International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Mobile Application Based Home Automation with Security Advancements utilizing IoT and Computer Vision

Aman Bagaria, Himanshu Khemani

Abstract*: Security has consistently been a numbers game. Time to discovery and time to reaction have been measurements security groups have looked to diminish since the get-go (or if nothing else the start of PCs…). However, what does it take to really decrease that number? Mechanizing security undertakings like the ones described in this paper is no longer a "nice to have." It's a "need to have." Automating house features incorporating security advancements can alleviate many of today's biggest security issues and offer us group operational efficiencies that can profit us now and over the long haul. Our work aims in automatic handling of security operations-related tasks. It takes care of executing these tasks, such as scanning for vulnerabilities, with minimal required human intervention. We propose a complete smart security system with home automation techniques complementing security advancements. The system is controlled by a mobile application which works in dual mode. In the first mode, the owner can control the home upon his/her discretion and can access the home automation features such as unlocking their house using the same application without being physically present. While the other mode requires the person (trying to enter the house) to be physically present and provide his fingerprint biometrics and face detection to access the house. The photo of the person is sent to the owner for his confirmation and the owner can then decide whether to identify and allow the guest as an acquaintance or to report to the police as a suspect. Both modes allow the use of home automation techniques using the dial pad of the owner's phone.

Keywords: Automation, biometrics, dial pad, face detection, measurements, mobile application, smart security system.

I. INTRODUCTION

At the point when we look at our family, and our home, we realize we need them to be protected, constantly out of harm and mischief's way. The developing wrongdoing rates crosswise over urban communities mirror the severe reality. Research led by the Rutgers University School of Criminal Justice demonstrated that alarm systems help discourage burglars. Another exploration directed by the University of North Carolina demonstrated that robbers would be reluctant to enter a home fitted with an alert framework.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Aman Bagaria*, Student at the School of Electrical Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu- 632014, India.
Himanshu Khemani, Student at the School of Electrical Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu- 632014, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Truth be told, 31% of burglars are likely to withdraw from a home if they come across a security framework. Hence security is the topmost priority nowadays.

On top of this automating house features has become another need of the hour. Home automation refers to handling and controlling house features by utilizing small scale controller or computer technologies.

Automation is well known nowadays since it provides ease, simplicity, security and efficiency. In this, several discrete systems are deployed which detects the status of connected appliances and updates to the central webserver. A user can also remotely control and access the status of the appliances i.e. switches it on/off. This paper will describe the approach of controlling house features completing security techniques.

This smart home automation and smart security systems is proposed to achieve the desired comfort with simplicity and utmost security. Wireless home automation and home security are the dual aspects are this project. The complete system consists of dual modes. The former mode allows the owner of the house to control the house automation features remotely upon his/her discretion. While the later mode requires the presence of the guest entering the house to serve his biometrics and allow the installed camera to do the face detection. The picture of the person is then sent to the owner through the webserver so that the owner can allow the person into the house or not. Several arrangements of the unexpected guest of the owner can be done such as opening the door, switching on various connected appliances inside the house and welcome the guest. In case of any suspect the owner can report the same to the nearest police station in demand of help. The same can be done when the owner himself enters the house and by virtue of the complete smart system, he can make arrangements from his doorstep such that as soon as he enters his house he can make himself at full comfort without manually having to switch on the electrical appliances or his favorite T.V. channel for an example. Thus, using the same set of sensory arrangements, the dual problems of home security and home automation can be solved on a complimentary basis. The main advantage of this IoT system is that everything is done and controlled by the mobile application and even if WiFi is not available we can access the arrangements using the dial pad of the phone which in turn is regulated by the mobile network services. In other existing strategies the same is not possible along these lines,

by overcoming all the drawbacks we have implemented this project Mobile application-based home automation with security advancements utilizing IoT and computer vision.
This project provides more comfort combined with simplicity brought at the fingertips and proves out to be very convenient and useful for old, aged, disabled the people who are advised not to do much physical work because of health conditions. Also, it makes the entry/exit record of the house entry digital and easier to access and view.

