unapproved clients to recognize the communication. Secure communication incorporates implies by which individuals can share data with changing degrees of conviction that outsiders can't intercept information that is being exchanged. Other than spoken eye to eye correspondence with no conceivable roof, it is most likely safe to state that no correspondence is ensured secure in this sense, albeit handy snags, for example, enactment, assets, specialized issues (interception and encryption), and the sheer volume of correspondence serve to restrain reconnaissance. With numerous interchanges occurring over long separation and intervened by technology and expanding attention to the significance of capture attempt issues, innovation and its bargain, are at the core of this discussion. RF verified communication frameworks have been around for quite a while with different applications. The advances spread an extensive assortment of abilities arranged to different needs. These have been continuing at a phenomenal rate, and their effect is clear in our day-to-day lives. This venture is expected to send safe and secure messages from the console which works with the fingerprint associated with the transmitting unit (TX) through RF interaction. The message then is flashed on the receiving unit (RX) only on entering the code selected by the personnel on the RX end. Hence, all our transaction of messages is being saved from the eyes of intruders. Interfacing is practiced utilizing either cement plastic strip with conductive follows stuck to the edges of the LCD board, or with an elastomeric connector, which is a portion of elastic or silicone with substituting layers of conductive and protecting pathways, squeezed between contact cushions on the LCD and mating contact cushions on a circuit board. The RF module which is utilized are the principle parts of the venture. Since the radio communication uses a certain frequency, we can set a secret frequency at which we want to have communication. The range being shorter, gives an enclosed proximity at which the communication is taking place. The short range gives it an advantage of not being able to catch the signals in a long range, which avoids to have communication beyond a particular boundary. We can also register any number of fingerprints to provide access to different authorized personnel, in case of multiple access. This undertaking is also capable of delivering messages to a specific authorized person without any knowledge to the other authorized people. This allows to add in additional security in case of highly confidential communication between two specific personnel only.

2. HARDWARE IMPLEMENTATION

Some Below is the representation of the hardware implementation in the form of block diagram:

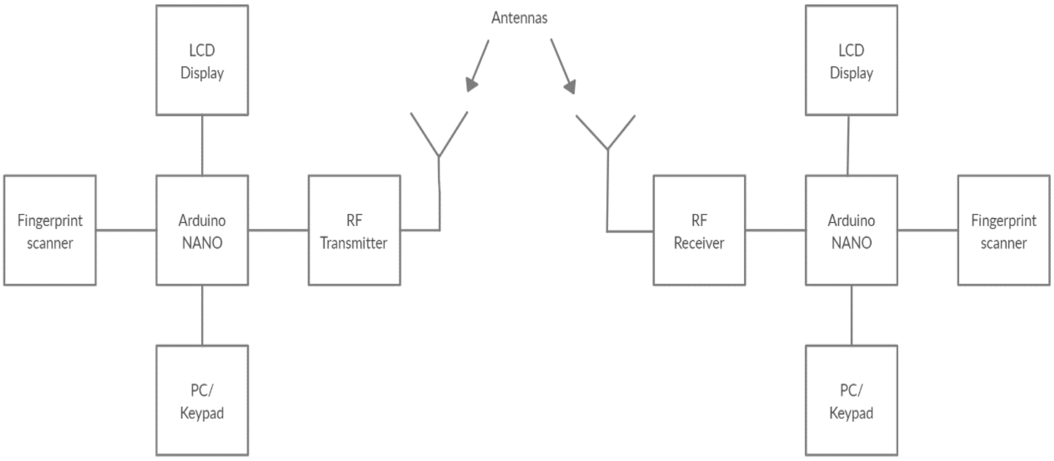

Fig. 1: Block diagram of the system

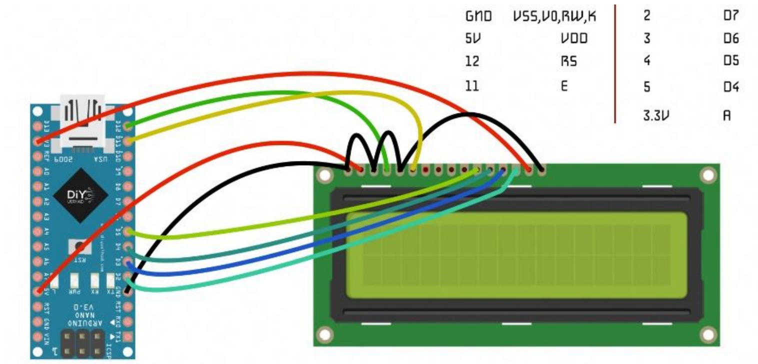

Fig. 2: Block diagram of the LCD interfaced with Arduino NANO

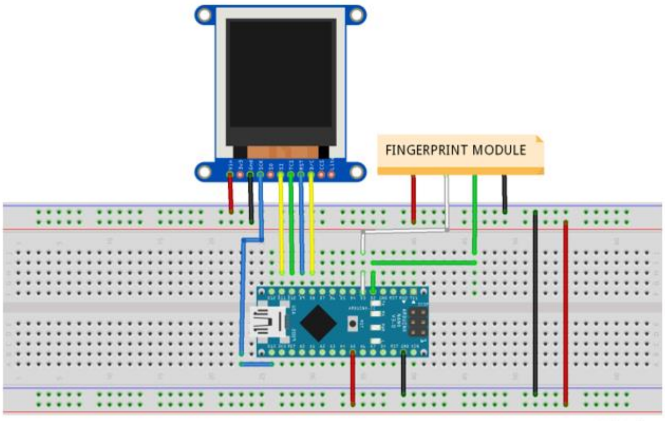

Fig. 3: Block diagram of the Fingerprint scanner interfaced with Arduino NANO on a breadboard

