Premises Based Smart Door Chains System Using IoT Cloud

Abdul Hannan[1], Faisal Hussain[2(✉)], Sehrish Munawar Cheema[1], and Ivan Miguel Pires[3]

[1] University of Management and Technology, Sialkot, Pakistan
abdul.hannan@skt.umt.edu.pk
[2] Al-Khwarizmi Institute of Computer Science, University of Engineering & Technology, Lahore 54890, Pakistan
faisal.hussain.engr@gmail.com
[3] Instituto de Telecomunicações, Universidade da Beira Interior, 6200-001 Covilhã, Portugal
impires@it.ubi.pt

Abstract. Internet of 'things (IoT) allows people and objects to be connected anytime, anywhere, in any way/shape and function that can build a dynamic network. IoT is a critical enabling technology for smart home facilities like smart locks, automatic light control, smoke detection, temperature monitoring, etc. With the adoption of these systems, security and privacy have come up as the primary concerns. Due to the security threats, developing such a system that can smartly identify and restrict the people coming within the house premises is needed. Although these systems exist in the modern world where the intruder's entry is based on authentication, these systems provide security until the intruder enters the house's premises. We propose a framework for a smart door chain system (SDCS) to ensure the home's security even after the visitor enters the house to overcome this security issue. The proposed framework provides access to visitor's categories that are family, friend, and unknown. The SDCS has a synchronized chain of doors that are unlocked accordingly after the authentication of a visitor. By implementing the proposed framework, it is determined that the security of the house increases compared to the security provided by the previous automated systems. The proposed SDCS framework is beneficial, especially for old ages, disabled and working people if any nasty situation is raised at home in their absence.

Keywords: Internet of Things · IoT · Home automation · Smart door · Smart home security · Smart home · Smart systems

1 Introduction

A home is where you dream or want to live in a long day of sorrow. People on return to home used to turn ON the lights, close the doors, play their favorite music, and many other things by using mobile app interface operate with virtual switches and sliders to monitor

T. Hara and H. Yamaguchi (Eds.): MobiQuitous 2021, LNICST 419, pp. 834–846, 2022.
https://doi.org/10.1007/978-3-030-94822-1_54

and control appliances. The IoT or Internet of Things is a system in which computing devices, physical objects, and various machines are interlinked via the Internet forming wired or unwired network infrastructure [1]. The term IoT was first coined in 1999 by Kevin Ashton [2]. In today's era, smart devices are commonly used to collect and control data and share information between them. Moreover, with the advancement in nanotechnology, microprocessors and small chips are used to convert simple physical devices into IoT devices. IoT joins the physical devices through the Internet and performs sensing, collecting, storing, and processing information or data [3].

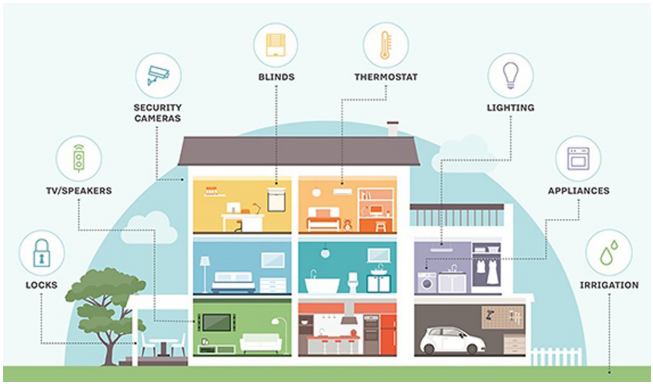

Fig. 1. Home automation system

The smart city is a tremendous application of IoT incorporating vast fields such as automating street lighting, managing transportation, video surveillance system, auto management of parking, municipal Wi-Fi, fire monitoring, weather forecast, measuring air quality, and managing electricity and waste and water [4, 5]. IoT enables chat-based, text, audio, and video-based commands fitted with natural language processing to control home devices and make the earth feel better [6]. In current circumstances, nearly 71% of the total use of IoT is in industry, and the rest of 29% use is under consumer [7]. Home atomization is emerging day by day, and it has gained a lot of attention in both research and the commercial field. As shown in Fig. 1, automated systems via different mediums have made it possible to reduce energy consumption [8]. Although wired networks were in demand at the early stages of the home automation systems, nowadays, wired networks are replaced with wireless communication to avoid the complex setup.