II. LITERATURE SURVEY

To comprehend the requirement for a cost-effective and scalable system, and before jumping in to give our own solution, we must initially comprehend the current research and work done in the field. [1] One of the papers proposed to operate remote-controlled Home Automation Systems using Domotics (interaction of different technologies and services applied to home automation systems) in order to make the system more comfortable, secure and reliable. Their primary objective was to use digital standards to provide outstanding emergency backup control in case if any of the technology used goes down at any moment. Few standard technologies which they used are XML, IP, HTML and WML. They were also successful in testing these technologies and their functionalities using UPnP or X-10 compatible devices. [12] Another paper focused more on migrating the initial control mechanisms of devices with simple functionalities to advance devices. One of their features was to incorporate a secure means to isolate other RF devices being added to the home network without being authorized. They achieved this using an easy handshaking protocol through the user interface. Users were required to obtain user login and password to access the site secured through the SSL algorithm protected server. [7] They focused on automating very few appliances in the flat as to serve a certain need arising at any moment. They incorporated a timer which switches ON/OFF two lamps cyclically for a defined period. Periodic illumination of lamps by a timer could stimulate the situation of a resident staying in the flat. [9] Their work was to make an IoT system which focuses on sending alert to the house owner through the internet in case of any trespass and to raise an alarm if required. They used TI0CC3200 to control all the electrical appliances in the home.
[5] Another paper objective was to use a web-based interface over the web, while the home appliances would be connected to the website remotely. They used a smoke detector to sense the fire and raise an alarm in case of any crucial circumstances. They employed LAN (Local Space Network) to connect various hardware modules, sensors and the server. An expensive option, complexity reduces, but accuracy compromised. [13] Their main motive was to incorporate SMS technique to all the major home automation features. GSM was also used in order to attain SMS features and detect the intrusion and start an alert about the breach or intrusion. Consequently, no certifiable conditions or difficulties were even tried, and subsequently it is may not dependable or beneficial to secure and protect the home. [2] They presented a cell phone-based low-cost home automation system. Applications are connected to the Arduino board and communicate wirelessly with the cell phone. Their device can be operated on Symbian operating system. Users need to obtain a password for pairing the Arduino BT and the cell phone in order to access the home appliances. This system has a very limited use case and can work on only Symbian OS cell phones because of the program written in python. Also, the applications on which the system is tested are very rare and will fail in case of long-range applications. This system employs the use of Bluetooth and thus wastes a lot of energy sensors such as gas sensor, humidity sensor, PIR and temperature sensor to monitor the environmental conditions and direct the signals to the Arduino UNO and then relay the appliances. The applications are only limited to environmental parameters monitoring and provide remote monitoring to the user with no security aspect involved. Thus, the system compromises accuracy to reduce cost.
[3] Another paper presented their work using a DTMG (dual-tone multiple frequencies) based system which consists of a DTMF decoder and an ATMEGA8 microcontroller. The control signal was sent via the remote mobile phone as a DTMF tone and is received by the domestic mobile phone which is further decoded by the DTMF decoder MT8870 IC. This output logic signal is fed as an input to the ATmega8 controller to control the output appliances. This system is very effective and cost-cutting but can fail in case of the logic signal being tampered on the way from the mobile phone to the decoder. [6] In this paper the home appliances are controlled using input voice speech. The speech recognition is done by SVM (Support vector machine) while the home automation system is implemented using GPRS (General Packet Radio Service). After converting the input speech to the text output, the keywords are extracted to match the command to an action and then is executed. This method requires many training datasets to achieve real-time and good accuracy to seamlessly convert demands into actions. Also, in case of any new command, the system may not recognize the desired action and fail. [8] A speech activated portal is constructed to assist disabled users with a speech recognition module that allows the interaction of only registered users followed by a speech recognition system. The connection is compatible to be deployed in a public network by using existing web services, and telecommunication voice services.
[4] This paper employs a PIR sensor to detect the motion of the person and sends the information to the ATmega 328p microcontroller which is connected to an ESP8266 WiFi module and an alarm system. The webserver is another ESP8266 WiFi module which allows the user to activate/deactivate any services using the internet with the help of the microcontroller.

