Building Automated Watchdog through Real Time Face Detection using IoT

Ms.Suganya. A[1], Aadithya Thyagarajan T[2], Aravinth.S[3]
[1]*Assitant Professor,* [2,3]*Final year IT Students,*
Karpagam College of Engineering, Coimbatore, Tamil Nadu.

Abstract - The safety and security of elderly people living alone at home must be given top priority in the modern digital environment. This article presents the Automated Watchdog System (AWS), a cutting-edge security and monitoring programme that makes use of facial recognition and Internet of Things devices. AWS creates an IoT device network that is networked and continuously monitors indoor settings, sending real-time data to a central computer. AWS's user-friendly and customisable design allows customers to easily modify the system to meet their unique requirements, including alarm settings, response procedures, and smooth connection with other security systems. As a safety for people to protect their properties and belongings in a variety of contexts, this proactive and strong approach responds to the growing need for state-of-the-art security solutions. AWS is particularly good for keeping older people safe who live alone by alerting their family members as soon as it notices someone not authorised at their door. This creative effort demonstrates a dedication to improving vulnerable people's security and well-being in the quickly changing technological environment of today.

Keywords: Automated Watchdog System, Elderly People, Safeguard, Facial Detection Technology, Modern Digital Environment, Central computer, Indoor Setting, Alert preferences, Customizable Design, Unauthorised Individual, Robust security, Alarm Setting, Vulnerable individuals, Technological Environment.

1. INTRODUCTION

Seniors living alone face a growing number of issues in today's society, which calls for immediate attention and creative solutions. A major concern for their welfare is the security issues they face when they arrive home. Because they frequently live alone, senior citizens have distinct vulnerabilities that leave them open to several kinds of hazards, especially at the point of entry into their homes. Problems like crises, possible intruders, and unauthorised access present major risks to these people's safety and mental well-being as they manage the difficulties of living alone. It is necessary to implement customised security measures to reduce the risks that senior citizens face in order to address these issues. These measures should be implemented especially at their doorstep, which serves as the main point of contact between their private space and the outside world. In order to specifically address the concerns of elderly people who live alone, this project aims to investigate and develop practical security solutions. We hope to create a complete security system that not only recognises and confronts any dangers but also gives these people a sense of comfort and support by exploring the particular difficulties they face on a daily basis. The ultimate objective is to use cutting-edge tactics and technology to improve elderly adults' safety and wellbeing so they may live independent, secure lives.

2. LITERATURE SURVEY

Using a smartphone, the advised system's smart home security control panel enables remote control of door accessibility and voice alerts. The system uses a Raspberry Pi as the smart home security system's embedded control unit (ECU) and a Remote Control Unit (RCU) that is installed on the user's smartphone. The PiCamera module and PIR motion sensor in the ECU are used to detect motion and take pictures of people at the door. Door accessibility is managed by an electromagnetic door lock module [1]. Additionally, the technology allows the homeowner to receive email and voice notifications that include collected photographs. Through an SSH website for Android, users can communicate with the system in real time. The complete system is intended to be highly efficient, reasonably priced, and low power consumption, which qualifies it for installation in a residential setting. The installation is configuring the Raspberry Pi, putting up the PiCamera, installing email alert software, and writing Python scripts to implement ECU features like email sending, motion detection, and picture capturing. Additionally, SSH commands and a Python script for the electromagnetic door lock are used to enable voice alarms and door access control. The system's convenient and effective way to monitor and manage access remotely is intended to improve home security. In order to improve security in a variety of locations, including homes, offices, stores, and banks, the Face Detection System (FDRS) has become essential. This technology recognises and verifies persons based on mathematical factors unique to human appearance. With the help of certification and validation, the FDRS programme allows the system to differentiate between the truth and falsehoods by analysing the image or face structure. Face recognition and an Internet of Things