Furthermore, the advanced wireless systems are more extensible and flexible than the previous ones [9]. A wireless smart home is getting popular nowadays because of its portability, flexibility, and lower installation cost. It reduces the effort of human beings to manage devices at home remotely and is especially beneficial for working people [10]. Low-cost sensing devices and Wi-Fi-enabled smart devices are commonly used to communicate with people or systems [11].

Traditionally, physical keys, security cards, passwords, or patterns are used to lock or unlock the doors. So, carrying out a bundle of keys, Cards for different locks is

clumsy. It also increases the chance of losing or misplacing, causing identity fraud and robbery. Moreover, it is very hectic for a household to enter a passcode every time enters the house. To overcome this problem, we propose a framework for a smart door chain system (SDCS) to ensure the home's security even after the visitor enters the house. The proposed SDCS framework requires no physical keys to lock or unlock the doors. Moreover, it also enhances the security and privacy of the home as security is one of the most critical elements in everyone's life, which cannot be compromised at any cost. So, to keep the house safe from unknowns or strangers, the proposed SDCS framework restricts the entry of every visitor unless or until the system has recognized them.

The proposed SDCS framework is an IoT-based efficient system that provides an optimal solution for breach of privacy by giving access to the home premises only to the authorized visitors. Moreover, for ease of people, the system is fully automated. The main aim of this framework is to make the home secure so that the people feel safer and more protected in their premises. The critical contribution of this work can be summarized as follows:

- The incoming visitors' identification is based on three defined categories (Family, Friend, and Unknown) to keep the house safe from unknowns or strangers.
- We synchronized the smart doors of the building in the form of the chain according to the respective building blueprint by establishing a connection among the smart doors chain and the cloud server to authenticate the incoming person.
- We proposed a hybrid computing architecture, i.e., edge and cloud processing, for decentralized computing tasks to minimize computational delay and increase response time.
- We notify the insiders of the house about visitors' arrival by sending text and speech notifications.

The rest of the paper is organized as follows: Sect. 2 discusses the literature review. Section 3 explains the proposed SDCS framework. The workflow of the proposed system is presented in Sect. 4. Experimental Analysis with results & discussion is described in Sect. 5. Finally, Sect. 6 concludes the work.

2 Literature Review

IoT envisioned a global network of devices and machines to interact with each other [1]. As a result, IoT has been recognized as a future technology paradigm and achieving vast attention in many domains due to its features like connectivity, safety, sensing, intelligence, dynamic nature, scalability, less energy consumption [12–15].

Almost everything is getting digitalized and automatic, so the concept of home automation is implementing day by day [16, 17]. With the implementation of home automation, home security has become one of the most concerning issues [18–23].

As the house doors are the essential means of accessing the premises of the specific house, to make the homes safer, we need to make the house doors secure considering all the privacy and security aspects. For this purpose, Smart locks used in traditional doors

are already introduced and named smart doors. Therefore, using smart doors instead of conventional doors ultimately opens the door to a new set of security and privacy issues, such as by taking control of surveillance devices or activating false alarms, user's private data can be accessed. Therefore, people are reluctant to adopt smart home technologies due to different security attacks [20].

Research conducted by Refni Wahyuni et al. developed a system for home security by using WEMOS D1, Buzzer, and HC-SR501 sensors for telegram notification when a theft or unknown person enters the house [24]. WEMOS D1 processes the pear sensor for motion detection and buzzer for putting an alarm in case of theft [24]. Balakrishna Gokaraju et al. implemented home security by comparing the design and implementation of ARM microprocessor ATmega microprocessor [25]. In a study conducted by G. M. Sultan Muhmud Rana et al., cost-saving and flexible home security systems were designed and implemented [26].

A study presented a motion detection technique for home security systems using IoT. Two low-cost motion detectors named pyroelectric infrared radial (PIR) and microwave sensors implemented this technique. Raspberry Pi acts as the leading platform to receive signals from sensors and notify a user when an intruder is detected [27]. The deep learning-based face recognition technique was proposed by A. R. Syafeeza1 et al. Raspberry Pi acts as the main controller to process face detection, locking, and youth systems. A camera captures the image of an intruder and enables the user to access the door control via IoT [28].

