ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 6, Issue 5, May 2021

IoT Embedded World

[1]Andhavarapu Swaroop, [2]Dumpala kalyani, [3]Gorusu Sunitha [4]Sreerama Murthy Velaga

[1][2][3] UG Student, Dept. of CSE, GMR Institute of Technology, Rajam, India
[4] Professor, Dept. of CSE, GMR Institute of Technology, Rajam, India
Email: [1]18341A0509@gmrit.edu.in, [2] 18341A0534@gmrit.edu.in, [3]18341A543@gmrit.edu.in,
[4]vsr_murthy@gmrit.edu.in

Abstract--- This paper focusses on IOT and its applications in real time scenarios. We are mainly focusing on three major applications i.e., IOT based Biometrics, Home Automation and security, Health monitoring system. With the increased number of Internet enabled devices in the modern world, authentication plays a crucial role for secure access. Raspberry PI is used to build a low-cost biometric system. It describes how biometric can leavage cloud's boundless computational resources and striking properties of flexibility, scalability and cost reduction. Home automation system describes about building a secure home with automation that helps in reducing energy, electricity and also more useful for elder people or people with physical disabilities. Health monitoring system achieves to develop a reliable patient monitoring system using IoT so that the healthcare professionals can monitor their patients, who are either hospitalized or at home using an IoT based integrated healthcare system by monitoring the patients 24/7.

Key Words--- IoT, Raspberry Pi, Home automation, Health monitoring, Arduino

I. INTRODUCTION

Internet of Things (IoT) technology has a wide range of uses, from consumer applications such as smart homes to infrastructure applications. IoT emphasizes the interconnection of all physical and digital items including sensors, smart devices, cyber sensors, and so much more, which allows the automatic and efficient data transmission and shared over the Internet. Biometrics deals with recognition of individuals based on their behavioral or biological characteristics. The human organs, which might be considered as biometric means, should have the following major desirable properties: universality, permanence, uniqueness, performance, collectability, acceptability, and circumvention. With the growing use of IoT devices, security has become a significant issue in IoT environment. Security in IoT can be examined under the following three main headings: ensuring the security of the collected data, using an encrypted communication channel, and using user authentication. User authentication is essential to protect the privacy of personal data. Traditionally, user authentication in IoT was done with pin-based password systems. However, biometric systems have started to be used due to the weaknesses of the pin-based password, such as being forgotten, stolen, and shared. Because biometric descriptors are inherent in an individual, it is more difficult to manipulate, share, or forget these characteristics. At the same time, Biometric data cannot be changed in case of stolen because it has unique characteristics of the person, and it creates serious privacy problems in case of leakage. Therefore, we can use encryption methods to secure biometric data. This paper is mainly concentrated on Biometric recognition or biometric security. It considers two grounds about human body characteristics, distinctiveness and permanence. Some of the most popular physiological traits, which are used in IoT biometric security, are fingerprint, face, iris, hand geometry, gait, DNA (deoxyribonucleic acid), etc. The selection of a biometric generally depends upon the necessities of the authentication application. For example, voice biometrics is suitable in mobile security matters because the device which senses vocal sound is previously embedded in the mobile phone, and the finest part of the IoT biometric authentication is that it can identify the person who is not registered in the system, but still trying to get the access. There are two types of biometric modalities, physiological and behavioral. Physiological features are based on direct measurements of part of the human body e.g., face, fingerprint, iris, and hand geometry. Behavioral features are one kind of indirect human characteristics measurement through the feature extraction and machine learning e.g., signature, gait.

Internet of things (IOT) is a network of physical devices with the network connection. A smart home is the integration of technology that enables users to achieve a better quality of living. It is a voice assistant for the remote control of all home appliances. It can help to improve security, comfort, convenience, and energy management. Smart home aids elderly and disabled people by providing

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 6, Issue 5, May 2021

them a safe and secure environment. Basically, SHs can be categorized into two types, namely, wired and wireless systems. Wired systems use optical fibers, bus lines, and power lines. Wireless systems are a combination of a sender and a receiver. At present, many new applications use wireless technology, such as radio waves or infrared, to communicate with other devices. SHs can simultaneously work on wireless and wired systems. In an SH environment, smart appliances can be directly connected to the home network, and the commands are given by users to individually control each appliance. Smart devices can automatically react when commands are given either through voice, smartphone, or computer. Majority of control applications are interrelated to lighting, motion, security, entertainment, and temperature. The use of smartphones and computers are crucial because they are technological benchmarks in the modern era. Users can bring these gadgets anywhere and directly configure them through the Internet to link with online devices.