III. METHODOLOGY

A. Algorithm Flow

As our system involves security features, we are using techniques such as computer vision to accomplish our purpose. A camera module is installed at the entrance of a house prototype whose task is to detect the face of the guest trying to enter the house.

The camera module is connected to the Raspberry Pi (referred to RPi from here) which exchanges information from the local system. When a person on the entrance is found, the camera captures the image and sends the same to the local system for image processing classification. The system has the provision to allow a specific set of people to enter the house without obtaining the consent form the owner. This can be done by classifying the guest as a resident of the house and storing it in the local server. Further, the image is sent to the owner of the house, through an Email along with an SMS (to avoid the risk of availability of the internet) to decide whether to allow him or not. Furthermore, if the guest is a resident of the house then his fingerprint is stored in the local database. A fingerprint sensor is also installed to obtain the biometrics of the person. This is an added security feature in the security system. The advantage of this method is that a part of time, power and money is saved by remotely performing processing over the local system along with an added advantage of comfort.

Finally, if the person is not identified as the expected guest or the permanent resident of the house, the owner can inform the nearest police station about the person determined as a suspect. In case the person is the expected guest the owner can open the entrance door from his mobile application nor from his phone's dial pad. Over the top of all features, the owner can handle the house appliances from his phone application according to his need and comfort. Fig. 1 shows the detailed flowchart of the same.

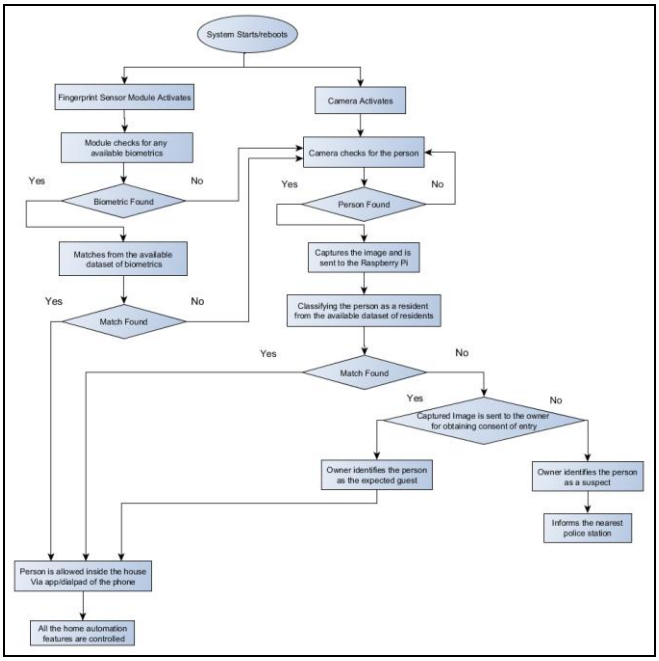

Fig. 1: System Flow

B. System Design

1. System Body Architecture

The system prototype is prepared on a commonly available cardboard box. At the front main entrance gate, a camera is installed which is responsible to capture the images of the person willing to enter the house. The main entrance is also fitted with a fingerprint sensor module to obtain the biometrics (fingerprint) of the person. The camera module and the fingerprint sensor module are connected to the sensor through the raspberry Pi. The raspberry Pi is also connected to a four-channel relay which in turn is connected to an Arduino UNO. Also, two small bulbs are connected to the relay demonstrating the house lights, one as the main entrance light and other as the backyard lighting. Everything is connected to the mobile application. Fig. 2,3 and 4 depicts the same.

2. System Circuitry Architecture

The central processing unit of the proposed system is the Raspberry Pi 3B, with an Arduino UNO aiding its functionalities.

