Smart Home Powered by Social Network for Citizen Security

Víctor H. Benítez, Gustavo C. Soto, Luis C. Félix-Herrán, and Jesús Pacheco

***Abstract*—Nowadays, the Internet of Things is used to transfer information from human to human and from human to machine. In this paper, we propose the use of IoT platforms to link those homes that are equipped with IoT capabilities, in order to increase security and prevent from a crime to a fire, and even monitor health status of a person. Using a microcontroller, it is possible to send information to a cloud server capable of sharing this information with other households connected to the platform, as well as allowing linking this data to one of the most used social networks in the world: Facebook. Linking smart homes with social network, allows to consult the status of sensors and IoT devices empowering citizen security against crime, violence and events that could put the integrity of people at risk both in their property and their health. The study is carried out for a particular region of Latin America, given its high rates of violence against citizens that have occurred in recent years.**

***Index Terms*—Security, internet of things, smart home, citizen security.**

I. Introduction

Nowadays it is possible to appreciate the notable increase of human dependence on technology and the need to be connected to the internet. Having control of different electronic devices at our fingertips generates great comfort for the human being because it satisfies various needs such as making payments for services, making purchases online or simply sending an email from a mobile device [1]. The Internet of Things for some years, came to revolutionize the industry and the possibility of carry out various types of control processes through the Internet, however, the rise of this topic lies in the interconnection of objects of everyday life through the Internet, which has allowed different productive fields such as smart industry, the smart city, means of transport and logistics, and also the smart home [2]. Nowadays, it is possible to observe how there is a way to track the exact location of a food transport or obtain information in real time of a manufacturing process, in addition to the recognition of activities of daily life and the monitoring of the temperature in home, thanks to the potential offered by the Internet of Things [3]. In this context, the capacities of the IoT are adopted to attend to one of the problems commonly present in Mexican society: Home robbery.

According to the National Citizen Observatory (*Observatorio Nacional Ciudadano in spanish)* [4], The robbery of a house consists of seizing without the consent of whoever that can legitimately grant it of someone else's personal property, in a closed place or in a building, dwelling, apartment or room that are inhabited or intended for room, including not only those that are fixed in the land, but also mobiles, regardless of the material from which they are built.

In the State of Sonora, according to the National Survey of Victimization and Perception of Public Safety. (ENVIPE in spanish), 50,861 crimes were committed during 2018 and 39,759 crimes during 2017, representing a variation of 27.9%, associated with 31,853 victims for 2018 and 31,184 victims for 2017, per 100,000 inhabitants, of which, 13% represents home burglary, which takes fourth place on the state's list of crimes [5].

On the other hand, some of the consequences that this high robbery rate represents have repercussions in the physical, emotional and economic fields, generating an estimated expense of 178,009.049 dollars of which 52.5% represent preventive action measures such as: change or install locks and / or padlocks, change doors or windows, put up bars or fences, carry out joint actions with your neighbors or buy a guard dog; 46.6% represent economic losses as a result of crimes and 0.9% represent expenses as a result of health damage [5].

Due to the numbers and consequences of crimes in the state, the government has implemented various security programs in order to promote prevention and reduce the percentage of crimes. Since 2016, the Citizen Shield program has operated in order to contribute to strengthening the Social Prevention of violence and crime to influence the causes and factors that generate it, favoring community cohesion to strengthen the social tissue through a Comprehensive preventive strategy for Citizen Security from the local level, in coordination with the three levels of government, civil society organizations, and citizens [6].

One of the tools currently active in the state is the "Safe Hermosillo Interactive Map", which allows to track the incidence of crime and their behavior patterns based on the reports generated by citizens when they are victims of robbery. In the event of theft of homes or vehicles, these complaints are generated through telephone assistance to the lines of the state emergency services [7], however, the ENVIPE mentions that 88.1% of crimes are not reported, so

Manuscript received August 20, 2020; revised September 20, 2020.

