Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, June 2021:1042- 1052

Research Article

Iot Based Face Recognition Using Pir Sensor For Home Security System

[1]PavanKumar Kolluru, [2]K . Sri Vijaya, [3]Anusha Marouthu

ABSTRACT

An intelligence system is installed in this research paper for home security. The Internet of Things(IoT) is used specifically to monitor the persons who are all entering by using a web application and Smartphone inside the home. The user can be able to monitor the home from everywhere anywhere at any time with the help of the application in the system. The locking device which we use currently in banks and home or not smartly secure and can we break easily in the system face recognition technology is also implemented where it allows only authorized persons to enter the home to initiate the process of face recognition. The system proposed is embodied with ultrasonic sensor and camera module to the desired functionalities are performed by Raspberry Pi which is already installed to generate the command signal in the system. The web application is used for adding new faces to the database by the owner and it is permitted by the application. Using Facial Recognition, the smart home manager is detailed as Home Automation System (HAS) which identifies the users and also enhances their home experience by smartly automating by the requirement. The user information is collected by the system and a profile is built for the use of which helps to automate home appliances that identify the user by his/her special characteristics. The required item which is used by the members of the family in the home is collected by the system through the web interface and then it stores the collected data. A profile is created by the system where it also captures the face of the members of the family. The system now distinguishes between the guest and the intruders by interacting with the members of the family by using the input of facial characteristics and then identify the actual family. The family and neighbors will be intimated about the intruders once they are detected. Also, the authentication of the user is provided in two ways as security is ensured every time. The member of the family can change the requirement via the web interface freely. With the help of facial characteristics, the members of the family are distinguished so the system can easily identify the user and guest user.

Keywords: HAS, IoT, Facial Recognition, Security, Passive Infrared.

[1]Assistant Professor, Department of Computer Science and Engineering, VFSTR Deemed to be University, Andhra Pradesh, India. Pavanwithu@gmail.com
[2]Assistant Professor, Department of IT, P V P Siddhartha Institute of Technology, srivijayak@gmail.com
[3]Associate Professor, Department of Computer Science and Engineering, Koneru lakshmaiah Education Foundation, Vaddeswaram, Guntur, India. anushaaa9@kluniversity.in

I Introduction

The world of home defense is evolving. A facial recognition system can be used to provide home surveillance. A standard UBS camera captures the image to identify the individual. It's a model that sets the guest apart. If the entryway recognizes the visitor, it will greet them by name and open the door called opened. If they aren't identified, the entranceway would be permanently bolted. The system will carry out the identification and acknowledgment in real time[1]. This makes use of the vital video cam, as well as the web connection, to create an entryway that opens itself based on facial recognition. Home security has become a serious issue in the general public. Anybody can be irritated in its own home. More seasoned security frameworks can't handle a few circumstances like hacking, separate in the framework[2]. Undesirable people like hoodlums, killers, and some realized lawbreakers will attempt to interfere in the home any time they need. Additionally, we realize that the contraptions nowadays are not unreasonably gotten and thus can be effortlessly hacked. Indeed, even interlopers have discovered their approach to assume control over these contraptions[3]. So to stay away from such circumstances, we need to build up the framework in such a manner that nobody ought to get an interruption to the framework. The utilization of IoT will improve some security level just as it will help in getting to and controlling the framework distantly. Subsequently, we are attempting to build up a face unmistakable [4] mechanized entryway opening framework utilizing an IoT.