2.1 The RPi is connected to the camera module and an Adafruit fingerprint sensor module GT511C3.

2.2 The relay module is connected to both the RPi and Arduino for controlling the AC sources.

2.3 The relay module is also connected with two light bulbs to prototype the house appliances.

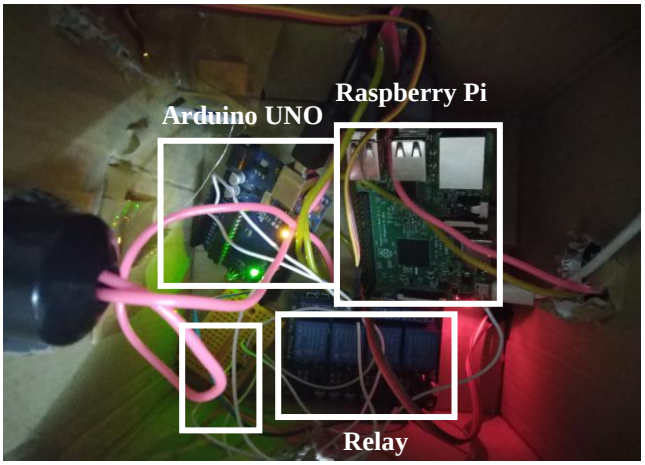

Fig. 2: Inside View of the System along with connected peripherals

Fig. 3: Front View

Fig. 4: Rear View

3. Network Architecture

Our smart system comprises of many appliances, but we have shown only two in order to demonstrate the features. Fig. 5 shows the complete network architecture of the system. All of them are connected to the central server via the RPi and hence the relay module. All the appliances are to be connected to a common WiFi hotspot. An association is thus settled among these. On the off chance that online arrangement administrations are to be utilized, for example, TensorFlow, at that point the server should be associated with the web.

This is clarified in detail, in the prospective segments.

4. Layer Wise Architecture

The subsequent subsections of this section have been organized as follows: the data accretion layer i.e. the physical layer of our framework the data link layer, the network layer, the transport layer and finally the application layer.

4.1 *The Data accretion layer (Physical layer)*: This is the basic layer of our proposed framework. It is responsible for the physical data accretion from the house environment. We currently employ it using a camera module and a fingerprint sensor module, the camera module clicks the picture of the intruder/acquaintance and converts it into a bitstream and

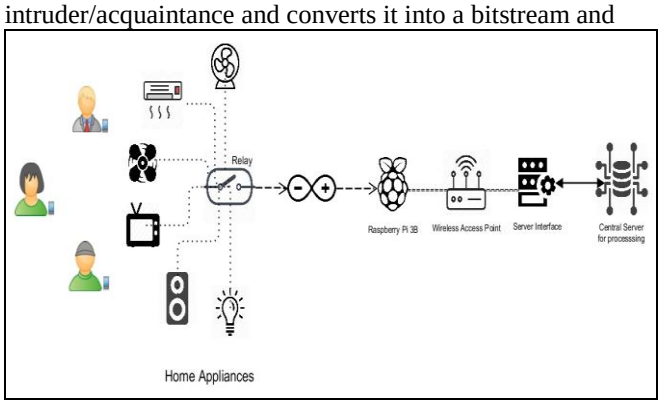

Fig. 5: Network Architecture of the Complete System

communicates it to the database through the transmission layer. The main objective is to record the information which can be gathered from the environment, at any given time in the real world.

4.2 *The data link layer*: This layer makes sure the confirm delivery of the data to the top layers for further processing. Any type of error occurrence is being controlled through this layer.

4.3 *The network layer*: This layer transmission of data from one host to the other located in different networks. It takes care of the packet routing and transfer of messages to the owner whenever an intrusion is detected through the camera. The technology used here to send the messages is using Twilio API in python framework. Also, there is a provision of a voice call received to the owner which is achieved through the use of VoIP(Voice Over IP) and the owner can control the actions of the door using the dial pad of the phone in addition to the control using a mobile phone application.

4.4 *The Transport layer*: This layer provides services to the application layer and takes services from the network layer. The data obtained in the transport layer is referred to as Segments. It is liable for the End to End conveyance of the complete message. It adds in a control mechanism to our framework such that it provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

4.5 *The application layer*: This is a user-oriented layer which has its own intelligent interfaces to communicate with the user. It is a general way of how the data which is obtained can be presented to the user without any coherency. The major technologies involved in this layer are the way the data is pushed onto the server, or how data can be retrieved. The data must be continuously monitored but to convey some special messages; an alert system can be deployed. The mobile application provides an easy to handle user interface from where he can control all the functionalities of his smart home automation and security system.