(IoT) door lock system using the Blynk app are combined in a two-step process used by this security system [2]. After ringing the bell, the ESP32cam takes pictures of the owner's face and notifies them on their smartphone. Hardware for the integrated digital circuit includes the ESP32cam and a solenoid lock, which responds to changes in current flow by opening or closing. The findings point to a trustworthy, cloud-controlled digital door lock system that detects face recognition to grant authorised access and alerts the owner to any unauthorised attempts. Due to its adaptability, the project can be used for home offices, bank vaults, automobile doors, and locker rooms. In comparison to more conventional fingerprint-based systems, the system's affordability, dependability, and simplicity of use are highlighted in the conclusion. Further information about similar technologies and implementations can be found in the references. To tackle the COVID-19 epidemic, a novel solution that combines deep learning, the quicker R-CNN algorithm, and the Industrial Internet of Things (IoT) has been unveiled. An IoT system using temperature sensors, mask detection, and social distancing monitoring is one of the major advances in the field that are examined in this research, along with a deep convolutional model for evaluating safety guideline compliance and a thorough assessment of deep-learning techniques for disease monitoring through medical imaging [3]. A highly accurate mask identification method utilising image preprocessing and face detection is presented in a different paper. Even in dimly lit environments, real-time people and social distancing monitoring is demonstrated via a deep neural network model. Further assisting in the reduction of COVID-19 transmission is a deep learning system based on computer vision that runs on a Raspberry Pi and allows for time-efficient mask recognition and social distancing monitoring [4]. In addition, the study suggests an Internet of Things (IoT) deep learning architecture for COVID-19 identification using chest X-ray analysis, providing extremely precise results for timely medical action.

3. PROBLEM DEFINITION

This journal article takes a close look at the wide range of hazards that elderly people who live alone must deal with, especially those that come right to their door. Investigating the complex circumstances that may render elderly people living alone more vulnerable to home invasions and burglaries is the first step in the inquiry. It is clear how criminals can target them as comparatively easy prey when factors like the possible sense of fragility are taken into account. The study examines seniors' financial hazards in addition to physical ones. It looks at complex frauds and swindles carried out by dishonest people who frequently take advantage of senior citizens by using highly skilled impersonation techniques. A further element of the research explores the psychological aspects of social isolation. It looks at the hazards of being duped by someone who appear to be kind, illuminating how seniors can be easily taken advantage of, particularly when they're lonely. Seniors might be coerced into making needless purchases or services by means of aggressive sales practices and unsolicited solicitations, as the investigation reveals. The effects of environmental dangers, utility problems, and medical emergencies on the safety and wellbeing of elderly people living independently are also thoroughly examined in this research. The study attempts to offer subtle insights into the general requirement for all-encompassing safety measures by addressing the dissociation from support systems.

The objective is to gain a thorough awareness of the difficulties encountered by this susceptible group and to suggest community-based solutions designed to successfully reduce these complex hazards.

4. METHODOLOGY

One proactive and efficient way to combat the numerous threats encountered by elderly people living alone is to put in place a centralised Internet of Things (IoT)-based security camera system. The incorporation of cutting-edge technology facilitates emergency response, communication, and monitoring in real-time. Motion-activated smart cameras can identify unexpected activity or unwanted entrance and send out instant alerts to the senior and other designated contacts. In addition to serving as a deterrent to potential burglars, this round-the-clock surveillance collects important evidence in the event of a security breach. By using facial recognition technology, doorbell cameras can authenticate visitors, adding an extra degree of protection against unsolicited approaches or possible dangers. Seniors have more control over who enters their living space because to access control technologies that let them remotely give or reject admission to their residences. When a medical emergency arises, the monitoring system can instantly alert emergency services or pre-designated contacts thanks to integration with wearable technology or panic buttons. When responding quickly to emergencies, centralised monitoring centres can help local authorities coordinate more quickly. Financial exploitation can be decreased by having Internet of Things (IoT) devices configured to identify and block unauthorised users or scammers. In order to enable seniors to make wise decisions, automated alerts and notifications can advise them in real time about possible scams or fraudulent activity. By incorporating the surveillance system into community forums, neighbours are encouraged to actively monitor and respond to alarms, which promotes a team approach to security. To counteract social isolation, social integration features like virtual community gatherings and communication channels can be enabled via the centralised system. The surveillance system can spot patterns and trends by using data analytics, which provides predictive insights into possible threats and the ability to take preventative action. Seniors should have easy access to the system's user interface, which will

enable them to use and comprehend its features, fostering their independence and sense of control over their security. Seniors can take advantage of an intelligent and integrated solution that manages their immediate security needs and improves their general well-being by utilising a centralised Internet of things (IoT)-based surveillance camera system. This system offers enhanced monitoring and communication features.

