

Smart Mirror Integrated Secure Room Automation with Facial Recognition

Kadambala Pavan¹, Chintada RoopKumar², Kamalsuryateja Dhumalrao³, Rupa Chiramdasu⁴

¹Dept. of CSE

VR Siddhartha Engineering College (A)
pavankadambala@gmail.com

²Dept. of CSE

VR Siddhartha Engineering College(A)
Vijayawada, India
kamalsurya.dhumalrao@gmail.com

³Dept. of CSE

VR Siddhartha Engineering College (A)
roopkumarchintada@gmail.com

⁴Dept. of CSE

VR Siddhartha Engineering College(A)
Vijayawada, India
rupamtech@gmail.com

Abstract— According to the EIA, around 34% of the electricity used in the world is wasted. Having smart and automated rooms can help us reduce our energy consumption and comfort our lives. Unfortunately, there are not many models of these systems available. One of the main advantages of having smart and automated rooms is that they can be easily operated by anyone. However, one of the main issues with this system is that it requires a lot of power to operate. To address this issue, the paper's model uses a web camera and a smart lock to provide various services. The paper's model can be used to provide various services, such as security and automation, to various organizations. Its end product can be mainly focused on reducing electricity consumption and security concerns at schools and universities.

Keywords— Facial recognition, smart lock, Intelligent power management, IoT, LBPH algorithm, automation, security, Smart Mirror.

I. INTRODUCTION

The innovation that has been happening in the world of technology has been able to change the lives of a billion people. One of the most notable innovations that has been brought about by this process is the emergence of the smart room robotization. This allows people to monitor what's happening in their house or room with their mobile devices. The pandemic has also changed the way we work and connect. Due to the pandemic, people are still staying in their homes and increasing their desire for security and comfort. This has led to the rise of the home machine and gadget craze. This is why buyers are now demanding more sophisticated and energy-efficient gadgets and home appliances. Aside from being beneficial, these items also tend to decrease the cost of ownership.

The concept of smart rooms[1] has been regarded as a way to enhance our lives and provide us with more convenient and well-being. However, there are still many models that are not secure. In addition to this, people can still easily operate these devices without having to provide their identity. One of the

biggest issues that people face when it comes to electricity is the rising cost of power.

The proposed system uses web camera to recognize the user's face and then uses a smart lock to unlock the door. It also has intelligent power management to cut down on power consumption. If the user's face is valid, then the door will automatically open. If the user is not authorized to enter the room, then the system will deny access. This model can offer various services such as security and automation. It can also cut down on electricity consumption by 18.70%. The system uses the data collected by the camera to identify the user's essence. It compares the approved attributes of the person with the images captured by the camera.

The proposed framework is composed of the raspberry pi programming language used for creating the code. It includes a module board that can be used for various equipment parts. This can be used for monitoring and detecting burglary and social violations. The paper also manages the connected work and the proposed system, results, further work and references

II. LITERATURE SURVEY

The expectations of client have been satisfied with the guide of machine-centered calculation which involves SVC gains from past utilization history. Cloud computing is a vital component of the model which is handled by various cells and UI on-net. It is also smart home framework by implementing Google's validation machine. The proposed device will help in setting up the related instrument by sensing the temperature and moisture of the area. It will not function properly if the cloud doesn't have the necessary settings saved in its database. Besides this, the device will also play a programmed role in setting off the various gadgets in the model. In addition to these security measures, the proposed model should also be equipped with a robust intrusion prevention system. This can be done through the use of virtual private networks.

In this paper, Zhaonan Mu and colleagues proposed a framework for the development of smart entryway locks using Bluetooth Technology[3]. The main idea is to create a connectable cell terminal that can be used to control the device. After the device is connected to the cell terminal, the Bluetooth report module sends demand for confirmation of the door. The main idea of this framework is to create a versatile terminal that can be used to control the device. With the help of the confirmation code, the basic regulator can send a loose sign to the device. In addition, this lock gadget can be distinguished from other similar devices by its limited discipline shut estimation. The ability to create a non-shopper emotional key through an entry door lock is also beneficial. It can be used to let loose reasonable doors by allowing the user to leave the device far away. The effectiveness of this strategy is continuously decreasing as the number of testing times for the device increases.

