International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 10 Issue 6, June 2023

ISSN: 2394-4404

Design And Implementation Of A Remote Security Model On Access Control Systems

Iroanwusi Sampson O.

Ogbonna Bartholomew O.

Centre For Information and Telecommunication Engineering,
University of Port Harcourt, Nigeria

Abstract: ***This project involves the design and implementation of a remote security access control system using RFID and ESP32 CAM with facial recognition capabilities. The system provides an added layer of security by using facial recognition to prevent unauthorized access. The project demonstrates how various technologies, including RFID, ESP32 microcontroller, camera module, and facial recognition algorithms, can be integrated to create a secure access control system that can be accessed remotely. To evaluate the effectiveness of the system, a quantitative approach is used to assess the system's performance. The evaluation includes measuring the accuracy of the facial recognition algorithm and the system's response time for granting access. The uniqueness of this project lies in the integration of RFID technology with facial recognition capabilities. The results show that the system achieves high accuracy in facial recognition and fast response times, making it a reliable and efficient security access control system.***

Keywords: Access control, remote, machine learning, IoT, Security.

I. INTRODUCTION

Technology is developing quickly in the modern world, so it is necessary to have a facility that can support and enable the use of this technology in all disciplines and the development of institutions related to the existence of more supportive technology (Restyohadi, 2007). Adapting to an increasing number of digital devices in our daily lives, especially in the industrial space, there is no doubt that they have impacted our routine living. We cannot even imagine one day without using them. Security and safety are one of the major issues or challenges facing all humans in different levels and fields of life. A lucrative project is the industrial internet of things (IIoT)-based remote security system, which helps to maximize and guarantee the best security measures in the business world and connected organizations.

The term "Internet of things" (IoT) refers to physical things (or groups of such things) equipped with sensors, computing power, software, and other technologies that communicate with one another and exchange data over the Internet or other communications networks (Gillis, A. 2021). Because items merely need to be connected to a network and be individually addressable, the term "internet of things" has been criticized as being misleading (Nilanjan Dey and others, 2018). The discipline has changed as a result of the confluence of several technologies, including machine learning, ubiquitous computing, inexpensive sensors, and increasingly powerful embedded systems (Hu J. and others, 2022).

The Internet of things is enabled by traditional domains such as embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and so on. IoT products are most often associated with the "smart home" in the consumer market because they support one or more common ecosystems and can be controlled by gadgets related to those ecosystems, like smart speakers and smartphones. These products include lighting fixtures, thermostats, home security systems, cameras, and other appliances. Moreover, healthcare systems use IoT. (Laplante, 2018).”A lot of works have been carried out already on remote access control and some of them are highlighted with limitations and gaps identified.

Shaik and Kishore (2016), did a study on IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone. This study discusses the establishment of a wireless control system and its accessibility in a home setting for authorized individuals only. The security system is activated when needed by a PIR motion sensor and a camera module, which are used to detect motion and take pictures, respectively. The door accessibility is controlled by an electromagnetic door lock module that has been conceived and built. The database that saves approved photographs for machine learning implementation was not taken into consideration in this study, it was only concerned with remote monitoring and feedback.

Another study was done by Leya et al, (2018) on home security system. "The suggested solution uses a USB webcam to capture images, a fingerprint reader to verify user identity, and Telegram, which has the amazing feature of a Telegram Bot that offers APIs to build solutions that are compatible with Raspberry Pi IoT infrastructure. A safety locker door is opened and closed by the system, which uses a fingerprint reader. Before entering the house, the person must utilize fingerprint verification to confirm his or her user identification." SMS home security system would have been one of the best measures for security ever, but the fact that it does not work well in case of an emergency make it vulnerable to attackers and hackers."