A. Limitations in adaption of technological solutions:

Even though technology has a lot of promise to reduce the risks that elderly people who live alone encounter, there are a number of restrictions and difficulties that need to be understood. Dependability and upkeep of IoT devices and surveillance systems are important factors to take into account. As system malfunctions or other technical issues could jeopardise these technologies' ability to deliver dependable security, their efficacy depends on regular maintenance and upgrades. One more notable restriction is related to cybersecurity issues. The security and privacy of senior citizens may be threatened by IoT devices, which are susceptible to hacking and illegal access. The significance of strong cybersecurity measures is highlighted by the possibility that malicious actors may take control of surveillance cameras or obtain sensitive data by employing system weaknesses. We also see difficulties related to usability and accessibility. Technology solutions user interfaces might not always be tailored to the unique requirements and skills of the elderly, which could lead to misunderstanding or make it harder for them to use and maintain the equipment on their own. Affordability and cost pose more difficulties. Senior's access to these useful technologies may be hampered by the high upfront and continuing costs associated with the acquisition, setup, and upkeep of advanced surveillance and Internet of Things systems, especially for those with limited financial resources. The technology landscape is further complicated by integration problems. Different IoT devices and surveillance systems may not work together properly, which could cause problems with data sharing and communication that reduce the integrated system's overall efficacy. Over-reliance on technology and false warnings are frequent problems. IoT gadgets like motion sensors have the potential to set off erroneous warnings, which could worry elderly people and the people who support them. Maintaining a balance between technological and human supervision is essential to prevent missing important details or giving insufficient responses to crises. Criminals may be able to take advantage of security camera systems' blind spots and limited coverage. To provide complete security and reduce risks, careful thought must be given to the placement and coverage of cameras. Constant surveillance by surveillance cameras gives rise to privacy concerns. It is crucial to strike a balance between the necessity for security and the right to personal privacy, keeping in mind that some elderly people could find it uncomfortable to live under continual observation.Another difficulty is technological literacy. The inability of seniors to fully connect with and profit from IoT-based solutions may be due to their difficulty understanding and adjusting to new technologies. Ensuring fair access to these breakthroughs requires closing the gap in technical knowledge. In conclusion, potential negatives include connectivity problems and power outages. IoT devices' reliance on energy and internet connectivity creates vulnerabilities in the event of outages. Maintaining continued functionality, especially in emergency situations, requires setting up backup power sources and resolving connectivity problems.

5. IMPLEMENTATION

The deployment of a centralised facial recognition system is identified as a critical remedy to address a number of issues that elderly individuals living alone encounter. Through visitor verification and access management, the system improves security by incorporating facial recognition technology into doorbell cameras. This lowers the possibility of unsolicited solicitations or possible threats by guaranteeing that only acknowledged and authorised individuals are allowed admission. Furthermore, by recognising and eliminating prospective con artists or unauthorised individuals trying to get access, the facial recognition technology makes a substantial contribution to the prevention of scams and fraud. Seniors are further protected from financial exploitation by this strong layer of defence. When designing facial detection systems, privacy must be taken very seriously to guarantee that the facial data collected is safely stored and utilised only for verification. Seniors who have privacy settings enabled have more control over when and how facial recognition technology is used in their homes, giving them a sense of control over their personal data. The system's success is largely due to its user-friendly interface, which makes it simple for seniors to control and alter facial detection settings. Seniors may more easily operate

the system with the help of straightforward controls and instructions, which encourages independence and gives them more control over security features