An architecture for a cost-effective door sensor was presented with its implementation. The system informs the user about door open events of a house or an office environment through the android application. The proposed architecture experimented with an Arduino compatible Elegoo Mega 2560 Microcontroller and Raspberry Pi to communicate with a web server that implements a RESTful API [29]. An IoT-based structure and model was proposed by E.Shirisha et al. for an automated earth system that supports a variety of earth tools, for example, an energy management system. The system uses a Raspberry Pi and a Wi-Fi module to control the devices via a mobile app using Google assistant. It also customized their project to a home protection system using ESP32 camera Node MCU module to notify the house owners of intruders' entry [30].

An efficient critical generation method named Triangle Based Security (TBSA) was proposed by Pirbhulal et al. Low power Wi-Fi was integrated with WSNs to develop an innovative IoT-based smart home for secure data transmission between sensor nodes over sensor nodes extended coverage of the network. The proposed TBSA algorithm observed relatively low energy consumption [31]. A smart wireless home security system was built to notify the house owner of trespass or raise the alarm as an option. The authors ensured that the same experimental setup could also be used for home automation. The system used a TI-CC3200 Launchpad board embedded with a micro-controller and an onboard Wi-Fi shield to control and manage electrical appliances in the home [32]. Two IoT frameworks NETPI and BLYNK hardware agnostic with cloud, websites, security systems, deep learning, smartphones, and data mining. A system using NETPI was proposed to manage various NODEMCU controllers within a single framework

and to monitor home appliances remotely [33]. In [34], Pirbhulal et al. discussed a resource allocation model named 'MMSA' for implementing energy, security, drain and cost factors in IoT-based systems. Experimental analysis of MMSA demonstrates its outperformance incorporating security and mobility factors with optimal resources allocation. The aforementioned related studies discussed the security challenges in home automation systems and proposed solutions, but these solutions are either costly or inappropriate or consume more energy.

3 Proposed Framework

The proposed framework for a smart door chain system (SDCS) consists of five stages. These stages include data collection, face recognition, user authentication, owner access, and action triggering, as shown in Fig. 2. The detailed description of each stage is shown below:

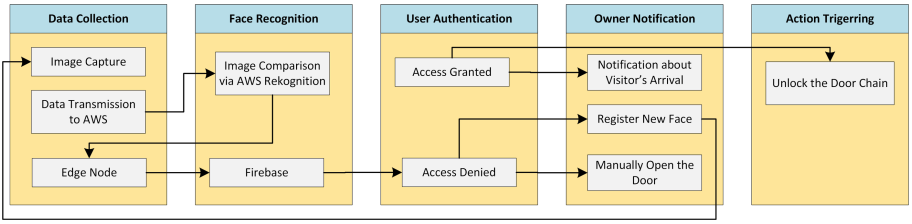

Fig. 2. Block diagram of the proposed framework

3.1 Data Collection

In this stage, the incoming visitor or intruder's face image is captured and sent to the Edge Node for the face detection process. The detected face image is sent to the Amazon Web Service (AWS) cloud server for recognition. The Raspberry pi (microprocessor) acts as an Edge Node, which has a camera mounted on it, to capture the picture of a visitor at run time. The edge node sent data to AWS S3 bucket storage and AWS Rekognition module. AWS S3 bucket storage is used to store the dataset of categories, namely friends, family, and unknown. Each category class starts with a unique ID such as Family = Famxx, Friends = Frxx. The dataset contains the images of the persons belonging to the friends and family categories. The dataset includes 20 images; 10 belong to the family category, and ten are from the friend category. Every image has a unique face Id. The face ids corresponding to all images are shown below in Table 1 and Table 2:

Table 1. Family dataset

Image Name	Face Id
Fam01	‘a4405fe3-797b-4235-9c07-12b3250549f6’
Fam02	‘83c3875d-8ad9-4d48-a91f-7c1a25275e87’
Fam03	‘99d832d4-a251-497f-ba7b-824b75ebd672’
Fam04	‘3364a3c3-0c52-4ade-b843-1356c6b3b605’
Fam05	‘4a6e01f6-4c48–4422-ae18-dbbd41549cca’
Fam06	‘11074d02-6bc7-441e-aae6-3afa3093ef03’
Fam07	‘58dee87f-aff2–4842-8370-2472d148f1d9’
Fam08	‘fbd3ea99-3ac7-4f5b-a175-41bd6df5eebf”
Fam09	‘eff90b32-c8d5-4bfb-81ee-7000aa2f034d’
Fam10	‘c3702087-e99f-4a10-8f38-04f565f257fa’

