ICIC Express Letters
Part B: Applications
Volume **12**, Number **10**, October **2021**

ICIC International ©2021 ISSN 2185-2766
pp. **965–970**

THE DEVELOPMENT OF A SMART DOOR DECISION SYSTEM, BASED ON PIR SENSOR, EMBEDDED FACE RECOGNITION AND SERVER REQUEST USING TTGO ESP 32

Anderies[1], Bakti Amirul Jabar[1], Rezki Yunanda[1]
and Alexander Agung Santoso Gunawan[2,*]

[1]BINUS Graduate Program – Master of Information Technology
[2]Computer Science Department, School of Computer Science
Bina Nusantara University
Jl. K. H. Syahdan No. 9, Kemanggisan, Palmerah, Jakarta 11480, Indonesia
{ anderies; bakti.jabar; rezki.yunanda }@binus.edu; *Corresponding author: aagung@binus.edu

Received December 2020; accepted March 2021

Abstract. *The Internet of Things is the use of Internet technology through objects connected to another. The current utilization of IoT can improve the security system and the accessibility of a home. Nowadays, most house locks use a physical or mechanical key, which can potentially damage, lose, and risk the lock key duplication by unwanted parties. This research discussed the smart door decision system using a motion sensor, face recognition, and mobile application in the opening-closing door. Our smart door design is pointing to affordable price and flexibility design. This study found that the door can provide a free price for Indonesian houses or individual homes without any server cost and cloud functions invocation charged monthly in heavy door activities at the individual house. The result is complemented by daily data recording for each door.*
Keywords: Internet of Things, Face recognition, Smart door, Smart home

1. **Introduction.** In this era of industrial revolution 4.0, the Internet of Things (IoT) is becoming a hot topic of conversation. The concept has the potential to influence our lifestyle and how we work. IoT can communicate with smart objects and lead to on-demand communication: anytime, anywhere, any media, and any device [1]. The Internet of Things is the global infrastructure of the information society, enabling advanced services through interconnection and communication technologies [2]. In principle, IoT can provide identification to devices with Internet-based communication structures. IoT is the evolution of Internet network technology by connecting devices such as sensors to carry out certain functions; IoT devices tend to save power but have shortcomings in data storage [3].

Cloud databases can handle shortcomings in data storage on IoT devices. Firebase is a cloud database and a platform to support mobile and web-based application development or back-end as a service [4]. Firebase provides services such as real-time databases, cloud messaging, authentication, and hosting. A real-time database is a cloud-based database in Firebase and does not require queries in managing the database or what is known as NoSQL the application of IoT for smart home now also concentrates on the security and accessibility of a home. Previously, for home security, mechanical locks were used for doors. The disadvantage of using a mechanical lock is that the door must be opened using the original key. This system is considered less safe and inefficient because the door's mechanical system can be modified to force opening the door. Besides, humans also carry a physical key to open the door and risk losing the key.

DOI: 10.24507/icicelb.12.10.965

Research conducted by [5] makes smart doors using Arduino and Amazon web services which notify the disturbance that occurs at the door by sending an email notification to the owner. This system only notifies the disturbance at the door and cannot control the door, such as locking the door automatically. Facial recognition enabled smart door using Microsoft face API conducted by [6]. In this work, an automatic door access system by using face recognition and detection is presented. Automatic face recognition is done by neural networks. Raspberry Pi controller controls the door access after successful output from the PC. This system's disadvantages are that system processing is slow, the door stays open indefinitely, and it is not suitable for real time. In a study conducted by [7] making a smart lock on a door connected to a smartphone, this tool allows the system to be accessed via mobile, but in this study, there is no scheduling system when the door is opening or closing. In previous research, we concluded that there is no robust system enough to manage multiple door activities or discuss the affordability of a smart door system.

This paper is pointing to the affordability and flexibility of smart door architecture and arranges Section one as an introduction, Section two as architecture overview and analysis, Section three as previous work review, Section four as network and affordability evaluation of architecture and finally completed by conclusions and suggestions.