A couple of years back, Satyendra K. Vishwakarma and his colleagues proposed a smart home automation system that utilizes the Internet of Things (IoT).[4] It can be controlled through the Google help and web-based platform. The system can be done with a regulator unit that's connected to a 24-hour Wi-Fi network. For the wellbeing conscious client, the team suggested that they should give their Google partner an option to check if they want to activate their home automation system on their own. After a triumph, the client can then utilize an IFTTT revelation order to activate their system. The team at Adafruit helped them by developing the necessary framework that will allow their Google associate and the Node.MX to communicate with each other. The home hardware will then be transferred to the essential regulator unit. The team then designed a switch that will act as an ON/OFF switch for the regulator unit. The main advantage of this model is that it allows the Google associate to communicate with the regulator without affecting its speed. However, this model is not ideal for everyone due to the lack

of connectivity and the noise generated by the commands being sent and received by the Google assistant.

A couple of years ago, K. Lova Raju and his colleagues proposed a machine that would automate and provide assurance in one's home using the Internet of Things and the Node MCU.[5] The project has gained widespread recognition due to its ability to connect various sensors and devices using Android. The proposed machine utilizes a small regulator known as the Node MCU to connect various equipment and client parts. It can also be used to perform various functions, such as sending and receiving messages. Another component of the project is a mini web server, which can be used to perform various functions related to insurance and remote gadgets. The proposed machine can be used to dispatch notices to its customers through a web-based application known as BLYNK. It can also be used to perform various functions, such as sending and receiving messages. Clients can also use various sensors, such as temperature sensors, to improve the efficiency of their home machines. Each of these devices can be connected to a GPS beacon and a successful local control system. The proposed machine is only able to collect updated data from its sensor, which is known as the DHT-11. It only gets this data once per 2 seconds.

A proposed IoT-based security system that would allow users to lock their doors using a mobile gadget. The system would be able to send a sign to a remote control via a link between the mobile gadget and an embedded computer. After the verification of the link is made, the system would continue to operate. The use of Bluetooth on mobile devices would allow users to easily access their desired section with just a tap of their phone's button. If the user's secret word or username is correct, the LOCK and UNLOCK buttons would be activated. The application would then send an expense to the device's embedded computer through the Bluetooth module. This will then allow the lock to be closed and the other way around once the buyer has tapped the button. This method works well when the user has the secret word, but it can also make issues if they forget it. One of the main drawbacks of this method is that it can allow unauthorized access to the device. This can also result in users forgetting their password.

Table-1: Literature Survey Summary Table

Authors	Hardware Interface	Algorithm For security	Mobile Interface
Tushar Chaurasia[2]	Arduino	AES	Not have

Zhaonan Mu[3]	STC15F2 K32S2 single chip, bluetooth module	Stream cipher	Not have
S.K.Vishakarma [4]	Arduino, Node MCU	No security	Google Assistant
K.L Raju[5]	Arduino, Node MCU	No Algorithm	Blink app
N.Y.L [16]	ESP32	AI Thinker	Not have
Proposed System	Raspberry Pi	LBPH (Facial Recognition)	Rasp controller

III.PLANNED PROCEDURE

The main objective of this scheme is to automate the room using the use of the Raspberry Pi[7] and the PIR sensor. It also uses a webcam to allow the authorized users to enter the room. This method can be performed by capturing and storing the photos of the people who are approved to enter the room. In addition, the model can also be used to collect and store other data related to the users in the data set.

When an individual enters the room, the webcam captures the image of them and checks if they are authorized to enter. It then uses the data collected by the camera to determine if they are valid or not. If the camera perceives the face as being that of an approved user, the door will be opened. On the other hand, if the camera perceives the face as not being that of a legitimate user, the door will remain locked. The door is then locked using a hardware lock. After the person has entered the room, the PIR sensor informs the device, which is the Raspberry Pi, about the presence of the person. The device then responds to the notification sent by the PIR sensor. This system can be automated by connecting various devices such as the fan and the light. If there are no people in the room, the PIR sensor will not detect the presence of the people. The device will then automatically switch off if there is no human presence for at least 10 minutes. The code for this system is generated through the openCV python program and the raspberry pi. The Rasp controller app is a free Android application that can be used with the Raspberry Pi. It allows users to interact with the device.

