ULUSLARARASI 3B YAZICI TEKNOLOJİLERİ
VE DİJİTAL ENDÜSTRİ DERGİSİ

INTERNATIONAL JOURNAL OF 3D PRINTING
TECHNOLOGIES AND DIGITAL INDUSTRY

ISSN:2602-3350 (Online)

URL: https://dergipark.org.tr/ij3dptdi

SMART DOOR LOCK DESIGN WITH INTERNET OF THINGS

Yazarlar (Authors): Samed Kaya, Elmas Aşkar Ayyıldız, Mustafa Ayyıldız*

Bu makaleye şu şekilde atıfta bulunabilirsiniz (To cite to this article): *Kaya S., Ayyıldız E. A., "Smart Door Lock Design With Internet of Things" Int. J. of 3D Printing Tech. Dig. Ind., 6(2): 201-206, (2022).*

DOI: 10.46519/ij3dptdi.1074468

Araştırma Makale/ Research Article

Erişim Linki: (To link to this article): https://dergipark.org.tr/en/pub/ij3dptdi/archive

SMART DOOR LOCK DESIGN WITH INTERNET OF THINGS

Samed Kaya[a], Elmas Aşkar Ayyıldız[a], Mustafa Ayyıldız[b]*

[a]Düzce University, Institute of Science, TURKEY
[b]Düzce University, Faculty of Engineering, Mechanical Engineering Department, TURKEY

* *Sorumlu Yazar: mustafaayyildiz@duzce.edu.tr*

(**Received:** 16.02.2022; **Revised:** 23.03.2022; **Accepted:** 28.06.2022)

ABSTRACT

Most of today's electronic devices are becoming smart and traditional house doors are lagging behind this technology. With the development of technology, the need for remote and rapid control of devices has increased. With the internet of objects, it was possible to make the devices remotely available over a Wi-Fi network. In this study, remote control of the devices has been done by using ESP32 development board which includes Wi-Fi module. Here, an intelligent system consisting of ESP32, android based remote control application, solenoid door lock, fingerprint sensor, RFID card reader and keypad is provided. With the ESP32 module, doors that can be controlled remotely and intelligently can be controlled and transmit data instantly. So; a device that is controllable, safe, economic, easy to control.

Keywords: Internet of Things, ESP32, Sensor, Smart Door Lock.

1. INTRODUCTION

As most of today's electronic devices have become smart, the lack of change in traditional doors has caused them to lag behind technology. In fact, everyone is a key for doors that cannot be opened without a mechanical key. The same can be said for the credit, bank, transportation or personnel cards used. It is thought that mechanical switches should disappear and keep up with technology. In these cases, the doors can be controlled remotely or without a key, either with the keypad on the door panel, fingerprint or card reader, with a scanner or a mobile application. Thus, a safer, easier and more economical life will be provided.

The Internet of Things enables devices to communicate with each other. Intelligent systems are developed to facilitate people's lives, to benefit economically, to save energy and to ensure human life safety. Changing the opening of doors with traditional methods has been made possible by the Internet of Things. There are studies in the literature in which these methods are applied separately. Park et al. conducted a study in which the door was integrated into the smart home system and controlled with the help of sensors [1]. Kassem et al. performed smart lock study using a wireless security system [2]. Delgado et al. studied for keys that cannot be physically cloned for smart lock systems using bluetooth [3]. Merkepçi and Özyazıcı worked on fingerprint-based door lock and personnel attendance control system [4]. Verma worked on a digital security system with door lock system using RFID technology [5]. Mishra et al. conducted research on the security of passwords in lock systems and concluded that they provide adequate security [6]. Turak worked on the internet and security of objects and shared them by mentioning a few problems. [7]. Uçar worked on the internet of things, smart classrooms and student tracking system [8]. Andreas et al. studied the door security system for home monitoring based on ESP32 [9]. Hwang and Baek worked on a wireless access monitoring and control system based on a digital door lock [10]. Mandula et al. studied mobile-based home automation using the Internet of things [11]. Süzen and Kayaalp designed an Arduino-based computer aided measurement system for students taking physics courses to use in laboratory applications [12]. Çelebi et al. a 6-axis robot arm, which is one of the industrial automation systems and widely used, was designed and produced with a 3D printer [13].

In this study, using the Internet of Things technology, which is a module of Industry 4.0, an open source programmable ESP32 card, a smart door lock that can be accessed with both remote control and fingerprint sensor and RFID Card reader, was carried out.