Víctor H. Benítez, Gustavo C. Soto, and Jesus Pacheco are with the University of Sonora, School of Industrial Engineering, Blvd. Luis Encinas S/N, Hermosillo 83000, Sonora, México (e-mail: vbenitez@industrial.uson.mx, a211200929@unison.mx, jesus.pacheco@unison.mx).

Luis C. Félix-Herrán is with Tecnologico de Monterrey, School of Engineering and Sciences, Blvd. Enrique Mazón López 965, Hermosillo 83000, Sonora, México. (e-mail: lcfelix@tec.mx).

doi: 10.18178/ijfcc.2021.10.1.571

the platform may not have really consistent data.

According to the statistical reports provided by ENVIPE we can infer that the programs are currently not effective enough, since we find a gradual increase in state crimes with a margin of 27.9% and practically zero monitoring due to the fact that 88.1% of crimes are not reported due to loss of time or mistrust in the authority, this has caused some cities to choose to implement a social program called "neighbors watching", which consists of organizing the inhabitants of the area in order to maintain active surveillance 24 hours a day, 365 days a year. However, these social programs are usually not very efficient since a fairly large effort is generated by adding the workload of the day and the activities of daily life.

Therefore, this article adopts the concept of smart home [8], in order to provide Internet of Things capabilities to an entire neighborhood and maintain active surveillance 24 hours a day, 365 days a year, in addition to being an effective proposal to automatically feed the database of the "Safe Hermosillo Interactive Map". References [9], [10] discuss that the smart home concept not only provides the ability to increase security to prevent theft, it would also provide the ability to generate reports regarding the consumption of water and electricity, monitor the vital signs of inhabitants with some type of disease, generate alerts in case of fires, etc., All this information would be sent to a series of microcontrollers installed in the home, which would receive the data from the sensors to organize, classify and present relevant information in a human-machine interface with IoT capabilities; capable of monitoring and controlling household actuators to increase security or respond appropriately to a potential burglary attempt.

II. Related Work

In order to understand the smart home and therefore the proposed concept of Home Social Network that aims to raise the level of security in a neighborhood in the face of the imminence of a house-room robbery, we will begin by defining the characteristics and functions that constitute them.

The home is called smart, when in it, it is possible to find a high level of connectivity between devices that operate inside and outside the home, with the purpose of improving and making the operations carried out in daily life more comfortable. The term "intelligent" is used to transmit acuity or high intelligence, the application of this, on the concept of housing, requires providing those devices to each of the spaces of the property, which allow the inhabitant to carry out an installation that starts from the configuration, to the functioning in an autonomous way and independent of the constant human intervention; These devices are interconnected with each other, making use of the home wireless network, which allows creating a network of devices called the Internet of Things [11]. The internet of things allows devices to collect, send and act on the data they obtain through integrated sensors, in addition to making them visible and making them available on a cloud platform to know their logical state, store and interpret the information and create tasks or events that can be triggered not only locally but also remotely [12].

A smart home with the IoT infrastructure usually has the following main functions:

A. Alert

Through the sensors installed in the home, it is possible to capture the complete environment of each of the spaces, and consequently send alerts to users on the registered device or account. This type of alert contains information on the current state of the environment and can provide data such as: temperature, humidity, presence of fire, movement, air quality, heart rate, etc., the alert can be sent through an application on the device mobile, mail, call or text message and even be published through a social network, all this, programmed to be sent at a time defined by the user.

B. Monitor

The alerts are generated based on the constant monitoring of the spaces in the home, since each activity carried out within the building is monitored and based on this it is possible to take actions or decisions. For example, monitoring the heart rate of a person with heart problems, and sending an alert to various users who can take immediate action in the event that the heart rate falls outside the acceptable range of the patient.

C. Control

Through this function it is possible to program the actions to be carried out based on the information collected by the sensors, on the other hand, it is possible to control different activities such as turning lights on and off, locking or unlocking doors, activating an emergency siren and many more. The user can carry out this function from his mobile device or a computer either in the same place or from a remote location.

