International Journal of Information Technology and Language Studies (IJITLS)

Design and Development of a Modified Access Control System Based on Mobile applications to Reduce the Risk of COVID-19 Spreading

Ahmed Abd Alrahman Khaleel[1], Hassan Mohamed Hassan[1], Hiba Ali Abdelmahmoud[1], Shroug Abd Elrazig Nouri[1], Hoyam Salah Elfahal[1], Elsadig Saeid[2], Yousif ElfatihYousif[1]

[1]Department of Computer Engineering, Faculty of Engineering, Alzaiem Alazhari University, Khartoum, Sudan
[2]Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Khartoum, Khartoum, Sudan

ahmedabdelrhmana816@gmail.com; hassanmohamd997@gmail.com; hiba.a.mahmoud97@gmail.com; shrougabdalrazig99@gmail.com; hoyam090@hotmail.com; els197778@gmail.com; yousifsiddiq@gmail.com

Article Information

Article type: Article

Article history:

Received: February 09, 2022
Revised: November 29, 2022
Accepted: December 28, 2022

Keywords:

Secure Access Control,
Biometric devices,
Fingerprint,
COVID-19,
Bluetooth,
Arduino Nano

Abstract

In this paper, a modified design of an access control system is developed and tested. The conventional access control systems that use fingerprints expose users to the risk of COVID-19 spreading by touching and using a central fingerprint device in an institute or private office. The proposed and tested design uses the fingerprint registered on users' smartphones. Using a simple mobile application, the individual fingerprint data is sent to the microcontroller via the Bluetooth device and compared with the fingerprints registered in the database to control the various functions and operations of the entire access system.

1. INTRODUCTION

Access control is a fundamental concept in security that minimizes risk to the business or organization. Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials, including passwords, personal identification numbers (PINs), biometric scans, security tokens, or other authentication factors (Huang, 2009). The Importance of a secure access control system is to increase the ease of access for employees, Get rid of traditional keys, Save money and energy, Protect against unwanted visitors, Give employees the freedom to work when they need and prevent data breaches (Haofeng & Xiaorui, 2019). Today, there are many applications for secure access control such as RFID system-based systems, encrypted steganography graphical password schemes for smartphones, secure access control through WIFI and Door locking through fingerprint and GSM, etc.

We will present a survey on various automatic identification and access control mechanisms that have been used to prevent unauthorized access. In the olden days, traditional lock systems or passwords were employed for high-security zones. But this solution was not secure. Due to the advancements in technology, RFID cards were used, but this was not useful for the user. Later various door lock security systems based on biometrics, GSM, OTP, cryptography etc., were developed. The Corona pandemic has significantly impacted the world of work and private life and has set new hygiene standards. Companies have had to rethink and redefine safety. Whereas before Covid-19 the priority was to reliably protect products and technologies (Ferreira et al., 2014). Biometric systems use scanners to verify the identity of human beings by measuring the patterns of their behavioral or physiological characteristics such as fingerprint verification systems, require the user to make direct physical contact with the scanner for a specified duration for the biometric pattern of the user to be properly read and measured. This may increase the possibility of contamination with harmful microbial. In this viewpoint, we establish the likelihood of infectious disease transmission through touch-based fingerprint biometric devices and discuss control measures to curb the spread of infectious diseases, including COVID-19 (Xie et al., 2015). The rest of this paper is organized as follows: Section II explains the system design methodology. Section III highlights the impact of COVID -19 on the secure access control system. Section IV presents the risk of COVID -19 due to the fingerprint biometric system. Section V presents the proposed system design. Finally, we conduct tests and conclude the paper.

2. PROPOSED SYSTEM DESIGN METHODOLOGY

Designing a system that controls the unlocking of doors through the phone's fingerprint by designing and installing an application on the phone and linking it to a Bluetooth device .Upload the code to the Arduino Nano, then turn on the Bluetooth on the mobile phone and pair it with the Bluetooth device used in the circuit. The fingerprint is scanned by your phone's fingerprint scanner to be compared, and the user's character is sent to the Arduino Nano. The sent character is compared to the characters in the database; If they match, a message will be displayed on the "LCD" screen alerting that hands must be sanitized before entering and the solenoid door lock will open, and if it does not match, the solenoid door will not open.