Facial Recognition, The Internet of Things (IoT), and force preparing at the edge. Facial acknowledgment has exhibited the capacity to altogether increment and improve an association's security and wellbeing. Face recognition frameworks use computer algorithms to choose explicit, unmistakable observations about a person's face. These details, such as the distance between the eyes or the state of the jawline, are then converted into a numerical representation and compared to data on various countenances collected in a facial recognition data set. The detection of front-facing human countenances is at the heart of face-discovery calculations. It's analogous to picture exploration, in which an individual's image is pieced together one small phase at a time. The inherited measurement is then used to create all of the possible face districts, including the eyebrows, the nose, and the mouth[5]. Face recognition is a more general concept than face exploration. Face position essentially means that a framework can detect the presence of a human face in a photograph or video. Face recognition can help to validate a person's personality. It is accordingly used to control admittance to delicate zones. Facial acknowledgment calculations are modified to search for evenness between the left and right sides of the face. Decline your odds of identification by making an imbalance, such as covering your left eye with a quill or a piece of styled hair. Utilize apparent reverse. It is used by law enforcement agencies and a few other organizations to identify criminals and victims by combining photos and video with data sets such as driver's license documents. Facial recognition, on the other hand, is said by friendly freedoms groups to contribute to security disintegration, create prejudice towards people of color, and be prone to violence. Facial Recognition Systems are exceptionally touchy to present varieties[6]. It turns into a test to distinguish the genuine face when the revolution point goes higher. It might bring about flawed acknowledgment or no acknowledgment whether the data set just has the front-facing perspective on the face.

In the present quickly moving reality where nearly everything is driven by innovation, it has become the focal and fundamental piece of living. With expanding pace of wrongdoing, ensuring

our friends and family and our possessions has gotten significant. Such circumstances can be tackled by misusing the most recent functionalities that current innovation has to bring to the table for example IOT which gives consistent information correspondence; controller capacity makes it simpler to mechanize the cycle of safety. Robotization of safety can be accomplished by planning an application on Raspberry Pi and ATmega 328 microcontroller through different sensors, for example, movement sensor - PIR (Passive Infrared) sensors for identification of any gatecrasher in the house, upon location a caution is raised and the proprietor of the house and warning messages are given[7]. The savvy home idea in the framework improves the standard of living at home. At whatever point an individual comes before the house the PIR movement finder sensor distinguishes the individual and a message will ship off the house proprietor and he can see the individual through the camera before the house. The camera is gotten to the page and the light, fan, entryway lock, caution can be controlled with the page. As indicated by the need of the individual the proprietor can handle the electrical apparatuses. The individuals who get the confirmation can open the entryway by entering a secret phrase on the keypad and utilize the home apparatuses relying upon the need set by the proprietor.

The essential point is to create a plausible answer for change a conventional doorbell into an insightful ringer that gives data of the outsider to the property holder accordingly empowering him to answer the entryway through an advanced mobile phone with a simple UI. The plan arrangement in the IoT framework is multidisciplinary and is dissipated through different space explicit difficulties. There are numerous explores that expect the disappointment of remote organizations which is developing as the utilization of innovation advances. The principal factors are network geography, the disappointment of organization estimation, and cost minimization which chooses the proficiency of the organization and information conveyance. The information conveyed or traded over the web can be a sound, video, or picture record[8]. These days home and building mechanization frameworks are utilized to an ever-increasing extent. That gives expanded solace, particularly when utilized in a private home. A significant factor to consider when we talk about home computerization is Security. Home security is a vital component of home computerization and perhaps the most critical one. Home security rolled out extreme improvements in the previous few decades and keeps on propelling considerably more in the coming years. Beforehand home security frameworks implied having a caution that would go off when someone would break in yet a brilliant secure home can do considerably more than that. In this manner, the principal objective of our work is to plan a framework that can caution the proprietor and others of a gatecrasher break-in by sending a warning to their advanced cells. The proprietor will likewise stop or begin the caution distantly utilizing only his PDA. This framework will assist the clients with defending their homes by putting the framework on the entryways and checking the movement through their advanced cells[9].

II Literature Review

The Internet of Things(IoT) has made it conceivable to set up shrewd home security through which you can conclude who can enter your home utilizing your cell phone and web application. It's additionally simplified and generally moderate to screen your home whenever and anyplace. the central question in a conventional home security framework is, it is effectively delicate and very obsolete. This reciprocally brings about theft and needs the establishment of an expensive security framework. To handle this issue, we propose a keen home security framework, which is IoT just as face acknowledgment empowered. In our framework, the web camera is utilized

