Website: www.aceiot.ur.ac.rw
Mail: aceiot@ur.ac.rw

College of Science and Technology

AFRICAN CENTER OF EXCELLENCE IN INTERNET OF THINGS (ACEIOT)

Research Thesis Title:

"IOT BASED SYSTEM TO MONITOR AND PREVENT INTRUDERS AT GENOCIDE MEMORIAL CENTERS: CASE STUDY OF KIBAGABAGA MEMORIAL CENTER"

A dissertation submitted in partial fulfilment of the requirements for the award of masters of science degree in internet of things-embedded computing systems.

Submitted By:

MUGIRANEZA Claude (Ref. No: 221031459)

Supervisor: Dr. BAKUNZIBAKE Pierre

Co-Supervisor: Dr. Gerd RUSHINGABIGWI

March, 2024

DECLARATION

I, **Claude MUGIRANEZA (Ref. No:221031459),** declare that this research project entitled " **IOT BASED SYSTEM TO MONITOR AND PREVENT INTRUDERS AT GENOCIDE MEMORIAL CENTERS: CASE STUDY OF KIBAGABAGA MEMORIAL CENTER** " is presented for the award of Master's degree in the Internet of Things at African Center of Excellence , especially in Embedded Computer System, University of Rwanda, is my work. It has never been presented or submitted in any University, Institution or High Learning for a similar award.

Claude MUGIRANEZA
Ref.No: 221031459

CERTIFICATE

This is to certify that the "**IOT BASED SYSTEM TO MONITOR AND PREVENT INTRUDERS AT GENOCIDE MEMORIAL CENTERS: CASE STUDY OF KIBAGABAGA MEMORIAL CENTER**" research project work is a record of the original bonafide work done by **MUGIRANEZA Claude (Ref.No:221031459**) in partial fulfillment of the requirement for the award of a Master's Degree in Internet of Things – Embedded Computer System from the University of Rwanda-College of Science and Technology through the African Center of Excellence in Internet of Things, from the Academic year 2021-2023.

Main Supervisor:
Dr. Pierre Bakunzibake
Date: ……/……/……

……

Co-Supervisor:
Dr. Gerard Rushingabigwi
Date: ……/……/……

.....

Head of Masters and Training ACEIOT
Dr James Rwigema

Date: ……/……/……

……

ACKNOWLEDGEMENT

My sincere efforts have made me to accomplish the task of completing this project. I have taken effort in this project. However, it would not have been possible without the kind support and help of many individuals.

First of all, I would like to thank God for all the blessings, guidance and protection during my studies. I would like to express my special thanks of gratitude to my supervisors Dr. and Dr. …. As well as African Center for Excellence in Internet of tings at the University of Rwanda readership who gave me the golden opportunity to do this wonderful project on the topic "**IOT BASED SYSTEM TO MONITOR AND PREVENT INTRUDERS AT GENOCIDE MEMORIAL CENTERS: CASE STUDY OF KIBAGABAGA MEMORIAL CENTER"** which helped me to learn a lot in the research and course of completion of this project.

I am also indebted to my wife, daughter, my family and friends for their valuable support, advice and love which help me to do this project with with the given time frame. May God continue to bless them.

ABSTRACT

Rwanda's Genocide Memorial Centres are powerful symbols of the country's tragic past, carrying substantial historical and cultural weight. Nevertheless, these locations are susceptible to encroachment and vandalism, both of which have the potential to harm the healing process and tarnish the memory of the victims. In response to this difficulty, An AI and IoT based security system has been proposed.

Strategically positioned throughout the memorial centre are motion detectors, cameras, light-level detectors (LLDR), and buzzers that comprise the system. In response to motion sensor detection of unauthorised movements, nearby cameras initiate the process of capturing images of potential intruders. Real-time analysis of these images by Convolutional Neural Network (CNN) algorithms detects suspicious activity. By differentiating between day and night conditions, the LLDR sensors guarantee precise threat detection.

The system activates its camera to transmit real-time video to a centralised control room in response to detected potential threats. In addition, sophisticated image processing and CNN algorithms scrutinise the footage to detect atypical activities. Additionally, a buzzer is promptly triggered by the system, notifying on-site security personnel.

By means of our web interface, authorised personnel are granted access to real-time video feeds and sensor data via remote monitoring functionalities. This significantly mitigates the requirement for a perpetual on-site security presence and facilitates prompt off-site responses.

The preservation of the integrity of these memorial sites serves to guard the remembrance of the victims and facilitates the process of national reconciliation. The integration of CNN algorithms, motion sensors, cameras, LLDR sensors, and buzzers serves as a prime illustration of the efficacy of IoT solutions in safeguarding and conserving historic sites of significance. The potential of technology-driven strategies to bolster security measures for historical and cultural assets is highlighted in this case study.

Key Words: CNNs, IoT, Genocide memorial, AI

TABLE OF CONTENTS

DECLARATION ..... *i*

CERTIFICATE ..... *ii*

ACKNOWLEDGEMENT ..... *iii*

ABSTRACT ..... *iv*

TABLE OF CONTENTS ..... *v*

LIST OF FIGURES ..... *viii*

LIST OF TABLES ..... *ix*

LIST OF ACRONYMS ..... *x*

CHAPTER ONE: INTRODUCTION *1*

1.0 Introduction **1**

1.1 Background **1**

1.2 Motivation **3**

1.3 Problem Statement **3**

Study Objectives **4**

1.4 ..... **4**

1.2.1 General Objective 4

1.4.2 Specific Objectives 5

1.5 Study Scope **5**

1.6 Significance of the study **5**

1.7 Organization of the study **6**

CHAPTER TWO: LITERATURE REVIEW *8*

2.0 Introduction **8**

2.1 Review of the existing face recognition for security purposes 8

2.2 Research gaps 10

CHAPTER THREE: METHODOLOGY 12

3.0 Introduction 12

3.1 System design and architecture 13

3.1.1 Selected components 14

3.1.2 System integration 16

3.2 System Architecture 18

3.3 Data collection 19

3.4 Algorithm development 19

3.5 Model development (Customized CNNs) 22

3.6 Model Training and optimization 24

CHAPTER FOUR: SYSTEM DESIGN AND ANALYSIS 26

4.0 Introduction 26

4.1 System Architecture 26

4.1.1 IoT Layers Architecture 26

4.1.2 Schematic Diagram 28

4.1.3 Database diagram 28

4.2 System functionality 29

4.2.1 User case diagram 29

4.2.2 Flowchart diagram 30

CHAPTER FIVE: RESULT AND DISCUSSION 32

5.1 Introduction 32

5.2 Experiment 32

5.2.1 Machine Learning Approach 32

5.3 The system results 33

5.1.1 Embedded system 33

5.1.2 The dashboard displays the results 34

CHAPTER SIX: RECOMMENDATION AND CONCLUSION 38

5.1 Conclusion 38

5.2 Recommendation 38

5.3 The future work 39

REFERENCES 40

LIST OF FIGURES

FIGURE 3. 1 THE PROJECT CONCEPTUAL BLOCK DIAGRAM----------17
FIGURE 3. 2 SYSTEM ARCHITECTURE ----------18
FIGURE 3. 3 CNN ARCHITECTURE DIAGRAM----------20
FIGURE 3. 4 SQUEEZED CNN ARCHITECTURE DIAGRAM ----------21
FIGURE 3. 5 SQUEEZED NETWORK ----------21
FIGURE 3. 6 CUSTOMIZED SQUEEZE NET CNN ALGORITHM----------23
FIGURE 3. 7 TRAINING PROGRESS----------24
FIGURE 3. 8 TESTED MODEL----------25
FIGURE 4 1 IOT ARCHITECTURE----------27
FIGURE 4 2 SCHEMATIC DIAGRAM ----------28
FIGURE 4 3 DATABASE DIAGRAM OF THE SYSTEM ----------28
FIGURE 4 4 USER CASE DIAGRAM ----------29
FIGURE 4 5 FLOWCHART DIAGRAM----------30
FIGURE 5. 1 HOW TO REGISTER NEW STAFF IN THE SYSTEM ----------34
FIGURE 5. 2 LIST OF THE EMPLOYEES ----------34
FIGURE 5. 3 IMAGE COMPARISON /MATCHING WITH ENCODED IMAGES THROUGH LIVE STREAMING35
FIGURE 5. 4 SMS SEND TO SECURITY AGENT. ----------35

LIST OF TABLES

TABLE 1: Selected components……..……3
TABLE 2: Describe the functions used in proposed system and its executed results ……...27

LIST OF ACRONYMS

IT: Information Technology

IoT: Internet of things

PCB: Printed Circuit Board

CNN: Convolutional neural networks

AI: Artificial Intelligence

API: Application Programming Interface

CSS: Cascading Style Sheets

DFD: Data Flow Diagram

FN: False Negative

FP: False Positive

GPIO: General-Purpose Input/Output

GPRS: General Packet Radio Service

GSM: Global System for Mobile Communications

IDE: Integrated Development Environment

JSON: JavaScript Object Notation

KNN: K-Nearest Neighbors

LCD: Liquid Crystal Display

LPB: Local Binary Patterns

MCU : Micro Controller Unit

PC : Personal Computer

ReLU: Rectified Linear Unit

SVM: Support Vector Machine

TCP/IP: Transmission Control Protocol/Internet Protocol

TN: True Negative

TP: True Positive

USB: Universal Serial Bus

WI-FI: Wireless Fidelity

CHAPTER ONE: INTRODUCTION

1.0 Introduction

This chapter presents the background of the project and the motivation behind, the study objectives as well as the scope and the significant of the study.

The coming together of Internet of Things (IoT) and machine learning (ML) technology has profoundly transformed several aspects of modern life in an ever-evolving environment of modern living. Security is one area where this integration has had a big impact. With more and more security concerns, protecting different areas and conducting intelligent monitoring have become increasingly important [1]. When more individuals use intelligent technology, the need to improve restricted area security against potential threats grows. The current master's thesis researches advanced security systems for genecide memorial centers. "IOT BASED SYSTEM TO MONITOR AND PREVENT INTRUDERS AT GENOCIDE MEMORIAL CENTERS," a research study into this point, proposes a novel system that can detect, analyze, and respond to movements in real time.

1.1 Background

The Genocide Memorial Centers in Rwanda are of enormous historical and cultural importance and serve as sad memories of the terrible incidents that transpired there in the past[2]. These memorial locations serve as venues for recollection, education, and healing as well as paying tribute to the victims' memories[3], [4]. However, acts of vandalism and infiltration may jeopardize the purity of these holy places, sullying not only the memory of the deceased but also impeding the nation's efforts at healing and reconciliation [5]

According to Kigali Today, one of the genocide memorials has been by passed with unknown people and try to deny Genocide against Tusti by defecating in the memorial center of genocide against the Tutsi victims in Huye district, Gishamvu sector, Akamabuye village, Nyakibanda cell, and those suspects have been arrested. However, according to the citizen, they were unable to

prevent those evil people from occurring, and they urge increasing security at the genocide memorial place [5], [6].

This project focuses on the development of a machine learning and IoT-based system specifically created to monitor and prevent the intruders from committing damage at a Genocide Memorial Center in Rwanda in order to address this pressing problem. By employing Internet of Things (IoT) and machine learning technologies[7], this system seeks to enhance the memorial center's security infrastructure while ensuring the conservation and preservation of the historical and cultural relevance of the location.

The IoT-based system makes use of a network of linked gadgets, such as sensors, cameras, and alarms, which are positioned at key locations around the memorial center's grounds. These tools cooperate to identify any attempts at unauthorized access, strange motions, or suspicious activity on the site. The system is capable of quickly identifying and reacting to potential security breaches thanks to the installation of motion detectors, door/window sensors, and ultrasonic sensors.[8]

The technology alerts the closest security camera to record live video footage in the event of a breach, which is subsequently broadcast to a central control room. Advanced image processing algorithms and machine learning models are used in this control center to assess the distinctive features of the Genocide Memorial Center in Rwanda. The device can reliably identify prospective intruders or people participating in actions that could harm the memorial site by continuously monitoring the live video feed[9].

The technology immediately creates alerts and notifications in the event of a potential threat, which are swiftly forwarded to on-site security staff. These warnings give security personnel the ability to act quickly and stop any damage or destruction to the memorial center. In order to improve coordination and reaction efficacy, the system can be integrated with already-existing security infrastructure, such as access control systems or security personnel communication devices.