We can use a PC/Keypad on the transmitting and receiving side to enter the message that has to been sent out from the transmitting end securely which is connected with Arduino Nano. Fingerprint scanner is also interfaced with Arduino Nano. The Radio frequency (RF) nRF24I01 is also interfaced with Arduino Nano which helps in transmitting the message or data in a specific channel or medium. The message received/transmitted, can only be viewed and sent by authenticated and registered people at the receiving end whose biometric fingerprints are registered in the system. This helps in maintaining absolute secrecy of the message or data. At the receiving end, there is a biometric fingerprint scanner and a PC/keypad which is interfaced with Arduino Nano for authentication purpose and an LCD display for the display of message. A simple demonstration of RF Communication with the assistance of Arduino NANO boards is given. The aim of the project is to with success transmit information between the RF Transmitter Receiver modules victimization of Arduino NANO microcontroller boards. The operating of the project is explained here. The project uses a special library known as VirtualWire.h. The project enforced here uses the library. If we wish to implement the project while not the library, then we'd like to alter the receiver a part of the circuit. VirtualWire.h is a special library for Arduino created by Mike Mary McCauley. It is a communication library that permits two Arduinos to speak with one another i.e. forming transmitter-receiver connection. This library consists of several functions that square measure used for configuring the modules, transmission of information by the transmitter module and information reception by the receiver module. during this project, the transmitter merely sends 2 characters i.e. it sends the character one and with a delay of few seconds, it sends the character zero. Whenever the one is distributed, the biometric fingerprint scanner on the transmission aspect of the project are going to be turned ON. As the fingerprint on the transmitter side is authenticated, one is transmitted via RF communication, the receiver can receive the info one. Once the receiver receives one, the Arduino on the receiver aspect of the project can activate the biometric fingerprint scanner on its side. Similarly, once the info zero is transmitted by the RF transmitter, the biometric fingerprint scanner on the transmitter aspect is turned ON. As a result, the receiver currently receives 0 and also the biometric fingerprint scanner on the receiver aspect is additionally turned ON. Hence, the purpose of is that the transmit the message through language Fingerprint device Arduino Hook up the fingerprint identification method has 2 steps that's 1. Enrolling Fingerprint, 2. Matching Fingerprint. These 2 steps make a microcontroller/ System to authenticate right fingerprint. This optical biometric fingerprint reader devices uses high high-powered DSP chip AS601 kind Synochip, that will conduct the image rendering, calculation, feature finding and looking. It provides TTL serial out thus we are able to hook up with any microcontroller or system.

3. COMPONENTS AND SPECIFICATIONS

3.1 Transmitter Part

- Arduino NANO (or any other Arduino board)
- 434 MHz RF Transmitter Module (or 315 MHz Module)
- Keypad/keyboard
- LCD Display 4
- Power supply (Adapter or battery)
- Fingerprint scanner
- Wires

3.2 Receiver Part

- Arduino NANO (or any other Arduino board)
- 434 MHz RF Receiver Module (or 315 MHz Module)
- LCD Display 4
- Keypad/keyboard
- Power supply (Adapter or battery)
- Fingerprint scanner
- Wires

3.3 Software used

Arduino IDE

4. MERITS

- Privacy is maintained.
- Can save a lot of private information from getting disclosed.
- Affordable
- Portable
- Can be used for short range communication services (which is of primary use in military).

5. DEMERITS

- The transmission of the message depends on the range of the transmitter and receiver.
- To increase the range of the communication, we need to attach an external antenna supporting the system.

6. Applications

This primarily has major application for military communication purposes, but can be used for other purposes where communication privacy is of paramount importance.

7. CONCLUSION

Based on the number of users, it is now the ideal technique of communication. A lot of systems in the past carried over the wire are now carried over wireless media. The complete privacy is maintained which is of utmost importance in the communication process. RF based secure communication is being developed by many organizations and utilized by many amputees. Many authors have presented issues and challenges in this technology. Research is being carried on this field to enhance this technology further. In this system it is possible to secure the messages sent to another user. In the future, it is possible to improve the system by making it a two-way communication protocol. Secure communication is when two entities are communicating and do not want a third party to listen in, which is completely implemented and assures the guarantee off maintaining the privacy at its utmost height.

8. REFERENCES

[1] Aditya Shah, Shahbaz Shaikh, Divyesh Parmar, Sarang Kulkarni.Department of Electronics, (Atharva College of Engineering,India). RF Based Secure Coded Communication System.IOSR Journal of Engineering (IOS-RJEN) ISSN (e): 2250-3021, ISSN (p): 2278-8719.Volume 9, PP 83-86https://www.iosrjen.org/Papers/Conf.ICIATE2018/Volume-9/17-83-86.pdf.

[2] https://en.wikipedia.org/wiki/Radio-frequency engineering

[3] https://educ8s.tv/arduino-fingerprint-sensor-module-tutorial/