C. **Modular Analysis**

1. The Image Capturing Module

Once a person is detected near the camera fixed at the main entrance of the house, it captures the image, and send to the classification module for checking the permanent feed set of residents and if found the actuation module is sent high otherwise the flag is set high and the picture is sent to the server using the communication module. Further, the same captured image is sent to the owner of the house as an email and a message to take further actions.

2. The Classification Module

The RPi performs the classification techniques on the image that it obtains. The algorithms to be utilized can be as very good quality as conceivable since the central server utilizes top of the line hardware equipment's. Hence the algorithms utilized ought to be performed by remembering precision.

For demonstration purposes, we have made use of 'dlib' library which helps to concentrate all the facial landmarks. We are also using image classifier which works on the top of the TensorFlow model. It classifies the captured image among the fed resident images by doing feature matching between the input captured image and the training images.

Other algorithms for the same can also be used such as Haarcascade image classifier.

3. The Fingerprint Sensing Module

The fingerprint module is attached to the Arduino UNO and has a set of input fingerprints to check from the input fingerprint. If the input fingerprint matches from the existing set, the information is sent to the actuation module to open the door and allow the guest inside the house.

4. The Home Automation Module

This module helps in controlling all the electrical appliances remotely through the mobile phone. In the presented prototype we are controlling light and fans through the mobile application. On a large scale, many appliances can be connected to the system such as TV, Air conditioner, speakers and so on. Even if the WiFi services are not available the services can be operated through the mobile network through the dial pad of the phone. This helps us to operate our home appliances according to our will and has a lot of advantages such as reducing the energy wastage, helping the aged and handicapped people to control the appliances according to their comfort.

5. The Security System Module

When the camera detects the presence of the person, the image is obtained and if forwarded to the owner through an Email on his phone (Mail Id is predefined in the programmed and can be changed), the owner verifies the identity of the person and he can take a call on the same. If he wants to allow the person inside the house as the guest he can unlock the door and can welcome the guest by switching ON the desired appliances otherwise if he wants to inform the police station about the intruder he can intimate the police with a single click.

The nearest police station (details predefined in the program and can be changed) receives the image of the intruder along with the location of the house. The police can then take the necessary actions.

6. The Communication Module

The system may contain several houses being connected to a central server. TCP/IP communication protocol is being employed here for communication between the clients which are each house and the central server. It is a client-server communication-based model, with the house RPi as the client, the principal server being the server. Since the entire RPi code is scripted in python, we have used python's socket programming API for the communication. The image is captured by the camera is being sent to the client RPi. If the sent image is classified as one of the fed images the actuation module is informed otherwise the image is sent to the server to be further sent to the owner. Once the image is received to the owner the response is being sent to the client through python socket.

In the case of several houses being connected to the central server for enhanced security in a society/locality, the individual house RPi clients should be connected to the same WiFi network. In case of any individual client gets cut-off from the network, the remaining connected clients will function as always beyond any problem. Also, if in case the server gets disconnected then communication will be getting interrupted and the system fails.

7. The Actuation Module

Depending on the response received from the RPi about the classification result or from the fingerprint sensor module and if the match is found the system actuates and unlocks the door otherwise the door is kept locked to ensure proper safety all around. This is done as follows: the RPi sends the information to the Arduino about the actuation, and if it is a positive signal the actuation flag is set high otherwise the flag is set low. The same signal information is being sent to the relay board to take the necessary action and hence the actuation works.

8. The Mobile Application Module

In the presented prototype the information is being stored on the tiny DB database and the mobile application is being made on MIT App Inventor. The information is sent to the database through the Raspberry Pi and is relayed to the mobile application back and forth. The server performs the exchange of data between the mobile app and the client RPI i.e. the input information such as unlocking the door, enabling/disabling the home appliances, is given by the owner in the application and is sent to the server and then to the RPi which process the instruction when the information needs to be relayed to the owner the same is sent from the RPi to the server and is then received by the mobile application. This way the to and fro communication is enabled.