Tushar et al, (2022) carried out a work a work on IoT based Digital Attendance System using RFID & ESP32. "There is no power supply for the passive tags employed here to produce radio waves. They only react when the reader sends radio waves their way, reflecting those waves back with the information they have stored in them. Usually speaking, passive tags are more common for little purposes. The ESP32 module receives the data from the RFID reader once it has read the data from the tag. The ESP32 module then modifies the data into a readable format and runs several comparisons on it to determine who owns the card. After this procedure, the ESP32 module uses the internet to deliver the user's roll number to a certain website." "One of the gaps in this work is that it didn't integrate remote monitoring and control where entry access can be granted to a user detail not found in the database during emergency situation.

Abhinab and Ritesh, (2021) carried out a work IOT Based load Automation with Remote Access Surveillance Using ESP 32 CAM and ESP 8266 Module. "In this project, a single platform may be used to swap electricity loads, water plants intelligently, and monitor specific locations. The ESP-32 CAM's remote access feature was implemented utilizing port forwarding and the NGROK.IO platform. This work may be beneficial in a variety of industries, including businesses, schools, and other areas where automation and surveillance are crucial. The work focused more on remote surveillance system, it didn't give much insight on authentication, database and machine learning applications."

II. METHODOLOGY

"The top-down design approach is the process employed to carry out this project. It will involve everything from design to real building to produce the desired result (prototyping). Creating the block diagram for the project. The project begins with a thorough examination of Convolutional Neural Networks (CNNs) for deep learning and progresses to using them in conjunction with AI thinker models for facial recognition and face detection in the esp32 Cam module. Using HTML and CSS, user interface design, simulation, and implementation is done.

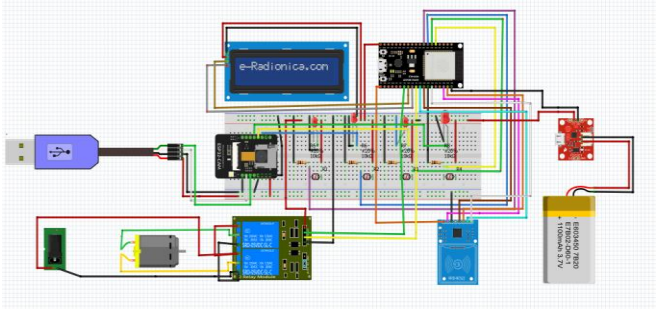

Figure 1: System schematic Diagram

"Once launched, the entire system essentially runs by itself and serves as a surveillance and access control system. One must first register their face with the system using the camera in order to obtain entry, and after that, the system will issue them an RFID card. In order to give access through the system, the system compiles the Face ID and Card ID. The system will deny access to the user if neither of the IDs is given. Security officers may keep an eye on the system's surveillance logs, and from these they can spot trespassers because the system scans everyone who enters its field of view for unregistered people".

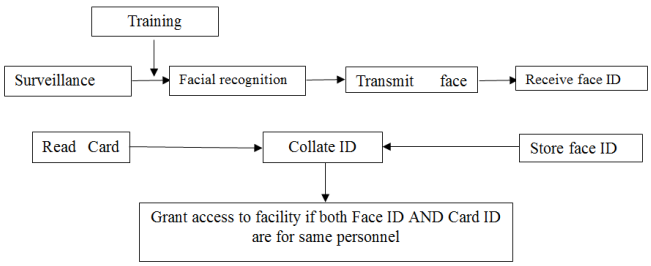

Figure 2: Remote Security Model on Access Control IOT

System Mode of Operation

Facial recognition: The system will recognize a user who has previously registered and advance to the next step. Otherwise, it will alert the system to an intruder."

"*Transmit face ID:* The access control system receives the user's face ID from the surveillance system, and the subsequent stage is then initiated."

"*Receive face ID:* The facial recognition system is continuously monitored by the access control system for Face ID, which is subsequently sent to the collation unit."

"*Store face ID:* The Face ID is kept in a temporary memory until it is utilized or until a new Face ID is received. After some time, the temporary memory is cleared to make room for the new ID."

"*Read Card ID:* The system uses RFID reader to read RFID card and send the Card ID to the collation unit."

"*Collate ID:* Users receive cards assigned to their offices and Face ID during registration. The system uses this information to provide users access to the facilities anytime

they attempt to do so, and if there is a discrepancy with this data, the system will deny the user access to the facility."