Table 2. Friends’ dataset

Image Name	Face Id
Fr01	‘e5a4c8fa-66d0-46cd-a0a2-d28638690cf1’
Fr02	‘be1bd738-6b4b-486a-a727-becd4c5a7a9f’
Fr03	‘3f119329–5090-4a31-acdb-439cad3488b4’
Fr04	‘63562c5f-0bcb-4b2d-9cf0-fec82eb185cc’
Fr05	‘fa7bb870-39b2-4c36-9d4f-a9da2d4ba1f6’
Fr06	‘91fbc9dd-c286–4488-a348-82d22415c79a’
Fr07	‘f9a17d59-3f4f-42c9-829d-3c47821ca4e0’
Fr08	‘e3d52ed3-3d1d-4f7e-be62-e74876ed302d’
Fr09	97362a21-71cb-4d1b-a33e-34fa0718baa7’
Fr10	‘8be3abe2-ba82-464c-a5a2-523e828a01f4’

3.2 Face Recognition on AWS

In this stage, the captured face detected image is sent to the AWS Face Rekognition module for recognition with the already defined categorized face images dataset. After face comparison with the AWS S3 bucket dataset, the face recognition result is sent back to the edge node to triggering the smart door chain pattern. Moreover, the connection of the edge node is also established with the firebase cloud database to send the categorized face comparison data. It is ultimately sent to all smart doors based on the action triggering module.

3.3 User Authentication

In this stage, the user is authenticated based on the comparison result received from the firebase. However, if the incoming visitor's picture is matched with more than 75% confidence index with any one of the face pictures placed in AWS categorized dataset, then they are declared as an authorized person, and the user "Access Granted" is enabled to get the access of the in-house premises according to the class category smart door pattern rule. On the other hand, if the visitor's face is not recognized after the comparison process, they have declared a person, and the user "Access Granted" module is in disable state.

3.4 Owner Notification

This stage provides an owner android-based interface to perform multiple actions such as register new faces, switching smart doors chain mode, and getting voice notifications about the incoming visitor. Moreover, if an unknown person arrives, the owner has an option in the application to register a new face, and user "Access Denied" is granted. However, the owner still wants to give access to in-house premises to the incoming visitor, and then it is done by using the "Switch Mode" to manual for smart doors chain pattern.

3.5 Action Triggering

This stage is liable for ongoing activities such as unlocking the door chain for a specific time interval according to the category. Moreover, the incoming visitor is recognized as an authorized person. Then, the chain of doors is opened for that visitor according to the respective category to whom the incoming intruder belongs.

4 Workflow of the System

Figure 3 represents the hierarchy of the proposed system. The proposed mechanism requires that whenever an intruder arrives, they have to stand in front of a camera in a particular line of the frame for at least 30 s so that the runtime picture of the visitor is captured more precisely. We have used the Amazon web services to store the dataset of two categories, namely friends and family, to the AWS collection. First, the intruder captured image is sent to the edge node module. Then, the face is detected on the edge node to reduce the computation delay on the AWS cloud service. Once the face is detected, the image is directed to the AWS face recognition module for face recognition, respective to the predefined stored categories of the incoming visitor. It matches the intruder face image with the Aws data collection category. The action triggering module is enabled once the user is authenticated. The comparison result is received on the edge node, which is ultimately passed to the real-time database (firebase). After that, the edge node unlocks the respective door chain according to the category for a specific time interval. The doors are closed automatically after that time interval.

In contrast, if the incoming visitor is declared an unauthorized person after the comparison, then the SDCS considered that person in the unknown category. In this class, house residents can switch the door lock mode from "automatic" to "manual" to give them access to the house premises. You have to register that face by using the android application as per the criteria mentioned above.