The smart home has a diversity of applications as extensive and delimited as the human imagination, however, in this article those applications that increase home security are adopted and are described below:

D. Motion Detection

The main objective of this application is to monitor the activity carried out in the different spaces of the smart home, that is, if the home is empty and the motion detection activated, if there is any movement inside, it generates an alert through the mobile device that indicates that there is a presence of an individual within the space determined by the sensor [13].

E. Gas / Smoke / Flame Detection

This application is used to prevent fires in the home, and is used to alert the user through the mobile application, turn on a siren or even alert the nearest fire station, since through the sensors it is possible to detect if there is a gas leak, either in the kitchen or at the main gas source [14].

F. Vital Signs Detection

This application is useful when you have a user with complications in their health, since it is possible to monitor vital signs such as oxygenation, temperature or heart rate, with this, alerts can be generated in case of abnormalities in vital signs, alerting mainly to the user in charge of the home or to the nearest emergency services [10].

G. Intelligent Light Control

Commonly this application is used to contribute to saving energy in the home, adapting the lighting to the environmental conditions and turning the lights on, off or dimmed according to the user's needs. However, it can also be useful as a home defense protocol by generating a sequence of lights in case of detection of an intruder, in addition to generating the corresponding alert. [12].

III. Materials and Methods

Once the architecture and characteristics of the smart home have been defined, we introduce the concept of Home Social Network. The main idea of this conceptualization lies in providing previously defined applications for each of the homes in a neighborhood, in order to establish communication between them as shown in Fig. 1.

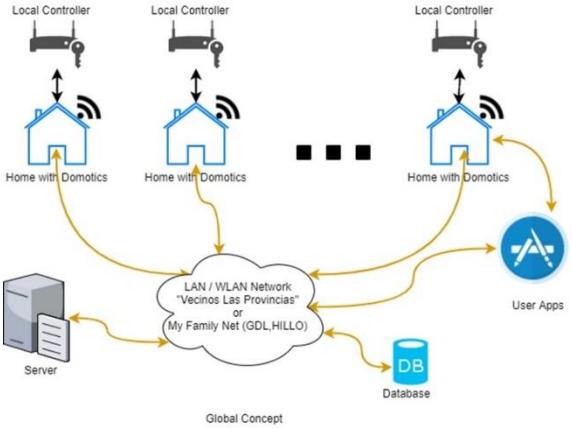


Fig. 1. Global conceptualization of home social network grouped in clusters.

By establishing communication between homes through an IoT platform, it is possible to generate different types of alerts depending on the situation that arises, and with this, establish security protocols between neighbors that allow a level of immediate response to the imminence of a risk situation for a home grouped into a cluster. On the other hand, each of the households will have an identifier and a link account to one of the most used social networks in the world, "Facebook", in which, through an exclusive page for neighborhood households hosted on This social network will publish the current information of each of the sensors in the home. This concept gives the user the possibility of allowing or not, the monitoring of the spaces of their home to the community of clusters that has access to the platform, which facilitates the response among users in order to prevent incidents in the home and protect the integrity of it.

IV. Methodology

The architecture of the hardware installed in each smart home is presented below as shown in Fig. 2.

A. ESP8266-12

The ESP8266-12 consists of a Tensilica microcontroller (32-bit) and 10-bit ADC and digital peripheral interfaces. It supports 2.4 GHz Wi-Fi (802.11 b / g / n). It has 16 GPIO, Inter-Integrated Circuit (I2C), SPI, I2S and UART interfaces. The ESP8266 development board, a system on chip (SoC) accesses the WiFi network with built-in TCP / IP protocol stack [15].

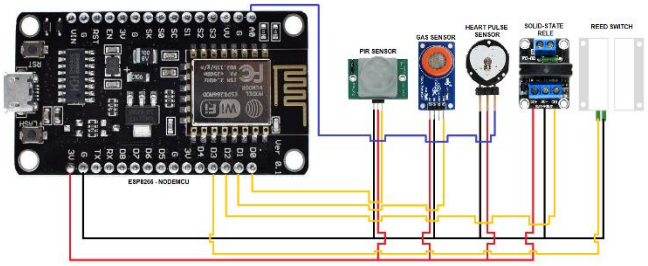


Fig. 2. Smart home hardware architecture.