The design of this system is based on the classical principle of the room as it eliminates the need for electricity consumption. It also provides a security through the use of the Pi-cam, which can only be used by authorized individuals. This system can be widely implemented in areas where security is most important. In addition to reducing the

electricity consumption, this system can also help in preventing people from committing crimes.

The concept of the room is designed to reduce the electricity consumption by automating it and providing security through the use of the Pi-cam. This system can be widely implemented in areas where security is most important. In addition to this, this system can also help in preventing people from committing crimes.

In the below Fig 1, The camera and 5V-2A power source of the Pi are connected to ground. The other components of the project are connected to LED and 12v solenoid. The relay modules are then connected to the light.

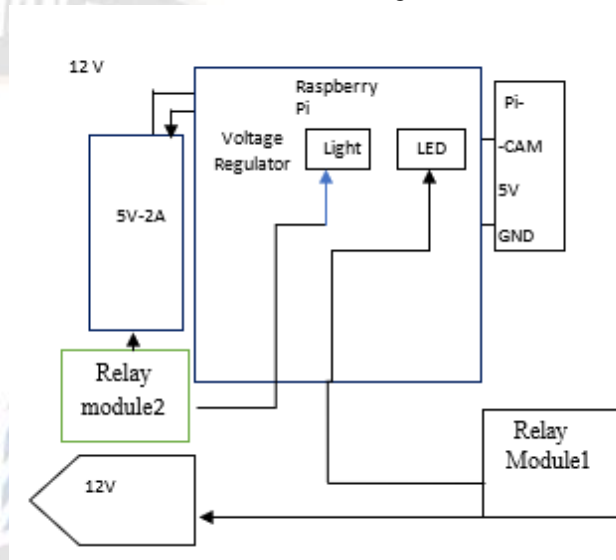


Fig 1. Proposed Architecture

The proposed work consists of three modules: room automation, facial detection, and authentication.

MODULE1: ROOM AUTOMATION

When the client is confirmed, a smart door lock will open and will display the message "access denied." This is an initial test, and the lights will remain on until the client has left or there is no movement. The system utilizes a PIR Sensor, which will recognize a human movement and will continue to illuminate the room until it senses that the person has left. If there's no human interaction, the PIR sensor will not recognize any individual. However, as the person or persons enter the room, the sensor will recognize the change in infrared radiation in the room.

The final product of the PIR Sensor is usually high. Since the data out of the sensor is connected to the Digital Pin eight of the Pi, it will eventually end up being HIGH. When this happens, the Pi will then initiate the hand-off by using the switch pin LOW to turn the light on. As long as there's advancement in the technology, the remaining parts of the sensor will remain on until the end of the day.

When the person enters the room, the IR Radiation will turn into normal. The data out of the sensor will end up being low, making the exchange between the two components of the Pi very important. This will cause the Pi to trade off the exchange pin, making the room light switch OFF.

Algorithm:

Step-1:

The PIR sensor will then detect the IR waves from the person inside the room

```
pre=detect (person presence) //1 if detected else 0
```

Step-2:

```
It will then send the data to the Pi.  
if 1 goto step-3 else step-4
```

Step-3: When the person enters the room, the devices will switch on automatically.

```
on(devices)
```

Step-4:

The same information will be sent to the Pi after the PIR sensor has failed to detect the presence of the person.

```
off(devices)
```

MODULE 2: FACIAL DETECTION AND RECOGNITION

The computation of the neighborhood binary patterns histogram depends on the paired administrator. This is regarded as one of the most impressive face acknowledgment techniques due to its computational ease and discriminative power.[20]

Step-1: Parameters

The LBPH utilizes 4 boundaries Radius, Neighbors, Grid X, Grid Y. [8,9]

Step-2: Training the Algorithm:

The preparation of the face acknowledgment computation is usually done in a dataset. This is done by taking into account the various facial pictures that people need to perceive. Each picture has its own unique ID, which gives the computation a unique idea about the individual. After extracting the information from the data, the program can then produce a final product that's similar to the one depicted in the picture

Step-3: Applying the LBPH action:

The essential computational strength of the LBPH estimation is that it makes a moderate picture that shows the essential photograph in an explicit and unprecedented manner. This method utilizes a sliding window to estimate the facial attributes of the picture.