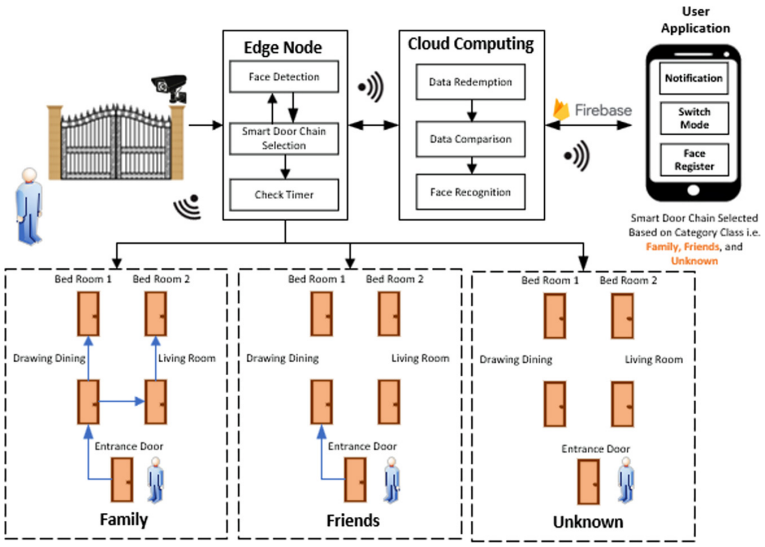

Fig. 3. Workflow of the proposed SDCS framework

5 Experimental Analysis

5.1 Experimental Setup

Figure 4 shows the proposed system architecture. Initially, the incoming visitor's picture is captured by the pi camera mounted on the microcontroller. Then the captured image is passed to AWS for comparison (face recognition). Microcontroller received that comparison result and further passed that result to firebase real-time database. After that, the Arduinos are placed on the doors received from firebase and then unlock the door chain according to the category. An Android application's connection is also established with firebase, and it is developed for performing the following tasks; "Notification about visitor's arrival", "Manually open the doors" (whenever required), and "Register new face" (if an unknown arrives).

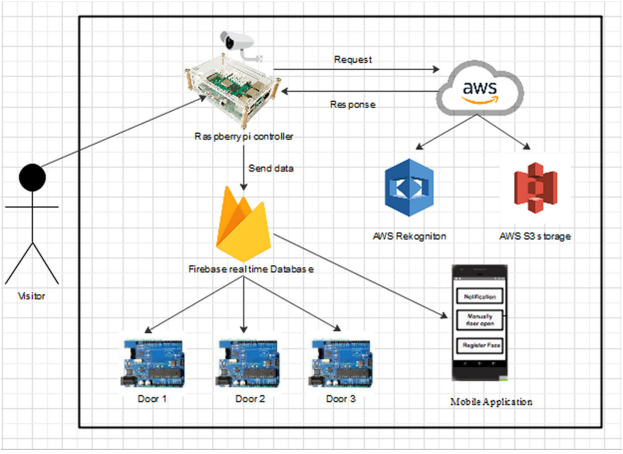

Fig. 4. System architecture of the SDCS

5.2 Performance Evaluation

The proposed smart door chain scheme is evaluated based on two performance metrics, i.e., accuracy and error rate. The parameters as defined as:

Accuracy: It is defined as the ability of the system to correctly classify the image of family and friend as family and friend respectively and other persons as an "unknown". It describes the ratio of correct predictions concerning all samples. mathematically, it is expressed in Eq. (1):

$$Accuracy = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{1}$$

Error Rate: The inaccuracy of predicted output values is termed the error of the method. It is also defined the proportion of cases where the prediction is wrong. Mathematically, it is expressed Eq. (2):

$$ErrorRate = \frac{|\text{Approximate Value} - \text{Exact Value}|}{|\text{Exact Value}|} \tag{2}$$

The performance of the proposed SDCS framework is successfully tested. Two face recognition techniques are compared to get the one with the highest efficiency and accuracy between HAAR and SDCS. We compared a typical face recognition algorithm (HAAR) and the proposed mechanism (SDCS) in terms of percentage similarity index. Our proposed face recognition mechanism (SDCS) employs hybrid computing architecture, i.e., edge and computational cloud nodes. Thus, SDCS is more effective for face recognition than the traditional HAAR algorithm. However, the percentage similarity index of the proposed system didn't drastically affect the system efficiency, as shown in Fig. 5.