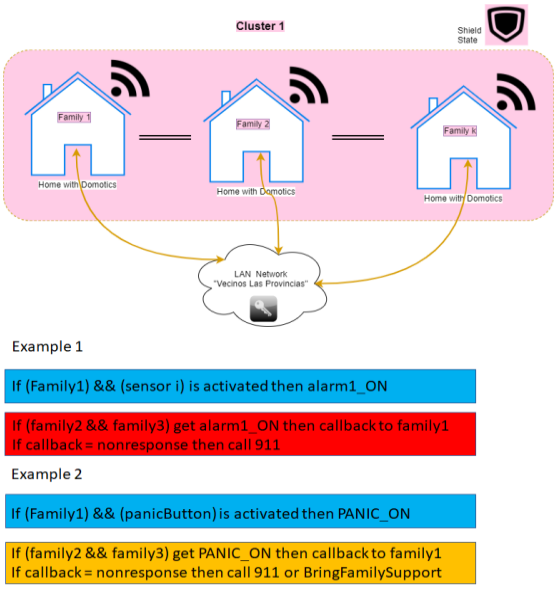


Fig. 3. Home social network framework proposed.

B. Ubidots IOT Platform

Ubidots is a server in the cloud that is used to send data from sensors and store data in the cloud, in addition, it is possible to create dashboards that display the information collected by the sensors, making data interpretation easier; This also allows the control of devices through the widgets it offers, in which it is possible to create an account holder, which contains a unique authentication key and a token key to provide security for the connection between the devices that send data to the platform and also has the advantage of generating alerts to registered mobile devices in the event that the status of a variable shows an anomaly [8].

C. IFTTT

IFTTT (If This Then That) is a service on a web platform that allows the user to create applets that automate the specified task [16]. In this study, IFTTT acts as an intermediary platform that connects the microcontroller and facebook, making use of the "webhooks" service, this is done in order to publish the current status of the home sensors so that users from different homes can consult them at any time from their private accounts [16].

Fig. 3, we introduce the proposed framework to build up a Home Social Network constituted by clusters, which incorporates homes with the ability to share the status of their sensors and the cluster provides the ability to families and neighbors to protect themselves.

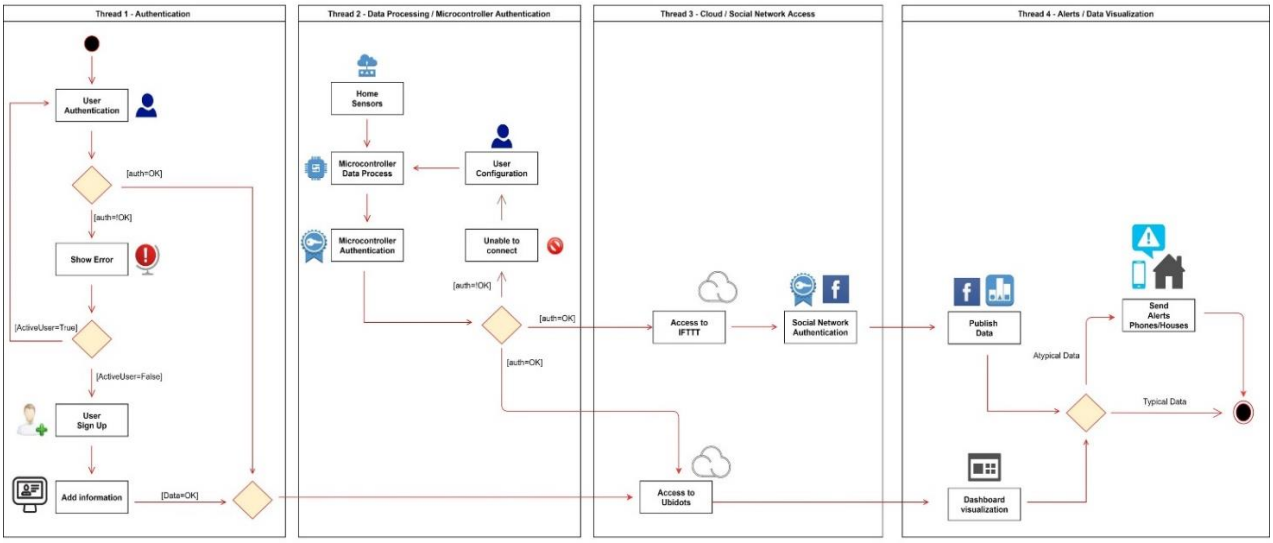


Fig. 4. Home social network UML activity diagram.

