Asian Journal of Natural Sciences (AJNS)
Vol.2, No.3, 2023: 153-162

Access Control System in the Tourism Resort by Using IoT to Increase Security and User-Friendly

I Gede Suputra Widharma[1*], Ketut Sumadi[2], I Nengah Sunaya[3], I Made Sajayasa[4], I Gde Nyoman Sangka[5]
[1,3,4,5]Politeknik Negeri Bali, [2]Universitas Hindu Negeri IBG Sugriwa Denpasar
Corresponding Author: I Gede Suputra Widharma suputra@pnb.ac.id

ARTICLEINFO

Keywords: Access Control System, IoT, Tourism Resort

Received : 2 July
Revised : 13 July
Accepted: 20 August

ABSTRACT

Radio Frequency Identification (RFID) technology is used to many applications, and among these applications is to determine the entry to rooms in different departments and hotels, RFID is used in technical process with Arduino program to control of access to rooms and buildings according references it's been connected to the LCD screen, in addition to a large animated LED display to display any phrase or statement using the Microcontroller, use Bluetooth instead of an RFID card to open the door with text or voice. RFID along with Internet-of-Things (IoT), is a secure, user-friendly and efficient method to safeguard things. This combination comes with advantages such as high security, simplicity, and cost-effectiveness. This paper proposes a Smart RFID-IoT based access control system

DOI: https://doi.org/10.55927/ajns.v2i3.4299
E-ISSN: 2986-2787
https://journal.formosapublisher.org/index.php/ajns

INTRODUCTION

Security and protection of personal belongings and valuables have always been a concern. Various locking and securing systems have evolved in due course of time. The locked and key turned out to be one of the most common and trustworthy methods of security. Access control systems have been around for quite some time, but there are always new innovations and technologies that are emerging to improve the security and convenient of these systems. The access control systems with RFID (radio frequency identifier) have been providing security and reliability to many kinds of medical and scientific facilities, laboratories, executive offices, official grounds, and locker room with limited access for people.

Biometric authentication is becoming more popular in access control systems as it offers a higher level of security and convenience than traditional methods like PINs and access cards. The biometric authentication uses unique physical characteristics such as fingerprints, facial recognition, or iris scans to identify and grant access to authorized individuals. Mobile devices such as smartphones and tablets can now be used as access control credentials. This technology eliminates the need for physical access cards or keys and allows users to access secured areas using their mobile devices. With cloud-based access control, users can remotely manage access control systems from anywhere with an internet connection. This technology provides greater flexibility and scalability, as users can add or remove access credentials and monitor activity in real-time.

Access control systems can now use artificial intelligence (AI) to learn and adapt to user behavior patterns. This technology can detect anomalies and potential security threats, and automatically adjust access privileges to mitigate risks. IoT-enabled access control systems can communicate with other smart devices to create a more integrated and automated security system. For example, when an access card is used, the system can turn on lights or adjust the temperature in the room. Technology of IoT implicates the use of other technologies, among which are: Transducers, sensors, RFID, smart technologies, and nanotechnologies. Also, another technologies such as bluetooth signal, Wireless Networking (Wi-Fi), and others, are used on most of smart-devices and applications. Identification of people, animals, or objects is essential in production chains and access control to buildings, warehouses, and shopping centers because it allows better control of merchandise or personnel. One of the technologies used to accomplish these tasks is RFID. This technology is widely used to automate the identification of objects and individuals. For example, it is common in most smartphones, RFID access cards to university campuses or residential subdivisions, and merchandise inside shopping centers. RFID systems are made up of two components: the transponder, which consists of the object to be identified, and the interrogator, the device that will identify the RFID cards. RFID-based access control systems can be classified according to their characteristics into online and offline systems, where the first implies the connection to the internet and the second does not, respectively. With the rise of

IoT devices, a wide variety of these devices with very different characteristics can be found, depending on the application for which they were designed.

