An Internet of Things-based House Monitoring System

Douglas Korgut
Electronic Engineering/DAELN
Federal University of Technology - Paraná (UTFPR)
Curitiba, Paraná, Brazil
Email: douglaskorgut@alunos.utfpr.edu.br

Daniel Fernando Pigatto
CPGEI/DAELN
Federal University of Technology - Paraná (UTFPR)
Curitiba, Paraná, Brazil
Email: pigatto@utfpr.edu.br

***Abstract*—The Internet of Things has become one of the most important examples of ubiquitous computing. The basic idea of this concept is the pervasive presence of a variety of devices or objects that are able to interact with each other and cooperate with their neighbours to reach common goals. A house monitoring application using facial recognition can benefit from the high connectivity of an IoT environment and produce better results at lower costs. Furthermore, the IoT system may also have its security improved by applying a monitoring system, helping to control who physically access environments and houses. This ongoing research paper presents an innovative system that unites all the aforementioned characteristics and provides a flexible, multi-platform way of accessing the monitoring system. Promising results are expected by the end of this research.**

***Index Terms*—Image Recognition, Internet of Things, Security, Smart Home**

I. Introduction

Notable discussions and publications on the Internet of Things concept have been taking place recently, changing the way we look at old applications and originating completely new ones that we might not know we needed. The main characteristic of an IoT-based environment is its high connectivity with surrounding elements and other services available through the Internet. That is the case of smart environments like houses, cars, buildings and others. There are new applications provided by the Internet of Things that should keep improving people's daily tasks in next years.

The surveillance and monitoring of a house or a commercial environment is crucial for privacy, safety and basic or advanced access control. Moreover, the association of well-known facial recognition techniques with high speed connectivity, ubiquitous environments allows the creation of more accurate, low-cost systems for monitoring. Based on that, this project proposes an IoT-based system to control personal access to environments via facial recognition and a complete, flexible range of interfaces to interact in real time with the features provided by the system.

The remaining of this paper is organised as follows: section II addresses IoT concept in details and its inherent security issues; section III provides an overview on how the monitoring system of this ongoing research project is modularised and implemented; section IV details hardware modules; section V details software parts; and, finally, section VI concludes the paper, highlighting the future steps.

The present work was carried out within the scope of the Institutional Program of Volunteer in Scientific and Technological Initiation of the Federal University of Technology - Paraná – UTFPR/Brazil.

II. Internet of Things and Security Issues

The Internet of Things (IoT) has been widely discussed in publications in the field of Computer Networks over the last few years, however it still lacks of a more assertive, well-accepted definition. IoT can be generally described as a large amount of everyday objects pervasively integrated in the environments around us, equipped with identifying, sensing, networking and processing capabilities, and able to communicate among themselves in order to complete common tasks [1][2]. As a consequence, it becomes a very distributed network system composed by entities that both provide and consume data from the physical world through sensors and actuators [3]. In fact, there is a vast range of IoT-based applications e.g. health-care, smart environments (smart homes, farms, cars, or cities), environmental monitoring, and disaster alert and recovering [1][2][4][5][6].

The merge of IoT with cloud computing provides easy access to virtually unlimited processing and storage capabilities on demand and at a low cost, enhancing IoT scalability and performance [4][7]. In fact, the amount of challenges linked to IoT is unsurprisingly big. Besides the fact that interoperability, scalability, the lack of standardisation, and the need for a proper integration with the cloud are utterly challenging subjects, there are also the issues related to security and safety e.g. the lack of data sharing policies, trust, and privacy [3][8].

III. An IoT-based House Monitoring System

To fulfil a growing necessity of constant monitoring of houses and commercial places, and have a full awareness of who left and entered these environments, this project presents a low cost monitoring system that can identify through facial recognition people who have been detected around the house by strategically positioned cameras. The main idea is to build a secure, responsive and functional mobile and web platforms, that allows the user to directly interact within the environments where the system is installed.

The project was built and based on several Raspberry Pi boards and their camera modules. Thus, it is possible to make it available to the user a live stream of the cameras placed throughout the environment, and also an online dashboard of pictures and videos of people who have been recognised by the facial recognition platform. The main idea is based on the fact that the user can register people by uploading their face pictures both via the web platform, and capturing directly from the smartphone camera provided by the mobile platform. Notifications about new recognised people will be delivered as smartphone notifications according to a preconfigured setting. The platforms will give the user options for recording videos from a specific camera, taking pictures, and remotely saving these image files in a real time database or even locally on the smartphone or computer.