Each of the installed microcontrollers will be programmed based on the structure shown in Fig. 3, this will be in charge of sending the information to the IoT platform and IFTTT as the case may be.

In order to explain each of the stages of operation clearly and concisely, the proposed system was modeled using the activity diagram shown in Figure 4, in which four stages can be seen, the first one consists in the authentication of the user to access the Ubidots platform, the second stage consists in representing the sending information from the sensors to the microcontroller installed in each home, which processes the information to send it using an authentication certificate that allows you to enter the data to the platform, as a third stage, access to the platforms is shown once the information of the user and the microcontroller has been validated, and later, as a fourth stage, the user can view the data and receive alerts.

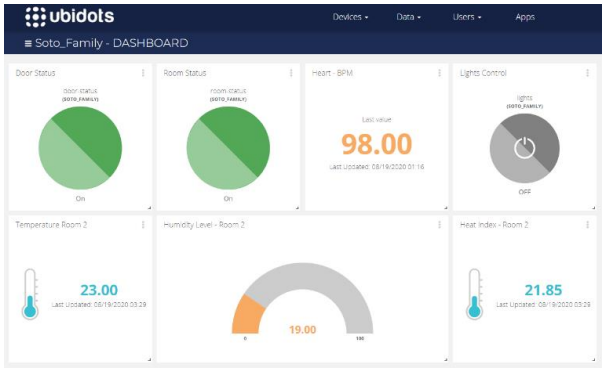


Fig. 5. Family 1 dashboard.

V. Results and Evaluation

Figs. 5 and 6 show how through the Ubidots Platform it is possible to control and monitor smart home rooms. Each of the families has a totally independent dashboard, and the administrator can assign privileges to users, like giving access to monitoring the spaces of another family if required.

On the other hand, the platform has a database where it stores a history of each of the variables assigned to the microcontrollers that are installed in the home, Fig. 7 shows the menu offered by the platform to access each one of the variables, where it is possible to export the data in Excel files if required, in addition to knowing exactly when an event occurred.

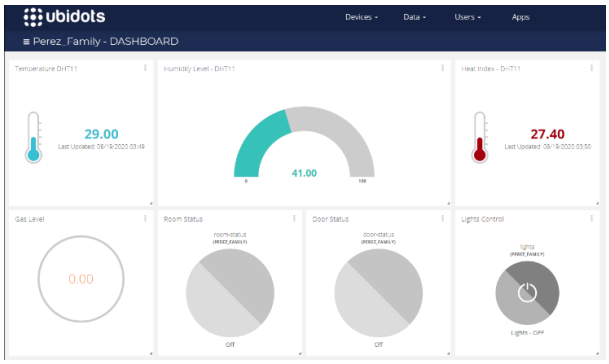


Fig. 6. Family 2 dashboard.

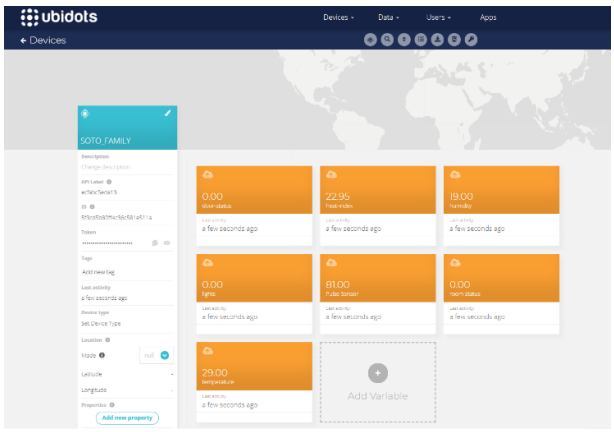


Fig. 7. Family 1 variables menu.