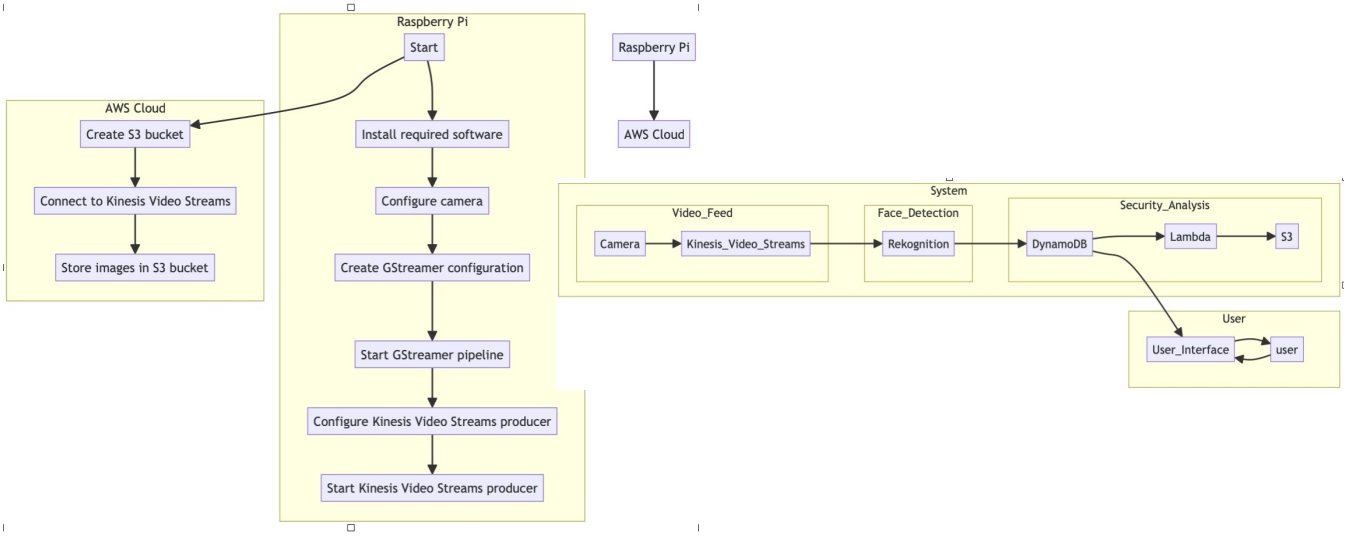

Figure 1: System Flow Diagram.

5.1. Leveraging Amazon Web Services (AWS) for a centralized face detection system provides several advantages, ranging from scalability and reliability to advanced machine learning capabilities. Here are some key benefits:

Main advantages:

5.1.1. Capability to scale:

The capacity to extend resources on-demand provided by AWS enables the face detection system to effectively manage a range of workloads. This scalability gives the system flexibility as user demand varies by ensuring that it can adapt to changes in usage patterns without requiring operator intervention.

5.1.2. Managed AI/ML Services:

Machine learning models that have already been trained for face identification, recognition, and analysis are available through AWS's managed services, such as Amazon Rekognition. This eliminates the requirement for deep machine learning knowledge and enables developers to include advanced face identification features.

5.1.3. Global Reach and Low Latency:

The face detection technology may be deployed closer to end users thanks to AWS's extensive worldwide network of data centres. Because of the decreased latency, users can expect prompt responses and a consistent experience regardless of their location.

5.1.4. Security and Compliance:

Amazon abides by strict compliance certifications and security standards. An encrypted environment, authentication and access control, and compliance with several regulatory frameworks are all provided by using AWS services for face detection.

5.1.5. Cost-Effective Infrastructure:

Pay-as-you-go pricing for AWS makes it possible to use resources economically. By just paying for the resources used and scaling resources in accordance with demand, organisations can minimise costs by eliminating up-front infrastructure investments.

5.1.6. Integration with Other AWS Services:

Amazon services are easily integrated with one another. The face detection system may readily integrate with other AWS services, including Amazon DynamoDB for database requirements, AWS Lambda for serverless computing, and Amazon S3 for storage. The deployment and development of networked systems are made easier with this connection.

5.1.7. Real-time Processing:

Real-time face detection is made possible by AWS services such as Amazon Rekognition. Applications that need quick responses, like security systems or user authentication procedures, must take this into consideration.

5.1.8. Automatic Scaling and Load Balancing:

AWS Auto Scaling and Elastic Load Balancing features enable automatic scaling of resources to handle changes in demand. This ensures that the face detection system remains responsive and available even during peak usage periods.

5.1.9. Managed Database Services:
Elastic Load Balancing and AWS Auto Scaling allow resources to automatically scale to meet demand variations. This makes sure that even during times of high usage, the face detection technology is available and responsive.
5.1.10. Continuous Innovation:
Face detection application development is encouraged by AWS's frequent release of new capabilities and services. Remaining on AWS gives you access to cutting-edge innovations and developments in machine learning and artificial intelligence. Using AWS for a centralised face detection system offers businesses a dependable, scalable, and affordable infrastructure in addition to cutting-edge machine learning features that improve the application's overall functionality and performance.