2. **Smart Door Design Architecture.** The following (see Figure 1) is the architecture of the smart door. In this decision-making system for door closing/opening activities, it has three parameters for a 5 V relay to drive solenoid action. The first parameter is passive infrared (PIR) sensor to detect a movement, the second is server response from a mobile application, and the third is modified TTGO ESP 32 cam to recognize a list of faces that have been registered before on the device. Face recognition is based on a light CNN algorithm implemented [8]. Input parameters and action output are controlled via an electronic board Wemos D1 Mini. This electronic board is equipped with ESP8266 [9], which can be connected directly to the Internet, and then this electronic board is connected to a back-end platform as a service with a Firebase real-time database. After

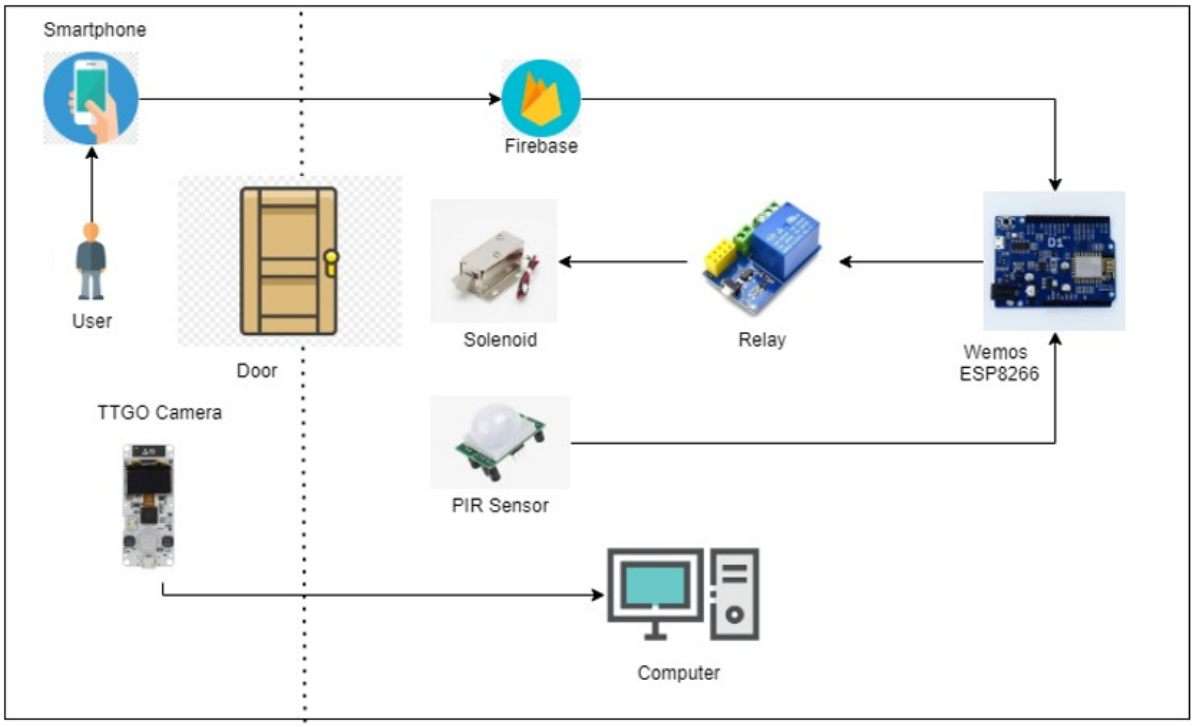

FIGURE 1. Smart door decision-making architecture

the electronic board is connected to the back-end platform, it can be controlled and monitored by user smartphone device.

Smart door components consist of two micro-controller TTGO ESP 32 cam and Wemos D1 Mini, for TTGO cam as face detection module and Wemos D1 Mini as the central controller to decide opening/closing door. For the power source and a motor, we use a 3.3 V relay as a switch connected to a solenoid motor, a solenoid door lock as a motor to open or close activities, and a 12 V adapter used as a power source of a solenoid door lock. The passive infrared sensor is also used as an input parameter for detecting movement in front of the door.

3. **Previous Work.** In this section, we analyze the smart door design by looking at the previously studies in smart door designs and compare to our smart door design.