In order to show a part of the system operation, Fig. 8 shows the graph of the behavior of the sensor located in one of the rooms of the home, which can be monitored by the system administrator. Likewise, it is possible to see a record of the values that the sensor sends to the platform attached to the date and time of sending, which in this case, the value "1" represents an occupied room and the value "0" represents an empty room.

Another of the characteristics of the framework proposed in this article, is the communication of households through

the publication of the status of their sensors on the Facebook social network, so two events are created for each household using the IFTTT platform, like it shown in Fig. 9.

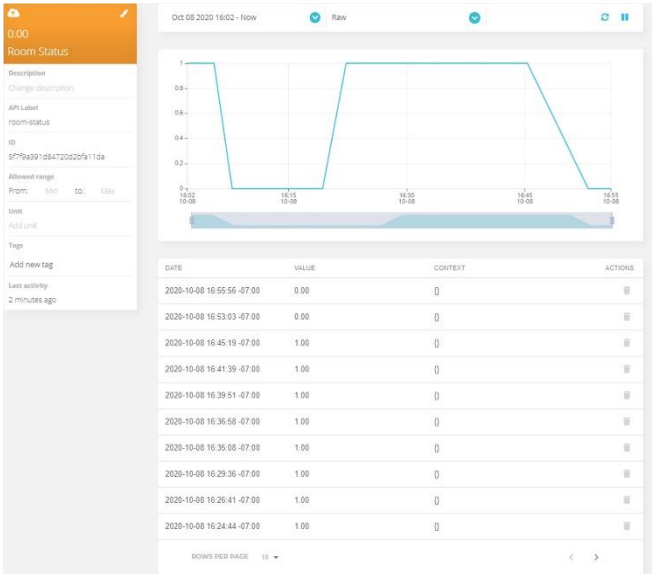


Fig. 8. Room status sensor record.

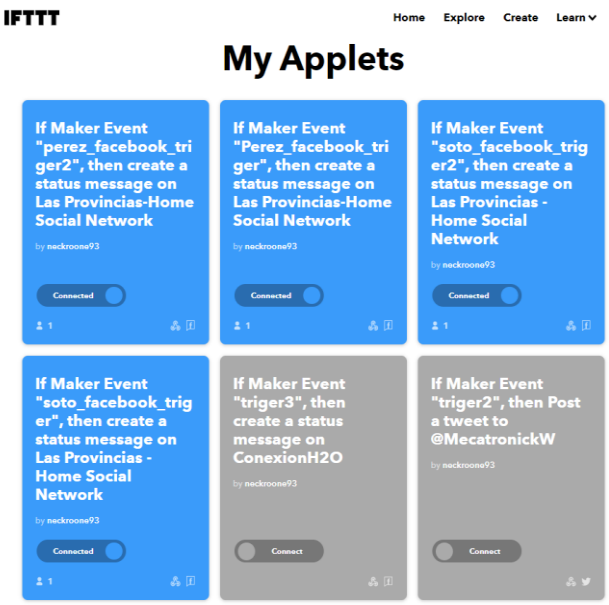


Fig. 9. Created events for trigger data from sensors to facebook.

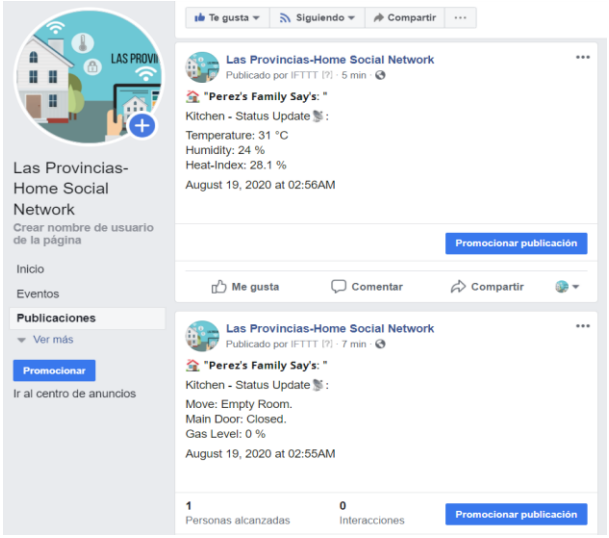


Fig. 10. Facebook page: "Las provincias – Home social network"