To continuously increase its accuracy, the IoT-based system also makes use of past data and breach trends. The system improves its ability to discern between false alarms and actual security breaches,

minimize unnecessary disruptions, and maximize the use of security resources by learning from previous instances[10].

Additionally, the system has remote monitoring features that let authorized staff access sensor data and live video feeds via a secure online interface or specialized mobile application. Real-time monitoring from off-site locations is made possible by this capability, providing quick responses and lowering dependency on physical presence for security.

The project's goal is to demonstrate the possibilities of deploying an IoT and AI-based system for monitoring and discouraging intrusions at a Genocide Memorial Center in Rwanda through this case study. The system aids in the preservation of the victims' memories and promotes the process of national healing and reconciliation by strengthening the security measures at these significant sites. This initiative emphasizes the value of utilizing IoT technology to conserve historical and cultural landmarks, highlighting how crucial it is to preserve the past for the benefit of current and future generations[8]

1.2 Motivation

The motivation behind this project stems from the imperative need to preserve the historical records and to honour of genocide memorial locations, ensuring that they remain untouched by acts of intrusion or vandalism. By harnessing the power of IoT-based solutions, we aim to establish continuous monitoring capabilities, thus guaranteeing real-time data access, irrespective of one's location, to maintain the integrity of these hallowed sites. Furthermore, the incorporation of advanced algorithms, particularly those for face identification and recognition utilizing convolutional neural networks, further reinforces our commitment to enhancing security measures, enabling more effective protection of these historically significant locations.

1.3 Problem Statement

The Rwandan Genocide Memorial Centers are solemn sites of remembrance that bear profound historical and cultural significance. However, acts of vandalism and intrusion persistently threaten these locations, impeding not only the nation's ongoing reconciliation efforts but also the memory

of the victims. The lack of a dependable and cutting-edge security system has presented considerable obstacles in the prevention and resolution of these concerns.

An interesting provide came up at our meeting with one of the memorial center's supervisors on July 9, 2023. The manager recommended investigating the system's ability to detect smoke, highlighting the need of monitoring and reducing smoking incidents at the genocide memorial. Because smoking is strictly forbidden in such solemn options, setting an ability into the system that can detect the presence of smoke aligns with the center's overall security goals. This added capability would not only assist in maintaining the sanctity of the memorial, but it could also deliver timely alerts in the event of a smoking violation, improving the overall effectiveness of the proposed system.

1.4 Study Objectives

1.2.1 General Objective

The main objective of this system is to prevent intruder in genocide memorial centers in Rwanda by designing and prototyping of IoT based system with machine learning by monitoring all event on cite and notify the owner if something happens.

Unidentified individuals recently attempted to deface and dismiss the gravity of the Tusti Genocide at a Genocide Memorial site in Huye District [6]. This incident highlights the critical nature of the situation. The current security measures, which consist primarily of periodic patrols and manual surveillance, encounter difficulties in differentiating between individuals who have good intentions and those who have malicious intentions [8]. The utilisation of these obsolete approaches is prone to errors, constrained in terms of resources, and frequently sluggish in identifying and addressing potential threats; consequently, the vast memorial grounds remain susceptible to threats. A proactive and technologically advanced security system is essential for the protection and preservation of these vital locations. The primary issue tackled by this project is the absence of a specialised Internet of Things (IoT) system intended to monitor and prevent unauthorised access to Genocide Memorial Centres in Rwanda that may initiate damage. By leveraging IoT technologies to improve intrusion detection, real-time monitoring, and rapid response capabilities, the project aims to establish a robust security framework that protects the

integrity of the Genocide Memorial Centres in Rwanda. To safeguard the remembrance of the victims and the integrity of these vital sites for posterity, this system endeavours to furnish security personnel with precise and dependable notifications, thereby empowering them to avert or alleviate instances of intrusion and damage.

1.4.2 Specific Objectives

- To review the existing literature on how to improve security situation are monitored by memorial center.
- To design and to protype an IoT with machine learning that can help genocide memorial to prevent intruder and alert the security guard to respond on the incident on time.
- To review the performance of the recommended system and compare it with other security system options available on the market.

1.4.3 Hypotheses

We hypothesised that by implementing machine learning alongside IoT-based technologies we can create a real-time security monitoring system tailored for Genocide Memorial Centres situated in Rwanda. It is expected that this system will efficiently resolve the existing difficulties associated with acquiring automatic updates on the status of events, thereby offering a resilient resolution for bolstering security measures at these memorial sites.

1.5 Study Scope

The study's scope encompasses the integration of machine learning with a real-time face recognition system to improve security measures at genocide memorials in Rwanda. The principal aim of the system is to monitor and authenticate visitors, with a particular focus on identifying and notifying the security office of any unauthorized attempts to enter the memorial sites. Furthermore, the technological system incorporates a functionality that detects occurrences of smoke inside the establishment, thereby guaranteeing an integrated approach to security and well-being.

1.6 Significance of the study

The thesis goal is to design and prototyping of an IoT based system to monitor and prevent intruders in genocide memorial in Rwanda; this can help in developing memorial center that will

help in recollection, education, and healing as well as paying tribute to the victims' memories. If this system deployed, the system would help the security guard to act and prevent the intruders access in memorial center and get real time logs. hyThe proposed architecture will also act as guide for use in integration of IoT systems into the existing solutions.

1.7 Organization of the study

This thesis is organized as follows:

Chapter 1: Explains the study's history, problem statement, general objective, particular objective, hypothesis, scope, significance, and organizational structure in the introduction.

Chapter 2: The Literature Review provides an in-depth examination of machine learning (ML), the Internet of Things (IoT), and current safety safeguards, highlighting the advantages and disadvantages of each.

Chapter 3: The research methodology used to ensure the project's effective completion is the main emphasis of this study. This scholarly article also clarifies the complex features of the proposed machine learning (ML) and Internet of Things (IoT) security system. The presentation includes a thorough analysis of its hardware components, software, hardware architecture, and methods for smooth integration.

Chapter 4: The "System Analysis and Design" paperwork provides an overview of several types of components, such as models, recommended simulations, system implementation, suggested models, parameters, and scenarios. Do a review of the system's performance following that, and then present the results.

Chapter 5: The interpretation and analysis of the results are the main objectives of this study. The results are compared with current solutions and their relationship is evaluated. In addition, the implications of the results are examined, and a detailed explanation is given for the graphs that show the outcomes.

Chapter 6: This section, "Conclusion and Future Work," provides a thorough summary of the study's results. It clarifies the advantages of the proposed system, points out potential directions to further research, and offers closing thoughts.

1.8 Summary

This chapter provides a summary of the study's setting and research focus, emphasizing how the genocide memorial center uses real-time machine learning (ML) and Internet of Things (IoT) technology to better protect against attackers. The integration project, which aims to increase the security of Genocide Memorial Centers, is a pertinent and promising endeavor that addresses the challenges of modern life, which are always evolving. The study's background has been given, and its purpose has been explained. The study's objectives, which include both general and specific goals, have been well outlined, and the issue statement has been clearly defined. The study's purpose and importance have been highlighted, and the hypothesis has been clearly stated.

The thesis has been organized to ensure the upcoming chapters have a clear direction. An in-depth review of relevant literature in the field will be given in the next chapter. It will cover research methodology, system analysis and design, implementation details, and conclusions that help bring real-time Machine learning (ML) and Internet of Things (IoT)-based intrusion prevention systems to life. It will conclude with thoughts on how real-time machine learning and IoT-based systems might be used to strengthen security systems in the future, providing insightful information.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter is dedicated to an in-depth review of relevant existing literature. This literature review serves as a critical foundation for our research, helping us identify gaps and devise strategies to address these pressing issues. It also sheds light on the application of IoT and AI technologies in previous research works. Over recent decades, diverse methodologies have been explored in the realm of security.

2.1 Review of the existing face recognition for security purposes

For security purposes, Almusaed, A., et al. [11] proposed a motion detection surveillance device that identifies activities of human entering in the house. The system immediately notifies users through the Internet of Things (IoT) upon motion detection. However, enhancements in cost management are imperative for the research due to the integration of body temperature sensors and audio recognition, with a particular focus on real-time alert systems. One limitation of this paper is the absence of visitor differentiation, which hinders the ability to determine whether an individual is an intruder or not.

Pandya et al. [9] presented a novel anti-intruders system designed specifically for smart houses, which exhibits the capability of detecting intruders even when their features are obscured. In illumination conditions where night vision is not applicable, standard CCTV cameras are utilized by the system. However, the rapid expansion of products that connect the physical and digital realms has raised concerns about privacy and security. To address these challenges, it is recommended to consider the deployment of machine learning algorithms capable of classifying visitors as intruders and alerting security personnel.

Neverova et al. [12] identified individuals through the analysis of their movement patterns using a deep learning approach. This study evaluates a variety of deep learning models capable of swiftly learning human motion patterns for multimodal authentication systems. Facilitating the development of these models were the extraction of characteristics and latency. The results of the analysis indicate that CNN-based models have the capability to accurately identify and

authenticate individuals. The main limitation of this paper is that it cannot differentiate intruders or not and no smoking detection.

Taiwo, O. et al. developed a smart home automation system [13] with the capability of motion within and around the residence. To discern motion patterns that are suggestive of intruders from those of occupants of a residence, a deep learning model is deployed. Nevertheless, the study fails to consider the integration of a real time to differentiate between Intruders and not intruders.

Kodali et al. [14]described a low-cost wireless home automation and security system that made use of a battery-backed, Wi-Fi-enabled microcontroller unit (MCU) called the TI-CC3200 LaunchPad. This system uses PIR motion sensors at building doors, with digital input and output pins coupled to the MCU. Wi-Fi connectivity can be enabled by programming the MCU with the use of the Energia Integrated Development Environment (IDE). The authors set up mobile phones to manage IoT devices connected to the MCU and get security alerts even in the absence of an Internet connection.

Tanwar et al.'s [15] economically feasible method of using an email alert system to monitor a home's security in real-time. This approach makes use of a PIR module and a Raspberry Pi MCU. The Raspberry Pi is linked to security cameras and PIR sensors through the exploitation of USB connections as well as general-purpose input and output pins. The system's ability to send residents real-time emails depends on the availability of a household Internet connection. The motion detection logic turns on the security camera to take pictures and send them to the occupant when it detects a change in the signal. The PIR sensors are used to obtain these pictures.

An object and intrusion detection feature were included in the home security system designed by Amrutkar, A., et al.[16]. This system uses an Android application to distinguish between invaders and householders and then sends out alarms. Nevertheless, in order to distinguish between normal and abnormal human gestures, as well as visits (friends, family), and intruders, and to send the right warnings to the homeowner, efficient time management and the integration of machine learning algorithms are necessary.

2.2 Research gaps

During the investigation, numerous gaps in the existing literature and research were identified. Firstly, the current security measures implemented at genocide memorials fail to adequately distinguish between unauthorized individuals and authorized visitors and setting the parameter where the intruder or unauthorized people cannot have the access during the frame time.

2.3 Research Contribution

The contribution of this study is notable in several respects in comparison to previous research:

- **Genocide memorial security system:** The main goal of the suggested research is to create a comprehensive solution for enhancing security systems at Genocide memorials, surpassing the constraints of existing models. Combining machine learning with Internet of Things (IoT) technology allows for this progress. One remarkable aspect of the system is its capacity to classify people into different groups, including employees and guests, and detect trespassers at genocide memorials. This specific skill has the potential to significantly lower the number of false alarms that occur during intrusion detection at genocide memorial centers.
- **Real-time alert and notifications:** The security staff can incorporate preventive measures into their regular work by using the real-time notification tool, which gives them fast updates on any new changes. This study's main goal is to use the revolutionary potential of AI and IoT technologies to improve the intelligence and efficacy of security systems at genocide memorial centers.
- **Real-time monitoring:** The security crew will be able to monitor the actions of employees, guests, and intruders at the genocide memorial thanks to the suggested system's monitoring and visualization dashboard. In addition, the system recognizes possible intruders and notifies the user of them. The dashboard's integration of live streaming makes it easier to visualize and monitor the genocide memorial center in real time. This study sets itself apart from earlier studies by providing a thorough dashboard with these cutting-edge features.

2.4 Summary

The literature review offers a thorough overview of earlier studies and scholarly publications on security systems that deter attackers. This discovery highlights the gaps and limitations that exist in the scholarly literature currently available, especially with regard to real-time alert systems and unwanted house invasions! The review clarifies the persistent issue of false alarms brought on by inadequate identification, which eventually lowers the efficacy of security systems, even though it accepts the limits of earlier studies.