3. IMPACT OF COVID-19 ON THE SECURE ACCESS CONTROL SYSTEM

The COVID-19 pandemic has forever changed the way we do business and keeps our families and employees safe. Companies around the world need to take a step back and reevaluate things as we're in uncharted waters now. With no clear path forward, the most important thing you can do is control the things that you can while taking preventative measures to ensure the safety and health of everyone. Social distancing guidelines require businesses to completely change processes and practices as well as find new cutting-edge tools to educate ourselves and prevent the pandemic from spreading further. Workplaces are primary locations for the spread of COVID-19 and similar diseases, so a shift in office policies and procedures is needed. Businesses are now working with lower staffing levels and remote staff, which significantly affects how employees are entering and exiting buildings and who has access (Hwang & Baek, 2007). Modern systems for access control set new long-term security standards in companies, hospitals and the like. The Corona pandemic has had a significant impact on the world of work and private life and has set new hygiene standards. Companies have had to rethink and redefine safety. Interpersonal contact should be prevented, any touching of surfaces such as door handles or switches should be avoided, regular hand washing, mouth-nose protection. Whereas before Covid-19 the priority was to reliably protect products and technologies, the pandemic now ensures that health protection for employees, customers and visitors is a top priority.

4. THE RISK OF COVID-19 BECAUSE OF FINGERPRINT BIOMETRIC SYSTEM

Biometric systems use scanners to verify the identity of human beings by measuring the patterns of their behavioral or physiological characteristics. Some biometric systems are contactless and do not require direct touch to perform these measurements; others, such as fingerprint verification systems, require the user to make direct physical contact with the scanner for a specified duration for the biometric pattern of the user to be properly read and measured. This may increase the possibility of contamination with harmful microbial pathogens or of cross-contamination of food and water by subsequent users. Physical contact also increases the likelihood of inoculation of harmful microbial pathogens into the

respiratory tract, thereby triggering infectious diseases. In this viewpoint, we establish the likelihood of infectious disease transmission through touch-based fingerprint biometric devices and discuss control measures to curb the spread of infectious diseases, including COVID-19.

5. PROPOSED SYSTEM DESIGN

As shown in figure 1, mainly five components were used to design the modified access control system. The mobile is equipped with an android application to acquire the fingerprint data and, on a positive match, send a signal to the Bluetooth module device, which is connected to a database and Arduino Nano board. The purpose of Arduino board is to drive the connected control circuit, (Solenoid to lock or unlock the door, LEDs and Buzzer to actuate and generate the required events) and display the action message on the LCD.

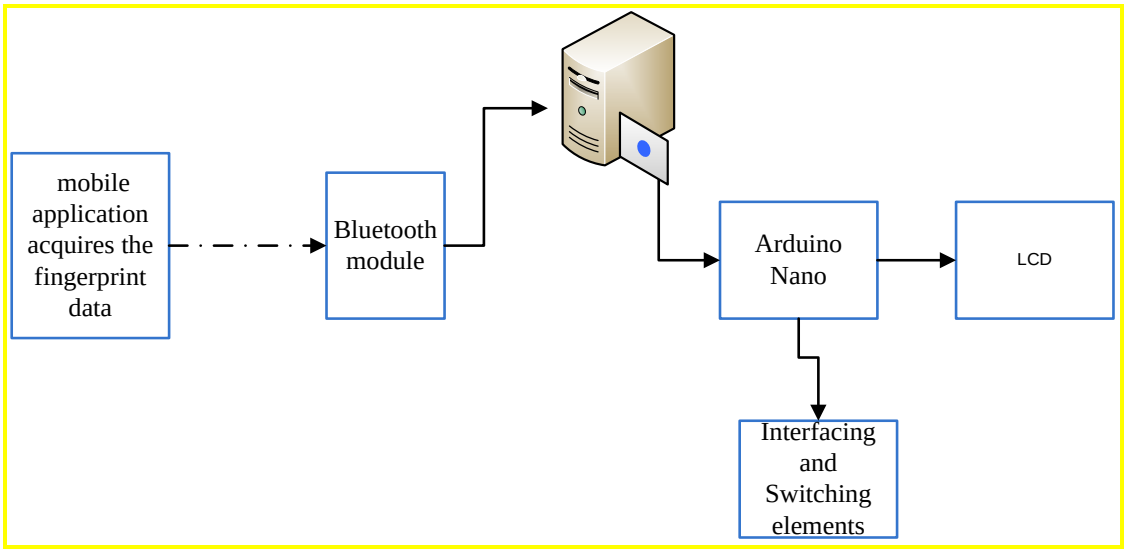

Figure 1. Block Diagram of the proposed system Design.