5.2. As a cost-effective and adaptable option for a range of applications, using a Raspberry Pi with a camera module as a door camera has several benefits. The principal benefits are as follows:
5.2.1. Affordability:
When considering commercial door camera systems, Raspberry Pi boards and camera modules are more affordable. For people or small-scale projects with little funds, this makes it an affordable option.
5.2.2. Customization and Flexibility:
Users can adjust and modify the door camera system to suit their own requirements thanks to the open-source and flexible Raspberry Pi platform. To accommodate many use cases, developers have the ability to enhance functionality, incorporate extra sensors, or adjust software.
5.2.3. Ease of Use and Setup:
The setup and configuration process of Raspberry Pi is renowned for being user-friendly. An easy-to-follow setup process for both enthusiasts and novices in the realm of electronics allows anyone to set up a door camera using a Raspberry Pi and camera module.
5.2.4. Compact Size:
For covert door camera installations, the Raspberry Pi's diminutive form factor makes it simple to integrate into small places. Additionally, portability is improved by the small size, which also opens up new deployment options.
5.2.5. Low Power Consumption:
Due to their low power consumption, Raspberry Pi boards are made to be energy-efficient. Since they don't greatly affect electricity bills, they can be used continuously.
5.2.6. Community Support and Resources:
Many online resources, tutorials, and forums are available for troubleshooting and help from the huge and active Raspberry Pi community. Through this community support, users can investigate fresh ideas for their door camera projects and get answers to frequently asked questions.
5.2.7. Integration with IoT and Home Automation:
Home automation systems and Internet of Things (IoT) configurations can readily incorporate Raspberry Pi.This enables users to remotely view and manage the door camera from a variety of devices by connecting it to a network.
5.2.8. Camera Module Quality:
Given their size and cost, the authorised Raspberry Pi camera modules have respectable image quality. They are available in many varieties, such as the regular camera module and the premium camera module, giving you choice depending on your photographic needs.
5.2.9. Open-Source Software Support:
A variety of open-source software packages for security, video streaming, and image processing are supported by Raspberry Pi. In order to meet their specific door camera requirements, users might create custom applications or utilise pre-existing software solutions.
5.2.10. Modularity and Expandability:
The usage of extra peripherals and sensors is supported by Raspberry Pi. By integrating motion sensors, infrared modules, or other parts to improve security features, users can increase the door camera's usefulness. A Raspberry Pi door camera is an affordable, adaptable, and educational option that is ideal for do-it-yourselfers, small projects, and anyone searching for a versatile and easily accessible door camera configuration, even though it might not have the sophisticated capabilities found in commercial systems.

5.3. Setting Up GStreamer Plugin:

5.3.1. Prepare Raspberry Pi:
Make sure Raspberry Pi is running the proper operating system, such as Raspberry Pi OS or Raspbian.
Connect the internet to the Raspberry Pi.
5.3.2. Install Gstreamer:

Open a terminal on Raspberry Pi.
Execute the following commands:
Update package list: $ sudo apt-get update.
Install Gstreamer: $ sudo apt-get install gstreamer-1.0.
Install development libraries: $ sudo apt-get install libgstreamer1.0-dev.
5.3.3. Write Gstreamer Plugin:
Develop the Gstreamer plugin, typically in C or Python.
Install development tools: $ sudo apt-get install build-essential
5.3.4. Build and Install Plugin:
If written in C, compile the plugin using the necessary build tools.
Install the plugin on Raspberry Pi, usually in /usr/lib/gstreamer-1.0/.
5.3.5. Test Plugin:
Create GStreamer pipelines using the custom plugin.
Verify functionality with multimedia sources.
5.3.6. Debug and Optimize:
Debug the plugin and optimize performance as needed.

5.4. Setting Up KVSSink:
5.4.1. Install AWS SDK and Configure Credentials:
Install AWS SDK for C++: $ sudo apt-get install libaws-cpp-sdk-kinesis
Configure AWS credentials using relevant commands.
5.4.2. Build KVS Element:
Obtain source code for KVSSink from AWS GitHub.
Build KVSSink element using CMake and compile the source code.
5.4.3. Install KVS Element:
Copy compiled KVSSink library to the appropriate GStreamer directory.
5.4.4. Create GStreamer Pipelines:
Develop GStreamer pipelines utilizing KVSSink, e.g., for streaming video to AWS Kinesis Video Streams.