The system provides an end-to-end solution which can be modularised in in four main steps: i) collect data, ii) send this data to a cloud service, iii) process collected data, and finally, iv) present data as a result to the user (Figure 1). The first step is performed by the cameras connected to the Raspberry Pi, which is connected to the internet, then being able to send the images to the cloud service. The live streaming is processed by a server to execute the face recognition. After that, the system sends a notification alert to the owner (main user) if there is any unauthorised personnel detected by the cameras. The notifications and alerts can be disabled at anytime by the user, and can be configured to only carry out the people flow control, registering everyone who has been detected. All described events are available for visualisation on the platforms dashboard.

IV. Hardware Elements

A. Raspberry Pi

Following the fact that Raspberry Pi and other platforms are now equipped with Wi-Fi modules, a new series of Open Source technologies started to be developed, combining the processing power of a personal computer, the communication and multimedia available with Web related technologies, the ability of interacting with general environments through processors and microcontrollers, and the portability of mobile devices. Such integration provides a very important scenario, allowing developers to create cheap and functional IoT systems.

Regarding hardware, as this project does not demand actuator modules, none of the GPIO (general-purpose input/output) pins were used as input or output. The online interface used is the Camera Serial Interface (CSI), which permits the collection and transmission of all captured images as a live stream.

B. Cameras

To record the live-streams, a Raspberry Pi camera module (refer to Table I) was used. This choice was based on the good quality that it can deliver, and its cheap cost. The Raspberry Pi camera module uses basically the same hardware that is used in the most moderns smartphones available on the market, and even not being a plug-and-play camera, it is easy to use given the good amount of online available libraries and platforms which already do the hardware-side configuration.

TABLE I
Raspberry Pi camera module configuration [10].

Camera specifications	
Sensor	5MP OV5647
Image resolution	2592x1944
Video	1080p, 30 fps with H.264 codec (AVC)
Board size	25 x 24 mm
Interface	CSI (Camera Serial Interface)

V. Software Elements

A. Node JS

According to the official website [11], Node.js is a JavaScript runtime built on Chrome's V8 JavaScript engine which uses an event-driven, non-blocking I/O model that makes it lightweight and efficient. It enables JavaScript to be used for server-side scripting, and runs scripts server-side to produce dynamic web page contents before the page is sent to the user's web browses. This allows web applications development to unify around a single programming language, rather than rely on a different language for writing server side scripts.

B. Mobile Platform

For iOS, the platform was entirely developed using the Apple programming language known *Swift*. Open Source modules for the Websocket implementation and the real time database interaction (Firebase) were used to implement transmission and data acquisition among platforms and cameras.

On the other hand, considering the popularity of Android operational System, a Java platform-based solution was created with the same functionalities and interface as the ones found in iOS platform. In fact, allowing the same experience in both platform results in better homogeneity among system applications.

C. Web Platform

For the Web Platform development, four main Frameworks were used: Firebase, Node JS, Express and Bootstrap.

As there was a requirement on the system implementation for a technology to allow the users to update their data throughout the platforms at the same time, the use of HTTP protocol became unfeasible. To overcome that, WebSockets protocol was used, allowing the browser and other platforms (mobile apps) to receive updates with no user requests, as shown in Figure 2 [9].

Regarding the user interface (see Figure 2), the user will be able to see images provided by cameras through a simple and responsive interface, where the first contact between the platform and the user is made by a Login or Register page. Once registered, the user can access the platform, all the cameras and the dashboard. The user will also be able to go through all the cameras installed, and utilise platform

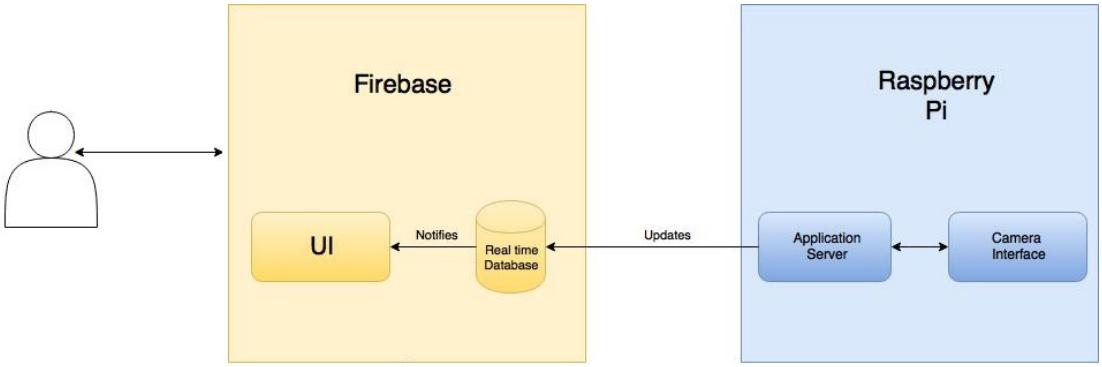

Fig. 1. System Architecture (Adapted from [9]).