Life expectancy has increased dramatically, especially in the more affluent nations, which is set to be celebrated and should be viewed as an opportunity for people to live longer and better. However, this requires substantial improvement in both the healthcare service and the living environment, as older people generally require more healthcare than their younger counterparts. Additionally, older people are more likely to suffer from chronic disease as part of the natural ageing process. Hence, empowering the utility of IoT in healthcare, with interconnected medical sensors, especially wearable or implantable, is considered to be able to provide smart accurate and cost-effective personalized healthcare service.

II. LITERATURE REVIEW

The literature review shows that there are not many studies on biometric authentication in IoT. S.Obaidat proposed a biometric system that takes into account the increased cost of hardware maintenance and processing power for databases[1]. G.I.Davida proposed a method of four components with gateway node and sensors. Access control, identity management, legal and technical issues are the key considerations for ensuring security [2]. Manjur Kolhar presented a survey of IoT based biometric solutions, their security features, embedded hardware design to help people. He introduced new radio technology which incurred low power consumption and cost [3]. Shobhan Mandal introduced the network and threat models [4]. Li Lu describes the fusion of face and mouth movements in multidimensional movements of multiple components [5]. M. Gofman proposed a method based on behavioral characteristics to reliable the users [6]. This system utilizes a node microcontroller unit (Node MCU) as a Wi-Fi-based gateway to connect different sensors and updates their data. The collected data from several sensors can be accessed via users' devices over the Internet regardless of their location [7]. It is an application of embedded system which integrates Android operating system, Arduino controller and the Bluetooth for the implementation of Smart Home [8]. Authors are mainly focused on the proposed system that includes smart door lock system using Radio Frequency Identification (RFID) card and password [9]. ESP8266 is used as a Wi-Fi technology. In the hardware interface, the integration of ESP8266 Wi-Fi technology for controlling home appliances and sensors is manifested, and an application is provided for controlling to multiple users of home, with smart phones, tablets, and laptops [10]. Mobile application provides convenience for user to be able to control the home appliance remotely by two alternative tasks; voice command and graphical user interface. The user interface employs the Google assistance for voice command environment while the graphical user interface is developed Blynk App [11]. Home Automation System (HAS) uses computers or webpage or android app for monitoring various parameters to control different electronic home appliances [12].

For Health Monitoring System, The main contribution of this paper include following: firstly, this paper presents a novel system, the WISE (Wearable IoT-cloud-based health monitoring system), for real-time personal health monitoring. Secondly, the majority of existing wearable health monitoring systems requisite a smart phone as data processing, visualization, and transmission gateway, which will indeed impact the normal daily use of the smart phone. Whilst in WISE, data gathered from the BASN are directly transmitted to the cloud [13]. Continuous online patient and patient's room condition monitoring is the main idea of the proposed system. The system introduced smart healthcare to monitor the basic important signs of patients like heart rate, body temperature, and some measures of hospital room's condition such as room humidity, the level of CO and CO_2 gases [14]. This paper introduces the review of the Internet-based healthcare monitoring system (HCMS) and the general outlines on opportunities and challenges of the patient's Internet-based patient health monitoring system. The main goal of the e-health monitoring system is to offer the patient a prescription automatically according to his or her condition [15]. This system uses Temperature and heartbeat sensor for tracking patient's health. Both the sensors are connected to the Arduino-uno. To track the patient health micro-controller is in turn interfaced to a LCD display and Wi-Fi connection to send the data to the web-server [16]. This paper portrays the current research and

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 6, Issue 5, May 2021

development in the field of health. Different implemented systems have been compared and evaluated to identify the concerned lacking areas and what can be done in order to provide better throughput than the current scenario systems. It discusses about the health monitoring system incorporated with GSM and Health Monitoring System incorporated with Mobile Phones [17]. This paper mainly focused on patient health monitoring system based on IOT technology where the collected data is communicated to thinkspeak cloud platform which can be accessible by doctor and family members [18].