5.5. Data Collection and Training:
5.5.1. Turn on Amazon Configuration:
Assign the required permissions for Kinesis Video Streams to an IAM user.
5.6. Launch the Example Programme:
Run the example application and set the environment variables:
$ export GST_PLUGIN_PATH=Directory Where You Cloned the SDK/amazon-kinesis-video-streams-producer-sdk-cpp/build
$ export AWS_DEFAULT_REGION=AWS Region i.e. us-east-1
$ export AWS_ACCESS_KEY_ID=Access Key ID
$ export AWS_SECRET_ACCESS_KEY=Secret Access Key
$ ./kvs_gstreamer_sample Your Stream Name

5.8. Using the AWS CLI, create a Collection_id with Amazon Rekognition:
5.8.1. Installing the Amazon CLI:
Make sure that your local computer has the AWS CLI installed.
5.8.2 Configuring the Amazon CLI:
Use the aws configure command to set up the required credentials in the AWS CLI.
5.8.3. Make an ID for the collection:
Launch a command prompt or terminal.
5.8.4 Using the Amazon CLI Command:
Utilising Amazon Rekognition, issue the subsequent AWS CLI command to generate a collection_id:
$ aws rekognition create-collection --collection-id YourCollectionId
5.8.5. Documentation and Policies:
Document the collection_id, and ensure that access policies are configured appropriately for security.

5.9. Developing a Lambda Function to Start the photos in a bucket of predefined dataset images
5.9.1 Configuring an AWS Lambda
Go to the Lambda service in the AWS Console to create a new Lambda function.
5.9.2. Set up a Lambda Function:
Go with "Author from scratch."
Give your Lambda function a name.

Select a suitable runtime (Python, for example).
Configure the fundamental execution role and rights, which include S3, KVS, and CloudWatchLog permissions. In Fig. 2, this phase is displayed.

5.9.3. Configure Trigger:

Shown in Figure 3: illustrates how to add an S3 trigger for the specified dataset images bucket. Name the bucket and, if necessary, set trigger conditions.

5.9.4. Code Deployment:

Write or upload the Lambda function code to process images when triggered.

5.9.5. Code Deployment:

Write or upload the Lambda function code to process images when triggered.
Ensure the Lambda function is designed to handle events from the S3 bucket.

```
import boto3
import json
from datetime import datetime
import pytz
import uuid
s3 = boto3.client('s3')
rekognition = boto3.client('rekognition', region_name='us-east-1')
sns = boto3.client('sns', region_name='us-east-1')
dynamodb = boto3.resource('dynamodb')
table = dynamodb.Table('match')
def detect_emotion(bucket, key):
response = rekognition.detect_faces( Image={'S3Object': {'Bucket': bucket, 'Name': key}}, Attributes=['ALL'] )
if 'FaceDetails' in response and response['FaceDetails']:
# Extract the emotions from the first detected face
emotions = response['FaceDetails'][0]['Emotions']
# Find the emotion with the highest confidence
highest_emotion = max(emotions, key=lambda x: x['Confidence'])
return highest_emotion['Type']
return None
def compare_faces_with_emotion(source_bucket, source_key, target_bucket, sns_topic_name):
try:
target_objects = s3.list_objects_v2(Bucket=target_bucket)['Contents']
except KeyError:
print(f'Target bucket {target_bucket} is empty. No faces to compare.')
return
# Detect emotion for the source face outside the loop since it is common for all comparisons
source_emotion = detect_emotion(source_bucket, source_key)
print(f"Source Emotion: {source_emotion}")
for target_object in target_objects:
target_key = target_object['Key']
# Compare faces
try:
response = rekognition.compare_faces(
SourceImage={ 'S3Object': {'Bucket': source_bucket, 'Name': source_key} },
TargetImage={ 'S3Object': {'Bucket': target_bucket, 'Name': target_key}},
SimilarityThreshold=80  # Adjust the threshold as needed )
print(f'Compare Faces Response: {response}")
except Exception as compare_faces_exception:
print(f'Error in CompareFaces operation for {target_key}: {str(compare_faces_exception)}")
continue
# Check if there are matching faces
if response.get('FaceMatches'):
# Process known face logic here
target_key_without_extension = target_key.split('.')[0]
ist_timezone = pytz.timezone('Asia/Kolkata')  # IST timezone
timestamp_ist = datetime.now(ist_timezone).isoformat()
unique_id = str(uuid.uuid4())
# Send SNS alert
```