2. INDUSTRY 4.0 AND THE INTERNET OF THINGS

2.1. Industry 4.0

The Internet of Things is like a change that is extensively restructuring the industry, it could even be said to be the next industrial revolution. This revolution is an innovation that follows the mechanization (1800), mass production (1900) and automation (2000) revolutions. As the fourth generation; It is an approach where software and hardware are monitored, analyzed and managed through the networks of the world. This approach; It is a term adopted by companies, universities, trade unions and the government in Germany [14]. It also represents the vision of the future of manufacturing not only in Germany but worldwide. The main purpose of this initiative is the desire to have the latest manufacturing technologies, starting from the term "smart factory". B.Heuchemer, vice president of marketing at Siemens, a technology company based in Germany, said that the aim of Industry 4.0; He said that restructuring the industry by combining virtual, physical and cyber systems and producing a new product is to ensure that it remains active continuously [15].

2.2. Internet of Things

The Internet of Things is defined as a world-wide network of uniquely addressable objects created between each other, and all addressed objects in this network are in communication with each other through certain protocols. Also; It is possible to say a system of devices that communicate with each other, connect with each other using various types of communication protocols, and have formed a smart, giant network by sharing information with each other. With the Internet of Things, first used by Ashton in 1999, each object will have the ability to be accessed over a network. It is estimated that by 2020 there will be more than 24 billion IoT devices.

Studies in the field of home automation are generally carried out on water and energy consumption [16]. Apart from these, remote control applications, thief detection and attack systems are established for museums. However, the most important risk factors for these systems are security and user privacy. In a study related to this, a total of 32 risk factors were determined, four of which were defined as serious risks. These are risks linked to software vulnerabilities and human behavior: Privacy, security, risk analysis, security and privacy design. In order to remove these risks, security and privacy must be properly integrated into the designed system at the initial design stage [17]. All objects in home automation communicate with each other via wireless networks. For this to happen, a machine-machine based smart home and security system can be set up. Cloud computing and smart building-based technologies can be used in a building and facility that cooperates with various sensors (detection devices) and can work efficiently. The use of building monitoring and management systems is very important for the energy consumed by smart buildings to be more efficient. The cloud-based building management system to be installed automatically selects the optimum feature of computer resources and storages [17].

3. MATERIALS AND METHODS

ESP32 is an open-source programmable electronic circuit. It has been produced to realize Internet of Things applications in an economical way. "C ++" programming language is used to program the ESP32 board. In order to convert the created algorithm into a language that the device can understand, it was connected to the card with the Arduino IDE program and the codes written were uploaded to the card [18]. The most important reason for this card to be preferred is that it can connect to wireless networks and it allows other devices to connect by spreading its own internet network. Flow diagram of the designed system is given in Figure 1.

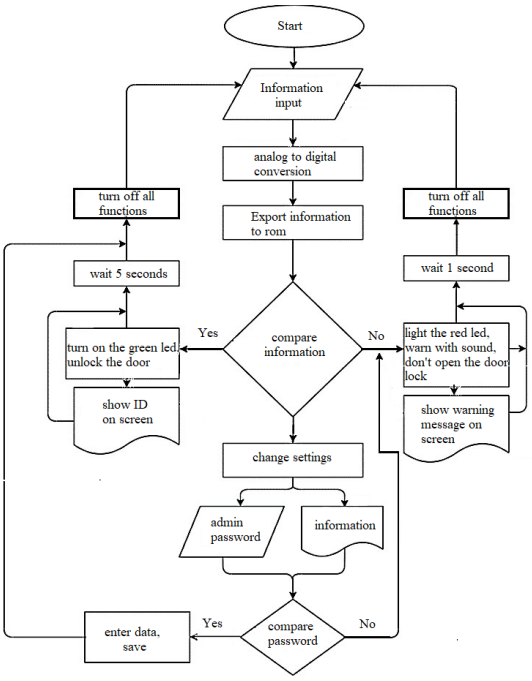

Figure 1. Flow diagram of the system.

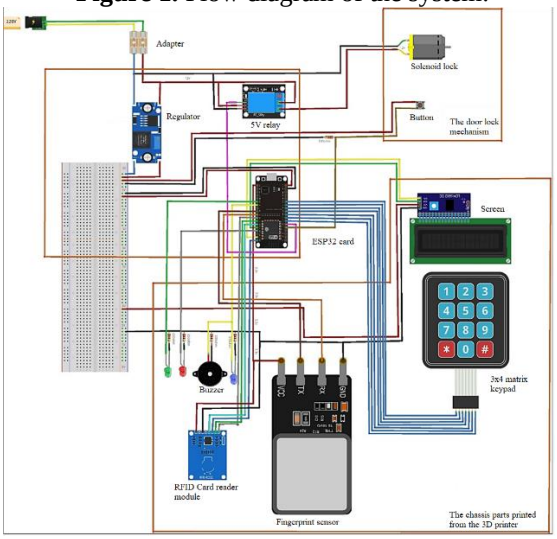

Figure 2. The electrical connection diagram of the designed hardware.