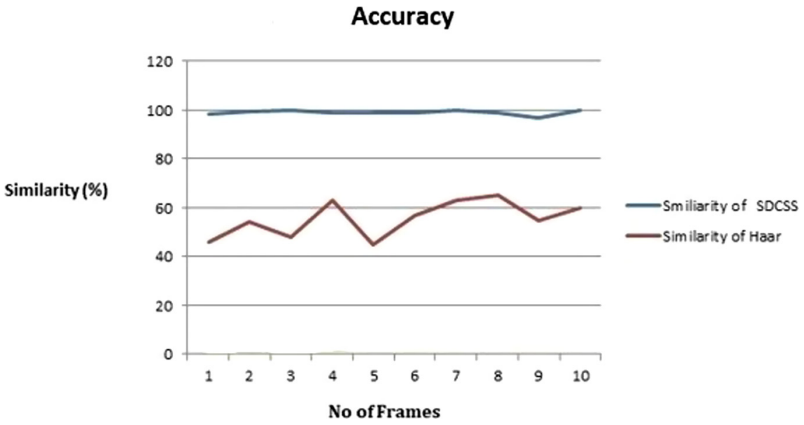

Fig. 5. Accuracy comparison of the proposed SDCS with HAAR algorithm

The error rate of the SDCS is computed by fixing a threshold at >60%. If the confidence value lies between 61–100%, the system recognizes the intruder and identifies them according to its predefined category. As the distance from the camera view focus increases, the confidence value starts to decrease. For example, Fig. 6 depicts, as the intruder goes beyond the camera's view, i.e., the distance greater than 29 cm, the mounted camera on the edge node will not capture the face image, increasing the error rate of the proposed system.

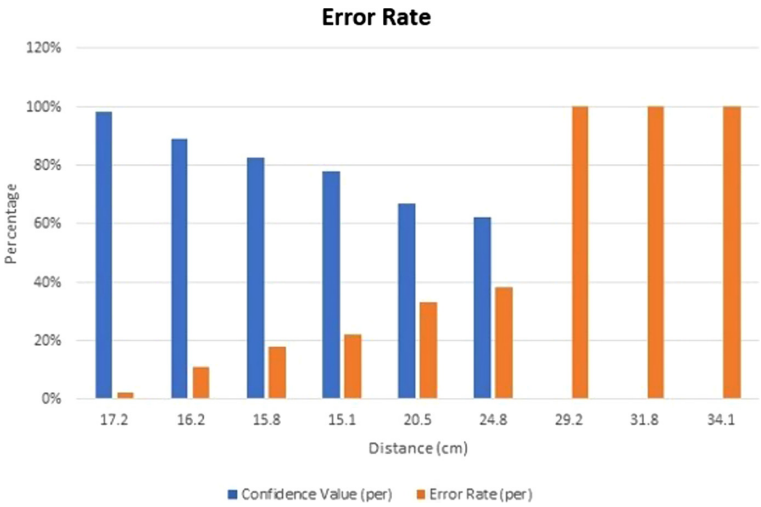

Fig. 6. Error rate of the proposed SDCS framework

6 Conclusion

The proposed framework for a smart door chain system (SDCS) is a real-time system that follows the IoT infrastructure. The SDCS framework used digital information such as face recognition through the Raspberry Pi camera for authentication instead of the legacy key system. It uses cloud services to verify the visitor's identity. Data processing and storage activities were done using the cloud server, far better and more efficient than the conventional file storage system. As there is a large amount of information to be stored for the recognition of the visitor, so we used a database. Three categories are specified based on which the visitor is identified, i.e., Family, Friends, and Unknown. In case of any familiar visitor whose data is not already been updated on the cloud server and falls in the third category, an action triggering module is enabled to switch the system mode from "automatic" to "manual" to give them access inside the home premises. The house doors are synchronized in the form of a chain and are unlocked according to each visitor category. SDCS is a source of pleasure and satisfaction for the people worrying about the security of their significance and small assets. Moreover, the proposed system helps the incoming intruder who experienced long-lasting wait due to the household patients, in-house privacy, and efficiently indulging in daily routine tasks.

Acknowledgments. This work is funded by FCT/MEC through national funds and co- funded by FEDER—PT2020 partnership agreement under the project UIDB/50008/2020 (Este trabalho é financiado pela FCT/MEC através de fundos nacionais e cofinanciado pelo FEDER, no âmbito do Acordo de Parceria PT2020 no âmbito do projeto UIDB/50008/2020).