sns_message = f'ALERT: {target_key_without_extension} is roaming in your premises with emotion {source_emotion}\n\nThanks\nAutomated WatchDog System'
sns.publish(TopicArn=f'arn:aws:sns:us-east-1:220694685394:{sns_topic_name}', Message=sns_message)
# Dynamically detect emotion for known faces
target_emotion = detect_emotion(target_bucket, target_key)
print(f"Target Emotion: {target_emotion}")
dynamodb_item = { 'name': target_key_without_extension, 'emotion': target_emotion, 'unique_id': unique_id, 'timestamp': timestamp_ist, 'source_key': source_key, # Add other attributes as needed }

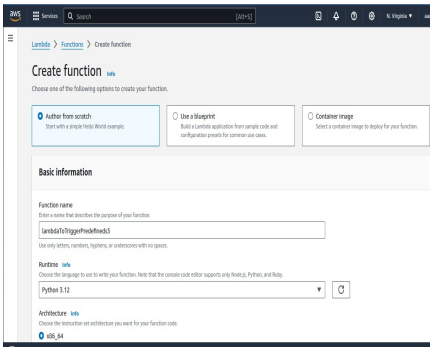

Fig 2: Illustrates how to create a lambda function in AWS.

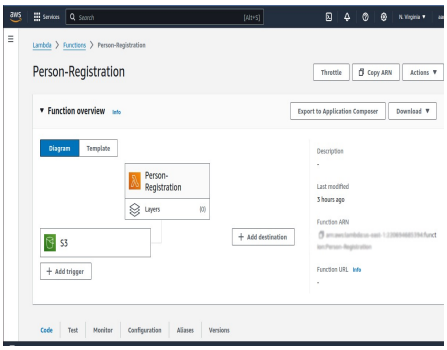

Fig 3: Lambda Function to trigger predefined Data Bucket (S3)

table.put_item(Item=dynamodb_item)
print(f"Entry added to DynamoDB for known face: {dynamodb_item}")
# Process unknown faces outside the loop
for unmatched_face in response.get('UnmatchedFaces', []):
confidence_threshold = 99 # Adjust the threshold as needed
if unmatched_face.get('Confidence', 0) >= confidence_threshold:
# Process unknown face logic here
target_key_without_extension = target_key.split('.')[0]
ist_timezone = pytz.timezone('Asia/Kolkata') # IST timezone
timestamp_ist = datetime.now(ist_timezone).isoformat()
unique_id = str(uuid.uuid4())
# Send SNS alert for unknown person
sns_message_unknown = f'ALERT: Unknown person is roaming in your premises with emotion {source_emotion}\n\nThanks\nAutomated WatchDog System'
sns.publish(TopicArn=f'arn:aws:sns:us-east-1:220694685394:{sns_topic_name}', Message=sns_message_unknown)
dynamodb_item_unknown = { 'name': 'Unknown', 'emotion': source_emotion, # Use source emotion for unknown faces 'unique_id': unique_id, 'timestamp': timestamp_ist, 'source_key': source_key, # Add other attributes as needed }
# Store unknown person in DynamoDB
table.put_item(Item=dynamodb_item_unknown)
def lambda_handler(event, context):
print(event)
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
try: # Compare faces with emotion in all images in the 'target_bucket' S3 bucket
target_bucket = 'predefinedcollection'
sns_topic_name = 'cam-alert' # Replace with your actual SNS topic name
compare_faces_with_emotion(bucket, key, target_bucket, sns_topic_name)
return { 'statusCode': 200, 'body': json.dumps('Lambda function executed successfully!') }
except Exception as e:
error_message = f"Error processing image {key} for bucket {bucket}: {str(e)}"
print(error_message)
raise Exception(error_message) from e.

5.9.6. Testing:

Make sure the Lambda function is tested to make sure it reacts correctly when users upload photographs to the specified dataset images bucket.

5.9.7. Monitoring and Logging:

Fig. 4 illustrates how to set up CloudWatch Logs and other monitoring tools to track Lambda function execution and find any problem.