which is associated with the raspberry pi joined by sensors like Passive Infrared(Pir) and Ultrasonic sensor[10]. On movement identification camera catches a picture of the individual before the entryway at that point continuous face acknowledgment is finished utilizing a nearby twofold example (LBP). On the off chance that an individual's picture matches with one of the home individuals, the entryway will open, else the doorbell will ring. if an interloper attempts to break the entryway, a caution will be raised simultaneously SMS and Email containing picture of the gatecrasher will be shipped off the property holder[11]. Face acknowledgment functions admirably in multi-face acknowledgment and more bizarre recognizable proof, which meet the necessity of home security. This framework is battery fueled if there should be an occurrence of force disappointment. Besides, the house proprietor can monitor movement occurring in the house utilizing android and web applications associated with the raspberry pi utilizing the web. Utilizing Android application or web application proprietor can likewise add new individual's countenances into the information bases eg., visitors.

Individuals observing and following exercises in reconnaissance framework, as a rule, create an enormous measure of information from Internet-of-Things (IoT) gadgets like cameras[12]. A few issues should be tended to, including information movement over restricted transfer speed and high inactivity in correspondence organizations. This paper presents a drive to build up a decentralized face acknowledgment conspire for a disseminated reconnaissance framework that utilizes a coordinated system of Internet-of-Things (IoT) and distributed computing. The decentralized face acknowledgment approach carries out a two-stage technique, including face location and extraction and face coordinating. Face discovery and extraction are performed on a cloudlet that is found near the observation cameras, henceforth limiting the requirement for gigantic information move to the far off preparing focus[13]. Then again, face coordinating with the measure is done on the face highlight vector inside a private cloud climate. A contextual investigation directed on the adequacy of the proposed plot in distinguishing "missing" individuals shows that the system works successfully in the IoT-Cloud foundation.

With the interest for interconnection, everything being equal, an ever-increasing number of sorts of sensors are associated with the Internet of Things. Unique about conventional sensors, for example, low transmission recurrence and little information volume, visual sensors have the attributes of high transmission rate and huge information volume. Vision sensors are broadly utilized in security, medical services, and other face acknowledgment. This paper [14] proposes a mix of edge-based man-made consciousness and distributed computing that is appropriate for territories, for example, face acknowledgment and security that require countless visual sensors and picture handling and examination.

K-Nearest Neighbors and Support Vector Machine calculation was applied to get familiar with the better boundary of the FoL calculation utilizing cross-approval. Exactness and the size after the pressure cycle were received to assess the proposed calculation. The FoL was tried in Celebi, Extended YaleB, AR, and LFW face datasets getting something very similar or better outcomes when contrasted and the methodology utilizing similar classifiers with uncompressed highlights, however with a decrease of 86 to 91% contrasted with the first information size[15].

As of late, it is critical to possess a solid security framework that can get our resources just as to ensure our protection. The conventional security framework needs a person to utilize a key, (ID) card, or secret key to get to a space like home and working environment. Notwithstanding, the current security framework has numerous shortcomings any place it is projected and taken. Most

entryways are constrained by people with the work of keys, security cards, catchwords, or example to open the entryway. The proposed framework [16] primarily comprises subsystems in particular picture catch, face identification and acknowledgment, email notice, and programmed entryway access the executives. Face Recognition upheld openCV is raised because it utilizes Eigen's faces and decreases the size of face pictures without losing indispensable highlights, facial pictures for some, people can be put away in the information base.

III. Proposed Methodology

The intelligence system installed in this research paper for home security the internet of things iot is used specifically to monitor the persons who are all entering by using a web application and smartphone inside the home the user can be able to monitor the home from everywhere anywhere at any time with the help of the application in the system the locking device which we use currently in banks and home or not smartly secure and can we break easily in the system face recognition technology is also implemented where it allows only authorized persons to enter the home to initiate the process of face recognition the system proposed is embodied with ultrasonic sensor and camera module to the desired functionality stick are performed by M Raspberry Pi I which is already installed to generate the command signal in the system as shown in figure 1.