LITERATURE REVIEW

RFID - Radio Frequency Identification Access controls

The access control systems (ACS) have been involving in different areas such as biometrics, mechanical, communications, and computer technologies to improve their safety and security. These systems include the implementation of single- factor authentication mechanisms, for example, the entry of a PIN, or an RFID card, or multifactor authentication such as RFID complemented with a password. The ACS characteristics that differentiate RFID systems are the frequency, the coupling method, and the information range. Figure 1 shows a diagram of the main components of an RFID system, where the interrogator supplies power to the transponder, which allows an exchange of information between them.

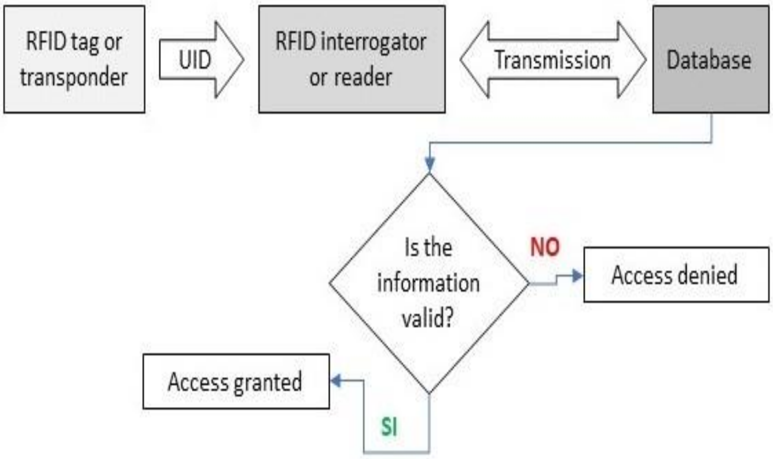


Figure 1. Flowchart of RFID Access Control

One of their characteristics for classifying RFID systems is based on how power is supplied to the transponder, which allows them to be classified as passive or active transponders. A passive transponder lacks a power source, so the magnetic or electromagnetic field of the reader supplies it with the energy necessary to function. On the other hand, the active transponder has its own power supply to operate.

Microcontroller System

The Arduino program (IDE) is a tool that allows you to develop programming codes in Arduino-C language and after that converting them to an executable format which could be loaded onto a board's microcontroller. Arduino (IDE) is straightforward and easy to use. Figure 2 shows the Arduino IDE, which is practically devoid of any complexity in its overall design and contains simply what a programmer needs to begin generating programs in Arduino-C language, which is also used for uploading the program straight to the microcontroller [3,4]. The IDE for Arduino is Integrated Development Environment. It is a cross-platform application (for many kind of operating system), which works with Java. It arose from IDE for the Processing and Wiring languages. The ESP8266 can be programmed using a variety of programming environments. The ESP8266 section developed an Arduino IDE which allows programming the ESP8266 with the Arduino IDE and its programming language [8].