The literature review also emphasizes how important it is to put in place real-time surveillance and alert systems in order to protect the residents of genocide memorials' safety and peace of mind.

By filling in the previously described gaps, a significant body of knowledge is added, offering priceless insights that can guide the creation of AI and IoT-based intrusion detection systems.

CHAPTER THREE: METHODOLOGY

3.0 Introduction

This chapter provides a comprehensive overview of the methodology used to design and implement the IoT based system with machine learning to monitor and prevent intruders from cause damage at genocide memorial center.

3.1 Systems Requirement

A full grasp of the requirements is necessary for the proposed approach to meet them. There are functional and non-functional aspects to all of these requirements.

Functional Requirement

The system must be able to:

- Detect motion in the area and turn on the camera
- Train an AI model to recognize differences between guests, staff, as well as potential intruders.
- Alert the security center if you detect an intruder accessing a critical location.
- Enable live streaming to able reviewed monitoring team to see what is going on the site to be able to take quick decision.

Non-functional requirement

- **Reactivity:** For improved action-taking, the system's time-response needs to be quick.
- **Accuracy:** The system needs to be able to distinguish between several captured persons with accuracy.
- **Dependability:** The system needs to be able to function in various monitored environments or at home.
- **Correctness:** The system needs to identify friends, family, and home residents using accurate data sets.
- **accessibility:** The interface should have an uncomplicated to use.
- **Scalability**: To ensure scalability with changing technologies, the system should be built to support future upgrades and expansions.

3.2 System design and architecture

We created the overall system architecture with IoT device integration and machine learning, data flow, and component connectivity. Its purpose was to identify the roles and responsibilities of each component, which included sensors, microcontrollers, data storage, AI algorithms, and user interfaces. The connectivity choices and protocols required for flawless data transmission and device-to-device communication were then determined.

The primary components of the design are the sensing data, communication, and data visualisation. The camera used to collect images and video are processed, analyzed by machine learning and the output are displayed on a dashboard and LCD monitor. The image and video streaming are sent to the cloud server via internet, where it is further processed, analyzed and make decision for incoming people, and displayed in a web-base as live streaming and notify the owner on the system if there is intruder on the place.

The system is a combination of Hardware and Software. The hardware consists of Esp 32 module, Raspberry pi, camera, Lcd display 16x2+I2C, Ultrasonic sensor, Gas sensor (MQ2) Motion sensor (PIR), Relay (5V), Speaker, Power supply, Buzze.

This section focuses on the system's functionality by going over how the sensors work, what kinds of parameters need to be watched, how data is collected, stored, and analyzed. The three main IoT components sensing, communication, and data analysis units that work together to monitor and deter intrusions at the Genocide Memorial.

Data collection requires the use of the proper components, such as a camera, motion sensor (PIR), ultrasonic sensor, gas sensor, relay (5V) sensor, and so on. Esp 32 module is used to process the data that is collected, and Raspberry Pi is also used to collect and process images from cameras and transfer the processed data to a cloud dashboard for analysis and storage. The security agents receive the processed data from the monitoring center, where they may view the dashboard, respond to incidents via mobile phone, and, in the event that there are unknown individuals there, display an LCD with a message advising them to stop and extend a warm welcome to those who are known to them.

3.2.1 Selected components

Components	The functionality
 **Raspberry Pi Camera Module V2-8 Megapixel,1080p (RPI-CAM-V2)**	The camera is utilised to record visual data. It monitors at genocide memorial center.
 **ESP 32 node MCU module**	This provides Wi-Fi dual-mode Bluetooth connectivity to embedded devices. While ESP32 is technically just the chip, modules and development boards that contain this chip are often also referred to as "ESP32" by the manufacture. Used it for connecting sensors and collect data from the site.
 **Raspberry pi**	Raspberry Pi is a series of small single-board computers. The Raspberry Pi in this project will used for image collecting and processing and local decision

 **Lcd display 16x2+I2C**	The I2C LCD component is used in these applications when we need a visual or textual display and this feature will use it when we want to display or communicate with the coming people.
 **Buzzer sensor**	Buzzer is like a magnetic sensor; it uses voltage and different frequencies for making a sound or beeper. It makes sound due to applied voltage to the piezoelectric, and this material deforms.
 **Ultrasonic sensor**	An ultrasonic sensor is an instrument that measures the distance to an object using ultrasonic sound waves. Ultrasonic technology is required to measure the distance between unknown individuals and critical areas.
 **Motion sensor (PIR)**	Motion sensor (PIR) will detect all movement at genocide memorial center.
	The Speaker will used for communicating between system and people.

Speaker	
 Jumper wires	An electrical wire, or set of them in a cable with a connector or pin at each end, is called a jumper wire, jumper cable, or cables. It is used to connect the parts of a breadboard or other prototype or test device.

3.2.2 System integration

The hardware components, which included sensors, IoT devices, and a central processing unit, were combined into a networked system. Figure 3.1 represents the system block diagram, which shows the components of our system as well as their linkages. The Raspberry Pi 3 was chosen as the single board computer to perform and coordinate all activities, the HC-SR501 PIR Motion Sensor Module was used to sense all movement at the memorial center, the Electromagnetic Buzzer - 12V - PCB Mount to provide sound when something unusual occurs, ultrasonic sensor for distance, Gaz sensor for detect Gaz and the camera sensor to capture images with detection and steaming the situation.

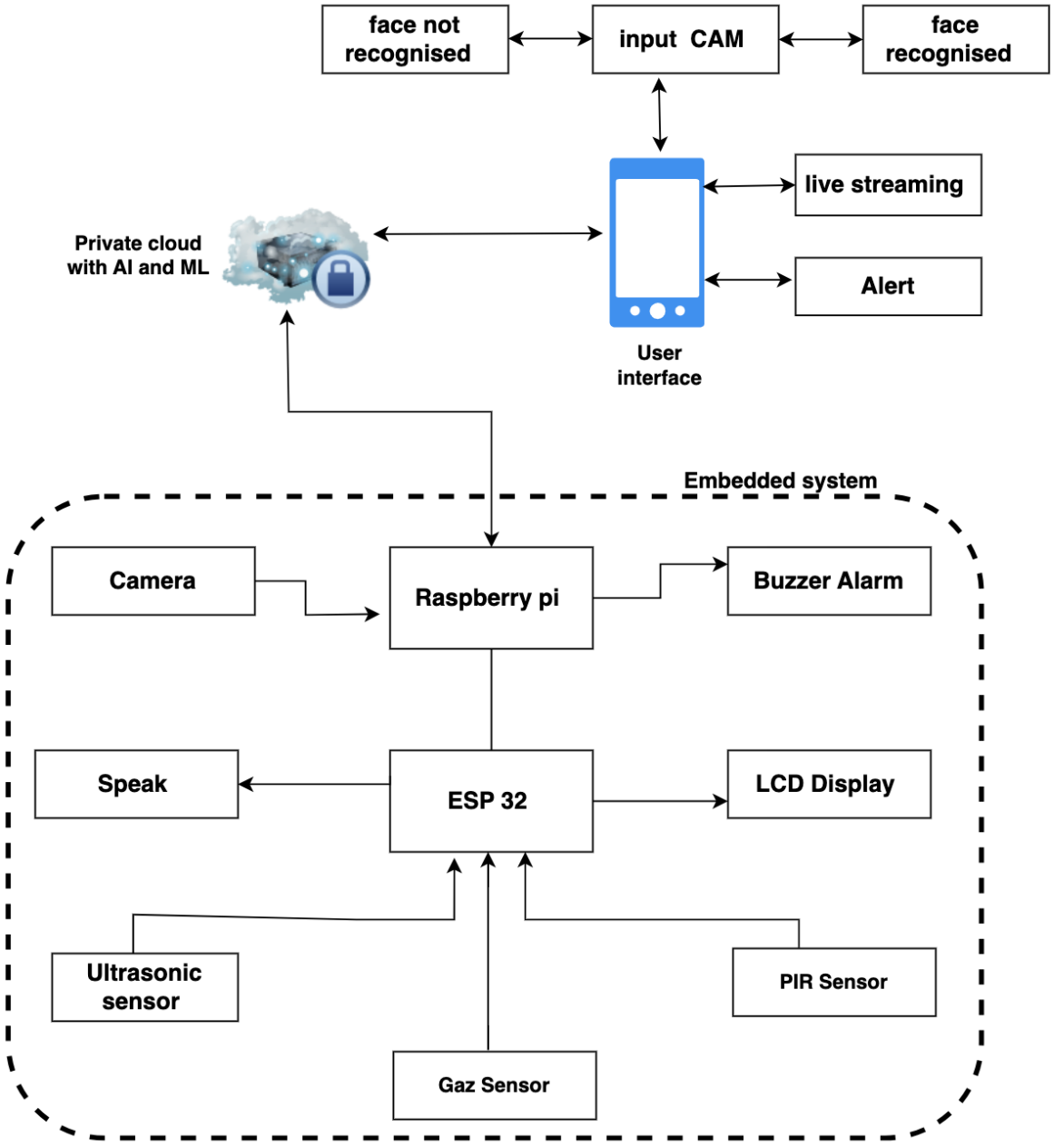


Figure 3. 1 The Project Conceptual Block diagram

3.3 System Architecture

System architecture is the conceptual design that defines the structure or behaviour of a system. An architectural description is a formal description of a system, organized to support reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which components can be purchased and systems developed, which will work together to implement the overall system.

system architecture, the sensing unit, and the microcontroller connected to the private cloud system are the main components of the architecture, via the internet. The Raspberry camera, buzzer, LED, Gaz sensor, PIR sensor and ultrasonic sensor connected to the raspberry pi 3 module is from the edge devices. Raspberry pi connected to the internet will process the data collected from the camera, then transfer them to the cloud. The processed data is accessed via a web server.

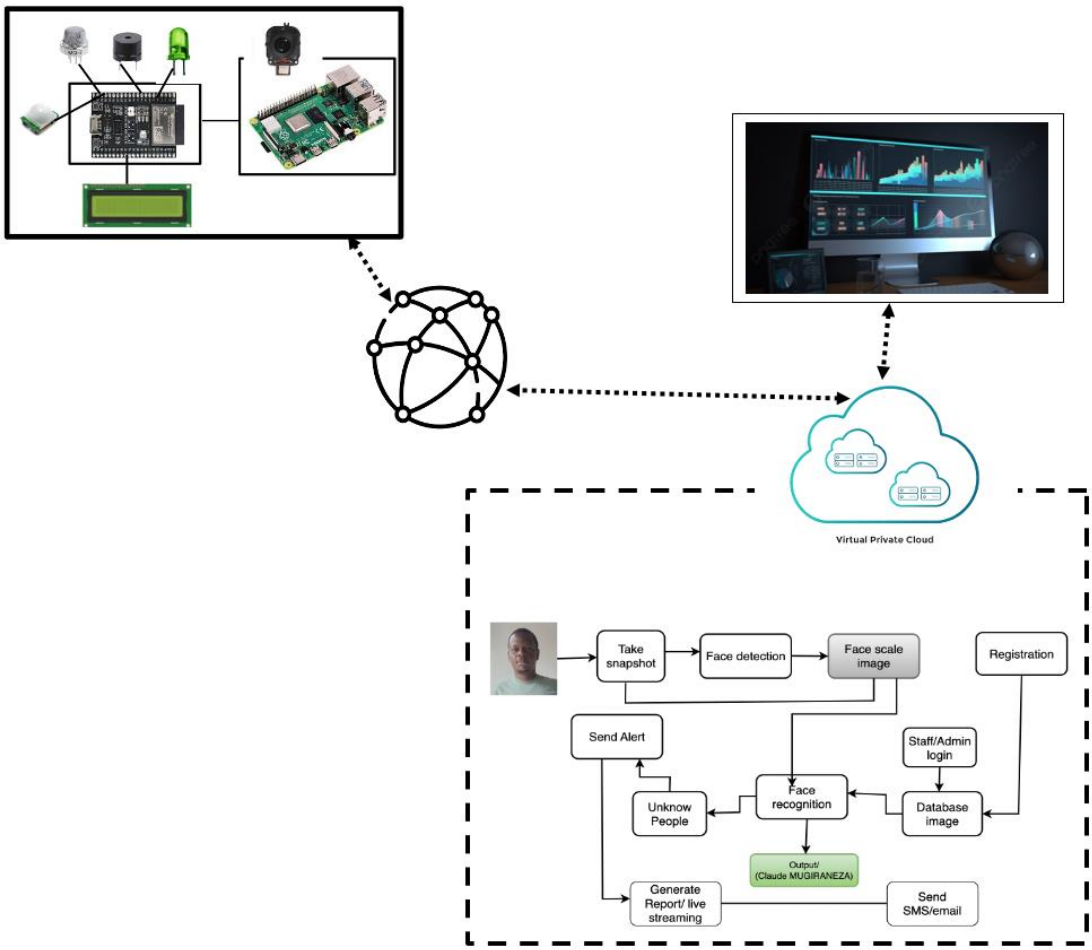


Figure 3. 2 System architecture

3.4 Data collection

The initial stage in gathering data for our project was to place our camera device at the Kibagabaga Genocide Memorial Center to acquire real-time data from staff members. A Raspberry Pi with vision camera was used to record photographs of allowed individuals, which served as both training and testing data for our model. The photographs were captured using high-resolution digital cameras under regulated lighting conditions to minimize unpredictability and ensure accurate input for the memorial center's trained model. Following data gathering, a data augmentation technique was employed to enlarge the dataset and improve the model's robustness during training. This expanded dataset contains a broad mix of authorized members and will be used to train our model.