Mostly embedded sensors are preferred in the system which can sense any disturbance or motion and its surroundings which consumes less power. the Raspberry Pi receives the command signal from the stepper motor we Incorporated to lock or unlock the door. the face detection algorithm is also comprised of the Raspberry Pi controller which helps to prevent the entrance of unauthorized persons into the home. along with the web interface to make the security connectivity the user interfaces such as tablets and mobiles are used.

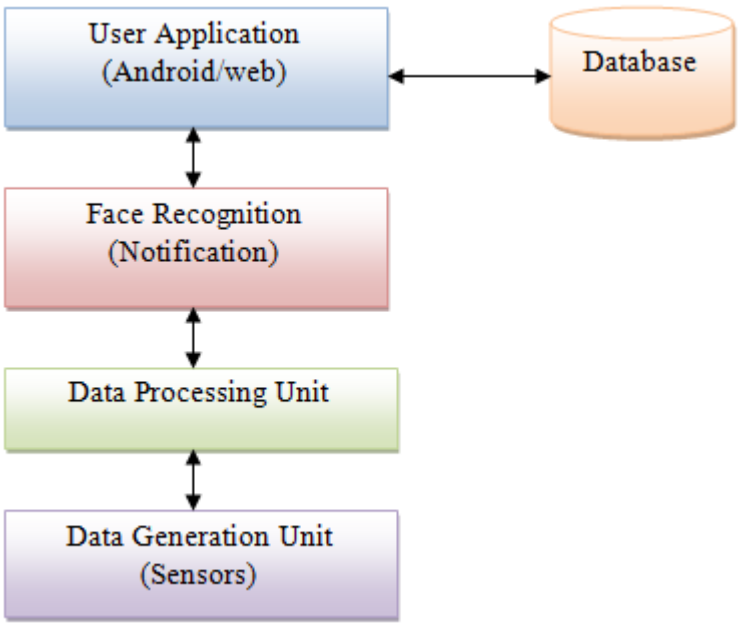

Figure 1. Block Diagram of Proposed System with its Components

Through the internet, the iot helps to conceptualize the idea of monitoring and connecting remotely with real-world objects. This concept can be incorporated to make our house smarter, safer, and automated. With the wireless system and at low cost the design of the Home Automation System(HAS) is presented in this project. The standard of living at the home is improved by implementing this smart system concept. The Passive Infrared (PIR) motion detector sensor is used to detect the persons entering the home and it immediately sends a message to the owner and they can see through the camera. On the webpage, the camera, door lock, alarm, light, and fan can be controlled and accessed. By the priority of the person, the Electrical appliances and devices can be accessed by the owner. When a person gets authority from the owner, they can open the door by feeding the password to the keypad, and also by the priority given by the owner, they can access the appliances.

While building a smart, secured and automated home two or more platforms are combined to create a reliable and flexible system that can be adapted and operated easily. To serve this purpose the deliberate choices have been made in the mode of operations, hardware components, and type of platforms.

PIR Sensor

In this system, the PIR (Passive Infrared) sensor is used to extract the face of the person who stands in front of the sensor which is operated in low power and maintenance. In this system, the PIR (Passive Infrared) sensor is used to extract the face of the person who stands in front of the sensor which is operated in low power. The range between the door and the person is approximately measured by the sensor and simultaneously to detect each person, the device data is transmitted to the Raspberry Pi controller. Figure 2 shows the diagram of the PIR sensor.