Step-4: Extracting the Histograms:

Through the use of the previous image, we can now isolate it into various networks using the Grid X and Grid Y restrictions. Each histogram will have 256 conditions that are related to the pixel power and its Classification. The level

below is used to associate the various histograms with a fresh new one. When we accept 8x8 grids, the last histogram will have 16384 conditions. The attributes of the special photo will be included in the last histogram.

Step-5: Performing the face affirmation:

The computation is now at its final stage, and it is ready to be used for the given dataset. Each of the histograms will be applied to adapt the image from the schooling dataset. For instance, if a records image is taken, the estimation will make a new histogram that tends to the picture. There are various techniques that can be used to consider the various aspects of the histograms, such as the chi-square, the Euclidean distance, and large truly worth.

Algorithm:

Step-1: Install Libraries

```
Install OpenCV and NumPy.
```

```
pip install OpenCV-python
```

```
pip install OpenCV-contrib-python
```

```
pip install numpy
```

Step-2: Read the input from the webcam for facial detection.

```
img=input(img.png)
```

Step 3: Detect Faces

```
Detection of faces using haarcascade classifier
```

```
For i in faces:
```

```
detect(i)
```

Step 4: Data Gathering

Creating the dataset by collecting all required photos of disallowed persons with a different expression.

```
for each person:
```

```
for i in n: // n indicates the no. of images taken
```

```
for each person
```

```
person(i)=image(person)
```

Step 5: The goal of this process is to create an intermediate photo that captures the authentic character of the individual.

```
intermediate_image=create_image(radius, neighbors)
```

Step-6: After the output image has been processed, separate the histograms from the rest. With the help of network y and matrix x, the resulting images can be easily labeled.

```
for i in each region:
```

```
histograms= extract (histogram of region)
```

Step 7: After comparing the input image histogram with the stored images, return the closest possible histogram. This method indicates that the image is authorized to be viewed.

```
if match:
```

```
return welcome else:
```

```
return access denied
```

Module 3: AUTHENTICATION SYSTEM

Step-1: When an individual enters an area, grab the photograph.

```
Image=capture (person)
```

Step-2: If the image is authorized to be viewed, compare it with the put away pictures of the other individuals.

Analyze (picture, put away pictures)

Step-3 The picture should coordinate with the approved pictures and the entrance should open once it has been opened also set dynamic transfer to valid

in the event that match ==True and dynamic relay==false:
unlock(door)

Step-4: However, if the picture doesn't match the put away pictures, the door will be locked.

in the event that match ==False and dynamic relay==True:

lock(door)

In the event that (match face == valid and dynamic transfer == bogus):

Open (entryway)

Step5: If the guest's face doesn't coordinate with the Authenticate pictures, the door will be locked.

On the off chance that (match face == bogus and dynamic transfer == valid):

Lock (entryway)

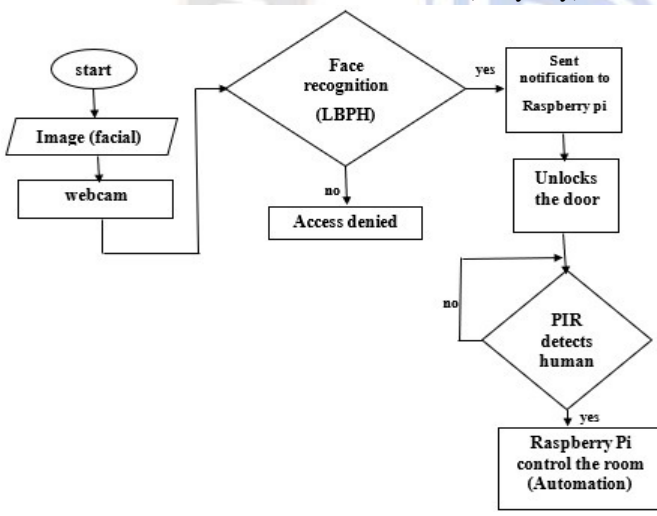


Fig 2: Process flow diagram

III. RESULTS

Fig 3 show that there is no human presence in the room. This means that the lights are off. Fig 4 and Fig 5 show that the lights are on when the humans are present. This helps in reducing power consumption. In the Fig 6, the authorized persons are shown entering the room through the door.