Table 1. Previous smart door

Design name	Design description
Basha et al. [5]	Using ADXL345 accelerometer to detect and to record data when the door is open but cannot open the door with a sensor.
Maheshwari [6]	Design with Rasberry and Microsoft API face recognition to open doors. The design made cannot record historical data and also still rely on server computation to detect face it will affect more cost to use cloud functions.
Park et al. [10]	Smart door automation is built based on Zigbee. The design is made quite modern, but the cost is high for implementing it.
Surantha and Wicaksono [11]	Design smart home security system using object recognition and PIR sensor with Raspiberry PI 3 and perform histogram of gradient and support vector machine to detect suspicious object.
Sandesh et al. [12]	Smart door recognition system uses face image capturing and processing with Raspiberry PI and Raspiberry PI camera.
Syafa'Ah et al. [13]	Smart home system which includes door, lighting, camera and infrared furniture is connected to a central server via WIFI media by using data communication based on HTTP protocol, using IP camera.

From Surantha and Wicaksono [11], it can be concluded that the respond speed for face detection and the appropriate method to open the door is really important. Sandesh et al. [12] proposed to use PIR or proximity sensor rather than taking a picture for detecting people. We would like to combine above approaches by using PIR together with camera for face detection.

In Syafa'Ah et al.'s study [13], appliances and door are connected using HTTP protocol and controlled via IP camera. Limitations of this application are that camera only can be controlled or monitored via the same WIFI and the system uses the HTTP protocol to transfer light data which causes waste of resources and resulted on pricey charge when implementing on large-scale door.

In Basha et al.'s architecture [5] it is tried to record door activities and send it to the cloud to monitor but using a not convenient method to open/close the door. In Maheshwari's architecture [6] using Microsoft API to detect the face of users, it will consume time and more bandwidth because computation is happening on the cloud and

this design needs much data transfer over the Internet and results in slow response of door activities.

Our study is to improve others' architecture and by replacing cloud Microsoft API invocation in Maheshwari to embed computation edge for owners and face detection, and pointing on flexibility by hardware built, simple database document format and affordability design in single or multiple doors based on MQTT protocol [14,15].

We used Firebase for database (See Figure 3) to achieve the goal of flexible architecture. The authors have designed a simple database format, if smart door architecture wants to expand controlling multiple doors. Adding data_home_numbers and histories_numbers, numbers here represent each door of houses.

4. **Result and Evaluation of Smart Door Architecture.** This section discusses the evaluation and result of smart door architecture implementation in the previous section by illustrating the house door prototype as shown in Figure 2.

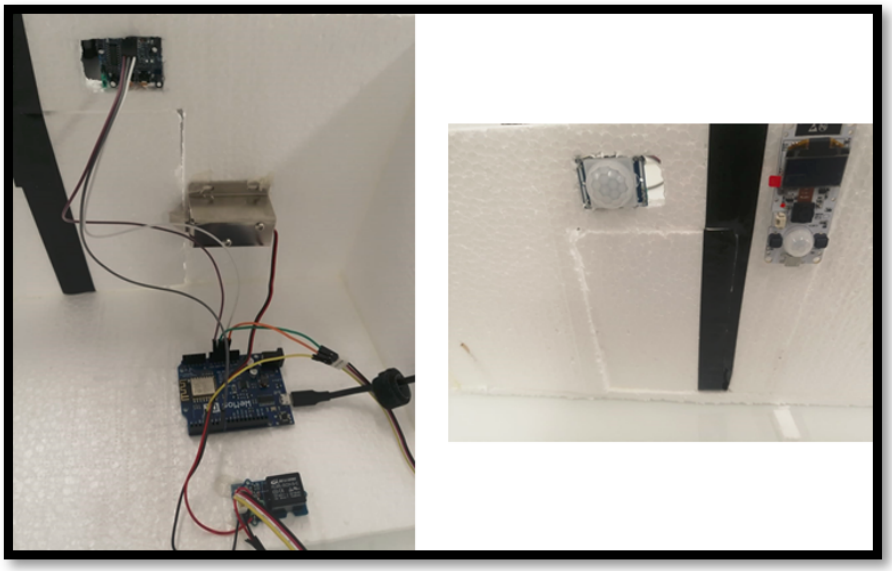

FIGURE 2. Smart door prototype using two microcontroller TTGO cam and Wemos D1 Mini

The results of smart door architecture are as follows.

a. Functionality logic testing

Solenoid lock opens if there is movement on the PIR sensor and presses the "open" button on the Android application. The procedure was carried out by giving treatment to the Android application and the PIR sensor. Table 2 explains the results of testing the PIR sensor and the Android application against the solenoid. From these outcomes, it was known that when the PIR sensor detects movement, and when the user presses the "open" button on the application, the solenoid can open the door. On the other hand, when the PIR sensor does not detect movement, the door cannot be opened even if the user presses the open button on the application.