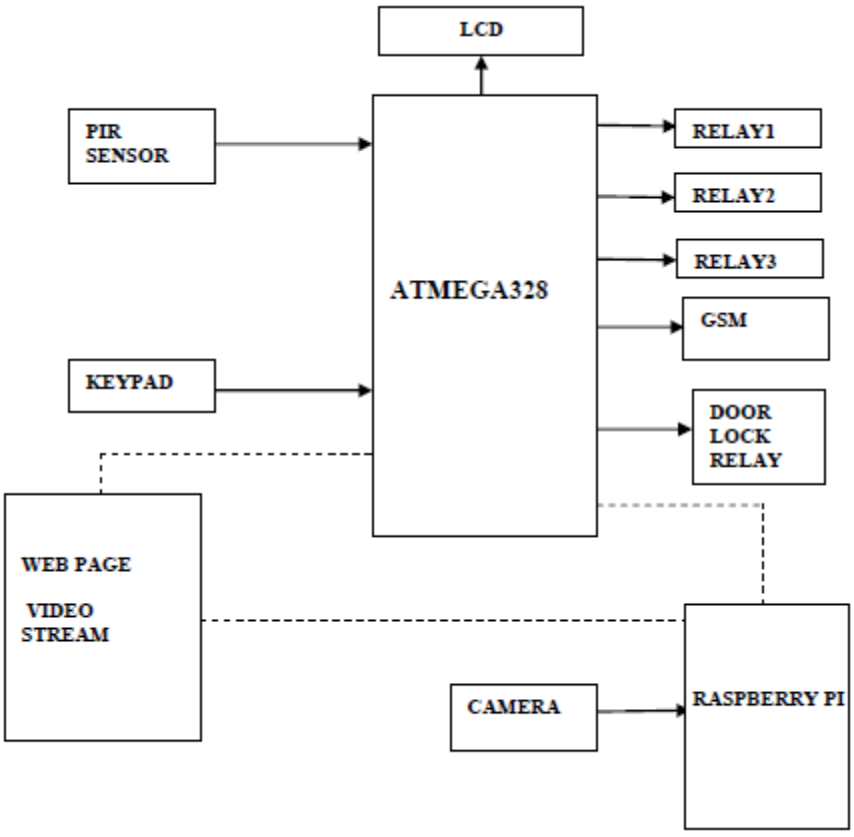

Figure 2. Pin Diagram of Proposed Methodology using PIR sensor

It is an adaptive, extensible, and low-cost surveillance system that focuses to identify and alert the home about intruders. Also, it allows us to interfere with the existing alarm and the new alarm can be customized by the users. Several IP cameras are processed by the system to distinguish between the faces which is available in the database and not available.

In this system, the surveillance system object is considered as a heart. It alerts the system by processing several IP cameras to monitor. The object of Face Recogniser provides the training functions to the classifier of linear SVM by using the database of the faces that are collect which includes all the necessary functions to perform the process of face recognition using the neural network which is pre-trained called Openface. The objects are directly streamed from the IP Camera which will be readily available for the Web Client to stream. Each IP camera owns a Face Detector and Motion Detector object which is used for the process of person tracking and face recognition. The object of Flask Socket Input-Output streams the frames in the jpeg format to the client and then it transfers the data of JSON by using the requests of the HTTP POST and web sockets. Lastly, the GPIO interface is controlled by the flask object of Raspberry Pi which is connected directly to the alarm panel that is wired and exists already.
The web-based communication and the central processing are performed by the main component and the alarm control interface is hosted by Raspberry Pi as shown in figure 3.

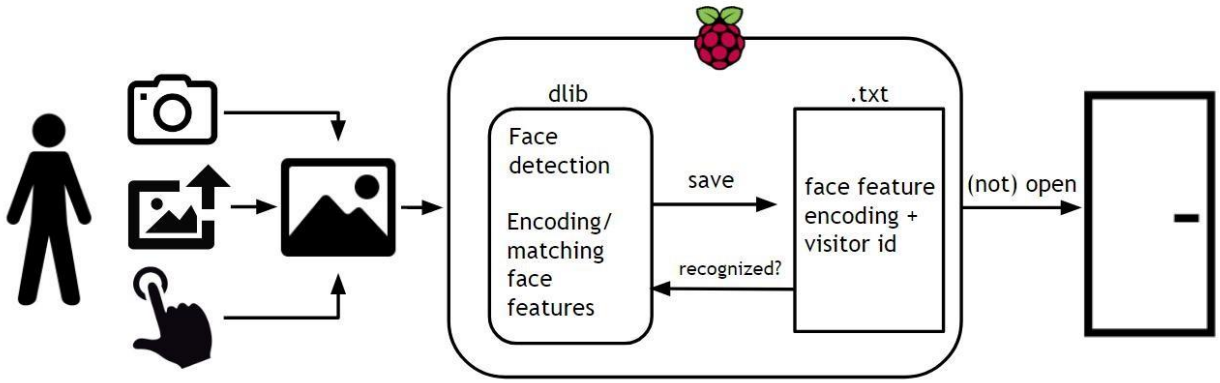

Figure 3. System Architecture of Face Recognition

The system depends on the technique of facial recognition which does in real-time. The user walks up towards the door that she/he wants to open or she/he wants to enter inside the home and then presses the button. Now the system will recognize the person either as a trusted visitor that authorizes to enter or a stranger by denying the access.