3.5 Algorithm development

AI and ML algorithms were created to analyze the acquired picture and video data. It additionally makes use of a customized Convolutional Neural Networks (CNNs) algorithm as well as Squeeze Net CNN[17].

Convolution neural network architecture

CNN's hidden layers are often made up of a sequence of sophisticated layers that change with convolution. The trigger function is often ReLU layers, followed by additional convolutional portions such as convolutional layers, pooling, and fully connected layers. Because the active functions and final convolution operators mask output, they are referred to as hidden layers[18].

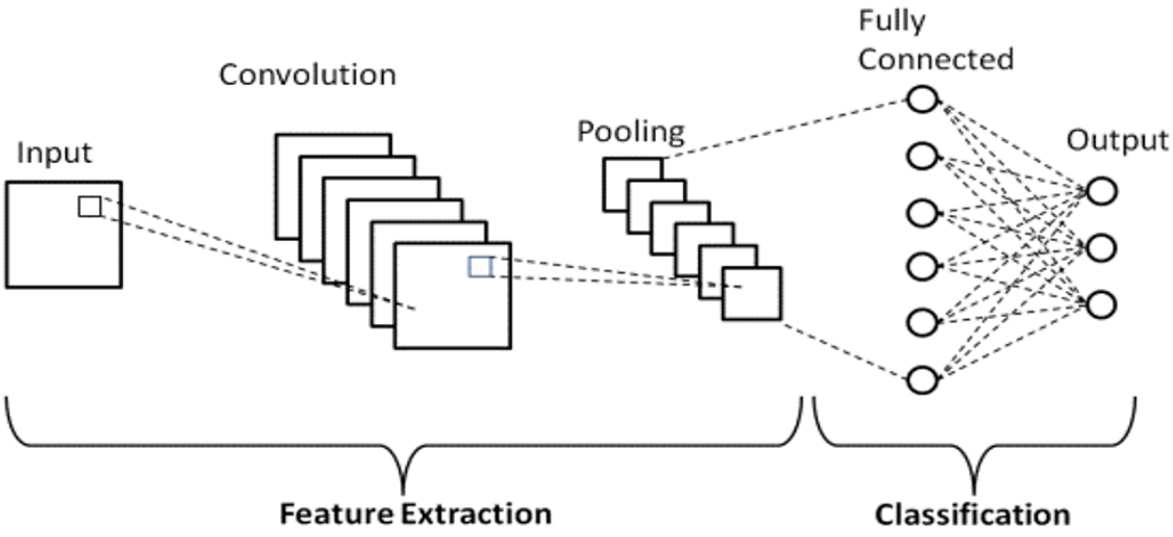


Figure 3. 3 CNN architecture diagram.[12][19]

SqueezeNet CNN Architecture

The squeeze Net algorithm is the better for image recognition because it offers ability of less communication across servers during distributed training, less bandwidth to export a new model from the cloud to an autonomous system and are more feasible to deploy on FPGAs and other hardware with limited memory[20].

The following section demonstrates how to train a convolutional neural network to detect human faces. Instead of starting from scratch, SqueezeNet, a popular convolutional network has been used. Transfer learning is the process of changing and retraining existing networks. The transfer learning approach is faster, more accurate, and easier to deploy[21].

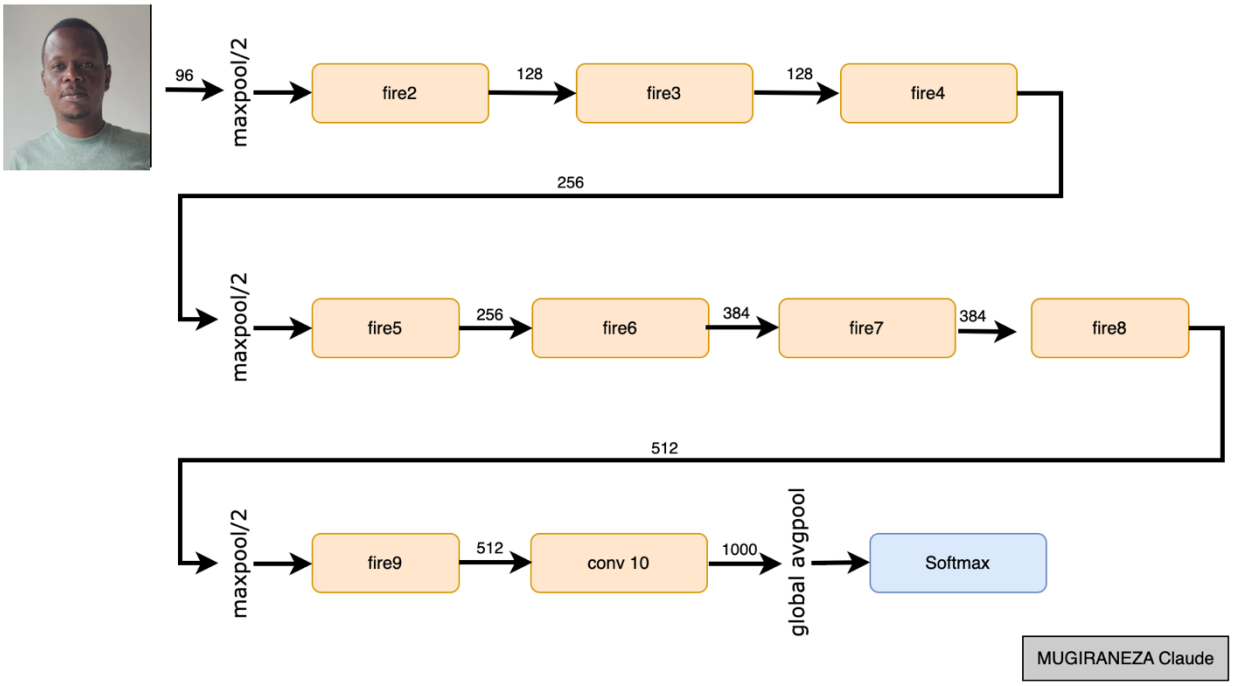


Figure 3. 4 Squeezed CNN architecture diagram [20]

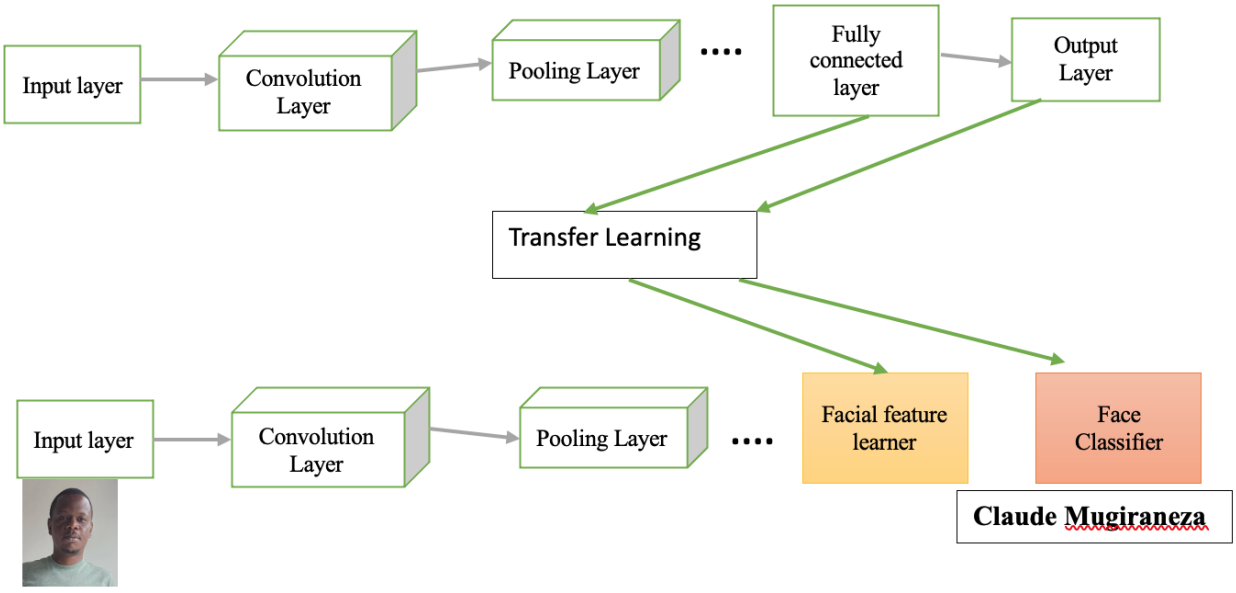
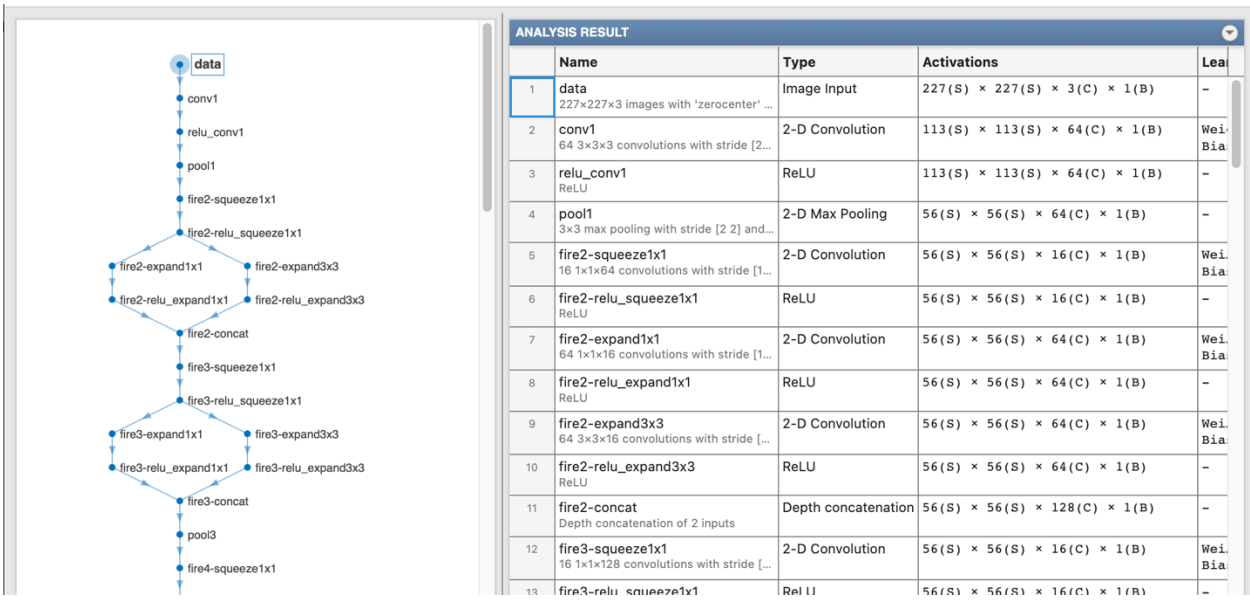


Figure 3. 5 Squeezed network

We use fire modules for the down sampling (DS) units in the Squeeze U-Net contracting path, inspired by SqueezeNet. In the contracting path, each fire module consists of one 1x1 convolution layer with C'_o output channels, $C'_o < C_i$,and an inception layer with two parallel convolutions with 3x3 and 1x1 kernel sizes and $C_o/2$ output channels each. The fire module output is formed by concatenating the parallel convolution output channels. It is transferred to the next contracting layer as well as the comparable layer in the Squeeze U-Net's expansive path with long skip connections. Instead of max or average pooling, we employ stride 2 convolutions for down sampling. Striding increases our network's expressiveness.