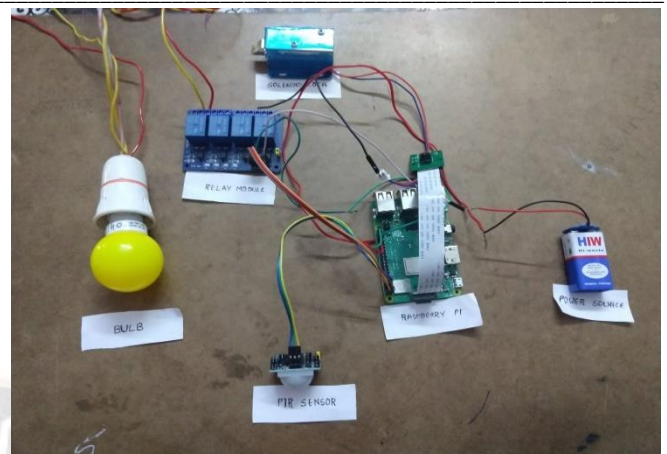


Fig 3: No detection of human presence

When the presence of the people is not detected, the lights are off.

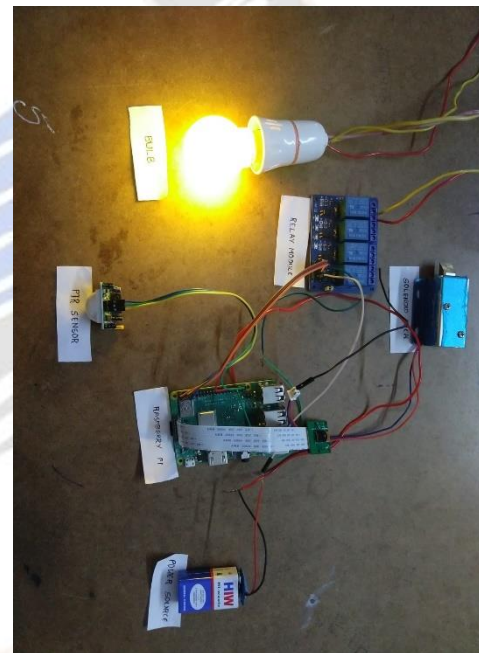


Fig 4: Detection of human presence

On the other hand, if the presence of the humans is detected, the lights are back on.

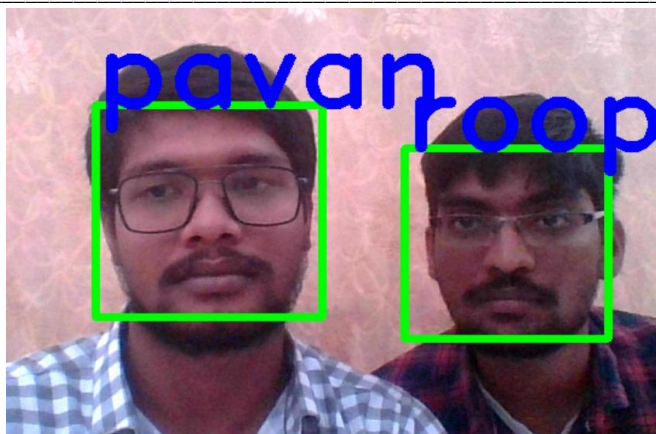


Fig 5: Facial Recognition (Authorized person)

When the face is found, a rectangle box is formed around it, which then it uses to confirm the presence of the person. If it's found that the person's name is on the top of face.



Fig 6: Facial Recognition (Unauthorized person)

If the face is not verified, then on the top of the rectangular box, it shows as unknown.