In this concept, the system is mostly looking for the faces. For clearance, the profile picture is created in a database for each user to analyze the unique features. When the same user tries to get into the building the system allows them to enter. Once the face is recognized, the LED will blink once and if the person is not recognized it blinks twice then the visitor doesn't match with the database, and the access is denied.

IV Experimental Results

In this project, the devices and appliances in the home are controlled and monitored and also to provide security from the entry of unknown persons. For the home automation technique, the

system is proposed. To design the system, computer vision technique, image processing algorithm, Open CV, and Raspberry Pi are used as shown in figure 4.

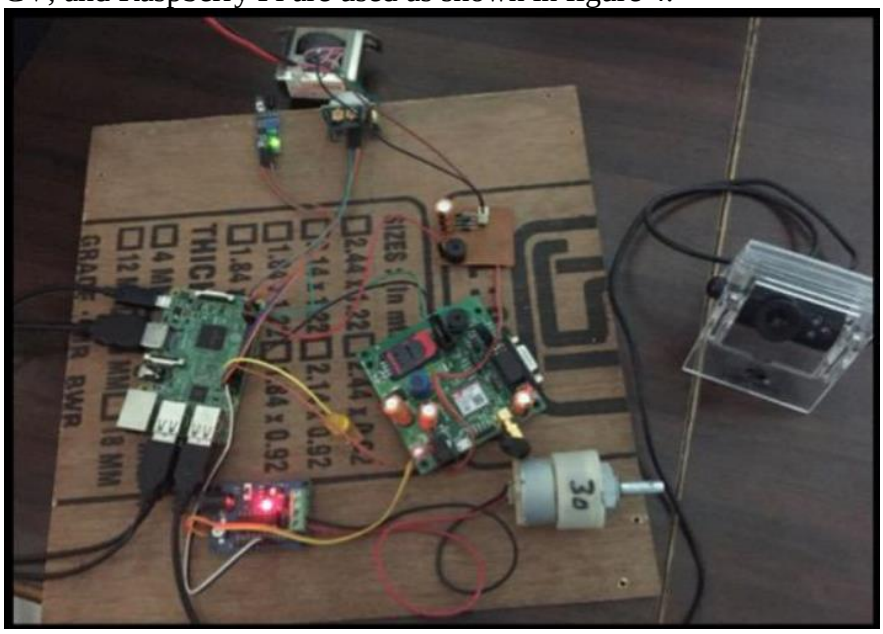

Figure 4. System Design setup

The outcome of the project is a prototype home security system the controls the appliances in the home by simple finger touch which is also capable of live video streaming monitoring the home. when a person comes in front of the home the sensor will be sending a message to the owner who can able to view the person standing in front of the home.