IV. RESULTS AND DISCUSSION

The preparation of mobile application with all the discussed features, image capturing, biometric capturing, home automation features, data communication (transmission and reception) and actuation were all performed successfully.

As discussed, the data control and display are done over the mobile application. Fig. 6 shows the home page of the app which asks the user to select the desired mode of operation. The mode of the security can be selected on the application as shown above as Mode 1 or Mode 2. On selecting mode 1 the next screen demands the user to open or close the gate. Fig. 7 shows the same.

The message bar above the gate open/close button displays the status of the gate. On selecting the option for the gate open/close the instruction signal is sent to the Tiny Web DB and then to the Raspberry Pi and then the servo motor compromising the actuation module controls the gate of the house.

The owner can also check the captured image from the camera on his/her phone. Fig. 8 shows the image.

Fig. 6: Home Page of the App

Fig. 7: Screen 2

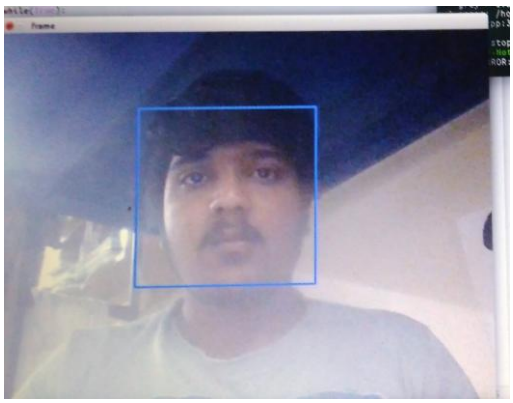

Fig. 8: Image being captured on camera (viewed on pc)

On getting the image and confirming the identity of the person the owner can take necessary actions as in allow the person to enter the house and enjoy the comfort facilities at the ease. Also, the person receives a phone call on his mobile number through the Twilio API to inform the presence of the person at the main gate. The owner can allow the person inside the house from the mobile app (needs internet facility) or through the dial pad of the phone (without internet facility). Fig. 9 shows the owner getting the phone call from Twilio API.

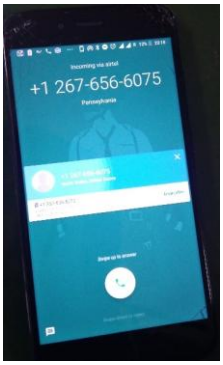

Fig. 9: Owner getting call through Twilio API

Moreover, the owner has the option to control the home appliances from the app. Fig. 10 shows the option to control/switch ON/OFF two appliances. In this project Switch 1 is used to control the main entrance lighting and Switch 2 is used to control the backyard lighting of the house. For switching OFF the lights the owner can long press the respective switch to turn OFF the respective light. Fig. 11 and 12 demonstrates the lights being controlled through the switches.

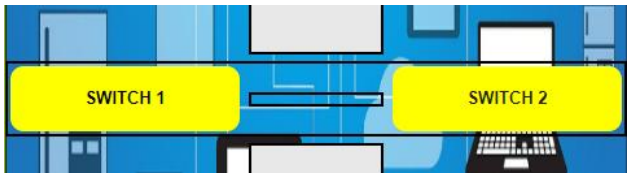

Fig. 10: App showing options to control/switch appliances

Fig. 11: Main Entrance light switched ON

Fig. 12: Backyard light switched OFF

Table- I: Proposed Prototype key features with respect to already existing works.