TABLE 2. PIR test matrix and Android application

Android application	**PIR sensor**	**Solenoid lock**
"Open" button is pressed	Motion detected	Opened
"Open" button is pressed	Motion undetected	Locked
–	Motion detected	Locked
–	Motion undetected	Locked

b. The system has successfully updated the data in Firebase

The test scenario was to open the Firebase real-time database server by pressing the "open" button on the Android application. Figure 3 explicates that the Firebase real-time database server adds one row of data to the "histories" when the user presses the "open" button, which can be likened to the time when the smart door opens. In addition, in Figure 3, the "data" column on the Firebase real-time database server is updated to "1" then returns to "0" after 5 seconds. This fact indicates that the solenoid unlocks when the "data" column in Firebase is valued "1" and will be locked when the value is "0" and after unlocking the door, it will automatically lock again in 5 seconds. The scenario above proves that the implementation of the smart door system successfully records data in Firebase in the form of a history log.

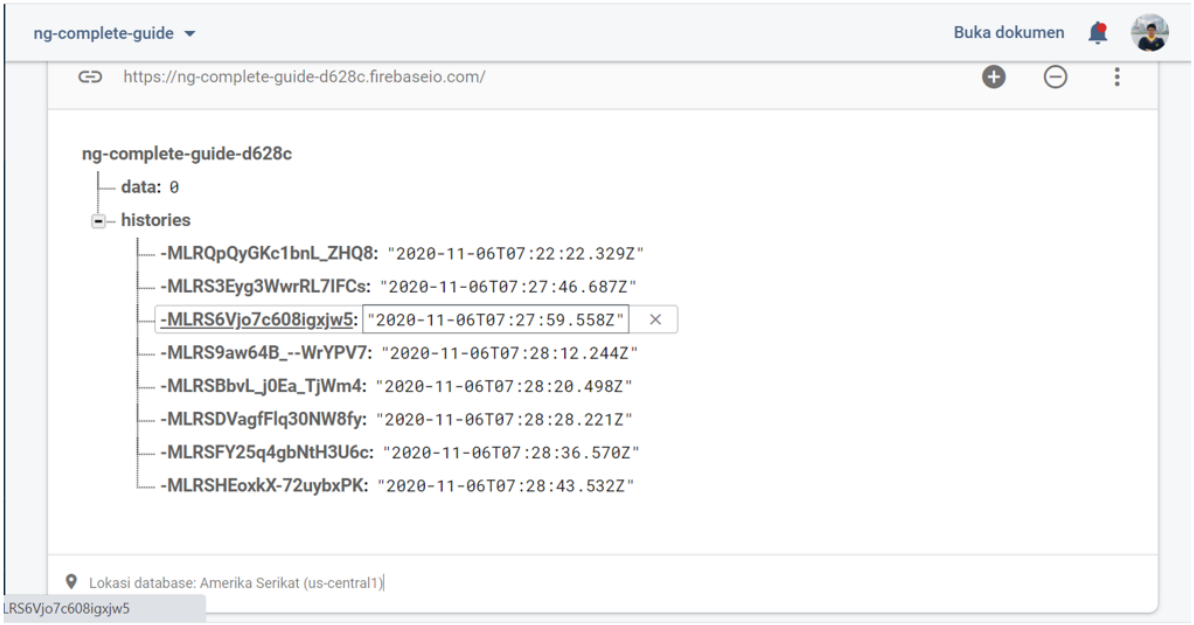

Figure 3. Firebase real-time database server for IoT smart door

c. TTGO camera can identify users

There were two elements tested; the first was the users' faces, which had been registered, and the second was those unregistered. The test was done by bringing the face closer in front of the TTGO camera. Table 3 shows the outcomes of the tests. These outcomes indicate that with the implementation of TTGO on a smart door, the TTGO camera can detect registered user faces on the device.

Table 3. Matrix of user's faces and TTGO camera

Users' face	TTGO camera
Registered	Users' faces are recognized.
Unregistered	Users' faces are unrecognized.