III. RESULT AND DISCUSSIONS

The testing and validation of the Remote Security Model on Access Control System Using Machine Learning are carried out in this section. The three Layers, namely the Physical Layer, Communication Layer, and Data & Control Units, were subjected to testing and validation. The isolation unit, the load sensing unit, and the microcontroller unit were the three-unit blocks used for the Physical Layer test. The Wi-Fi connection to the "Master" ESP32 controller was more of a focus of the communication unit test. The Data & Information Layer underwent a last round of testing to ensure that the switching commands supplied from the web application correctly performed on the system's Physical Layer."

"To start up the system turn on the and the system the system will display system online and the server will be start if any Wi-Fi device is close by it will be able to detect the system network but only the security persons with security key or password is able to access the system dash board. Security person connects to the system by connecting to the server ESP-32 CAM hotspot network using the password (password). Once connection is established go to the next phase (Enroll face for identification and Assign RFID card to users according to face ID)."

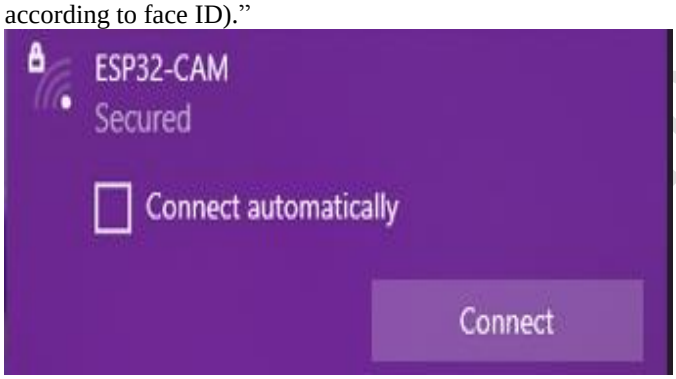

Figure 3: Connection to the Wifi Server

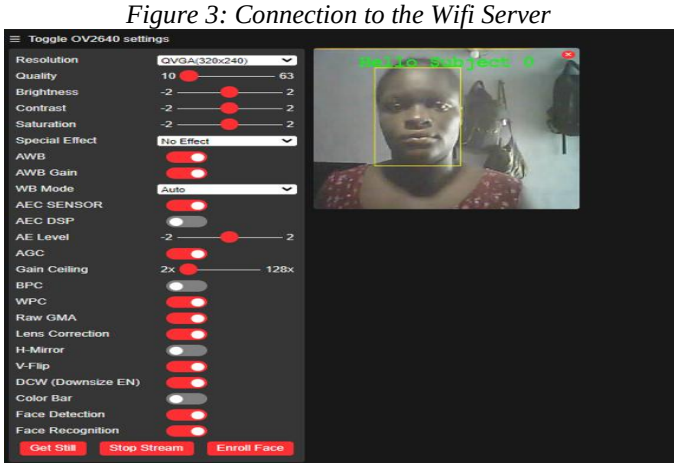

Figure 4: Connection phase test

After connection users are expected to Enroll to the camera system and are assign RFID cards that are assigned to their face ID. To do this the Security personnel assigned to surveillance will use the IP address 1922.168.44.1 to access the systems dash board through the security server of mobile device. Then setup the interface for both surveillance and access control using face detection and recognition. The figure in the next pages shows the complete setup, once it is ready the users are expected to register to the system to gain access to the work environment, note as registration process is done an access card is assigned to the user, this card ID is tied to the face ID of the user it was given."If anyone uses a card not assigned to him the system will deny the person assess to the environment.