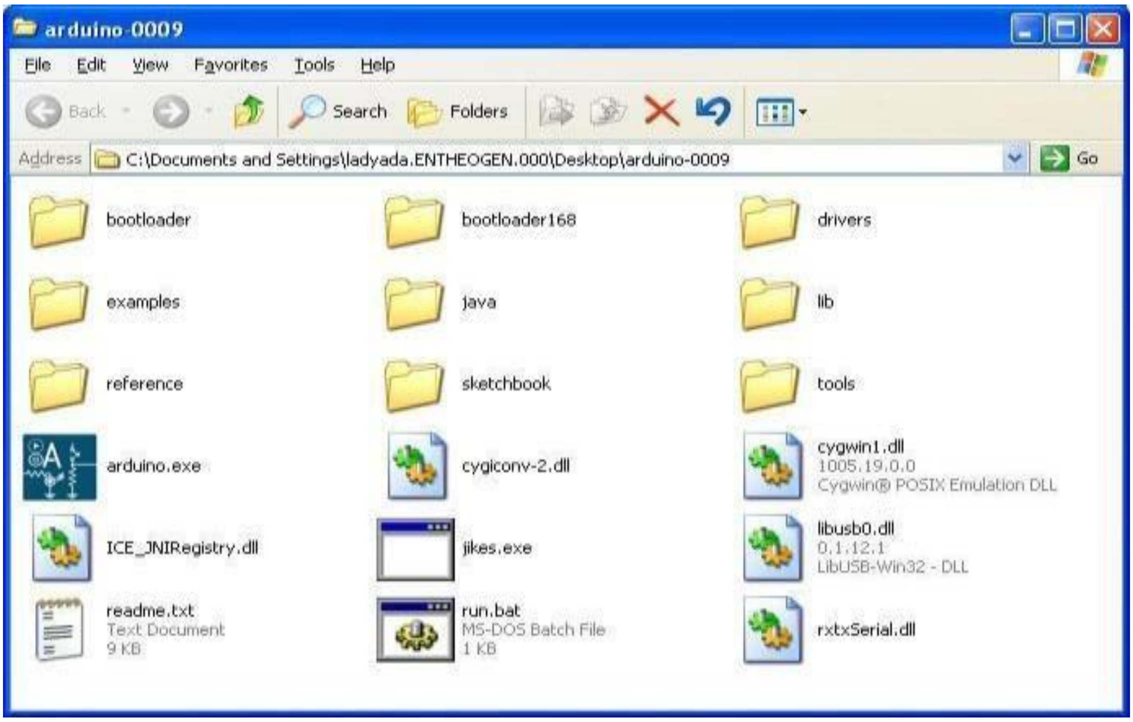

Address C:\Documents and Settings\ladyada.ENTHEOGEN.000\Desktop\arduino-0009

Figure 2. Applicated Software on Arduino IDE

Arduino IDE consists of a simple interface is divided into four main parts:

- First: the menu bar.
- Second: fast-orders bar.
- Third: an area of writing-codes.
- Fourth: display alerts and programming errors.

Managing the attendance of guests in a tourism resort is a difficult endeavour. Manually recording attendance is often a challenge. This study seeks to provide a smart attendance system which successfully manages and monitors the guest attendance in a given resort. The entire system is built around ESP8266 Arduino microcontroller and the MFRC522 RFID reader module. Unique RFID tags can be deployed in guest's id card. In this paper, the entry and exit of guest to and from the resort is controlled, and the project can also be used to take attendance of guests.

Access Control System

The access control system is consisting of five elements. They are sensor, computer, communicator, actuator, and data management elements, as illustrated in Figure 3.

- Sensor for sensing elements that are responsible for gathering data from the environment, such as transducers or RFID reader and another sensor. These collect the data and processes it further to the computing elements.
- Computer for computing elements that are the central of the system, these elements are responsible for processing, arithmetical, and performing logical operations.
- Communicator for communicating elements such as the wireless module and local cloud are responsible for establishing a communication channel between the sensing elements and the computing-data management elements.
- Actuator for actuating elements that are responsible for physical actions such as solenoid, electrical motor, mechanical locking system of the smart locker.
- Data management elements is a part to store information for administration and monitoring.

