System Access Control Using Smart Fencing at Stockyards

Kulvir Singh, Aryan Bhatt, Deepa Karuppaiah
Vellore Institute of Technology, Vellore, India
Corresponding author: Kulvir Singh, Email: kulvir06singh@gmail.com

This project work is made for Stockyards where there is a constant risk of injury and fatality to the people working in field. The project deals with an IOT device which gets triggered when the magnetic field of a magnet comes in contact with a magnetic switch. A smart fence is made for the people to cross into and work in the danger prone area. When a person crosses the fence, a signal is triggered by the IOT device to the central access control system which disables the machinery and rail cables. The connection is re-established only when the fence is closed by the person who crossed it earlier. Therefore, the project comprises a smart fence which can access the system and control the machines accordingly in order to prevent human fatality.

Keywords: Internet of Things, Wireless Sensor Network, Raspberry PI.

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 343–347. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-34

1 Introduction

An occupancy sensor is a piece of electronic equipment that detects the presence of people. Occupancy sensing technologies include magnetic, microwave, ultrasonic, and video image processing. The sensors are typically linked to a building's Internet of Things (IoT) network and feed data back to building management systems and booking systems, which can automate systems for lighting, HVAC, and ventilation control, as well as provide data for occupancy analytics systems to understand desk usage, meeting room efficiency, and space utilisation. In this project we will be making a smart fence that will be coded in Universal Windows Platform which will be installed in the Raspberry PI.3. There will be a web application interface which will act as a frontend and the full application will be hosted in the backend of a cloud service. The IOT device will trigger and the Raspberry PI 3 will call for an API with a particular input. The API will return and perform the function according to the input given to it. This will allow us to take control of the entire system.The proposed work can be applied across various manufacturing and production industries where a logistics unit is present. It can be used in places where man and machine interaction are fairly high and hence the risk of accidents and fatal injury increases. Apart from accident and fatality prevention, the proposed work can be issued in places where security systems can be implemented.

2 Proposed System

Our proposed system includes using a Raspberry Pi as a controller which reads the data from a magnetic switch to determine if there is fatality risk inside the smart fenced area. The data is then sent to the Azure server with our custom API. Ultimately with the help of the API an output will be given whether to close the fence and activate the machine or to leave the fence open with no machinery inside the fenced zone on.

2.1 Architecture of Proposed System

The architecture of the proposed system has been explained through the representational state diagram (see Fig. 1). The start of the application can be visualized with the initialization of the Raspberry PI and a click of the button in the application which would be present on site. The magnetic switch will be read and according a status code will be generated. The status code would be binary with 1 indicating that the fence is closed and 0 indicating that the fence will be open. The data would be sent to the Azure cloud backend as an API request.

The button click in application signifies that an API request has been sent to the Azure cloud which would in turn check the status of the fence table. The fence table would be populated according to the data received from the Raspberry PI. Once checked, the fence status can be displayed to the user and changes can be made accordingly.

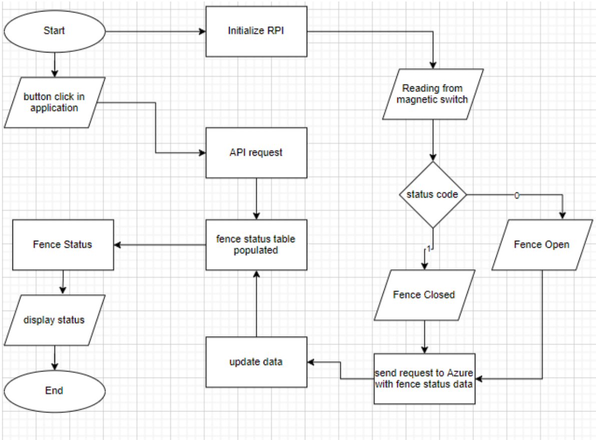

Fig. 1. Architecture Diagram of the proposed system. Each module and the flow of control can be seen with the help of unidirectional arrows

2.2 Proposed System Module Workflow Model

The module workflow would give a detailed explanation of how each module in the proposed system will traverse and interact with the other modules and services. From the architecture, it can be concluded that the model would be divided into three components which would be hardware (Raspberry PI), cloud (Microsoft Azure) and frontend (Webpage). As seen in the workflow model (see Fig. 2), the proposed system would interact in the following manner discussed below. The hardware component would send data to the cloud service and on successful transmission of data an acknowledgement would be received to the hardware system which would stop the transmission. The frontend of the proposed system would receive data from the cloud service and send an acknowledgement back to it in a similar fashion. Thus, communication is done in a handshaking way and a fully secure transmission is created with error handling inbuilt within the cloud service.