3.6 Model development (Customized CNNs)

Squeeze net was used in conjunction with a TensorFlow backend to assist model construction, ensuring a dependable and effective framework. Figure 3.4 represents the architecture of our custom designed model and demonstrates the evolution of the squeeze net neural network's formation.



ANALYSIS RESULT

	Name	Type	Activations	Lea
1	data 227×227×3 images with 'zerocenter' ...	Image Input	227(S) × 227(S) × 3(C) × 1(B)	-
2	conv1 64 3×3×3 convolutions with stride [2...	2-D Convolution	113(S) × 113(S) × 64(C) × 1(B)	Wei Bia
3	relu_conv1 ReLU	ReLU	113(S) × 113(S) × 64(C) × 1(B)	-
4	pool1 3×3 max pooling with stride [2 2] and...	2-D Max Pooling	56(S) × 56(S) × 64(C) × 1(B)	-
5	fire2-squeeze1x1 16 1×1×64 convolutions with stride [1...	2-D Convolution	56(S) × 56(S) × 16(C) × 1(B)	Wei Bia
6	fire2-relu_squeeze1x1 ReLU	ReLU	56(S) × 56(S) × 16(C) × 1(B)	-
7	fire2-expand1x1 64 1×1×16 convolutions with stride [1...	2-D Convolution	56(S) × 56(S) × 64(C) × 1(B)	Wei Bia
8	fire2-relu_expand1x1 ReLU	ReLU	56(S) × 56(S) × 64(C) × 1(B)	-
9	fire2-expand3x3 64 3×3×16 convolutions with stride [...	2-D Convolution	56(S) × 56(S) × 64(C) × 1(B)	Wei Bia
10	fire2-relu_expand3x3 ReLU	ReLU	56(S) × 56(S) × 64(C) × 1(B)	-
11	fire2-concat Depth concatenation of 2 inputs	Depth concatenation	56(S) × 56(S) × 128(C) × 1(B)	-
12	fire3-squeeze1x1 16 1×1×128 convolutions with stride [...	2-D Convolution	56(S) × 56(S) × 16(C) × 1(B)	Wei Bia
13	fire3-relu_squeeze1x1	ReLU	56(S) × 56(S) × 16(C) × 1(B)	-

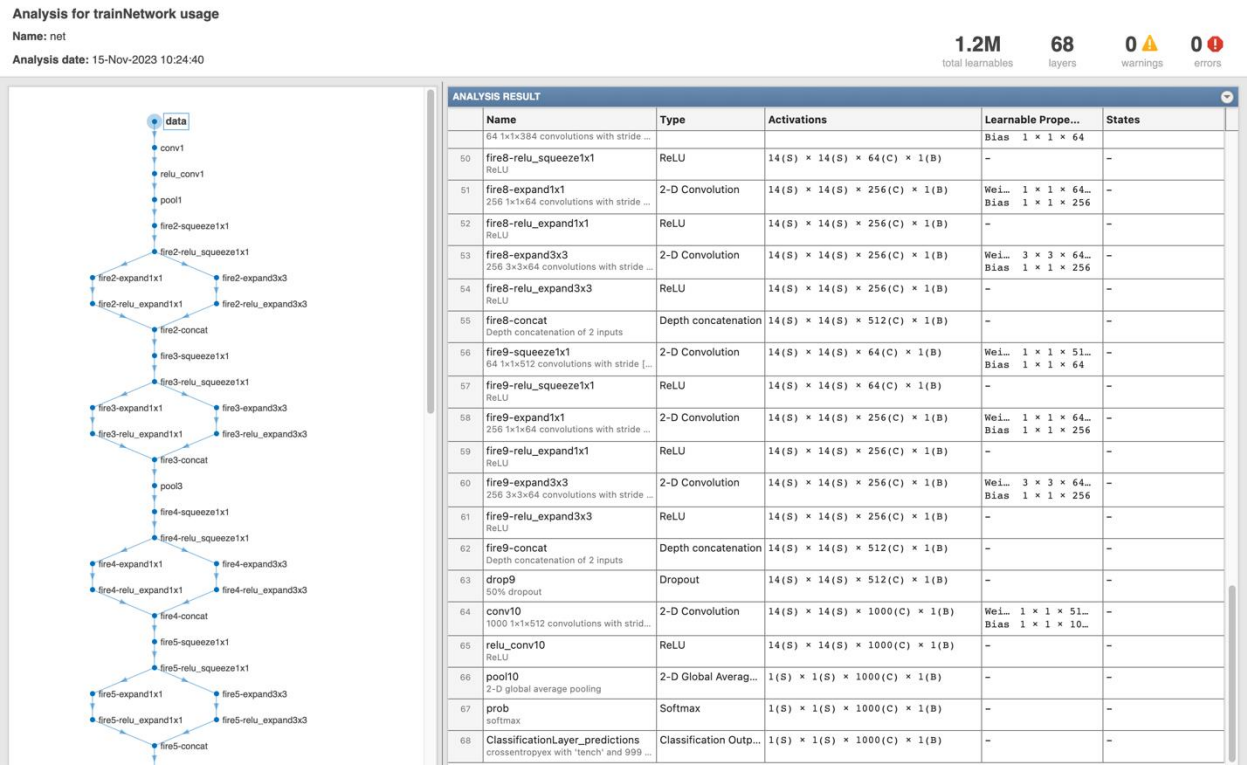


Figure 3. 6 Customized Squeeze Net CNN algorithm

Our customized model development procedure begins with the integration of a convolutional layer consisting of 64 filters, each measuring 3x3 pixels. The rectified linear unit (ReLU) activation function improves the network's capacity to detect complicated patterns in input data. Furthermore, the model considers the input (227, 227, 3), allowing it to recognize the input photos.

Following that, a max-pooling layer is used to help reduce feature map dimensions while retaining their most clear properties. The initial approach is repeated by including an additional convolutional layer made up of 64 filters, followed by another max-pooling layer.

The feature maps created by the convolutional layers are flattened before generating a sequence of tightly linked layers. Two dense layers of 512 and 256 neurons are used for improving feature abstraction and representation. Finally, the sigmoid activation function is applied to the output layer, which is made up of a single neuron. This layer's precise function is binary classification, which uses the incoming picture data to distinguish between known or unknown people.
In mathlab, a CNN model was trained using the mathlab script framework.

The CNN model was then trained on the pre-processed image dataset and correctly classified as genocide memorial staffs or unauthorized individuals where intruders will be considered.
During the training process, various strategies such as data augmentation were used to improve the model's performance and generalization capabilities.

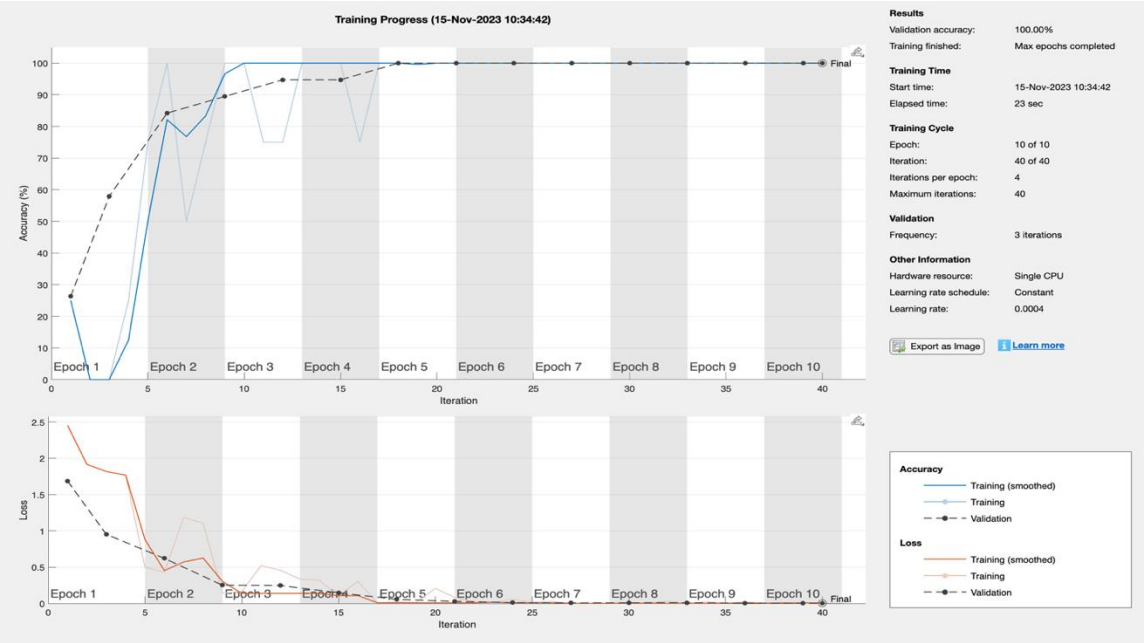


Figure 3. 7 Training progress

3.7 Model Training and optimization

We optimized and fine-tuned our customized CNN for detect and recognized if the incoming people is known or not. Accuracy of this model training is around closed 98%.