6. SYSTEM COMPONENTS

Table 1 lists and summarizes the component functions used in the proposed access control system circuit.

Table 1. List of System Component and Application Functions.

No	Component Type	Component function in the design
1	Arduino Nano	Main component in the circuit, it controls the circuit through the developed codes that are
2	Bluetooth module	Used to connect signals from the smartphone to the Arduino Nano board controller
3	Liquid-crystal display	The LCD screen is used to display a specific system output message.
4	LED and Buzzer	To alarm the system output events
5	Relay	Interfacing and Switching elements
6	Mobile application	Mobile equipped with android and applications to acquire the fingerprint data

7. OBTAINED DESIGN FUNCTIONAL TEST

Figure 2 illustrates the modified proposed system internal connections. To prove the concept, all the parts are connected as circuit design in figure 2. The Arduino controller is programmed to generate the required commands and events signal on both positive and negative results of the fingerprint comparison as shown in figure 2. Furthermore, mobile application is developed to acquire the fingerprint data of the user as shown in figure 4. In summary, the developed modified access control system components shown in figures 3 and 4 are designed to authenticate the identity of the user using the mobile application. Firstly, the system allows the user to connect the smartphone to the Bluetooth device and entering his fingerprint data through it into the system. Then the fingerprint entered is compared with predefined user data. If the fingerprint matched and correct the system display authorized person on the LCD.

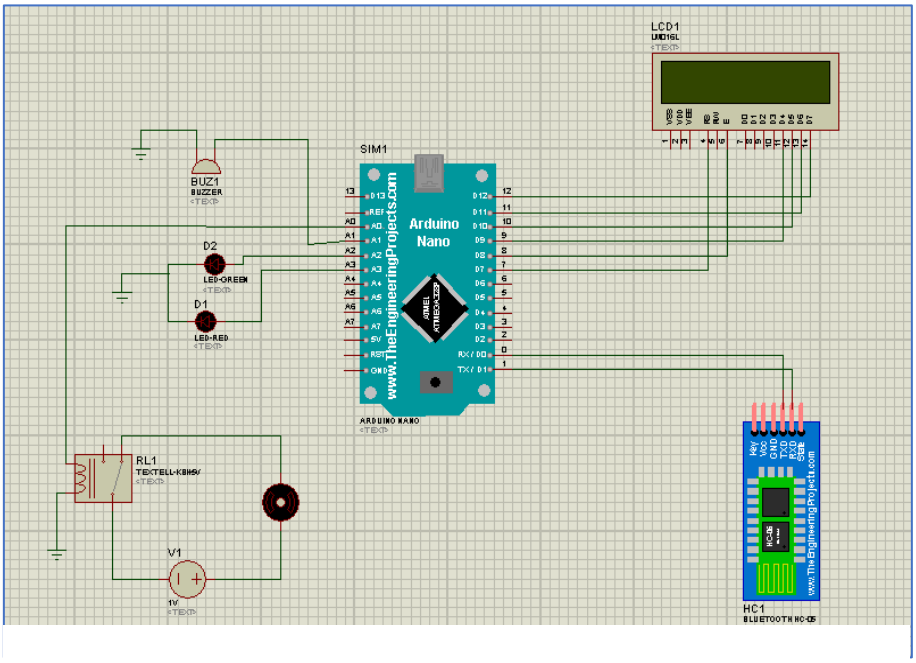

Figure 2. The Circuit Diagram of the Obtained Design.

7.1 The obtained design function test: system initialization

The power on the obtained design is initialized as shown in Figures 3 and 5, respectively, The Arduino displays the system initialization message as it appears on the screen. Figure 3 reflects the normal position of the access control system. Furthermore, the Android application in the mobile system displays an initiation screen, as shown in figure 4.