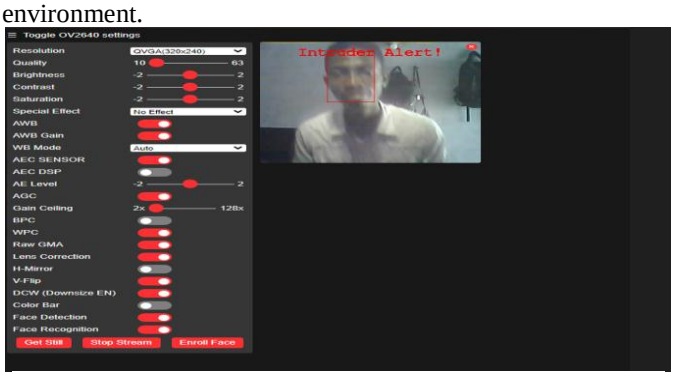

Figure 5: Video Streaming Web Server Up and Running with Face Detection and Recognition of an intruder

Figure 6: System Reading Card Test

Figure 7: Result for unmatched face ID

Figure 8: Result for matched face ID and RFID

The system runs on battery power that can last for twenty-four hours before recharge so it also has a charger device which should be tuned on for charging when system is not in use. Once the system is running it becomes autonomous in the event of granting special guest of high authority assess to facility the system has a card for maintenance and high authority granting them access even if their face ID have not been scanned, this card should be assigned to the director and the system engineer respectively.

Figure 9: The Complete System on line Line

IV. CONCLUSIONS

The system consists of a door system, a control board, a two-channel relay module for the IOT controllers, and an LCD display unit. The power supply is hidden inside the system frame. The IOT Machine learning system and microcontroller are interfaced with the access control system. This solution offers a cutting-edge method for assuring intelligent security in the industrial sector."

The results show that the system achieves high accuracy in facial recognition and fast response times, making it a reliable and efficient security access control system. The project also incorporates machine learning to improve the system's facial recognition capabilities. The ESP32 microcontroller's processing power is utilized to implement the machine learning algorithm, which learns from images captured by the camera module to improve facial recognition accuracy. The machine learning approach enhances the system's performance and demonstrates the potential of integrating machine learning in remote security access control systems. In conclusion, this project demonstrates the practical implementation of a remote security access control system using RFID and ESP32 CAM with facial recognition capabilities. The system's effectiveness is evaluated quantitatively, and the incorporation of machine learning highlights its potential for further improvement. This project's contributions to knowledge lie in demonstrating how various technologies can be integrated to create a more secure access control system with facial recognition capabilities that can be accessed remotely and how machine learning can be incorporated to improve the system's performance.

REFERENCES

[1] Abhinab, S. & Ritesh, D. (2021). IOT Based load Automation with Remote Access Surveillance Using ESP 32 CAMand ESP 8266 Module. Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 6904 – 6914

[2] Gillis, A. (2021). "What is internet of things (IoT)?". IOT Agenda. Retrieved 17 August 2021

[3] Nilanjan, D., Aboul E. H., Chintan, B., Amira, A., Suresh, C. S., Cham, S. (2018). Internet of things and big data analytics toward next-generation intelligence. p. 440. ISBN 978-3-319-60435-0. OCLC 1001327784

[4] Hu, J., Lennox, B. Arvin, F., (2022) "Robust formation control for networked robotic systems using Negative Imaginary dynamics" Automatica, 2022.

[5] Laplante, P. A., Kassab, M., Laplante, N. L., Voas, J. M. (2018). "Building Caring Healthcare Systems in the Internet of Things". IEEE Systems Journal. 12 (3)

[6] Leya, L., Sherin, S., Janet, J., Willson, J. (2018) "HOME SECURITY SYSTEM", 2018 INTERNATIONAL JOURNAL OF CURRENT ENGINEERING AND SCIENTIFIC RESEARCH (IJCESR)

[7] Restyohadi, W. A. (2007): "Pengelolaan Parkir Mobil Information System Application of Car Park Management"

[8] Shaik, A.& Kishore, D. (2016) "IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone" International Journal of Engineering Research & Technology (IJERT). 2016

[9] Tushar, S., Aasha, C., Megha, D. & Alok, A. (2022) "IoT based Digital Attendance System using RFID & ESP32". International Journal for Modern Trends in Science and Technology 2022, 8 pp. 122-126. https://doi.org/10.46501/IJMTST0802020