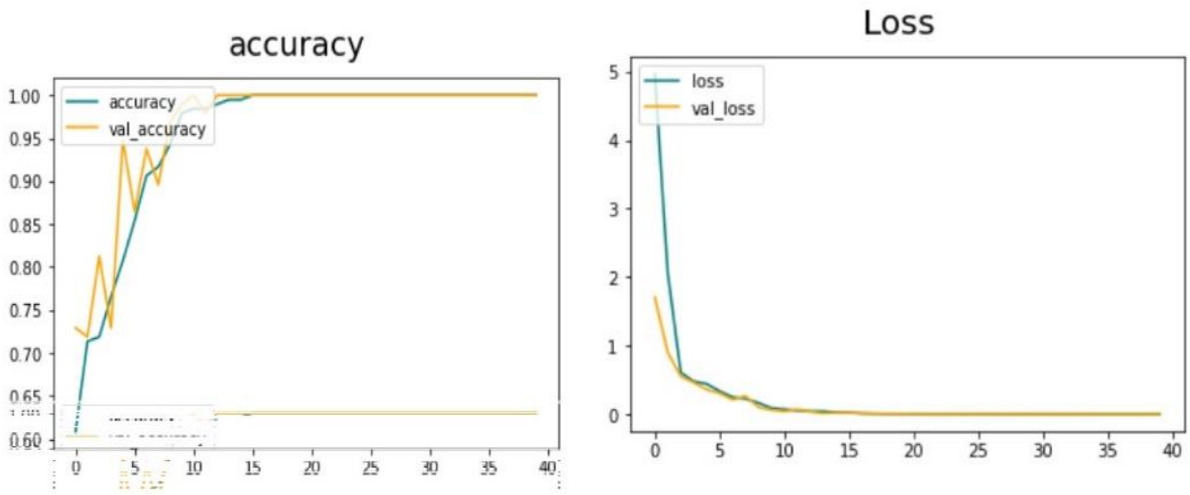


Figure 3. 8 Training result

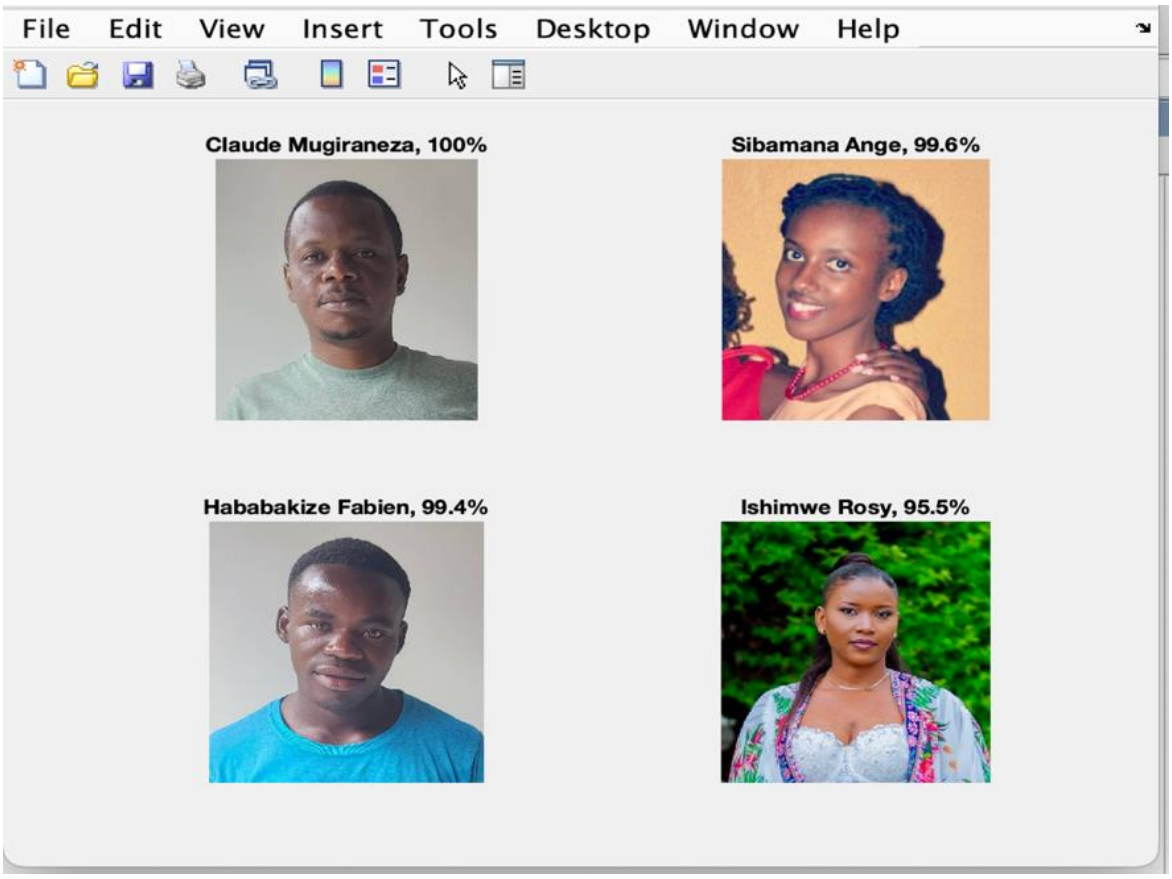


Figure 3. 8 Tested model

CHAPTER FOUR: SYSTEM DESIGN AND ANALYSIS

4.0 Introduction

The architecture of a system is a high-level description of the complete system that identifies its key components and functions, as well as the rules that each element must follow in order to interact and collaborate. The Internet of Things is built on embedded systems and other technologies like pervasive systems and sensor networks. The Internet of Things (IoT) is a network-based system in which "things" collaborate and carry out tasks while interacting with the physical and digital worlds. Using the IoT architecture paradigm, a real-time facial recognition system was constructed.

The embedded system level design is discussed in this section; first, the system architecture is described, followed by the system IoT Layers architectural design, Schematic diagram, and database diagram. Finally, system flow charts and use case diagrams will be used to show the system's functionality.

4.1 System Architecture

4.1.1 IoT Layers Architecture

IoT architecture how the real-time facial recognition security system functions as designed and developed. It describes hardware and software systems and shows workflows and procedures. This four-layer architecture is organized primary physical layers: the embedded system, the network layer, the data processing and management layer, and the application layer.

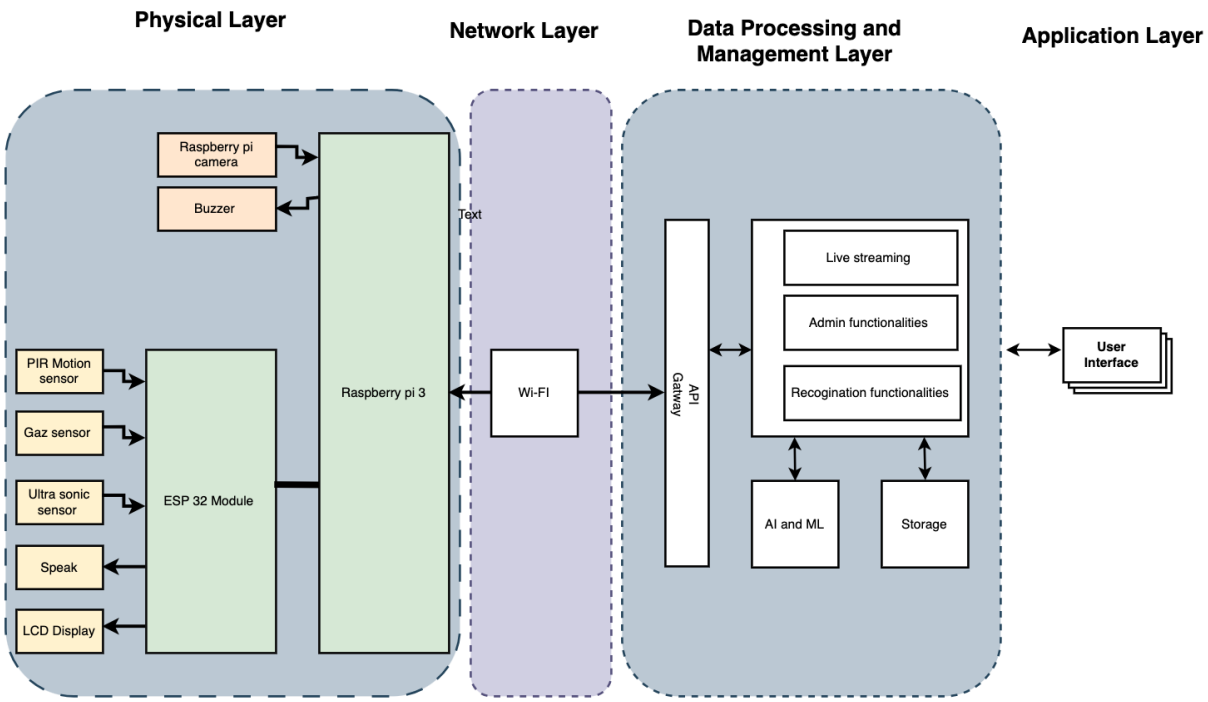


Figure 4 1 IoT architecture

- Physical Layer: this part consists of different IoT components with different technologies, which are interconnected together to perform the main goal of this research. Raspberry pi 3 Model is used as a control unit, raspberry pi camera, Buzzer, Gaz sensor, ultrasonic and PIR motion sensor which are connected and controlled by a raspberry pi.
- Network layer: used WIFI as a communication network to link the Control unit with the cloud server
- Data processing and management Layer: which is the data engine of the system from cloud services such as data storage, security, machine learning, and execution of the instruction.
- Application layer: This Layer consists of a web application interface that helps the admin to manage and monitor the system for data analysis. It allows the admin to manage and monitor memorial center events and generate reports. This is Web App and a personal computer or smartphone. In this layer, the Short Message Peer to Peer (SMPP) protocol used to send your SMS.

4.1.2 Schematic Diagram

The schematic diagram is the representation that shows the functionality and connectivity between elements of the system.

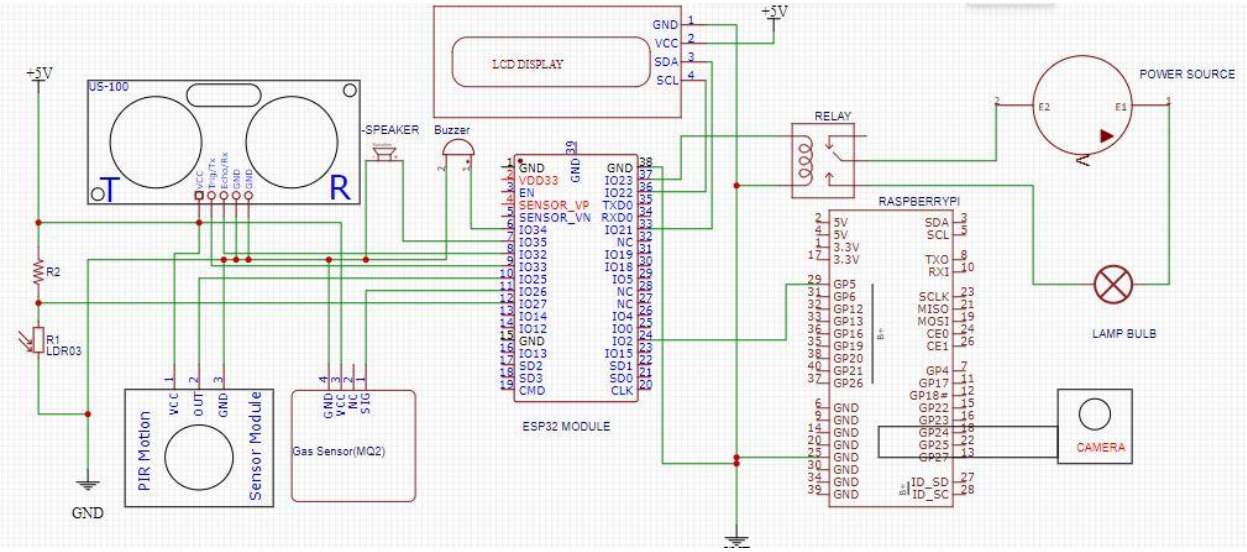


Figure 4 2 Schematic Diagram

4.1.3 Database diagram

Database diagrams graphically show the structure for the database and the connections between its components. You can draw a diagram for a data source, a schema, or a table. To establish relationships between database objects, consider using primary and foreign keys.

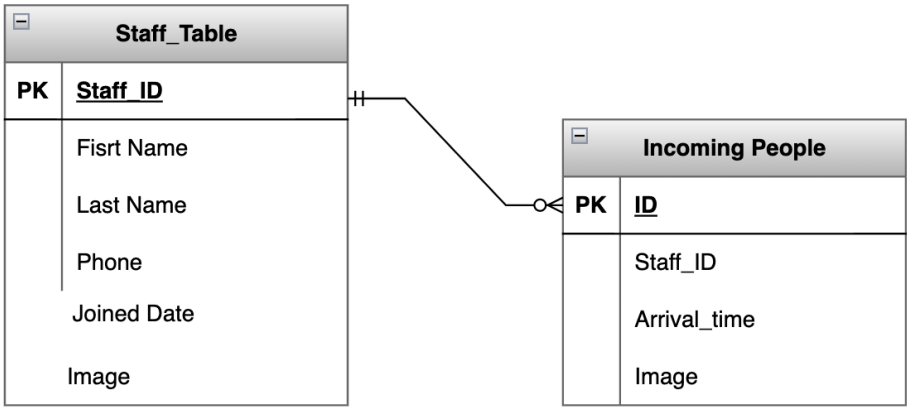


Figure 4 3 Database diagram of the System

4.2 System functionality

This section addresses how the system works and how instructions and data flow through it. It covers a system flow chart as well as use case graphics.

4.2.1 User case diagram

A use case diagram in the Unified Modeling Language (UML) can summarize the details of your system's users (also known as actors) and their interactions with the system. The use cases diagram is used to depict the system's primary actors and the relevant actions they conduct. The system administrator, employee, server, and embedded system are among the actors.

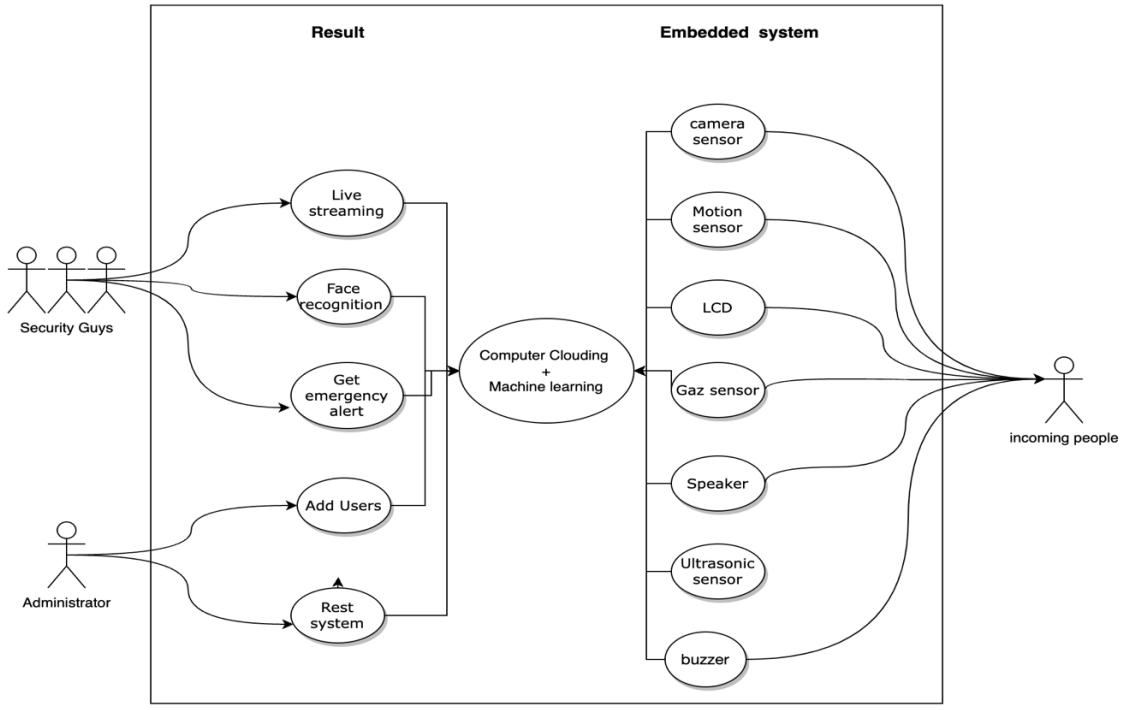


Figure 4 4 User case diagram

4.2.2 Flowchart diagram

A flowchart is a graphical representation of phases that aids in clearly illustrating a process from start to finish. The flow charts depict the data and command flow in the embedded system linked to the web server.