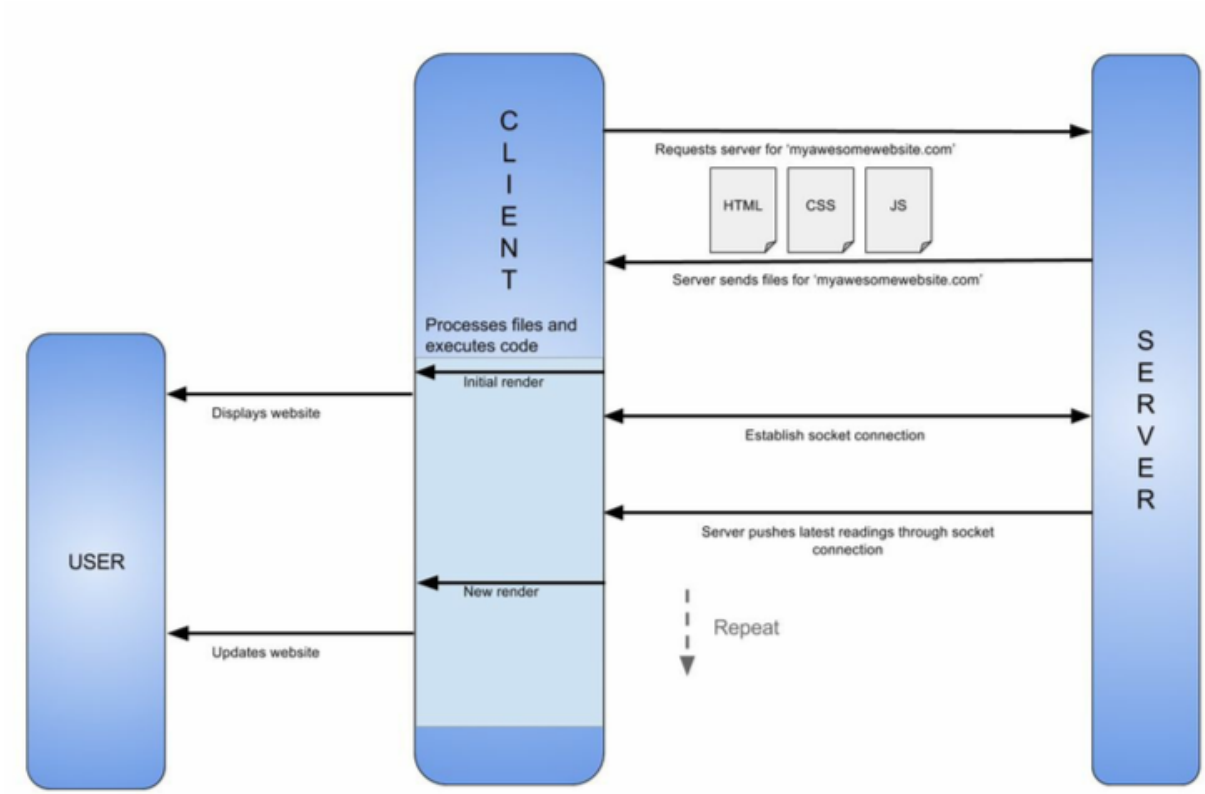

Fig. 2. Websockets engine on client-server connection [9].

functionalities to verify and record images. Another available feature is the possibility of storing all the data related to a period when a detection has been made by the Facial Recognition Algorithm. There will be the option of storing such data (images, videos, detection time and date) in the user's own devices, in a database, or just discard in case the information is considered not useful.

D. Facial Recognition

Facial recognition is based on geometric characteristics of a determined face. The Eigenfaces method is the algorithm used by OpenCV, which was developed to provide more efficient results for this operation, and also for being computationally less expensive. The method is based on a mathematical procedure called PCA (Principal Component Analysis). Eigenfaces and PCA were used by Sirovich and Kirby to represent images more efficiently [12]. The PCA goal is to replace the correlated vector of larger dimensions for non-correlated vectors of smaller dimensions. Another goal is to calculate a basis for the set of data that is being analysed. The main advantages of PCA are low sensibility to noise, reduced necessity of memory to execute all the computational math, and increased efficiency due to smaller dimensions in calculations [13].