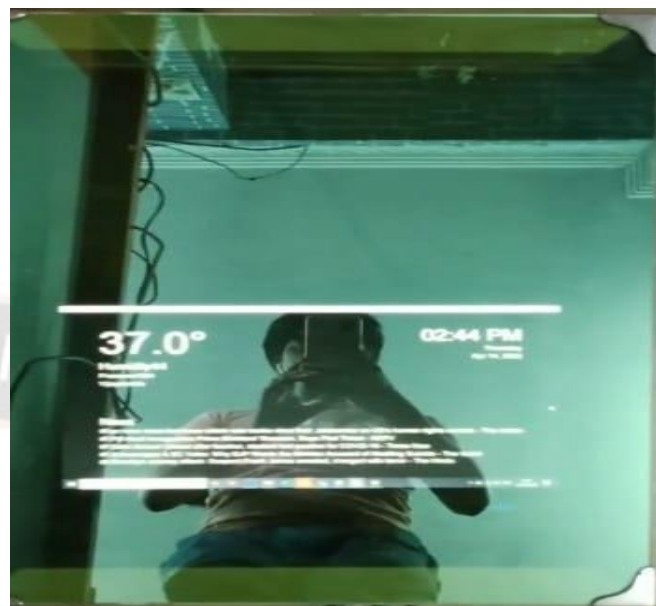


Fig 7. Smart Mirror

Smart mirror interface displaying weather and realtime information

Table 2. Correlation with the Existing Systems

Methods Features	Tushar Chaurasia[2]	Zhaonan Mu[3]	S.K. Visha karma [4]	K.L Raju[5]	N. Y.L [16]	Proposed System
Wi-Fi/ Bluetooth	Yes/No	Yes/Yes	Yes/No	Yes/No	Yes/Yes	Yes/Yes
Camera Support	Yes	No	Yes	No	No	Yes
Power Consumption	95%	85%	92%	85%	87%	80%
Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Web Application	Yes	No	No	No	No	Yes
Automatic lock	No	No	Yes	No	No	Yes

V. CONCLUSION AND FUTURE WORK

The proposed framework is mainly focused on providing security and mechanization to people at a reasonable cost. It includes various components such as the Pi board, a hand-off module, and a solenoid lock. The system can also be

programmed to open and close the door with a simple facial recognition. This helps in reducing energy consumption and provides an aid to people with limited mobility. The proposed framework is simple to implement and can be accessed by anyone. It can also monitor the surroundings and prevent unauthorized access. It can also turn on and off the lights and

fans using a PIR sensor. The proposed framework can also be used to keep track of people. An overload power can be made by implementing a hand-off module. This can help in protecting the private data of an individual. The proposed framework also helps in limiting human mediation. Due to its structure, it is more likely to be stretched out for further confirmation. This model can be easily updated to meet the needs of different users. For instance, it can help in opening a door after a person loses their key. It can also help in remembering their keys. The proposed framework can be used in various areas such as banks, workplaces, and servers. In the future, we can also add a Smart mirror to the room automation modules.