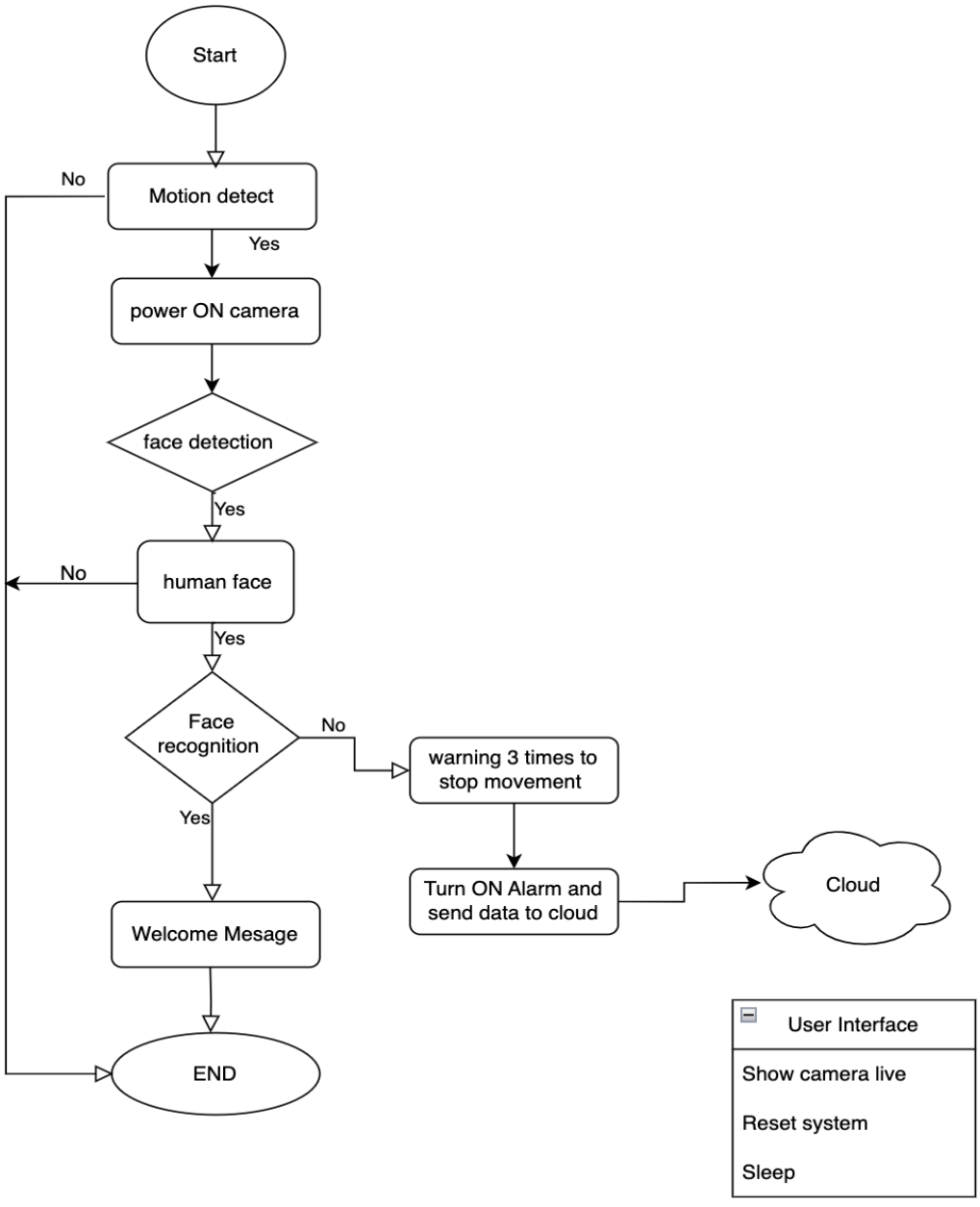


Figure 4 5 Flowchart diagram

A flow chart is a method of displaying data in the system and describing where the decision is made. It covers how to monitor and prevent every movement at the memorial center using the Internet of Things, as well as how to speed up real-time information to the security team and monitoring center. The system's primary duty is to monitor characteristics such as mobility, face identification on people at the memorial center based on face detection, and recognition by distinguishing between actual persons and intruders. When the motion detector detects movement, the camera begins to collect images and videos and recognizes faces. If the recognized face is the existing faces, the status returns to normal, but if it is not recognized, the buzzer begins warning the incoming face, and if the movement continues, the security guys receive an alert and inform them that there are intruders on the site, after which the camera begins streaming and saves all events on the site. The graphic above depicts an algorithm utilizing a flowchart that describes how an IoT system is used to track all movement at the memorial center in this thesis. Except when there are technical challenges, the system functionality continues to monitor all events on the site, track the distant location of invader people, and automatically inform the security guys on site.
The system functioning is based on embedded devices, and the integrated system includes both software and hardware components.

CHAPTER FIVE: RESULT AND DISCUSSION

5.1 Introduction

This section contains recognition of faces results obtained from images captured by a camera sensor and collected via live streaming, as well as statistic reports made based on the images captured.

5.2 Experiment

5.3 Machine Learning Approach

Images should be placed in a file called images, and every person you want to recognize should have their own directory containing the image and its corresponding names.

Convolutional Neurol Network assists us in detecting and locating faces by constructing a bounding box around their extend, while FaceNet extracts features from images. As a result, it compares the new faces to existing encoded photos, adds a rectangle-bounding box to the frame, and transmits the results to the web to be marked as recognized or not in the dashboard.

TABLE 1: DESCRIBE THE FUNCTIONS USED IN PROPOSED SYSTEM AND ITS EXECUTED RESULTS

Test data	Expected Result	Observed Result	Pass/Fail
Cv2.imread() Cv2.imwrite()	Use CV2 function to read and write image to corresponding files	Read and write images	Pass
PiCamera ()	use the capture () function from the camera object to take a Videos	Camera started	Pass
face_encoding ()	Retrieves all images stored at a person's images locations, resizes and normalizes. Then using MTCNN to detect the face in frame and crops where the face of a person is located, then extracting features using FaceNet Pre-trained model.	Detected and extracted images features, then stored in encodings.json file	Pass

Face comparison ()	A new image with a person is then turned to its encoding using facenet and compared to other encodings stored in encoding. json using the cosine rule with a tolerance of 0.3.	Face matching	Pass

Table 2: Describe the functions used in proposed system and its executed results

5.4 The system results

The system for preventing intruder to access unauthorized place at memorial center consists of two main parts: the first part is embedded system which contain sensors and actuate for preventing intruder to access where is not supposed to access and the second one is cloud platform where all decision are taken. Both parts are essential for the system, and employees can obtain notification in case of delay or absence.

5.1.1 Embedded system

After designing the full circuit of the system, I implemented the circuit. I did a test of my prototype to check if it is working. This is a prototype of the system which consists of a raspberry pi camera, LED, PIR motion Sensor, ultrasonic sensor and buzzer connected to the Raspberry pi 4 with 2GB of RAM.

Figure 5.0 Embedded system or prototype

5.1.2 The dashboard displays the results

Furthermore, a web interface was developed to allow authorities to present data on the dashboard. You can register new employees with full details by clicking the add employee button.

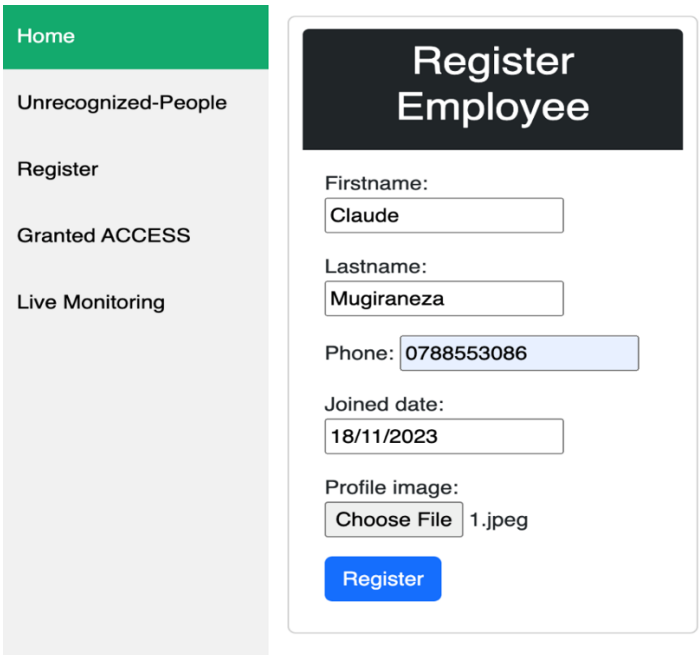


Figure 5. 1 How to register new staff in the system

After saving the employee's information, you may view it in the employee list file and filter it accordingly.

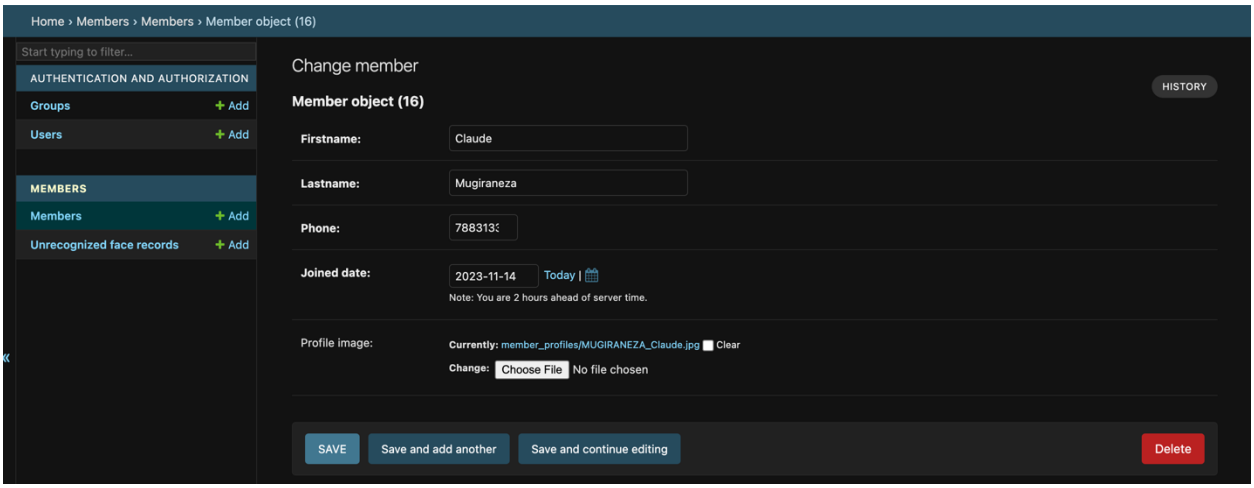


Figure 5. 2 List of the employees

After the new employees are saved, their faces will be compared to other encoded images, and it will be displayed whether the images captured are known with corresponding names or unknown.