3.1. Hardware Design

In addition to the ESP32 card used as the processor of the designed system, Adafurid brand fingerprint sensor, RFID Card reader module, 12 V solenoid lock mechanism, 3x4 matrix keypad, adapter, 5 V to 3.3 V converter regulator and the chassis parts printed from the 3D printer. are available. A 5 V relay circuit has been integrated into the system in order to trigger the open or closed positions of the solenoid lock. The electrical connection diagram of the designed hardware is shown in Figure 2. After the electronic design is completed, a case and panel are designed in a design program. Later, these designs were produced with a 3D printer (Figure 3). All parts are designed modularly for easy assembly. The assembled form is shown in Figure 4.

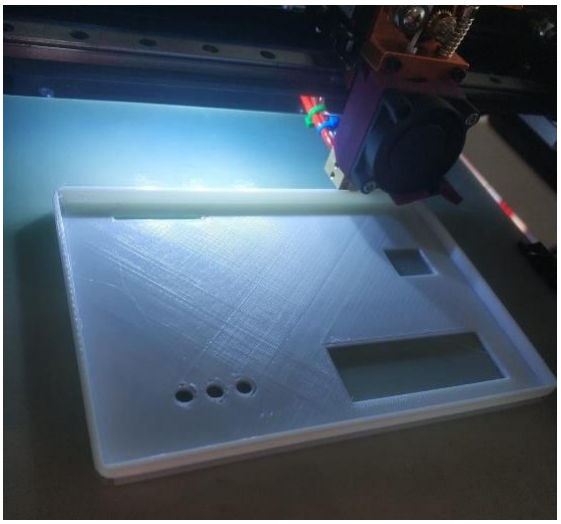

Figure 3. Panel part printed on a 3D printer.

Figure 4. The case and panel assembled.

3.2. Software Design

The system can be controlled both via internet browser and mobile application. The mobile application is programmed for android devices with the site named "App Inverter" and its output is shown in Figure 5. Turkish was chosen as the user language of the designed program. When the lock is always active, no input can be made on the device. In order to activate it, it is necessary to press the "Sürekli kapat" button on the application.

Figure 5. Door open status in Android application.

From the moment the device is turned on, it waits for the user to input using any method. Data entered; If it matches the one in the memory, the lock opens and closes automatically after a while. If the incoming data does not match, it gives an audible and visual warning. Methods that can be input:

- By entering the password, which was previously stored in the memory and can be changed by the administrator at any time, from the keypad.
- By scanning one of the compatible fingerprints on the sensor, which were previously stored in memory and can be changed by the administrator at any time.
- Using one of the entry cards previously stored in memory.
- By opening the door with the button inside for the exit.
- By pressing the relevant button on the internet browser or mobile application.

In Figure 6 and Figure 7, fingerprints are separated from each other and shown on the screen according to the user registration number.

Figure 6. Smart Door Lock Warning: Approved fingerprint.

Figure 7. Smart Door Lock Warning: Rejected fingerprint.

To add a new fingerprint, a new and idle user number is prompted to be entered and saved. Finger deletion proceeds in the same way. In addition, these operations are only activated by the administrator using the application, with the signal sent from the application, and can be performed after entering the administrator password correctly. These interventions are shown in Figure 8.

Figure 8. Smart Door Lock Operations: Admin Login.

When logging in with an RFID card, it can open the door after reading one of the cards in the memory. Regardless of whether it is true or false, the "ID" numbers of all cards read on the screen are shown in Figure 9.

Figure 9. ID number of the unconfirmed card.

The last added sound feature is; It is added to test the buzzer and lights in the system and it is

possible to make a melody on the application if desired.

4. DISCUSSION AND CONCLUSION

Providing remote control of electrical devices and goods provides serious security and economic savings. It is certain that smart locks will make people's lives noticeably easier in the market. In this study, an exemplary smart door lock prototype was created by using the ESP32 development board, designing an android application and creating a safe from a 3D printer. With the application created, the door can be controlled by accessing the application at every point via Wi-Fi. The final product is obtained by assembling the electronic components to the parts printed from the three-dimensional printer. Thus; An auditable, safe, easy-to-control and developable prototype was designed.

ACKNOWLEDGES

A part of this study was presented as an oral presentation at the 5th International Congress On 3D Printing (Additive Manufacturing) Technologies and Digital Industry held between 3-5 June 2021 and was included in the abstract booklet.