III. METHODOLOGY

The main part of the biometrics based on IOT is feature extraction. There are two types of extraction methods in computer vision: low-level and high-level feature extractors. Low-level feature extractor transforms the visual content of a biometric template by associating features such as color, gradient orientation, texture, and shape with the content of the input template high-level algorithms are typically associated with the machine learning field. These procedures are concerned with the transformation or classification of a scene. Multiple methodologies are presented for each of these visual features, and each of them symbolizes the feature from a different perception. According to Fig1., description on the components is included here.

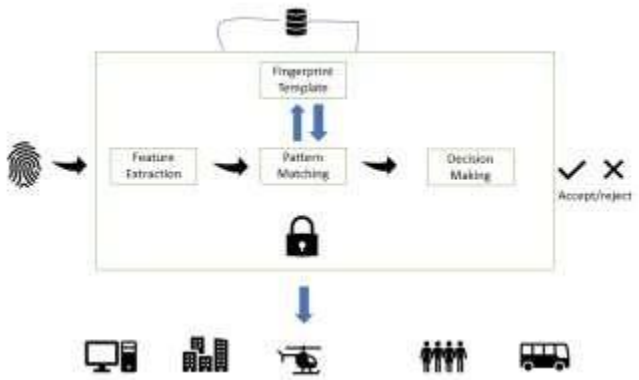

Figure1: Framework for IoT based biometrics

Sensor or acquisition module: It obtains the biometrics of an individual. As an example, fingerprint sensor captures the fingerprint impressions of a user.

Feature extraction module: The assimilated data is managed to extract feature values. As an example, the positional and orientation-related features are extracted from a fingerprint image in the feature extraction module of a fingerprint recognition system.

Matching module: The feature values are compared and calculated against the template by making matching. An example, here the matching score is calculated between query and template in this module, which helps in the next section.

Decision-making module: The requested identity is either rejected or accepted here based on the similarity score.

The effectiveness of a biometric scheme is assessed by taking account the false acceptance rate (FAR) and false rejection rate (FRR). These two measurements are graphed together in receiver operating characteristic (EER) curve, which plots FAR against FRR.

We designed a system to ensure security and privacy with biometric authentication as shown in Fig2, which consists of two layers: client and server. Raspberry Pi-4, as an IoT device, is used in the client part. The server part of the system is installed on a PC. In this system, first the fingerprints of the user or users to be registered to the system are taken with the help of a sensor, and these fingerprint images are sent to the Raspberry Pi device. After fingerprint images pass through the necessary image processes in Raspberry Pi, a biometric template consisting of minutiae points to be used in fingerprint authentication, is obtained. Minutiae points are friction ridge skin impressions believed to be unique on each fingerprint. The biometric template is sent in encrypted form as a precaution against hacking attacks on the communication channel between the server and the Raspberry Pi.

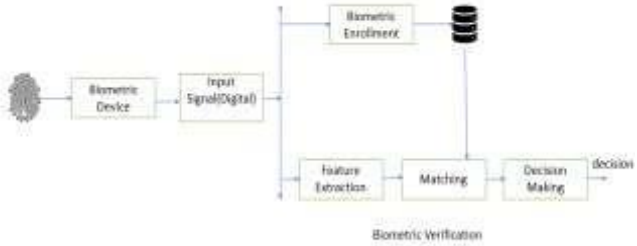

Figure2: Working procedure of biometric security system: a part of IoT system

the path followed while creating the database of a system. This system is ready for use after the fingerprints of authorized users are registered in the database. The user sends his fingerprint to the system through the fingerprint sensor. The fingerprint taken from the sensor is sent to the Raspberry Pi, and the biometric template is extracted after the necessary image processing operations. The extracted biometric template is sent in encrypted form as a precaution against hacking attacks on the channel between Raspberry Pi – Server. The encrypted biometric templates previously saved in the database with the fingerprint template coming from the user are decrypted and compared on the server part one by one. If the user's fingerprint matches one of the

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 6, Issue 5, May 2021

previously registered fingerprints in the system, they are permitted to access the system. If this fingerprint does not match the registered fingerprints in the system, they are not permitted to access the system.