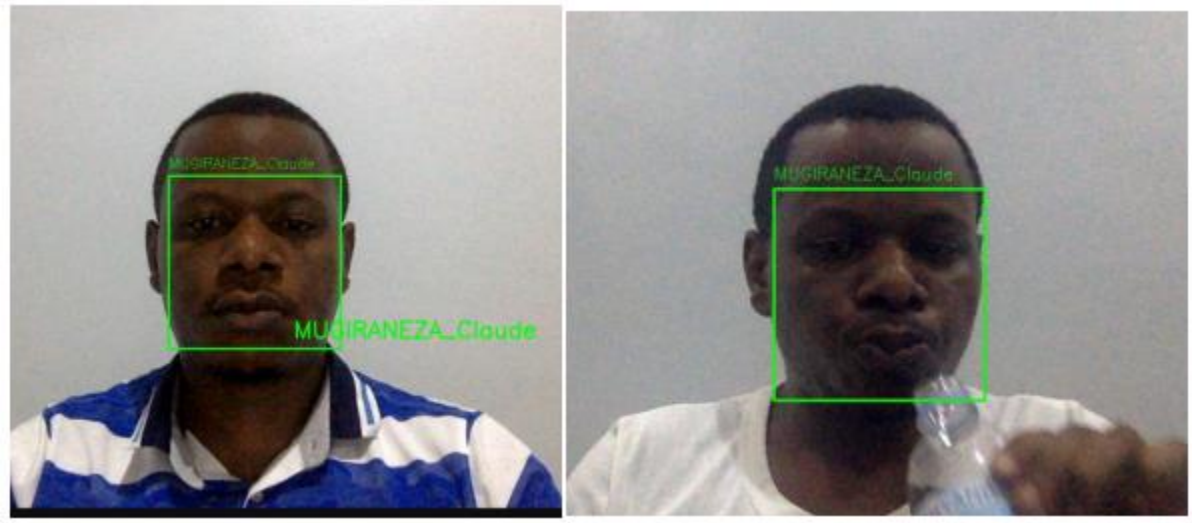


Figure 5. 3 Image comparison /matching with encoded images through live streaming

If unknown is detecting the alert send to security agent via SMS and save the images of unknow people.

Figure 5. 4 SMS send to security agent.

DISCUSSION

This work makes a significant contribution to the field of security technology by introducing an innovative and comprehensive approach to the protection of Rwanda genocide memorials, the approach can be scalable to other historical locations like museums. The incorporation of a real-time face recognition attendance system, coupled with machine learning algorithms and IoT devices, enhances the accuracy and efficiency of intrusion detection. The study's scope extends beyond conventional security measures, addressing critical gaps by focusing on the differentiation between intruders and authorized visitors and set the perimeter where intruder can't pass if he is already entering in the center as well as integrating smoke detection for fire prevention. By emphasizing these aspects, the research not only advances the capabilities of security systems but also establishes a practical model for the preservation of historical and cultural.

The current system can detect and recognized the intruder but the novelty of our proposed system is inclusion of human detection and recognizes capability-based convolution neuro network (CNN) algorithm and buzzer as method to warn the security agents of memorial center but setting ON buzzer and send the SMS to security agents for alerting them that intruder has bypass all security parameter.

The existing system faces limitations in detecting unauthorized access attempts based on the distance between where movement was detected and the location of the unauthorized area [3]. However, significant enhancements have been implemented to address this issue. The updated technology can now detect movement and determine if an intruder is trying to enter an area that is not authorized place before authentication. The system triggers an alarm or buzzer and promptly notifies the owner via phone. Users can also watch live streaming of the memorial center's events, which enables them to make educated decisions and act quickly in an emergency. This all-encompassing strategy helps to prevent fire accident like smoking at the genocide memorial which is not allowed in addition to enhancing security which harmful the place.

These developments strengthen the overall security protocols at the genocide memorial by ensuring quick reactions to potential security breaches and providing extra protection against unexpected threats.

Based the result collected through the assessment done on the site on the site all person how tried to access the genocide memorial in different category in different

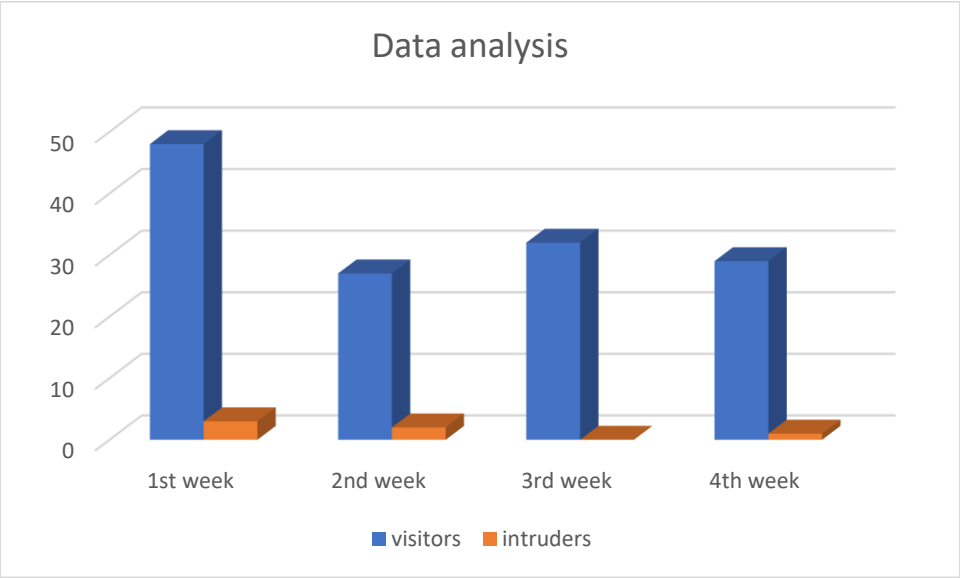


Figure 5.5 The data collected in 4 weeks

In the context of this study, chart was used to represent the percentage to represent the staff vs intruders how tried to access the genocide memorial center based on specific parameters, such as intruders and staff. This chart serves as a visual tool to convey the composition of how to the people accessing the critical place at different points in date and time. The chart is divided into two segments: one representing the percentage of staff people and the other representing the percentage of the intruders.

CHAPTER SIX: RECOMMENDATION AND CONCLUSION

5.1 Conclusion

The findings presented in the preceding sections provide compelling evidence that a machine learning and IoT-based system is a viable solution for monitoring genocide memorial centers, effectively preventing intruders from breaching the site's security parameters, and promptly alerting the monitoring center. This validation indicates the possible benefits as well as efficacy of such a system to enhance the overall security framework of sensitive venues such as genocide memorial centers.

Despite these encouraging outcomes, it is critical to recognize the need of an IoT design that interacts seamlessly with existing systems. The current analysis emphasizes the relevance of coexistence between the proposed machine learning and IoT solution and the existing infrastructure. Recognizing this need, we advocate for the deployment of an IoT architecture that aims to work with and interact with the existing systems. The suggestion is addressed to the genocide memorial center's supervisor, demonstrating the need of a cohesive integration approach that allows the successful deployment and operation of the proposed security system.

5.2 Recommendation

The project's prototype provides useful insights into limitations, with a particular emphasis on a security risk relating to hardware systems. It is clear that the prototype's current condition exposes weaknesses in the hardware components' security infrastructure. Addressing this issue is critical to the project's overall success because it has a direct impact on the system's reliability and robustness. As a result, diligent attention and strategic planning are required to correct and strengthen the security measures linked with the hardware components in later stages of the project.

Given the limits outlined, a critical feature for the future progress of this study is a given focus on the resolution of the security issue within the systems' hardware. Recognizing the potential implications for project functionality as well as the larger implications for data integrity, it is critical to develop a thorough strategy for improving the hardware infrastructure's security. This not only ensures the project's resilience in the face of potential risks, but also contributes to the

development of a more trustworthy and reliable prototype, creating a solid foundation for the project's advancements in later phases.

5.3 The future work

The next stage of our efforts to improve security at the genocide memorial center focuses around recognizing and detecting possible threats that may be caused by intruders. In addition to recognizing and preventing breaches, the next effort will focus on the items that an intruder might be carrying in their pockets or hands that might compromise the integrity of the memorial center. By taking a proactive stance, we want to intercept any attempts to damage or harm the memorial and guarantee a more thorough and focused security plan.

Through analyzing the property for potential intruders, we hope to improve the security protocols in place by anticipating and avoiding any specific risks that can jeopardize the integrity of the genocide memorial center. This strategic change is suggestive of a dedication to a comprehensive and proactive security posture, supporting the measures already in place to preserve the memorial's historical and cultural significance.

REFERENCES

[1] I. G. M. Ngurah Desnanjaya and I. N. A. Arsana, “Home security monitoring system with IoT-based Raspberry Pi,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 3, pp. 1295–1302, Jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1295-1302.

[2] “Outreach Programme on the 1994 Genocide Against the Tutsi in Rwanda and the United Nations”.

[3] “A place of remembrance & learning - Kigali Genocide Memorial”.

[4] “Collections Genocide Memorials GENOCIDE MEMORIALS.” [Online]. Available: https://genocidearchiverwanda.org.rw/index.php/Category:Memorials1/8

[5] A. Sodaro, “Politics of the Past: Remembering the Rwandan Genocide at the Kigali Memorial Centre,” 2011, pp. 72–88. doi: 10.1057/9780230319554_5.

[6] “Abakekwaho gusiga amazirantoki ku rwibutso rwa Jenoside yakorewe Abatutsi bafashwe - Kigali Today”.

[7] V. Padmakar and B. V. R. Murthy, “Face Recognition System with Machine Learning,” in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Nov. 2021. doi: 10.1088/1742-6596/2089/1/012047.

[8] G. Lulla, A. Kumar, G. Pole, and G. Deshmukh, “IoT based smart security and surveillance system,” in *2021 International Conference on Emerging Smart Computing and Informatics, ESCI 2021*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 385–390. doi: 10.1109/ESCI50559.2021.9396843.

[9] S. Pandya *et al.*, “Smart home anti-theft system: A novel approach for near real-time monitoring and smart home security for wellness protocol,” *Applied System Innovation*, vol. 1, no. 4, pp. 1–22, Dec. 2018, doi: 10.3390/asi1040042.

[10] G. Karuna, R. P. R. Kumar, R. Kapse, and S. Revulagadda, “Home Automation Based on IoT,” *E3S Web of Conferences*, vol. 391, p. 01159, 2023, doi: 10.1051/e3sconf/202339101159.

[11] U. Sirisha, D. Poojasri, N. Gayathri, K. Heshma, and G. R. Sekhar, “IOT BASED ANTI THEFT DETECTION AND ALERTING SYSTEM USING RASPBERRY PI,”

International Research Journal of Engineering and Technology, 2020, [Online]. Available: www.irjet.net

[12] A. Ritahani Ismail, A. S. Mohd Khalili, N. F. Adilah Rahim, and S. Q. Nisa, "Deep Convolutional Generative Adversarial Networks for Imbalance Medical Image Classification.," *International Journal on Perceptive and Cognitive Computing*, vol. 9, no. 2, pp. 98–103, Jul. 2023, doi: 10.31436/ijpcc.v9i2.409.

[13] O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model," *Wirel Commun Mob Comput*, vol. 2022, 2022, doi: 10.1155/2022/9307961.

[14] M. A. Hoque and C. Davidson, "Design and implementation of an IoT-based smart home security system," *International Journal of Networked and Distributed Computing*, vol. 7, no. 2, pp. 85–92, 2019, doi: 10.2991/ijndc.k.190326.004.

[15] M. S. (Mohammad S. Obaidat, Institute of Electrical and Electronics Engineers, IEEE Communications Society, Society for Modeling and Simulation International, and Dalian li gong da xue, *IEEE CITS 2017 : 2017 International Conference on Computer, Information and Telecommunication Systems : July 21-23, 2017, Dalian, China*.

[16] M. R., R. Y., R. R., and S. A., "Smart Home Security System using Iot, Face Recognition and Raspberry Pi," *Int J Comput Appl*, vol. 176, no. 13, pp. 45–47, Apr. 2020, doi: 10.5120/ijca2020920105.

[17] I. National Institute of Technology (Punjab, I. D. of C. S. & E. National Institute of Technology (Punjab, Institute of Electrical and Electronics Engineers. Delhi Section, and Institute of Electrical and Electronics Engineers, *ICSCCC 2018 : International Conference on Secure Cyber Computing and Communication : December 15-17, 2018*.

[18] "IRJET-V7I11204".

[19] W. Rawat and Z. Wang, "Deep convolutional neural networks for image classification: A comprehensive review," *Neural Computation*, vol. 29, no. 9. MIT Press Journals, pp. 2352–2449, Sep. 01, 2017. doi: 10.1162/NECO_a_00990.

[20] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size," Feb. 2016, [Online]. Available: http://arxiv.org/abs/1602.07360

[21] "1711.05491".