Sr. No.	*Paper Ref. No.*	*De-Merit of the discussed technique*	*Problems solved by our work*
1.	[9]	Doesn't works fully if internet connectivity is absent	Yes
2.	[5]	Accuracy compromised to reduce complexity	Yes
3.	[13]	Area of implementation and use cases are very limited with no real-world problems being tested.	Yes
4.	[2]	High Energy Wastage and within range use cases	Yes
5.	[10]	Accuracy trade-off to reduce cost	Yes
6.	[3]	Lack of real-time capabilities and transmitted information signal can be tampered.	Yes
7.	[6]	Low Algorithmic Accuracy in case of new commands	Yes

V. ADVANTAGES

1. The home automation and security system work without an active internet connection and thus can be useful on the internet cut off situations.
2. Fingerprint and face detection along with verification helps to provide high security for the house and to keep the records of the people entering and leaving the house.
3. The records maintenance, in this case, turns simple, easy and digital and can be accessed and used anywhere according to requirements and in case of any thefts reporting's.
4. This low-cost system with minimum possible requirements takes care of both home automation and house security at the same time.
5. The system is helpful to the handicapped, old and aged people and the people who are advised not to do much physical work because of health conditions.
6. The automation of the home in no way lowers the security features of the system instead proves to be timesaving, secure and reliable.

VI. CONCLUSION AND FUTURE SCOPE

The proposed system has been successfully implemented and tested. This paper presents a low cost, smart and cost-effective system that employs IoT and image processing to optimize the security process of the house. Moreover, the use of exact needed hardware's allows the user to change and reprogram the features according to the need and desires of the residents. In addition, the appropriation and enhancement of the best highlights from advances, into a solitary incorporated framework, makes it exceptionally productive. The deployment of OpenCV in a real-time scenario for image detection and classification makes the whole module very dynamic, efficient. Also, to optimize the memory, time and speed, the images are being sent to the central server from the raspberry pi to ignore the necessity of huge data storage. This central server can also handle a lot of tasks (pull and push requests and storage tasks) at once without any lag and delay. Thus, this method comes out to be easy to expand and very fast and easy to receive. The system can also be integrated with furthermore sensors and actuators to realize and analyze more data from the house in real-time. We can also direct ore functionalities to the application in order to make the functionalities broader and more convenient for the owner and guests in the house. The image processing algorithm can be improvised, and some more security protocols can also be integrated to keep the house data more safe and secure. This smart system can also be used for the smart cities under the division of security and surveillance and to keep the city safe and clean.