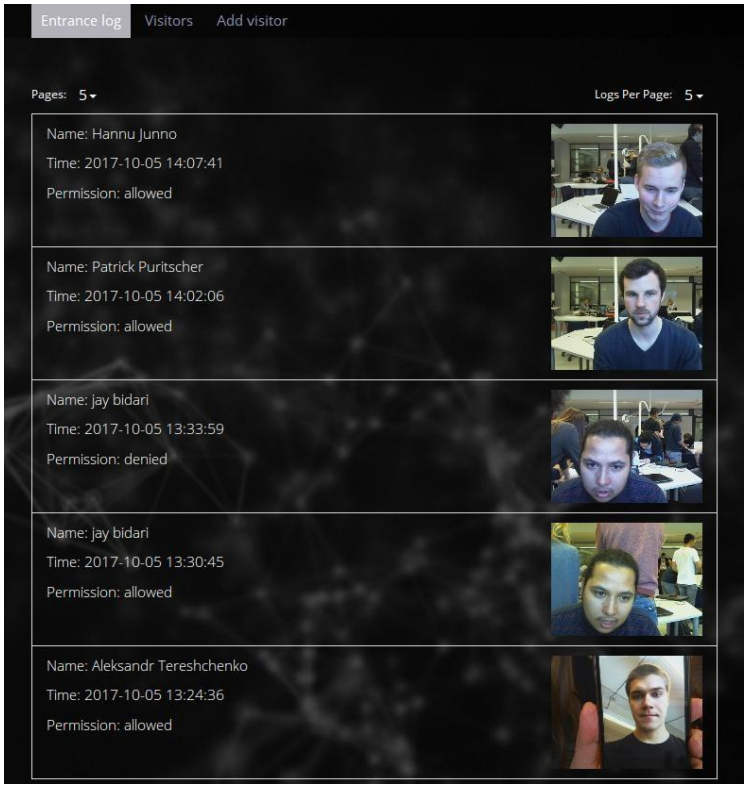

Figure 5. Face Recognition with Permission Access

V Conclusions

In today's world, security is of real essential importance where the traditional available systems have also attempted to provide available microcontrollers under technologies. the system proposed to provide security for the home meditating the intruder's face. An alarm will be raised and also the message will be sent to the owner of the home if any intruders are noticed. This proposed system eliminates the drawbacks of the traditional system like high downtime during maintenance and repair which allows the intruders and hackers to enter and also the low cost and low power consumption. A high level of security is provided for the home where the leading Technologies like IoT and face recognition are combined. The above-mentioned technologies are fast-growing ones and scientists keep researching them. This significant security system doubles up the security. Remote monitoring and controlling are possible because of using IoT Technology and hacking is highly impossible because of face recognition. ATmega 328 microcontroller Raspberry Pi controller is used in this system which provides flexibility and compatibility with the latest devices and sensors to enhance the features of low power consumption and management. This concept can be taken to the next phase like the automation market for detecting the price points with a few improvements in the technologies.

References

1. Elsisi, M., Tran, M. Q., Mahmoud, K., Lehtonen, M., & Darwish, M. M. (2021). Deep learning-based industry 4.0 and internet of things towards effective energy management for smart buildings. Sensors, 21(4), 1038.
2. Radzi, S. A., Alif, M. M. F., Athirah, Y. N., Jaafar, A. S., Norihan, A. H., & Saleha, M. S. (2020). IoT based facial recognition door access control home security system using raspberry pi. International Journal of Power Electronics and Drive Systems, 11(1), 417.
3. Peixoto, S. A., Vasconcelos, F. F., Guimarães, M. T., Medeiros, A. G., Rego, P. A., Neto, A. V. L., ... & Reboucas Filho, P. P. (2020). A high-efficiency energy and storage approach for IoT applications of facial recognition. Image and Vision Computing, 96, 103899.
4. Garikapati, P., Balamurugan, K., Latchoumi, T. P., & Malkapuram, R. (2020). A Cluster-Profile Comparative Study on Machining AlSi 7/63% of SiC Hybrid Composite Using Agglomerative Hierarchical Clustering and K-Means. Silicon, 1-12.
5. Medapati, P. K., Tejo Murthy, P. H. S., & Sridhar, K. P. (2020). LAMSTAR: For IoT-based face recognition system to manage the safety factor in smart cities. Transactions on Emerging Telecommunications Technologies, 31(12), e3843.
6. Ezhilarasi, T. P., Kumar, N. S., Latchoumi, T. P., & Balayesu, N. (2021). A Secure Data Sharing Using IDSS CP-ABE in Cloud Storage. In Advances in Industrial Automation and Smart Manufacturing (pp. 1073-1085). Springer, Singapore.
7. Kumar, M., Raju, K. S., Kumar, D., Goyal, N., Verma, S., & Singh, A. (2021). An efficient framework using visual recognition for IoT based smart city surveillance. Multimedia Tools and Applications, 1-19.
8. Sekaran, K., Rajakumar, R., Dinesh, K., Rajkumar, Y., Latchoumi, T. P., Kadry, S., & Lim, S. (2020). An energy-efficient cluster head selection in wireless sensor network using grey wolf optimization algorithm. TELKOMNIKA, 18(6), 2822-2833.