IMPLEMENTATION OF BIOMETRICS:

First of all, fingerprint images of the users who want to be registered in the system are passed through the necessary pre-processing, and biometric templates are created with feature extraction. In our system, biometric templates are shown with some variable. Later, this variable data are recorded in the database in an encrypted form. Aes-128 Bit method has been chosen as the Encrypted method.

Biometric templates containing minutiae extracted from fingerprint images. The data containing minutiae points extracted from fingerprint images should not be confused with the variable used in the encryption method. The result is returned according to the threshold value. There are four functions here. These include removedot (), which reduces the noise by improving the given image, getdescriptors (), which returns minutiae points of the given image, desfromcsv (), which we explained earlier, and finally, calculate () function which calculates the similarity of the two minutiae according to the threshold value.

In the client part of our system, the fingerprint images obtained from the fingerprint sensor are sent to the raspberry pi. In Raspberry Pi, variable data containing fingerprint minutiae points are obtained with the removedot() and getdescriptors() methods that we have explained before.

CREATE DATABASE:

- Extract image from sensor and insert the path into the database.
- Extract minutiae points from image and assign a name to it.
- Note the start time in a list.
- Then encrypt the points from image and store it in a database.
- Now store the end time for the encryption of the image which was taken in the path.
- Encrypted points are append in a list and name it as a particular database.
- Now store the names along with encrypted database in a list.

PATTERN MATCHING:

- Extract image from sensor and a name if required.
- Then match it with a existing database.

DECISION MAKING:

- Then check if a pattern is matched or not.
- if it is matched then user can access else cannot access.

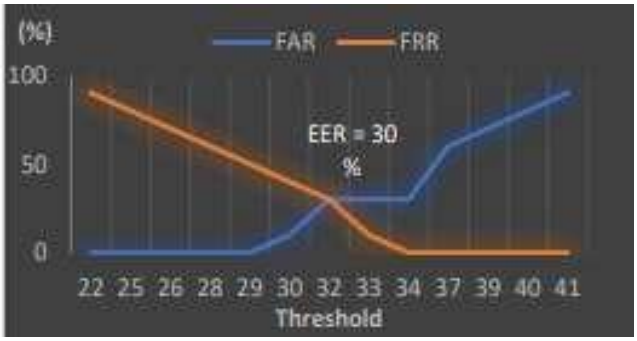

Fig 3: FAR-FRR graph of the fingerprint authentication

IMPLEMENTATION OF HOME AUTOMATION AND SECURITY:

The main part of the home automation system based on IoT is the microcontroller. A node microcontroller unit (Node MCU) Wi-Fi-based controller board is an opensource platform for IoT applications and is used as the main microcontroller in this. Node MCU is basically used to gather data obtained by sensors as shown in fig.4 and uploads the data to the IoT server. In addition, this microcontroller receives commands given by users via smartphones/laptops to perform specific tasks.

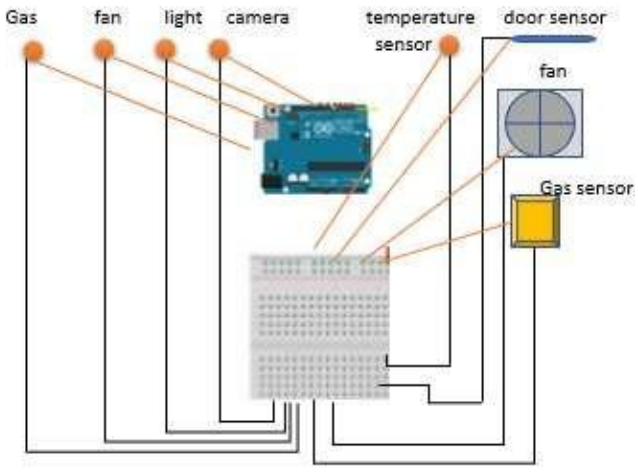

Figure4: circuit diagram

Smart Home System Algorithm

1. **if** motion sensed by the sensor
2. **then**
3. turn ON Light
4. **else**
5. keep sensing
6. **end if**
7. **if** gas value greater than or equals to 1050 **then**
8. start Alarm
9. **else**

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 6, Issue 5, May 2021

10. keep sensing
11. **end if**
12. **if** electromagnetic door sensor lost the line-of-sight connection for 30 sec **then**
13. start Alarm
14. **else**
15. keep checking
16. **end if**
17. **if** temperature less than or equals to 24 **then**
18. turn ON Fan (speed of fan increased with the increase in temperature)
19. **end if**

end if

Node MCU consists of a physical programmable circuit board similar to any other development board such as Arduino or Raspberry Pi as shown in fig 5. Node MCU can be programmed on Arduino software, which is an (IDE) integrated development environment (which provides programs for software development) to write the instruction codes and uploads them to the microcontroller.