Experimental Output

7. CONCLUSION:

In conclusion, the project is a major step towards improving the security and safety of elderly people living on their own. With its sophisticated features like facial feature identification and emotional expression analysis (shown as a label in Fig. 11), the integration of AWS Rekognition provides valuable insights into seniors' mental health. Furthermore, illustrates how the system's proficiency at identifying possible intruders based on visual features, such as recognising people or calculating the emotion, strengthens security measures. This effort is unique in that it has a collective effect, as the system's capacity to identify suspicious individuals goes beyond individual homes and promotes a more secure public area. Beyond the characteristics listed above, an Angular application (shown in figure 6) has been painstakingly designed to create frictionless interaction with essential AWS Cloud services, such as S3 bucket (shown in figure 7), S3 File upload helps to collect predefined collection data (shown in figure 6), Rekognition which helps to compare predefined S3 bucket, and 'cam1feed' bucket and registered the record in DynamoDB (shown in figure 10 and figure 6). The "View Image" buttons make it simple for users to navigate between images thanks to this clever integration's user-friendly layout. This improves the system's ability to quickly identify possible intruders and expedites the picture analysis process, strengthening overall security measures. In addition, the project has added Amazon Simple Notification Service (SNS) (shown in figure 9) to strengthen security protocols. With this effective addition, the system will be able to promptly alert relevant individuals, including family members or authorities, via email or SMS in the case of a security breach or suspicious conduct. Combining modern technologies not only protects individual households but also enhances community security as a whole. This study highlights the necessity for ongoing improvements and community involvement to ensure sustained efficacy, while also demonstrating the positive role technology can play in tackling real-world difficulties encountered by vulnerable people.

REFERENCES:

[1] [Shaik Anwar, D. Kishore, "IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone" IJERT, Vol.5 Issue 12, December 2016.

[2] Ashirwad Rakhonde*1, Kiran Kapse*2, Harshada Bamnote*3, Sandhya Dharpure*4, Shweta Ghagare*5, Prof. Sarvesh Warjurkar*6, "IOT based door access control system using Face Recognition" IRJMETS, Vol.03 Issue 6, June 2021.

[3] S.Meival, Nidhi Sindhwani, Rohit Anand, Digvijay Pandey, Abeer Ali Alnuaim, Alaa S. Altheneyan, Mohamed Yaseen Jabarulla, "Mask Detection and Social Distance Identification using Internet of Things and Faster R-CNN Algorithm" Hindawn Computational Intelligence and Neuroscience, Volume 15 ,2022.

[4] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[5] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[6] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[7] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical &Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[8] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[9] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[10] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[11] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[12] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique

[13] with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[14] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[15] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[16] M. I. Uddin, S. A. A. Shah, and M. A. Al-Khasawneh, "A novel deep convolutional neural network model to monitor people following guidelines to avoid COVID-19", Journal of Sensors, vol. 2020, Article ID 8856801, 15 pages, 2020.

[17] Asep Najmurokhman, KusnandarKusnandar, Arief Budiman Krama, Esmeralda Contessa Djamal, and Robi Rahim, "Development of a secured room access system based on face recognition using Raspberry Pi and Android-based smartphone", MATEC Web of Conferences 197, PP[1-3], 2018.

[18] Leyla G.Muradkhanli, Eshgin A.Mammadov, "Real-Time Face Detection on a Raspberry Pi", PP [38-45], 2022.

[19] Fadi Boutros, Marco Huber, Patrick Siebke, Tim Riber, Naser Damer, "S-Face Privacy-Friendly and accurate face recognition using synthetic data", PP[1-8], 2022.
[20] Chorowski, J. Wang, and J. M. Zurada, Neurocomputing, Review and performance comparison of SVM- and ELM-based classifiers, vol. 128, pp. 507–516, 2014.
[21] A survey of face recognition techniques, Journal of Information Processing Systems, R. Jafri and H. R. Arabnia, vol. 5, no. 2, pp. 41–68, 2009.
[22] Y. Qian, M. Gong, and L. Cheng, Springer, Stocs: an efficient self-tuning multiclass classification approach, in Canadian Conference on Artificial Intelligence, 2015.
[23] Y. D. Zhang, S. Chen, S. H. Wang, J. F. Yang, and P. Phillips, Magnetic resonance brain image classification based on weighted-type fractional Fourier transform and nonparallel support vector machine, International Journal of Imaging Systems and Technology, vol. 25, no. 4, pp. 317–327, 2015.