Each of the events allows an Http request to transport the sensor values to the social network, making a publication on a page, as shown in Fig. 10.

Each of the households publishes updated information on a non-public page on Facebook, which is managed by a Super User who provides privileges to each of the household representatives to consult the information that is published.

Fig. 11. Sensor alert publication.

Fig. 12. IFTTT push notification alert.

When an atypical data is presented during the capture of sensor information, a mostly visible alert is generated on the Facebook page, so that it can be easily seen by the users of the page. Fig. 11 display a publication created by the IFTTT service, which contains the current information of the sensors and an action instruction, so that users can take a response to check the issue.

On the other hand, Fig. 12 shows a push notification generated by the IFTTT service through the mobile application, which allows users to obtain alerts on their mobile devices.

VI. Conclusions

We proposed a new approach to integrate smart homes to social media using the technology offered by the Internet of Things, gives users a greater capacity to respond to the imminence of a crime at home. This concept is dedicated to monitoring and controlling rooms with the help of sensors (PIR, magnetic, Gas, etc.) that are integrated into the ESP8266-12 microcontroller, which sends the information to the IoT platforms using WIFI communication.

In conjunction with the ESP8266-12, Ubidots and IFTTT,

allow us to carry out effective monitoring and control, because the information presented on the platforms is monitored in real time and the user can consult them from anywhere in the world. On the other hand, making the information public through a social network for the members of the smart home network increases communication between households and users, it is possible to make responses in each publication on the Facebook page by consulting the homeowner.

Research is in progress in our laboratory to validate the reliability of the approach and to figure out some other relevant aspects such as security issues.

We propose this system in order to provide security to cities that have a high rate of crime at home, health problems at home, fires, etc. implementing the technology that the IoT offers to generate a response of attention to the different problems that arise. This system increases the development of technology in cities, making them smart communities that protect each other.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Victor Benitez, Conceptualization, methodology development, project administration, supervision, writing—review and editing.

Gustavo Soto, data curation, investigation, software development, validation, writing—original draft.

Félix-Herrán, supervision, writing—review and editing.

Jesus Pacheco, writing—review and editing, resources.

All authors had approved the final version.

References

[1] R. B. Khanderay and S. S. Khan, "Analysis on present status of internet of things," *Int. J. Sci. Technol. Res.*, vol. 9, no. 2, pp. 915–918, 2020.

[2] C. K. Ng, C. H. Wu, K. L. Yung, W. H. Ip, and T. Cheung, "A semantic similarity analysis of Internet of Things," *Enterp. Inf. Syst.*, vol. 12, no. 7, pp. 820–855, 2018.

[3] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, "Internet of things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *J. Clean. Prod.*, vol. 274, p. 122877, 2020.

[4] Reporte sobre delitos de alto impacto. [Online]. Available: https://onc.org.mx/uploads/mensual - febrero 2020 D.pdf.

[5] Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2019. [Online]. Available: https://www.inegi.org.mx/contenidos/programas/envipe/2019/doc/envipe2019_son.pdf

[6] Escudo Ciudadano. [Online]. Available: http://sspsonora.gob.mx/index.php/escudo-ciudadano.html

[7] AlertaPreventiva. [Online]. Available: http://apps.sspsonora.gob.mx/MAPAINTERACTIVO/Inicial/AlertaPreventiva

[8] G. Kesavan, P. Sanjeevi, and P. Viswanathan, "A 24 hour IoT framework for monitoring and managing home automation," in *Proc. Int. Conf. Inven. Comput. Technol. ICICT 2016*, vol. 1, 2016

[9] A. R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar, "A smart home energy management system using IoT and big data analytics approach," *IEEE Trans. Consum. Electron.*, vol. 63, no. 4, pp. 426–434, 2017.