Figure 5: LCD display and Real time load

Figure 6 shows how enabled home security system provides low-cost open-source hardware components like the Arduino and Raspberry Pi MCU boards and a combination of sensors. Passive Infrared sensors are used to detect motion and can work in sync with a webcam that captures images to alert users of trespassing.so, that it can make possible for the users of household to view when a particular door has been opened.

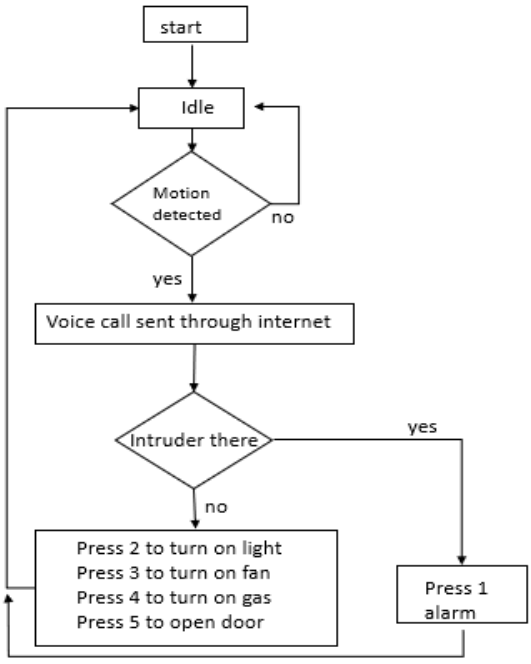

Figure 6: Flowchart of home security system

An advanced form of smart home automation system is the use of gadgets to access and control all home appliances and sensors. The commonly used gadgets are developed as mobile apps on top of operating systems of smartphones, such as Android or as web-based dashboards integrated to open-source IoT platforms. With the aid of IoT cloud computing servers, all data obtained from sensors are aggregated and analysed to become valuable information for addressing specific requirements when they are uploaded to the server. All data can be used to display the reading patterns in terms of graphs and detect possible occurring problems and provide recommendations or alert the user.

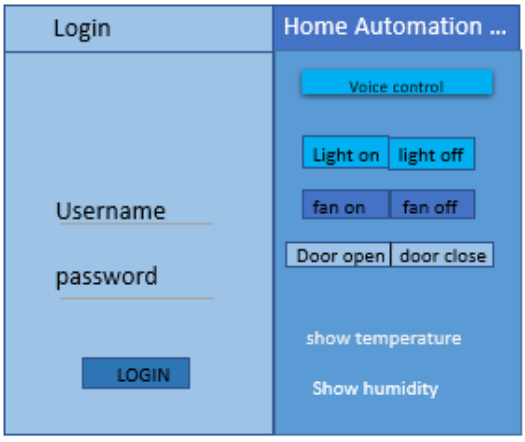

Figure 7: software application at user side in mobile/laptop

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 6, Issue 5, May 2021

Implementation of Health Monitoring System:

The WISE system contains three fundamental components which are the WISE body area network (W-BAN), the WISE cloud (W-Cloud), and the WISE Users. The WISE is developed based upon Arduino sensor platform integrated with the required sensor nodes. Firstly, a portable RFID reader is connected to the Arduino platform, which facilitates the identification of different users, thus a RFID tag should be amounted to each individual user. WISE is also empowered with a Wi-Fi module, which enables the transmission of the data to the cloud and then allows the authorized users to access the real-time data from anywhere at any time. The identification and accurate diagnoses of a potential disease often require a certain amount of historical data; therefore, a cloud database is established within the WISE-Cloud to store the sensor data from the WISE-BAN for each individual user. The implementation of the WISE-Cloud is based upon a HTTP server and a storage server that of the MySQL database. Authorized users can log in to the cloud server

to visualized the data from the web. All users must register with WISE via the GUI displayed before accessing the data.