9. Kumar, K., Kumar, N., & Shah, R. (2020). Role of IoT to avoid spreading of COVID-19. International Journal of Intelligent Networks, 1, 32-35.
10. Albahri, A. S., Alwan, J. K., Taha, Z. K., Ismail, S. F., Hamid, R. A., Zaidan, A. A., ... & Alsalem, M. A. (2021). IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. Journal of Network and Computer Applications, 173, 102873.
11. Latchoumi, T. P., Vasanth, A. V., Bhavya, B., Viswanadapalli, A., & Jayanthiladevi, A. (2020, July). QoS parameters for Comparison and Performance Evaluation of Reactive protocols. In 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) (pp. 1-4). IEEE.
12. Mohammed, M. N., Syamsudin, H., Al-Zubaidi, S., AKS, R. R., & Yusuf, E. (2020). Novel COVID-19 detection and diagnosis system using IOT based smart helmet. International Journal of Psychosocial Rehabilitation, 24(7), 2296-2303.
13. Zhang, L. L., Xu, J., Jung, D., Ekouka, T., & Kim, H. K. (2021). The Effects of Facial Recognition Payment Systems on Intention to Use in China. Journal of Advanced Researches and Reports, 1(1), 33-40.
14. Rahman, A., Hossain, M. S., Alrajeh, N. A., & Alsolami, F. (2020). Adversarial examples–security threats to COVID-19 deep learning systems in medical IoT devices. IEEE Internet of Things Journal.
15. Masud, M., Muhammad, G., Alhumyani, H., Alshamrani, S. S., Cheikhrouhou, O., Ibrahim, S., & Hossain, M. S. (2020). Deep learning-based intelligent face recognition in IoT-cloud environment. Computer Communications, 152, 215-222.
16. Biswal, A. K., Singh, D., Pattanayak, B. K., Samanta, D., & Yang, M. H. (2021). IoT-Based Smart Alert System for Drowsy Driver Detection. Wireless Communications and Mobile Computing, 2021.
17. Arunkarthikeyan, K., & Balamurugan, K. (2021). Experimental Studies on Deep Cryo Treated Plus Tempered Tungsten Carbide Inserts in Turning Operation. In Advances in Industrial Automation and Smart Manufacturing (pp. 313-323). Springer, Singapore.
18. Mohammed, M. N., Hazairin, N. A., Syamsudin, H., Al-Zubaidi, S., Sairah, A. K., Mustapha, S., & Yusuf, E. (2020). 2019 novel coronavirus disease (Covid-19): detection and diagnosis system using IoT based smart glasses. International Journal of Advanced Science and Technology, 29(7 Special Issue).
19. Liu, Y., Kong, L., Chen, G., Xu, F., & Wang, Z. (2021). Light-weight AI and IoT collaboration for surveillance video pre-processing. Journal of Systems Architecture, 114, 101934.
20. Sneha, P., Balamurugan, K., & Kalusuraman, G. (2020, December). Effects of Fused Deposition Model parameters on PLA-Bz composite filament. In IOP Conference Series: Materials Science and Engineering (Vol. 988, No. 1, p. 012028). IOP Publishing.
21. Yarlagaddaa, J., Malkapuram, R., & Balamurugan, K. (2021). Machining Studies on Various Ply Orientations of Glass Fiber Composite. In Advances in Industrial Automation and Smart Manufacturing (pp. 753-769). Springer, Singapore.
22. Jadon, S., Choudhary, A., Saini, H., Dua, U., Sharma, N., & Kaushik, I. (2020). Comfy smart home using IoT. Available at SSRN 3565908.
23. Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K., ... & Baik, S. W. (2020). Raspberry Pi assisted face recognition framework for enhanced law-

enforcement services in smart cities. Future Generation Computer Systems, 108, 995-1007.