As described by [14], "the strategy of the Eigenfaces method

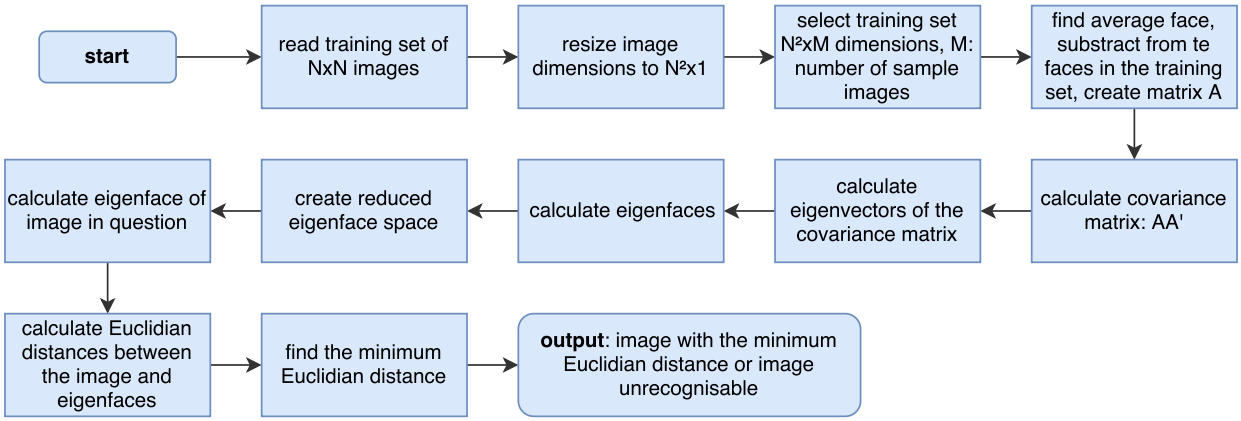

Fig. 3. Eigenfaces Algorithm Flowchart (Adapted from [14]).

consists of extracting the characteristic features on the face and representing the face in question as a linear combination of the so called 'eigenfaces' obtained from the feature extraction process. The principal components of the faces in the training set are calculated. Recognition is achieved using the projection of the face into the space formed by the eigenfaces. A comparison on the basis of the Euclidian distance of the eigenvectors of the eigenfaces and the eigenface of the image under question is made. If this distance is small enough, the person is identified. On the other hand, if the distance is too large, the image is regarded as one that belongs to an individual for which the system has to be trained." The complete algorithm flowchart can be seen in Figure 3.

VI. Conclusion

The relevance of Internet of Things in our daily lives is becoming greater everyday. The lack of privacy, security and safety also increase as more sensitive information is exchanged throughout small devices. This paper has presented an innovative, flexible system for house monitoring which is still in development. Most of the modules that integrate the system are already functioning, and the cost and information security have been considered since the beginning of the project.

Despite being an ongoing project, one can point out that the system will be affordable by most home and commercial users, robust enough to allow the user to monitor who access their target areas, and be flexible to interact with (web and mobile platforms). Furthermore, it is an example on how a monitoring system can be integrated to the Internet of Things and provide benefits to smart environments that need a solution to control authorised personnel.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010, ISSN: 13891286.

[2] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things A Survey of Topics and Trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, 2015, ISSN: 1387-3326.

[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, ISSN: 15708705.

[4] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016, ISSN: 0167739X.

[5] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, "Iot-based smart cities: A survey," in *16th International Conference on Environment and Electrical Engineering (EEEIC) June 7-10, 2016, Florence, Italy*. IEEE, Jun 2016, pp. 1–6, ISBN: 9781509023202, URL: http://dx.doi.org/10.1109/EEEIC.2016.7555867 [accessed: 2016-09-14].

[6] R. Kumar and A. Pandey, "A Survey on Security Issues in Cloud Computing," *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, vol. 2, no. 3, pp. 506–517, 2016, ISSN: 2394-4099.

[7] E. Cavalcante, J. Pereira, M. P. Alves, P. Maia, R. Moura, T. Batista, F. C. Delicato, and P. F. Pires, "On the Interplay of Internet of Things and Cloud Computing: A Systematic Mapping Study," *Computer Communications*, vol. 89-90, pp. 17–33, 2016, ISSN: 01403664.

[8] J. A. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014, ISSN: 2327-4662.

[9] S. Kamani, *Full Stack Web Development with Raspberry Pi 3*. Packt, 2017.

[10] Pi Supply, "Raspberry Pi Camera Board v1.3." [Online]. Available: https://www.pi-supply.com/product/raspberry-pi-camera-board-v1-3-5mp-1080p/

[11] Node.js, "Node.js." [Online]. Available: https://nodejs.org/en/

[12] M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces," in *Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Jun 1991, pp. 586–591.

[13] P. Y. V. Lata, C. Kiran, B. Tungathurthi, H. R. M. Rao, a. Govardhan, and L. P. Reddy, "Facial Recognition using Eigenfaces by PCA," *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp. 587–590, 2009.

[14] M. Çarkç and F. Özen, "A Face Recognition System Based on Eigenfaces Method," *Procedia Technology*, vol. 1, pp. 118–123, jan 2012.