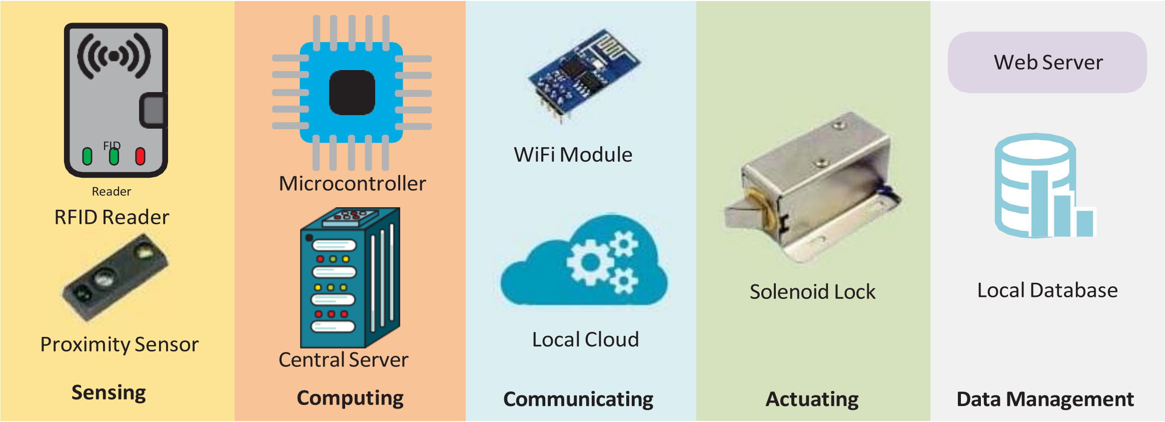


Figure 3. Step by Step in Access Control System

METHODOLOGY

There are two system were designed to develop the IoT access control system, the first system is for reading all of information and the other system is for record all of information on this type of card. For the development of RFID technology is ability with open-source hardware, a nano technology, cryptographic processor, and other components were used. In addition, also to increase communication between the RFID and the website was achieved through TCP sockets.

The implemented system includes 3 main subsystems that are integrated and worked together to access control system. These subsystems are:

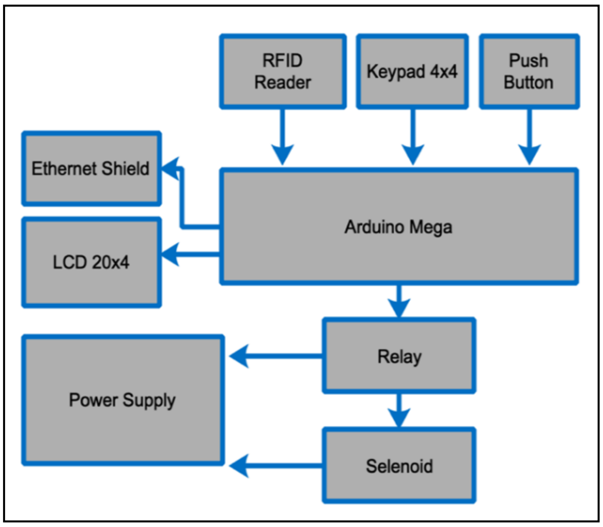
- RFID
- Microcontroller
- Data Base

The hardware system is simple in design and requires only 5 inexpensive components. Also, this system enables wireless communication, and the major hardware system uses Wi-Fi for transferring data to the server [7].

- RFID Tag: this component consists of a silicon microchip connected to a small antenna, put on a substrate, enclosed in different materials such as glass or plastic veil, and with a sticky on the backside to connect to objects.
- RFID reader: this component consists of a scanner with antennas for transmitting and receiving signals, as well as a load for connecting to the tag and receiving data from the tag.
- NodeMCU: this component is a free IoT platform. It consists of firmware which is installed on the Express ESP8266 Wi-Fi Sock and hardware that is installed on the ESP-12 module. By default, the term "NodeMCU" refers to the firmware instead of the development kits. The firmware's scripting language is Lau. It's set up on the Eula system, and if using the Non-OS SDK for ESP8266, it's configured on the Express. Various free origin systems, like spiffs and Lua-cjson, are affected.
- Servo Motor: a servo motor can be defined as one of the motor types which could rotate with a high degree of precision. Servo motors often have a control circuit which offers feedback on the current position regarding the motor shaft; such feedback allows them to rotate with high precision.
- A jump wire: this component is an electrical wire and a set of them in a cable, each with a pin at one end, that is typically used for interconnecting the breadboard's components. Without soldering, either internally or with external components or equipment.
- 16×2 LCD: it has 2 Rows and 16 Columns which a common screen that used.

RESEARCH RESULT

The access control system measures the time it takes for the data management system to record a user’s data on an RFID card when the operator clicks on the record button in the web application until the encrypted information is recorded in the data blocks for the RFID card. This experiment aims to test the efficiency of reading RFID cards in a reader and consists of placing 100 RFID cards consecutively in thirty iterations.