REFERENCES

- [1] A. S. Hasban *et al.*, "Face recognition for Student Attendance using Raspberry Pi," *2019 IEEE Asia-Pacific Conference on Applied Electromagnetics (APACE)*, 2019, pp. 1-5, doi: 10.1109/APACE47377.2019.9020758.
- [2] T. Chaurasia and P. K. Jain, "Enhanced Smart Home Automation System based on Internet of Things," *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2019, pp. 709-713, doi: 10.1109/I-SMAC47947.2019.9032685.
- [3] Z. Mu, W. Li, C. Lou and M. Liu, "Investigation and Application of Smart Door Locks based on Bluetooth Control Technology," *2020 Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, 2020, pp.68-72, doi: 10.1109/IPEC49694.2020.9115189.
- [4] S. K. Vishwakarma, P. Upadhyaya, B. Kumari and A. K. Mishra, "Smart Energy Efficient Home Automation System Using IoT," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019, pp. 1-4, doi: 10.1109/IoT-SIU.2019.8777607.
- [5] K. L. Raju, V. Chandrani, S. S. Begum and M. P. Devi, "Home Automation and Security System with Node MCU using Internet of Things," *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, 2019, pp. 1-5, doi: 10.1109/ViTECoN.2019.8899540.
- [6] G. S. Pravallika, L. Kundana, K. S. Thanvi, G. Sirisha and C. Rupa, "Proficient Smart Soil based IoT System for Crop Prediction," *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2020, pp. 752-757
- [7] A. S. Hasban *et al.*, "Face recognition for Student Attendance using Raspberry Pi," *2019 IEEE Asia-Pacific Conference on Applied Electromagnetics (APACE)*, 2019, pp. 1-5, doi: 10.1109/APACE47377.2019.9020758.
- [8] [8]Rupa C., Srivastava G., Gadekallu T.R., Maddikunta P.K.R., Bhattacharya S. (2021) A Blockchain Based Cloud Integrated IoT Architecture Using a Hybrid Design. In: Gao H., Wang X., Iqbal M., Yin Y., Yin J., Gu N. (eds) Collaborative Computing: Networking, Applications and Worksharing. CollaborateCom 2020. Address Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 350. Springer, Cham. https://doi.org/10.1007/978-3-030-67540-0_36
- [9] Harshitha M., Rupa C., Priya B.B., Sowmya K., Sandeep N. (2021) An Intelligent and Smart IoT-Based Food Contamination Monitoring System. In: Chaki N., Pejas J., Devarakonda N., Rao Kovvur R.M. (eds) Proceedings of International Conference on Computational Intelligence and Data Engineering. Lecture Notes on Data Engineering and Communications Technologies, vol 56. Springer, Singapore. https://doi.org/10.1007/978-981-15-8767-2_22
- [10] S. Irfan, C. Rupa, K. Vinay, M. K. Veni and R. Rachana, "Smart Virtual Circuit based Secure Vehicle Operating System," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2020, pp. 386-390, doi: 10.1109/ICIMIA48430.2020.9074940.
- [11] Ch. Rupa, "An Integrated digital authentication mechanism for intrusion detection system", *Big data analytics for smart and conected cities*, IGI, 2019
- [12] N. Y. L. Venkata, C. Rupa, B. Dharmika, T. G. Nithin and N. Vineela, "Intelligent Secure Smart Locking System using Face Biometrics," *2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, 2021, pp. 268-273, doi: 10.1109/RTEICT52294.2021.9573869.
- [13] Chen, Joy Iong Zong, and Lu-Tsou Yeh. "Graphene based Web Framework for Energy Efficient IoT Applications." *Journal of Information Technology* 3, no. 01 (2021): 18-28.
- [14] Bashar, Abul. "AGRICULTURAL MACHINE AUTOMATION USING IOT THROUGH ANDROID." *Journal of Electrical Engineering and Automation* 1, no. 2 (2019): 83-92.
- [15] Raj, Jennifer S. "Optimized Mobile Edge Computing Framework for IoT based Medical Sensor Network Nodes." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 3, no. 01 (2021): 33-42.
- [16] Madhura, S. "IoT Based Monitoring and Control System using Sensors." *Journal of IoT in Social, Mobile, Analytics, and Cloud* 3, no. 2 (2021): 111-120.
- [17] Jacob, I. Jeena, and P. Ebby Darney. "Design of Deep Learning Algorithm for IoT Application by Image based Recognition." *Journal of ISMAC* 3, no. 03 (2021): 276-290
- [18] P. A. Teja, A. A. F. Joe and V. Kalist, "Home Security System using Raspberry PI with IOT," *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, pp. 450-453, doi: 10.1109/ICACITE51222.2021.9404551.
- [19] Z. Lu and X. Liu, "IoT Application Development Based on Java and Raspberry Pi," *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2021, pp. 0600-0606, doi: 10.1109/IEMCON53756.2021.9623242.
- [20] G. Singh and A. K. Goel, "Face Detection and Recognition System using Digital Image Processing," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2020, pp. 348-352, doi: 10.1109/ICIMIA48430.2020.9074838.

- [21] Sathesh, A. (2020). Computer Vision on IOT Based Patient Preference Management System. *Journal of Trends in Computer Science and Smart Technology*, 2(2), 68-77. doi:10.36548/jtcsst.2020.2.001
- [22] Ganesan, T., Sathigari Anuradha, Attada Harika, Neelisetty Nikitha, and Sunanda Nalajala. "Analyzing Social Media Data for Better Understanding Students' Learning Experiences." In *Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2020*, pp. 523-533. Springer Singapore, 2021.
- [23] M. Shanthini, G. Vidya and R. Arun, "IoT Enhanced Smart Door Locking System," *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2020, pp. 92-96, doi: 10.1109/ICSSIT48917.2020.9214288.