[10] L. J. V. Escobar and S. A. Salinas, "E-Health prototype system for cardiac telemonitoring," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS*, vol. 2016-Octob, pp. 4399–4402, 2016.

[11] J. Harvey *et al.*, "The smart home: How consumers craft new service networks by combining heterogeneous smart domestic products," *J. Serv. Res.*, 2020.

[12] I. C. P. Mendoza, S. M. Timbol, M. J. C. Samonte, and E. B. Blancaflor, "ImHome: An IoT for smart home appliances," in *Proc. 2020 IEEE 7th Int. Conf. Ind. Eng. Appl. ICIEA 2020*, pp. 761–765, 2020.

[13] M. Z. Saeed, R. R. Ahmed, O. Bin Samin, and N. Ali, "IoT based Smart Security System using PIR and Microwave Sensors," in *Proc. MACS 2019 - 13th Int. Conf. Math. Actuar. Sci. Comput. Sci. Stat. Proc.*, pp. 1–5, 2019.

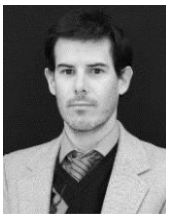
[14] Z. H. C. Soh, S. A. C. Abdullah, M. A. Shafie, and M. N. Ibrahim, "Home and industrial safety IoT on LPG gas leakage detection and alert system," *Int. J. Adv. Soft Comput. its Appl.*, vol. 11, no. 1, pp. 131–145, 2019.

[15] R. Kodali and A. Anjum, "IoT Based HOME AUTOMATION Using Node-RED," *Second Int. Conf. Green Comput. Internet of Things*, vol. 8, no. 12, pp. 5044–5047, 2019.

[16] S. Katangle, M. Kharade, S. B. Deosarkar, G. M. Kale, and S. L. Nalbalwar, "Smart Home Automation-cum Agriculture System," *2020 Int. Conf. Ind. 4.0 Technol. I4Tech 2020*, pp. 121–125, 2020.

Victor H. Benitez received the B.E. degree in electronics from the Universidad de Guadalajara, Mexico, in 1999, and the M.Sc. and Ph.D. degrees in electrical engineering from the Advanced Studies and Research Center, CINVESTAV-IPN, in 2002 and 2009, respectively. He has worked in the manufacturing industry related to the manufacture of printed circuits boards, and in the area of testing engineering. He is currently a Full Professor of mechatronics with the Industrial Engineering Department, Universidad de Sonora. His research interests include myoelectric control systems, neural networks applied to control electromechanical systems, and embedded systems applied to the Internet of Things.

Gustavo C. Soto received the B.E. degree in mechatronics from the Universidad de Sonora, Mexico, in 2018. He has worked in the IT Department, Universidad de Sonora, working on the area of telecommunications, analysis of electronic circuits and developing embedded systems applied to the Internet of Things. His research interest includes internet of things, artificial intelligence, mechatronics control systems and Machine learning.



Luis C. FÉlix-Herrán received the B.Eng. degree, in 2001, the M.S. degree in 2006, and the Eng.Sc.D. degree, in 2011. He is currently a professor with the School of Engineering and Sciences, Tecnólogico de Monterrey. In addition to his teaching activities, he conducts a research on modeling and control of linear and non-linear systems as well as educational innovation in undergraduate engineering programs.

Jesus Pacheco received the bachelor's degree in electronics engineering with a focus on digital systems and the M.Sc. degree in computer science from the Tecnológico de Hermosillo and the Ph.D. degree from the Electrical and Computer Engineering Department, The University of Arizona. He is currently a full professor with the Industrial Engineering Department, Universidad de Sonora, and the Director of the NSF Center for Cloud and Autonomic Computing. His research interests include cyber security for the Internet of Things and cyber-physical systems.