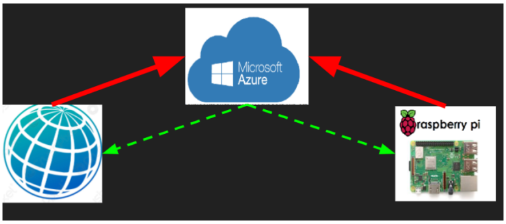

Fig. 2. Workflow diagram of the proposed system

3 System Design and Analysis

In this section, the system model and the analysis of the proposed system will be discussed. The proposal of making and testing of the IOT device is explained and elaborated. The UWP (Universal

Windows Platform) code has to be installed in the Raspberry PI 3. The web application can be coded in C# ASP.NET and shall be tested in an IDE like Visual Studio using swagger UI and published in Azure Cloud. The webpage for the frontend would be made in HTML and can be integrated to any web service to host it.

3.1 System Specification

To build a model of the proposed system, certain number of hardware components are required. For installation, Raspberry PI 3, GPIO extension ribbon cable, magnetic switch, strong round neodymium magnets, stopper and screws, epoxy adhesive is required. For testing, a monitor, keyboard, hdmi cable and a power cable is required. As for the software requirements, visual studio and UWP is required.

3.2 Design Approach

Raspberry PI 3: The hardware component of Raspberry PI 3 installation will be divided into two sub components. Firstly, connect the magnetic switch to the raspberry pi via GPIO pin no.40 and GPIO pin no.30. This magnetic switch will act as a sensor for the magnetic field. The code in this UWP is for sensing the magnet on the stopper and consume a post API (Application Programmable interface) of the web application which is published in the Azure cloud. While consuming the POST API it sends a parameter to the API function according to the status of the fence. Also a main page or landing page coded as an xaml file. This is the frontend and used in testing purpose.

Web Application: This is a web application which is published in the azure cloud and has 2 APIs GET and POST. The post api takes in a parameter and sends that parameter to the azure cloud table storage. And the get API retrieves that particular parameter from the azure cloud table storage. Similarly, a web form needs to be designed which will be integrated with a major system which controls the entire system. According to the data retrieved, it will display the fence status and the application can be programmed to disable or enable the system control.

3.3 Results

On successful implementation, a full fence like system access control system is created. A monitor displaying the status of the fence is present. When the magnets are connected to each other, the status of the fence is set to close. Also, when the magnets are not connected to each other, the status of the fence is set to open. Depending on the status of the fence, the entire system of machinery is controlled.

4 Conclusion

The proposed system is based on simple hardware which is easily available and cheap. It provides a cheap solution to real world problems and can be fairly used in accident prone regions to prevent fatality. The system is optimized than most other fencing system present. Overall, more research and a heavy implementation can make this system more optimized and more feasible for industry level implementation.

The proposed system can be improved and be used in various real world application including smart fencing for security, smart parking applications, smart fencing applications. The proposed architecture can be extended to be used in other products such as smart locking system and smart safes.

References

[1] Nikhade, S. G. (2015). Wireless sensor network system using Raspberry Pi and zigbee for environmental monitoring applications. In *International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*.

[2] Mamata, K. et al. (2015). Implementation of internet of things for home automation. *International Journal of Emerging Engineering Research and Technology*, 3(2): 7-11.

[3] Faisal, E. M., Awad, A. I. and Hesham, F. A. (2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*, 7: 21.

[4] Kodali, R. K. and Rajanarayanan, S. C. (2019). IoT based indoor air quality monitoring System. In *International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*.

[5] Yunwan, J. et al. (2018). IoT-based occupancy detection system in indoor residential environments. *Building and Environment*, 132: 181-204.