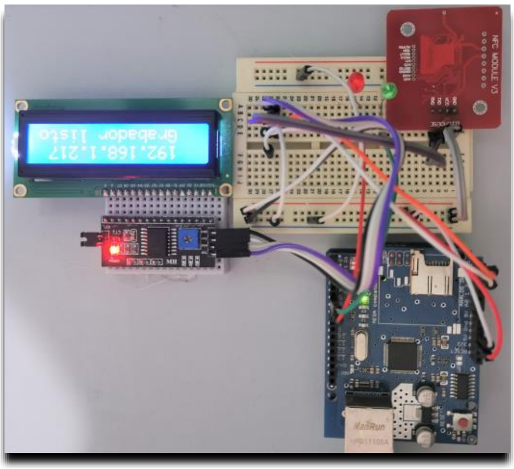


Figure 4. Diagram and Wiring Diagram of The Access Control System

Figure 4 shows the results where it can be seen that process in the access control system shows the number of iterations, from sensing part to identification and authentication user-information on the RFID card, then computing information to data base, communicating by IoT ability to receiving the information from the web application and saving information in data management to use it for another process.

The access control system by using RFID technology performs two operations, the first operation is the door accessing system, and the second operation is the data logging and alert mechanism after reading the card. Regardless of these operations, the microcontroller gets data of date and time from the WIFI module. For this reason, the WIFI module is always connected to the web server. But provided that the WIFI module can only be connected to a single web server, to handle this disadvantage the WIFI module is made to connect with the administrator web server only at certain intervals; intervals when the door is accessed, when data logging and when alerting the administrator. The administrator web server is not always connected to the system. So, the web server is designed to wait the connection, once the connection is set the control data is passed to the microcontroller, which will lock or unlock the door appropriately. Hence, the WIFI module is made to connect with the administrator web server to fetch control data for every minute time limit in a 10 minutes time interval. When a person tries to access the door using RFID tag or Keypad methodology, the microcontroller will receive the provided password from the modules and will crosscheck it with the password provided by the system or the organization's database. Upon success, the access to the door is granted. Upon failure, the LCD display module will display the message "WRONG PASSWORD", this entry will get registered in the data log on the web server and the user will have to provide the right password to gain access to the door. In case of multiple wrong entries, the system will finalize it as a fraudulent access and will permanently lock the door from anyone's access and also alerts the administrator. The permanent lock can only remove by resetting the system using a special administrator password by the admin. In case of a thief trying to break the door, the vibration sensor will sense this act and alerts the administrator and again permanently locks the door.

DISCUSSION

The significance and application of each component are explained in the proceeding paragraphs.

- The access control system with RFID technology has the function to read the unique RFID code from the RFID tag. Then pass the code onto the IoT board, where it is manipulated further for the authentication process.
- Communication with IoT Board serves the purpose of authentication of the user. It does so by accepting the input code from the RFID module and matching it with the one already registered. If the codes match, it signals the actuator, else denies access. Here, the ESP8266 IoT board is used for this purpose. The IoT board also has the responsibility to report the authorization attempts to the server to facilitate tracking.
- Actuator here has the task to open the lock on receiving the appropriate signal from the IoT card, therefore allowing the user to access the locker. In this case, a relay is used.

The usage of automation technology has been growing over the years and with the incorporation of IOT technology, existing security and automation systems have upgraded themselves to a new leash. People can now control their automation systems at office, in the comfort of home and vice versa. With the upgrades of science and engineering, the access control system will be upgraded to a pure camera in based to sensor system, where the user doesn't need a password, key card or other ID. The AI system would be heightened that the users' face is automatically scanned and identified, without needing him to stand in front of the door; he or she can simply walk past the door without having to open with the upgraded systems. Such is the future of these systems and Automation.

CONCLUSIONS AND RECOMMENDATIONS

One of the most significant approaches for taking the attendance of guests in tourism resort is designing and developing wireless smart systems. The modern creation of new technology in the monitoring system, which offers a more beneficial approach to monitor guests, will be very effective in enhancing the present conventional technique to monitor guests. As a result, Access Control System with RFID and based on IoT has solved all of such issues. Those RFID could identify visitor admission as well as mark their attendance in under a minute, sending a notification to the admin and storing the visitor's whole information in a database server.