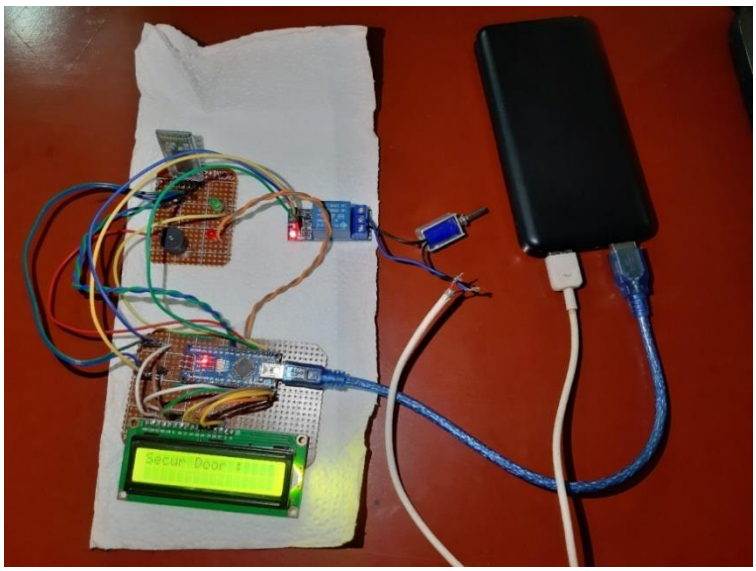

Figure 3. Obtained Design in Normal states (initialization state).

Figure 4. Mobile application initialization page Icons.

7.2 The obtained design function test: system connection

When the user opens the mobile application, the system directly prompts the user to connect the smartphone to the Bluetooth module in the circuit, as shown in figure 5. When the Bluetooth icon is pressed in the application, the list of available Bluetooth devices appears, as shown in figure 6, and the Bluetooth module of the circuit HC-05 should be selected.

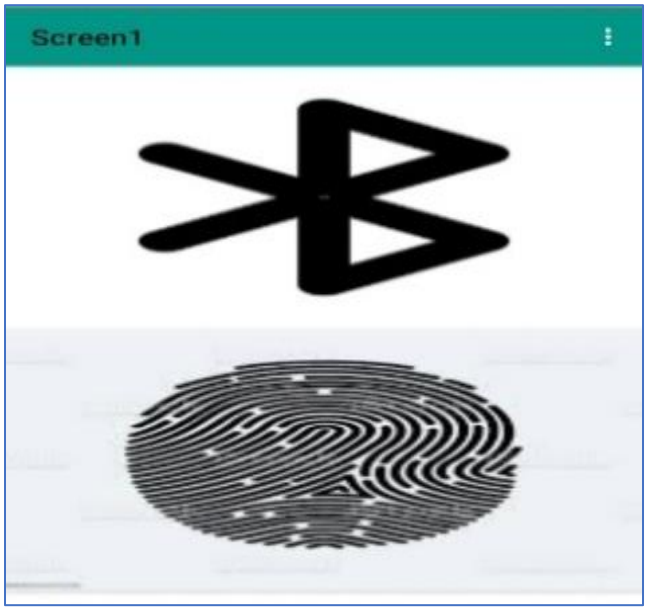

Figure 5. Mobile Application Interface.

Figure 6. List of Bluetooth Devices Shown by The Mobile Application.

7.3 The obtained design function test: User authentication

When the mobile application is connected to the system through the Bluetooth module, the application prompts the user to read the fingerprint from the smartphone, as shown in figure 7.

Figure 7. Read the Fingerprint.

If the entered fingerprint matched the predefined use, the mobile application displays the message fingerprint has been recognized as shown in figure 8