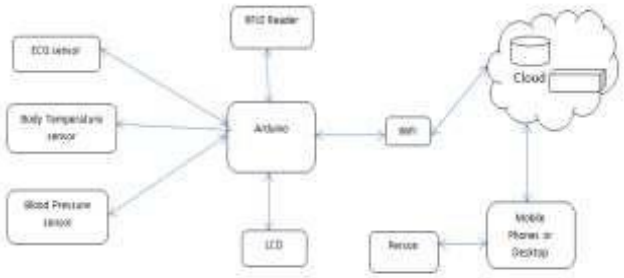

Figure 8: Architecture of the WISE System

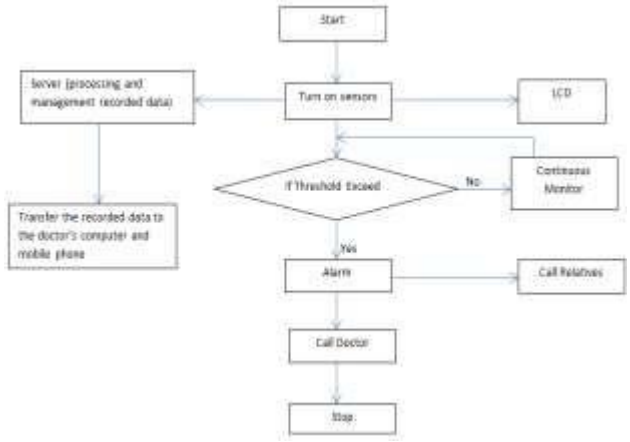

Figure 9: Flow graph to illustrate possibilities offered by IOT in HCMS

IV. RESULTS

In this paper IOT based biometrics is proposed. We use Raspberry PI integrated with sensor nodes for testing of the prototype. In biometric systems, the accuracy rate of the system is calculated by drawing a FPR - TPR. Along with the changing threshold value, FPR and TPR amounts also change by a trade-off with each other. This system gave the most optimum performance. According to this system, users who want to log into IoT will be able to enter the system with fingerprint authentication, thus ensuring the security and privacy of IoT.

An IoT based algorithm is proposed for the smart home system to automate the Fan, monitor the gas leakage and notify by means of an alarm, intrusion detection and energy monitoring. The proposed algorithm was practically implemented on Arduino for the testing purpose. The result shows that, the algorithm is capable to observe the motion of a human being, to observe the intrusion by monitoring the line-of-sight communication between door and senor. The temperature and power consumption are monitored on a web page globally and can be monitored and controlled being away from home. Simulation results show that, the system is efficient and cost effective in terms of providing reliable information and automation. In future, this work can be to implement in a real-world home to automate it as smart home.

Whenever the device is attached to patients' body, reading of the parameters are displayed for the doctors, patients, and person itself. If the reading goes beyond the threshold value, an alert signal will be given to all the connected people related to that particular person through this model. When one need to access the data they need to register through the GUI displayed for patients confidential information

V. CONCLUSION

Biometric technology is mainly popular for identity authentication or verification in highly secure environment. Biometric-based security systems are becoming popular day by day. The change is exponentially increasing. The first challenge is the cost of biometric technology. There are some reasons for increasing cost of biometric technology like hardware maintenance, processing power for databases, experimental infrastructure and others. Multimodal biometrics is the next logical step in biometric authentication for consumer-level mobile devices. The challenge remains in making multimodal biometrics usable for consumers of mainstream mobile devices, but little work has sought to add multimodal biometrics to them.

This paper presents an architecture that can be used as framework to build a low-cost smart home and security

system. Using affordable components such as microcontrollers, sensors and RF signals as a communication channel between the devices, it is possible to develop an IOT system that allows user of a household to view when a particular door is opened or any critical situation takes place.

A need for real-time health and activity recognition with wearable sensors is a prerequisite for assistive paradigms. The system introduced smart healthcare to monitor the basic important signs like heart rate, body temp and blood pressure Although the system looks somewhat bulky, it will be a tiny device by proper manufacturing in the near future the video feature can be added for face-to-face consultation between the doctors and patient's future.