Implementation of RFID is very helpful for the process of identifying and authenticating access to the room and building in tourism resort. Implementation of RFID can increase security in tourism resort where guest no longer need to take the key so that only visitors who have permission to use the space can open the room or building. Implementation of RFID for identification and authentication of access to use of resort space, the department is assisted in collecting data on use of resort.

Access control system with RFID based compact locking system. RFID enabled to identification and authentication was used for user verification. The system provides impressive security in a user-friendly manner requiring minimum human intervention. The system was also able to track and monitor the locker activity over definite intervals of time. IoT used to communicate with a centralized server, where the locker records were stored in a database allowing continuous tracking and surveillance.

ADVANCED RESEARCH

With the upgrades of information technology, science and engineering, the access control system will be upgraded to a pure camera in based to sensor system, where the user doesn't need a password, key card or other ID. The AI system would be heightened that the users' face is automatically scanned and identified, without needing him to stand in front of the door; he or she can simply walk past the door without having to open with the upgraded systems. Face identification, finger identity, voice identity, and eye identity, as a suggestion for future works, can offer better protection.

ACKNOWLEDGEMENTS

This opportunity to thank our colleagues in Bali State Polytechnic and Vocational College of Ganesha Indonesia – Tanah Ampo who provided suggestions for this paper. And appreciation for the financial and material assistance from Ganesha Publisher, in completing this research.

REFERENCES

Abbas, H. H., Jaaz, Z. A., Al Barazanchi, I., & Abdulshaheed, H. R. (2021). Survey on Enhanced Security Control Measures in Cloud Computing Systems. Journal of Physics: Conference Series 1878(1), 012004.

Abdulshaheed, H. R., Abbas, H.H., Al Barazanchi, I., & Hashim, W. (2022). Control and Alert Mechanism of RFID Door Access Control System Using IOT. 3C Tecnología. Glosas de innovación aplicadas a la pyme. ISSN: 2254 – 4143 Edición Especial Special Issue Febrero 2022, 269-285.

Anagnostopoulos, T., Zaslavsky, A., Kolomvatsos, K., Medvedev, A., Amirian P., Morley, J., et al. (2017). "Challenges and opportunities of waste management in IoT-enabled smart cities: a survey," IEEE Transactions on Sustainable Computing, vol. 2, pp. 275-289.

Alamillo-Montes, G. I., Martinez-Cruz, A., Uribe, C. F. (2022). Security Scheme for an RFID Access Control based on IoT. IEEE Mexican International Conference on Computer Science (ENC). Xalapa, Veracruz, Mexico.

Bharatiraja, C., Chitoor, P., K., Bhargava, Y. V. (2023). An IoT based Centralized Smart Locker Using RFID Technology. Conference Paper in AIP Conference Proceedings.

Cheah B. C., Manmeet M. S., Kam C. W., Tan W. S., Mohd H. H., Nurul H. A., Malim, H. (2015). "The Society of Digital Information and Wireless

Communications", The Society of Digital Information and Wireless Communications, School of Computer Sciences. Malaysia.

Farooq, Umar and Hasan, et al. (2014). "RFID Based Security and Access Control System", International Journal of Engineering and Technology, pp. 309–314.

Ihsan, Safa, Al-Janabi, H. D. K., Al-alnabi, L. (2022). Smart Attendance Student System using IoT RFID. Conference Paper on Appl. Sci.

Sabri, M. Y., Aziz, M. A., Shah, M. M., & Abd Kadir, M. F. (2007). Smart Attendance System by suing RFID. Asia-Pacific Conference on Applied Electromagnetics (pp. 1-4), IEEE.

Widharma, I. G. S., Narottama, A. A., Sudayana, I. W. (2017). The Light Lamp Control by Using Remote Based on Microcontroller ATMega328 System. Journal Logic: 16 (3).