REFERENCES

1. Armando Roy Delgado, Rich Picking and Vic Grout, "Remote-Controlled Home Automation Systems with Different Network Technologies" published in International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 4 Issue IX, September 2016.
2. R.Piyare, M.Tazil , "Bluetooth Based Home Automation System Using Cell Phone" presented in 2011 IEEE 15th International Symposium on Consumer Electronics.
3. Md. Tanvir Ahammed, Partha Pratim Banik, "Home Appliances Control Using Mobile Phone" presented in Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering 17-19 December 2015, Dhaka, Bangladesh.
4. Safa.H, Sakthi Priyanka.N, Vikkashini Gokul Priya.S, Vishnupriya.S, Boobalan.T, "IOT based Theft Premption and Security System" published in International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 3, March 2016.
5. Pavithra.D, Ranjith Balakrishnan, "IoT based Monitoring and Control System for Home Automation" published in Proceedings of 2015 Global Conference on Communication Technologies (GCCT 2015).
6. M.Tharaniya soundhari, Ms.S.Brilly Sangeetha, "Intelligent Interface Based Speech Recognition for Home Automation using Android Application", presented in IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15.
7. K. Balasubramanian and A.Cellatoglu, "Improvements in Home Automation Strategies for Designing Apparatus for Efficient Smart Home", published in IEEE Transactions on Consumer Electronics, Volume: 54 , Issue: 4 , November 2008.
8. I. Potamitis, K. Georgila, N. Fakotakis, G. Kokkinakis, "An Integrated System for Smart-Home Control Of Appliances Based On Remote Speech Interaction", presented in 8th European Conference on Speech Communication and Technology, Eurospeech 2003 - Interspeech 2003, Geneva, Switzerland, September 1-4, 2003.
9. Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana, "IoT Based Smart Security and Home Automation System", presented in International Conference on Computing, Communication and Automation (ICCCA2016).
10. R.P. Pandav, S.P.Dahatonde, G.W.Bonde, H.S.Bhadke, A.I.Rokade," Security System And Home Appliances Control Using IoT", presented in 2016 International Conference on Computing, Communication and Automation (ICCCA).
11. Humaid AlShu'eili, Gourab Sen Gupta, Subhas Mukhopadhyay, "Voice Recognition Based Wireless Home Automation System", presented in 2011 4th International Conference on Mechatronics (ICOM), 17-19 May 2011, Kuala Lumpur, Malaysia.
12. Ali Ziya Alkar Member, IEEE and Umit Buhur, "An Internet Based Wireless Home Automation System for Multifunctional Devices", published in IEEE Transactions on Consumer Electronics Volume: 51 , Issue: 4 , Nov. 2005.
13. Malik Sikandar Hayat Khiyal, Aihab Khan, and Erum Shehzadi, "SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security", Issues in Informing Science and Information Technology Volume 6, 2009.
14. Mohsen Hallaj Asghar, Nasibeh Mohammadzadeh, Atul Negi, "Principle Application and Vision in Internet of Things (IoT)", presented in International Conference on Computing, Communication and Automation (ICCCA2015).
15. K. Balasubramanian and A. Cellatoglu, "Analysis of Remote Control Techniques Employed in Home Automation and Security Systems", published in IEEE Transactions on Consumer Electronics, Volume: 55, Issue: 3 , August 2009.
16. H. ElKamchouchi, Ahmed ElShafee, "Design and Prototype Implementation of SMS Based Home Automation System", presented in 2012 IEEE International Conference on Electronics Design, Systems and Applications (ICEDSA).
17. Rozita Teymourzadeh, CEng, Member IEEE/IET, Salah Addin Ahmed, Kok Wai Chan, and Mok Vee Hoong, "Smart GSM Based Home Automation System", in 2013 IEEE Conference on Systems, Process & Control (ICSPC2013), 13 - 15 December 2013, Kuala Lumpur, Malaysia 978-1-4799-2209-3/13/$31.00 ©2013 IEEE 306.
18. Chathura Withanage, Rahul Ashok, Chau Yuen, Kevin Otto, "A Comparison of the Popular Home Automation Technologies", published in: 2014 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA).

AUTHORS PROFILE

Aman Bagaria, was born on August 4, 1998, in Bhagalpur, Bihar. He is currently a 4th-year student pursuing his Bachelor of Technology in Electronics and Instrumentation Engineering from Vellore Institute of Technology, Vellore, India. He will be joining as an Associate Developer in IBM India, Bangalore from January 2020 Onwards. He has a bone-deep passion for core electronics, Embedded Systems and Internet of Things. He served as the Student Convener of graVITas'19 – An International Techno-management Knowledge Carnival hosted by VIT-Vellore annually in October. He is currently serving as the Club Head of the VIT-Vellore's Electronics Club and the President of Ayuda NGO. Amidst getting involved in so many activities, his sheer passion for technology strives him to develop a plethora of projects and maintain a brilliant academic record in his stream. He has received merit scholarships and Chancellor's Special Achiever's award due to his extraordinary performance in academics and real-life projects. He has worked on Embedded Systems and IoT with cloud services as a Project Intern in Johnson Controls India and Danfoss Industries Pvt. Ltd. respectively. He has also been the Student Convener of SELECT Make-A-Thon 2019 – A national level hackathon hosted annually by School of Electrical Engineering, VIT-Vellore. His areas of interest include Event management, Electronics, Automation, Consulting and Business analytics.

Himanshu Khemani, was born on May 30, 1998, in Agra, Uttar Pradesh. He is currently a 4th-year student pursuing his Bachelor of Technology in Electronics and Instrumentation Engineering from Vellore Institute of Technology, Vellore, India. He will be joining as Graduate Engineer Trainee in Varroc Engineering Ltd, from June 2020 Onwards. He has served as the Project Head for VIT-Vellore's, Robotics Club. He has worked as a Project Intern in Danfoss Industries Pvt Ltd and as a Summer Intern in NTPC Ltd. He has done numerous projects in the field of Internet of things, Electronics, Computer Vision and Robotics. He has a keen interest in core of electronics, automation and Robotics.