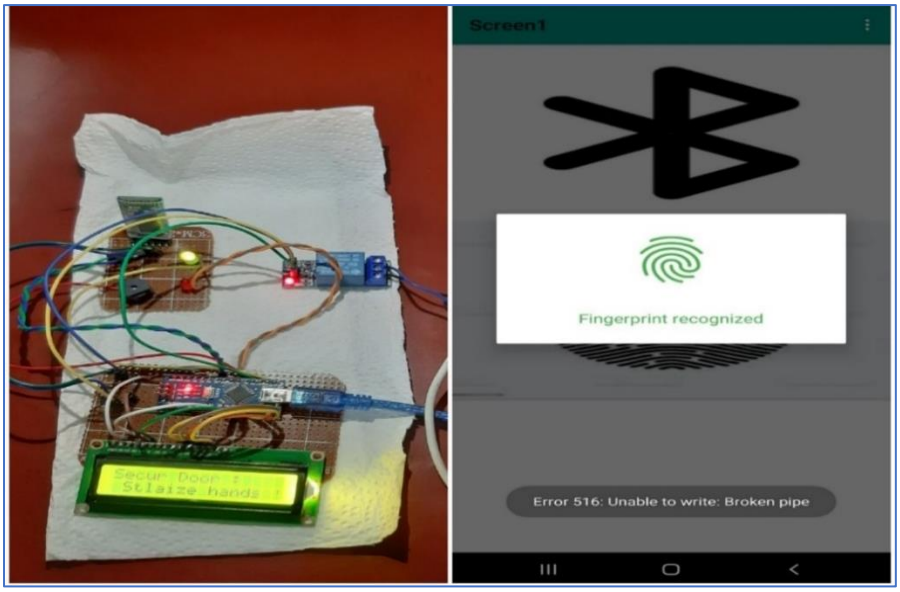

Figure 8. Authentication success (Fingerprint Matches).

7.4 The obtained design function test: User authentication

Suppose the entered fingerprint does not match any predefined user. In that case, a message will appear on the smartphone informing the user that his authentication is failing, as shown in figure 9 (the fingerprint is not recognized), and the buzzer alerting three times to call for any further action.

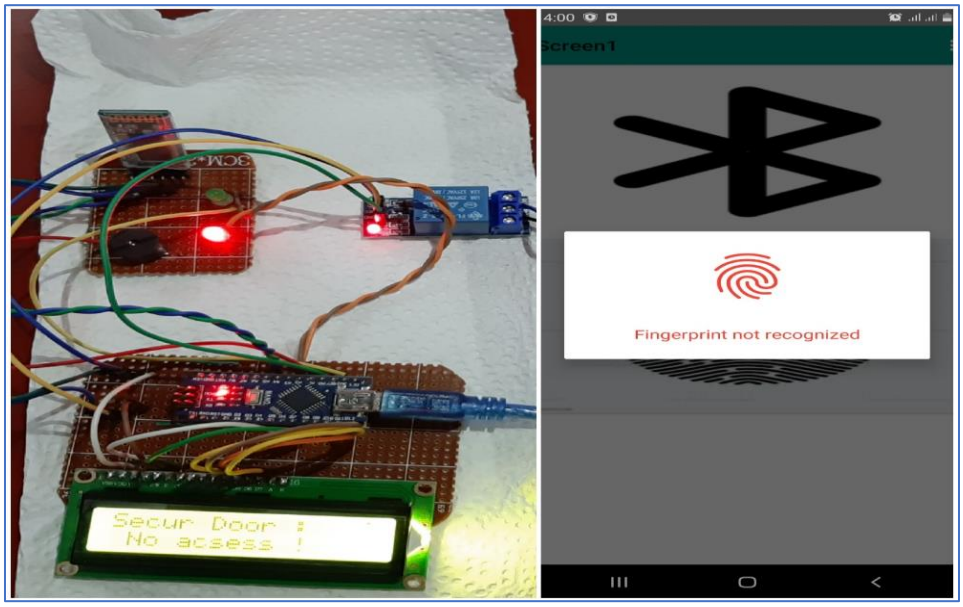

Figure 9. System State on Authentication Fails (Fingerprint Dose Not Match).

8. CONCLUSION

In this work, a modified access control system is developed and tested. The modified and tested design will not expose the users to touching a central system. Thus, it will eventually comply with the COVID-19 social distancing spreading touch restrictions. The obtained design test results show that with a simple mobile application, the individual fingerprint data is sent via the Bluetooth device to the microcontroller to be compared with the fingerprints registered in the database to control the overall access system different functions and operations.

References

Ferreira, A., Lenzini, G., Santos-Pereira, C., Augusto, A. B., & Correia, M. E. (2014). Envisioning secure and usable access control for patients. 2014 IEEE 3nd International Conference on Serious Games and Applications for Health (SeGAH),

Haofeng, J., & Xiaorui, G. (2019). Wi-Fi secure access control system based on geo-fence. 2019 IEEE Symposium on Computers and Communications (ISCC),

Huang, Y.-C. (2009). Secure access control scheme of RFID system application. 2009 Fifth International Conference on Information Assurance and Security,

Hwang, I.-K., & Baek, J.-W. (2007). Wireless access monitoring and control system based on digital door lock. *IEEE Transactions on Consumer Electronics*, *53*(4), 1724-1730.

Xie, Y., Wen, H., Wu, J., Jiang, Y., Meng, J., Guo, X., Xu, A., & Guan, Z. (2015). Three-layers secure access control for cloud-based smart grids. 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall),