World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.924

A SYSTEMATIC APPROACH TO AN IOT BASED DOOR ANSWERING SYSTEM

Aishwarya S.* and Dr. Kamalraj R.

Department of MCA, Jain Deemed-To-Be University, Bangalore, India.

Article Received on 31/12/2021 **Article Revised on 21/01/2022** **Article Accepted on 11/02/2022**

***Corresponding Author**
Aishwarya S.
Department of MCA, Jain Deemed-To-Be University, Bangalore, India.

ABSTRACT

All around the world, home automation has become the epicenter of convenience and security. One of the most important parts of home automation is automating the door answering process. Failure risk, reliability, and incurred expenses are only a few of the issues that have arisen as a result of the inefficient smart automation process. We've seen a lot of models and strategies developed to improve the efficiency and security of the door answering process. This system takes a more central approach, resulting in a system that is efficient, dependable, secure, and moderately less expensive. A person approaching the end-user's home where the IoT module is embedded on the front door, the recorded facial image, is then sent to the server and returned to the end-server application to execute an authentication procedure to determine if the person is who they say they are. The backend server application will perform an authentication process to determine whether or not the image has been saved in the database. If the authentication procedure is successful, a token is raised, and a random secret code or key of a specified length is generated. The secret code and image will then be transferred to the database, which will cause a notice to be delivered to the client device. Following that, if the customer decides to accept the request, they can provide the secret code/key to gain entrance to the house. Key Words-PUF, AIoT, DNN.

INTRODUCTION

After Xiaomi, a global market leader in smart devices released a survey on January 6, 2021, which revealed that an overwhelming consensus of 82% consumers agree that there are significant advantages of having smart devices in the house. And according to a survey, there

were around 24,000 home invasion robbery cases that were reported in 2021 in India. With the aforesaid statistics, one cannot set aside the advantages that a door answering system brings to one abode. The outline of the paper is as follows – Section 2 sheds light on the problem statement, followed by section 3 which discusses the proposed solution, section 4 about discussions and recommendations in section 5. And finally, Conclusion and references in sections 6 and 7respectively.

Problem Statement

The current IoT-based door answering system uses IoT based sensors to enable and run key-less entry devices, which allow users to unlock doors remotely using a smartphone or other internet- connected device. Variety in the used sensors, processes don't elevate the level of efficiency in these systems.

The following are some of the major factors to be considered concerning the door answering process:

i. Security
ii. Accessibility and validation
iii. Expenditure.

Security: The ability to unlock doors without a physical key and to be able to share virtual keys isitself the major security issue in the existing system. The sharing of virtual keys must be done with extreme caution. Because if not, the system is vulnerable to a high-level security compromise.

Accessibility: Not anyone and everyone should be given the virtual keys to gain access for enteringpurposes.

Validation: The process of validating an entry to the house must be done rigorously.

Expenditure: Home security devices are not easy spending. And if a customer invests in an in- efficient door answering system, it will burn the client’s investment. A state-of-the-art system willcost a fortune, which again not everybody can afford.

Thus, a system, ensuring maximum efficiency at a relatively lesser cost wherein the quality and security measures are not compromised needs to be administered.

Proposed Solution

The proposed solution to the above-mentioned problem is an IoT-driven door answering system honed to create an efficient and secured system. This system allows clients to carefully monitor their house [remotely too].

First is the IoT module comprising of an Arduino board, GPS Module, Camera Module, Wi-Fi Module, Motion sensor, Keypad module modeled and attached to the front door. Arduino codingis hassle-free which makes it easy to couple the sensors and other associated modules very easily.Secondly, the system requires a server. The server will have a back-end application running, whichwill run authentication against the images captured, and if the authentication gets a positive hit, itwill then continue to generate a secured key and pass it on.

Thirdly, the system is linked to a database, which records all of the photos acquired by the camera module and allows the server perform authentication checks on them. It will also receive the servergenerated protected key.

Last, the client's smartphone will be equipped with a mobile application, that is in turn connectedto the database. This application will receive alerts from the database during a real-time change inthe environment. This mobile application provides many functionalities to the client like sign-up,login, register users, access feeds, share secured key / secret code, send emergency alerts. JavaScript can be used to create the front-end of this application. For front-end application development, JavaScript is the most utilized language. Java code may now be ported to iOS in a variety of ways, including Codename One, Gluon, and others. As a result, java may be used to create apps for both Android and iOS. Setting the logic of the back end is just as important as writing the front-end, from performance to database interfaces. PHP can be used to code the backend of this application. PHP works seamlessly with Windows, Unix, and Mac.

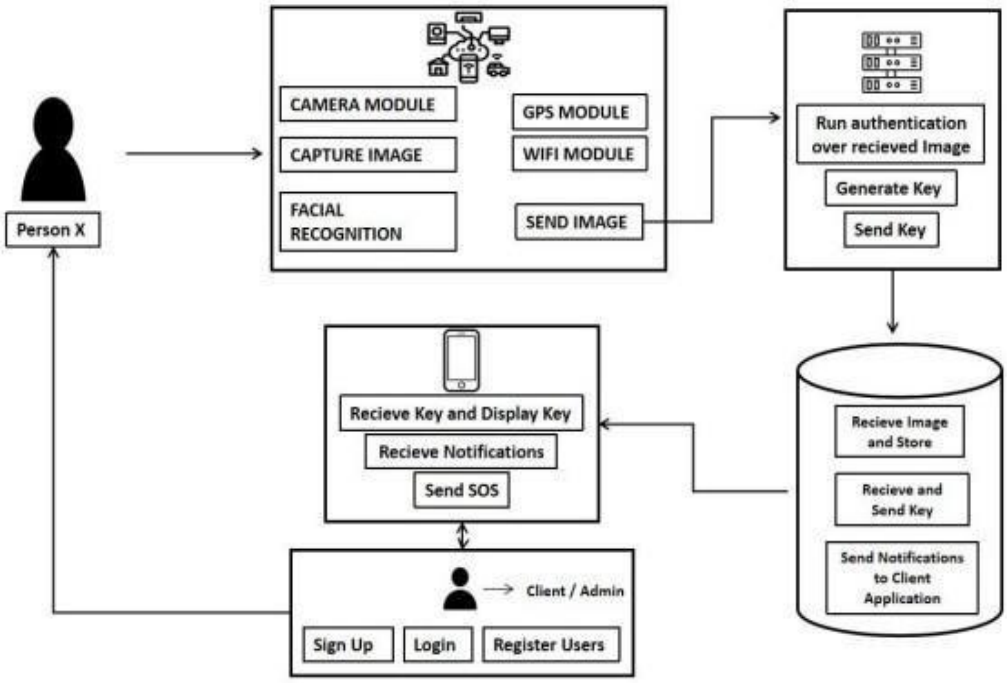

Fig. 1: System architecture.

Literature Study

In this section, we will discuss and review recently published papers respective to the proposed system.[1] In this paper published in 2020, the authors discuss the two types of techniques that are currently being followed in face recognition patterns. The two methods are the Eigen Face method and the Fisher face method. Principal component Analysis [PCA] is used in the Eigen faceapproach to reduce the face dimensional space of the facial features. They mainly talk about how to use digital image processing to build a face recognition system.

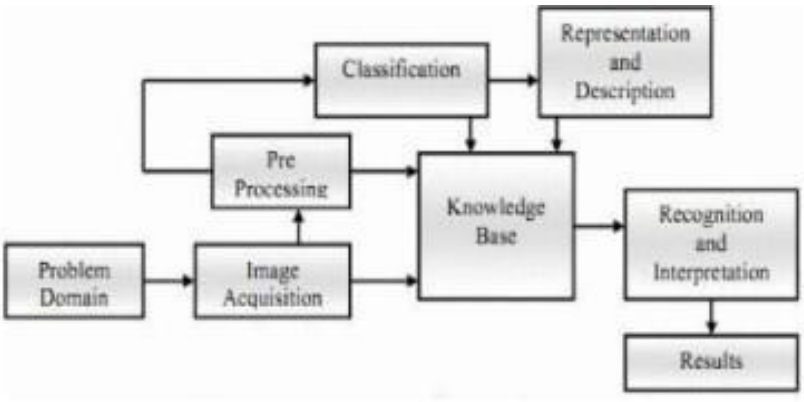

Fig. 2: Fundamental steps in digital processing.

[2]In this paper published in 2019, the authors take a note of how to design and implement a

remote deep face model face recognition system based on the NB-IoT module and sbRIO FPGA Platform. They talk about how still conventionally high-definition picture needs to be transmitted back to the PC for processing and how the low bandwidth, low-capacity, low-processor scene face recognition problem is still not solved. Considering all this, they have combined embedded FPGA technology with low-powered narrow-band communication NB-IoT module to form a narrow bandwidth application framework. FPGA stands for field programmable gate array and is a micro-controller like device. Rather than running a software application, when programmed an FPGA, it rewires the device itself to implement the functionality. NB-IoT, Narrow-band IoT is for M2M and IoT devices and applications requiring wireless transmission over a more extended range using little power for long battery lives. Using the DNN based with graphic FPGA programming, the front face recognition of the deep face model and extraction of 7 layers DNN convolution result is performed on the chip. The categorized data is then sent back to the local server via NB-IoT remote transmission for comparison using the CoAP protocol, and the face recognition task is accomplished.

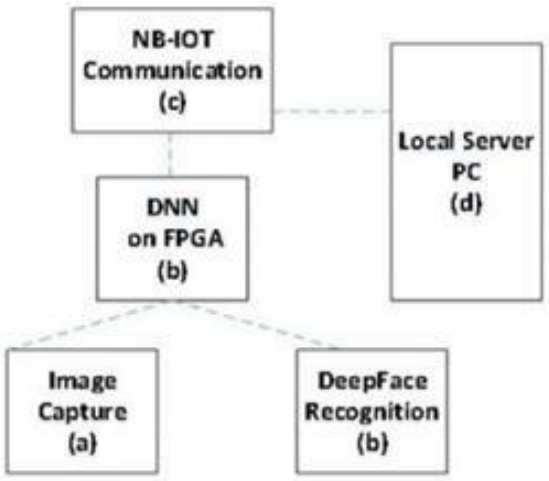

Fig. 3: Basic system function model.

[2]In this paper published in 2019, the authors talk about Image and face recognition using CV Lens machine learning which they have implemented in a mobile application. The center area of the paper is using Google lens to process images and navigate search. The system uses a Google lens to process the image into text, translate, navigate, and then search the text. Two key modules, TEXT and IMAGE are used to process the image. TEXT module contains OCR, translation maps, related images. IMAGE module contains face emotions and image recognition. Face emotion detects a face and reveals one's reactions such as happiness or sadness etc.

Fig. 4: Extraction of text from the image.

Recommendations

The future is always in a flux state. More features are likely to be added to the planned system.

- PUF &
- AioT

PUF: Physically unclonable functions, or PUF have emerged as a viable lightweight alternative to classical encryption for authentication. By combining IoT devices with PUF technology, the chipwill offer an internal flash option. It's used to safeguard IP addresses and bogus data.

AioT: Facial recognition combined with AioT expands on existing use cases. The merging of artificial technologies with internet of things infrastructure to enable more efficient IoT operationsis known as artificial intelligence of things, or AioT. Facial recognition becomes a compelling usecase for businesses and consumers when paired with AioT.

CONCLUSION

Nobody can deny the fruitful outcomes of technology. Technology has made our present more convenient, reliable, fun, and so on. The majority of our days are now heavily reliant on technology. The objective of this project is simple, to expand the touch of IoT, in Possible and viable ways. One that preferably makes it easy for us in our human life. Gone are the days, when humans were more dependent on other humans be it food, security, etc. The "technological era" has now given way to the "Artificial intelligence" era. This is how far we have come in the last few decades. This project can help the community be a much safer place and not burn customers' pockets to the extent where they might look away. By being ethical and more responsible, the system can prove to be very efficient by not putting the client's data into jeopardy.

REFERENCES

1. G.Singh and A. K. Goel, "Face Detection and Recognition System using Digital Image Processing," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2020; 348-352. DOI: 10.1109/ICIMIA48430.2020.9074838.
2. "L. Peng, Z. Xin, and G. Ping, "Design and Implementation of Remote Deep Face Model Face Recognition System based on sbRIO FPGA Platform and NB-IOT Module," 2019 2nd International Conference on Safety Produce Informatization (IICSPI), 2019; 505-509. DOI: 10.1109/IICSPI48186.2019.9095951."
3. "C.N. Vanitha, V. N. Jeevaa and S. P. Shriman, "Image and Face Recognition using CV Lens Machine Learning Android Application," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019; 972-975. DOI: 10.1109/ICACCS.2019.8728435."
4. "J.R. Paone et al., "Double Trouble: Differentiating Identical Twins by Face Recognition," in IEEE Transactions on Information Forensics and Security, Feb. 2014; 9(2): 285- 295. DOI: 10.1109/TIFS.2013.2296373."
5. "R. Prema and P. Shanmugapriya, "A review: Face recognition techniques for differentiating similar faces and twin faces," 2017 International Conference on Energy, Communication, Data Analyticsand Soft Computing(ICECDS), 2017; 2899-2902. DOI: 10.1109/ICECDS.2017.8389985."
6. U. Park and A. K. Jain, "Face Matching and Retrieval Using Soft Biometrics," in IEEE Transactions on Information Forensics and Security, Sept. 2010; 5(3): 406-415. DOI: 10.1109/TIFS.2010.2049842.
7. Agarwal, A. Agarwal, and G. Misra, "Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I- SMAC), 2019; 629-633. DOI: 10.1109/I- SMAC47947.2019.9032629.
8. Samuel Manoharan, "Image Detection Classification and Recognition for Leak Detection in Automobiles", Journal of Innovative Image Processing (JIIP), 2019; 1(02): 61-70.
9. Md. Khalid Rahmani, M.A. Ansari, and Amit Goel, "An efficient indexing algorithm for CBIR", Proceedings - 2015 IEEE International Conference on Computational Intelligence and Communication Technology CICT, 2015; 73-77.
10. Junjue Wang, Brandon Amos, Anupam Das, Padmanabhan Pillai, Norman Sadeh, and Mahadev Sathyanarayanan, "Enabling Live Video Analytics with a Scalable and Privacy-Aware Framework", ACM Transactions on Multimedia Computing Communications and

Applications (TOMM), 2018; 14(3s): 64.

11. Y Taigman, M Yang, M Ranzato, et al., "Deep Face: Closing the Gap to Human-Level Performance in Face Verification[C]", Conference on Computer Vision and Pattern Recognition (CVPR), 2014.
12. Home Automation & Wiring (1 ed.). New York: McGraw-Hill/TAB Electronics, 1999-03-31.ISBN 978-0-07- 024674-4.