After hardware functionality testing, we do another evaluation of our smart door prototype. First is network latency evaluation after ten trials of aggressive send and transfer data. We found that it needs 0.3 s from smartphone to server and 4 s from server to Wemos D1 Mini. We can consider this as the average result of network latency and lead to further improvement. Secondly, in the affordable evaluation of system design, we tested our smart door system design with quite a lot of useful activity during the smart door development phase and testing phase in a week without any server's cost. We also found a service price list from the Firebase website announcing that 20,000 read/write usage

in a day is still within the free service limit and it shows that we can implement these services more than one door, it can be 200 doors with 100 closing/opening activities as long as it does not exceed the limitation of 20,000 closing/opening in whole day usage activities and 100 simultaneous connections.

5. **Conclusions and Suggestions.** This study points to the affordability and flexibility architecture of the smart door, authors have successfully built a simple database document format and minimum hardware required with embedded face recognition and endure aggressive transfer read and write data and smart door are working properly complemented by record history data feature. In further studies, authors want to reduce network latency of architecture design and add a more robust feature that enables homeowners to gain more flexibility and convenience usage.

REFERENCES

[1] L. Atzori, A. Iera and G. Morabito, The Internet of Things: A survey, *Comput. Networks*, vol.54, no.15, pp.2787-2805, DOI: 10.1016/j.comnet.2010.05.010, 2010.

[2] K. K. Patel and S. M. Patel, Internet of Things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges, *Int. J. Eng. Sci. Comput.*, vol.6, no.5, 2016.

[3] F. E. Barnicha, A. Khallaayoun and R. Lghoul, *Smart Home Energy Management System Monitoring and Control of Appliances Using an Arduino Based Network in the Context of a Micro-Grid*, Project Report, Alakhawayn Univ., 2015.

[4] W.-J. Li, C. Yen, Y.-S. Lin, S.-C. Tung and S. Huang, JustIoT Internet of Things based on the Firebase real-time database, *2018 IEEE International Conference on Smart Manufacturing, Industrial & Logistics Engineering (SMILE)*, pp.43-47, DOI: 10.1109/SMILE.2018.8353979, 2018.

[5] S. N. Basha, S. A. K. Jilani and M. S. Arun, An intelligent door system using Raspberry Pi and Amazon web services IOT, *Int. J. Eng. Trends Technol.*, vol.33, no.2, pp.84-89, 2016.

[6] K. Maheshwari, Facial recognition enabled smart door using microsoft face API, *arXiv.org*, arXiv: 1706.00498, 2017.

[7] K. S. Viraja, K. Kumar, C. Keerthi and G. Sandeep, IOT based smart door system, *Int. J. Res. Appl. Sci. Eng. Technol.*, vol.6, pp.438-443, DOI: 10.22214/IJRASET.2018.4077, 2018.

[8] Y. LeCun, B. Boser, J. S. Denker et al., Backpropagation applied to handwritten zip code recognition, *Neural Comput.*, vol.1, no.4, pp.541-551, 1989.

[9] M. Schwartz, *Internet of Things with ESP8266*, Packt Publishing Ltd., 2016.

[10] Y. T. Park, P. Sthapit and J.-Y. Pyun, Smart digital door lock for the home automation, *2009 IEEE Region 10 Conference (TENCON2009)*, DOI: 10.1109/TENCON.2009.5396038, 2009.

[11] N. Surantha and W. R. Wicaksono, Design of smart home security system using object recognition and PIR sensor, *Procedia Comput. Sci.*, vol.135, pp.465-472, 2018.

[12] R. Sandesh, A. Sridhar, T. P. Rishikesh, S. Farheen and S. Tameem, Smart door lock/unlock using raspberry Pi, *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol.6, no.3, DOI: 10.32628/CSEIT2063135, 2020.

[13] L. Syafa'Ah, A. E. Minarno, F. D. S. Sumadi and D. A. P. Rahayu, ESP8266 for control and monitoring in smart home application, *Proc. of 2019 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE2019)*, pp.123-128, DOI: 10.1109/ICOMITEE.2019.8921287, 2019.

[14] U. Hunkeler, H. L. Truong and A. Stanford-Clark, MQTT-S – A publish/subscribe protocol for wireless sensor networks, *The 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08)*, pp.791-798, 2008.

[15] D. Thangavel, X. Ma, A. Valera, H.-X. Tan and C. K.-Y. Tan, Performance evaluation of MQTT and CoAP via a common middleware, *2014 IEEE the 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2014.