REFERENCES

[1] Mohammad S. Obaidat, Soumya Prakash Rana, Tanmoy Maitra, Debasis Giri, and Subrata Dutta, "Biometrics security and Internet of Things", Biometric-Based Physical and Cybersecurity Systems, pp.98734-98739, 2019.

[2] G.I. Davida, Y. Frankel and B.J. Matt,"Fingerprint based biometrics authentication in IoT for resolving security challenges", International Journal of Research and Analytical Reviews, pp.2349-2354, 2019.

[3] Manjur Kolhar, Fadi Al-Turjman, Abdalla Alameen, and Mosleh M Abualha, "A three layered decentralized IoT biometric architecture for city lockdown during covid-19 outbreak", Special section on emerging deep learning theories and methods for biomedical engineering, IEEE Access, vol. 8, pp.163608-163617, 2020.

[4] Shobhan Mandal, Basudeb Bera, Anil Kumar Sutrala, Ashok Kumar Das, Kim-Kwang Raymond Choo and Youngho Park "Certificateless-Signcryption-based three-factor user access control scheme for IoT environment", IEEE Access, IEEE Xplore, vol. 7, pp. 3184-3197, April 2020.

[5] Li Lu, Jiadi Yu, Yingying Chen, Linghe Kong, Yanmin Zhu, Hongbo Liu,"Lip reading-based user authentication through acoustic sensing on smartphones", Transactions on Networking, IEEE,vol. 27, pp. 447-460,2019.

[6] Mikhaial Gofman and Sinjini Mita, "Multimodel biometrics for enhanced mobile device security", Communications of the ACM 59(4):58-65, ACM,2016.

[7] Waheb A. Jabbar, and Tee Kok Kiran, "Design and fabrication of smart home with internet of things enabled automation system", IEEE Access, vo. 7, pp. 144059-144074, 23 September 2019.

[8] Parth Thakar and Mohit Pant, "Smart home using android", International Conference on Trends in Electronics and Information (ICOEI), IEEE Xplore, 2018.

[9] Jahid Hasan and Shahin Alom, "Wireless home automation system using IoT and paas", International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), IEEE Xplore, 2019.

[10] Urvi Singh and M. A. Ansari, "Smart home automation system using internet of things", International Conference on power energy, environment and intelligent control(PEEIC), IEEE Xplore, 18 October 2019.

[11] Poonphone Suesaowaluk, "Home automation system based mobile application", 2020 the 2nd World Symposium on Artificial Intelligence, IEEE Xplore, 22 July 2020.

[12] Md. Mohaiminul Islam, Md. Nahiyan Farook, "Design and implementation of an IoT based home automation", International Conference on Advanced in Science, Engineering and Robotics Technology (ICASERT), IEEE Xplore, 2019.

[13] Wan, J., A. A. H. Al-awlaqi, M., Li, M. et al."Wearable IoT enabled real-time health monitoring system", EURASIP Journal on Wireless Communications and Networking, 22 December 2018.

[14] Islam, M.M., Rahaman, A.and Islam, M.R, "Development of smart healthcare monitoring system in IoT environment", SN COMPUT. SCI. 1, 14 May 2020.

[15] Kadhim, K.T., Alsahlany, A.M., Wadi, and S.M. "An overview of patient's health status monitoring system based on Internet of Things (IoT)", Wireless Pers Commun 114 , pp.2235-2262, 15 May 2020.

[16] D. S. R. Krishnan, S. C. Gupta and T. Choudhury, "An IoT based patient health monitoring system," International Conference on Advances in Computing and Communication Engineering, IEEE Xplore, 2018.

[17] N. Gupta, H. Saeed, S. Jha, M. Chahande and S. Pandey, "IoT based health monitoring systems," 2017 International Conference on Innovations in Information, Embedded and Communication Systems(ICIIECS), IEEE, 17-18 March 2017.

[18] Z. b. S. A. Brashdi, S. M. Hussain, K. M. Yosof, S. A. Hussain and A. V. Singh, "IoT based health monitoring system for critical patients and communication through think speak cloud platform," 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), IEEE Xplore, 2018