REFERENCES

1. Park, Y.T., Sthapit, P., and Pyun, J. Y., "Smart Digital Door Lock For The Home Automation", In TENCON 2009-2009 IEEE Region 10 Conference, Pages 1-6. Singapore, 2009.

2. Kassem, A., El Murr, S., Jamous, G., Saad, E., and Geagea, M., "A Smart Lock System Using Wi-Fi Security", 3rd International Conference On Advances İn Computational Tools For Engineering Applications (ACTEA), Pages 222-225, Lebanon, 2006.

3. Prada-Delgado, M.A., Vazquez-Reyes, A., and Baturone, I., "Physical Unclonable Keys For Smart Lock Systems Using Bluetooth Low Energy", In IECON 2016-42nd Annual Conference Of The IEEE Industrial Electronics Society, Pages 4808-4813, Italy, 2016.

4. Merkepçi, M., and Özyazıcı, M.S., "Kablosuz Ağ Tabanlı, Parmak İzi Tanımalı Personel Takip Sistemi", Anka E-Dergi, Cilt 2, Sayı 2, Sayfa 48-58, 2015.

5. Verma, G.K., and Tripathi, P., "A Digital Security System With Door Lock System Using RFID Technology", International Journal Of Computer Applications, Vol. 5, İssue 11, Pages 6-8, 2010.

6. Mishra, A., Sharma, S., Dubey, S., and Dubey, S.K., "Password Based Security Lock System", International Journal Of Advanced Technology İn Engineering And Science, Vol. 2, Issue 5, Pages 100-103, 2014.

7. Turak, Y., "Nesnelerin İnterneti ve Güvenliği",http://www.yigitturak.com/wp-content/uploads/IoTGuvenligi.pdf, Nisan 2, 2021.

8. Uçar, A., ve Uludağ, M.H., "Nesnelerin İnterneti (Iot) İle Akıllı Sınıf Ve Öğrenci Takip Sistemi Tasarımı", DÜMF Mühendislik Dergisi, Cilt 9, Sayı 2, Sayfa 591-600, 2018.

9. Aldawira, C.R., Putra, H.W., Hanafiah, N., Surjarwo, S., and Wibisurya, A., "Door Security System For Home Monitoring Based On ESP32", Procedia Computer Science, Vol. 157, Pages 673-682, 2009.

10. Hwang, I.K., and Baek, J.W., "Wireless Access Monitoring And Control System Based On Digital Door Lock", IEEE Transactions On Consumer Electronics, Vol. 53, Issue 4, Pages 1724-1730, 2007.

11. Mandula, K., Parupalli, R., Murty, C.A., Magesh, E., and Lunagariya, R., "Mobile Based Home Automation Using Internet Of Things (Iot)", In 2015 International Conference On Control, Instrumentation, Communication And Computational Technologies (ICCICCT), Pages 340-343, India, 2015.

12. Süzen, A.A., and Kayaalp, K., "Free fall test system controlled by computer with Arduino", Mühendislik Bilimleri ve Tasarım Dergisi, Cilt 7, Sayı 4, Sayfa 878-884, 2019.

13. Çelebi, A., Korkmaz, A., Yılmaz, T., and Tosun, H., "3 boyutlu yazıcı ile 6 eksenli robot kol tasarım ve imalatı", International Journal of 3D Printing Technologies and Digital Industry, Cilt 3, Sayı 3, Sayfa 269-278, 2019.

14. Yıldız, A., "Endüstri 4.0 ve Akıllı Fabrikalar," Sakarya University Journal Of Science, Cilt 22, Sayı 2, Sayfa 546-556, 2018.

15. Lasi, H., Fettke, P., Kemper, H. G., Feld, T., and Hoffmann, M., "Industry 4.0", Business & İnformation Systems Engineering, Vol. 6, Issue 4, Pages 239-242, 2014.

16. Gökrem, L., ve Bozuklu, M., "Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki

Mevcut Durum", Gaziosmanpaşa Bilimsel Araştırma Dergisi, Sayı 13, Sayfa 47-68, 2016.

17. Ercan, T., ve Kutay, M., "Endüstride Nesnelerin Interneti (Iot) Uygulamaları", Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, Cilt 16, Sayı 3, Sayfa 599-607, 2016.

18. Turley, C., Montironi, M.A., and Cheng, H. H., "Programming Arduino Boards With The C/C++ İnterpreter Ch", In ASME 2015 International Design Engineering Technical Conferences And Computers And Information İn Engineering Conference, Pages 10, Boston, 2015.