This article is based upon work from COST Action IC1303–AAPELE–Architectures, Algorithms and Protocols for Enhanced Living Environments and COST Action CA16226–SHELD-ON–Indoor living space improvement: Smart Habitat for the Elderly, supported by COST (European Cooperation in Science and Technology). More information in www.cost.eu.

References

1. Ghazanfar, S., Hussain, F., Rehman, A.U., Fayyaz, U.U., Shahzad, F. and Shah, G.A.: March. IoT-flock: An open-source framework for IoT traffic generation. In: 2020 International Conference on Emerging Trends in Smart Technologies (ICETST), pp. 1–6. IEEE (2020)
2. Ashton, K.: That Internet of Things Thing. RFID J. (2009)
3. Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., Guizani, S.: Internet-of-Things-based smart cities: recent advances and challenges. IEEE Commun. Mag. **55**(9), 16–24 (2017). https://doi.org/10.1109/MCOM.2017.1600514
4. Pires, I.M., Hussain, F., Garcia, N.M., Zdravevski, E.: Improving human activity monitoring by imputation of missing sensory data: experimental study. Future Internet **12**(9), 155 (2020)
5. Talal, M., et al.: Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. J. Med. Syst. **43**(3), 42 (2019)
6. Hamdan, O., Shanableh, H., Zaki, I., Al-Ali, A.R., Shanableh, T.: IoT-based interactive dual-mode smart home automation. In: 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–2. IEEE (2019)

7. Ray, A. K., Bagwari, A.: IoT based Smart home: security aspects and security architecture. In: 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), pp. 218–222. IEEE (2020)
8. Marikyan, D., Papagiannidis, S., Alamanos, E.: A systematic review of the smart home literature: a user perspective. Technol. Forecast. Soc. Change **138**, 139–154 (2019)
9. Sivapriyan, R., Rao, K. M., Harijyothi, M.: Literature review of IoT-based home automation system. In 2020 Fourth International Conference on Inventive Systems and Control (ICISC), pp. 101–105. IEEE (2020)
10. Vaidya, V.D., Vishwakarma, P.: A comparative analysis on the smart home system to control, monitor, and secure home, based on technologies like gsm, IoT, Bluetooth, and pic microcontroller with Zigbee modulation. In: 2018 International Conference on Smart City and Emerging Technology (ICSCET), pp. 1–4. IEEE (2018)
11. Gyrard, A., Zimmermann, A., Sheth, A.: Building IoT-based applications for smart cities: how can ontology catalogs help? IEEE IoT J. **5**(5), 3978–3990 (2018). https://doi.org/10.1109/JIOT.2018.2854278
12. Pires, I.M., Hussain, F., Marques, G., Garcia, N.M.: Comparison of machine learning techniques for the identification of human activities from inertial sensors available in a mobile device after the application of data imputation techniques. Comput. Biol. Med. **135**, 104638 (2021)
13. Ashraf, M.U., Hannan, A., Cheema, S.M., Ali, Z., Alofi, A.: Detection and tracking contagion using IoT-edge technologies: confronting COVID-19 pandemic. In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), pp. 1–6. IEEE (2020)
14. Hussain, F., et al.: A framework for malicious traffic detection in IoT healthcare environment. Sensors **21**(9), 3025 (2021)
15. Munir, M.S., Bajwa, I.S., Cheema, S.M.: An intelligent and secure smart watering system using fuzzy logic and blockchain. Comput. Electr. Eng. **77**, 109–119 (2019)
16. Stolojescu-Crisan, C., Crisan, C., Butunoi, B.P.: An IoT-based smart home automation system. Sensors **21**(11), 3784 (2021)
17. Sheikh, J.A., Cheema, S.M., Ali, M., Amjad, Z., Tariq, J.Z., Naz, A.: IoT and AI in precision agriculture: designing smart system to support illiterate farmers. In: Ahram, T. (ed.) Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2020 Virtual Conferences on Software and Systems Engineering, and Artificial Intelligence and Social Computing, July 16-20, 2020, USA, pp. 490–496. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-51328-3_67
18. Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., Baldini, G.: Security and privacy issues for an IoT-based smart home. In: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1292–1297. IEEE (2017)
19. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B.: A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access **7**, 82721–82743 (2019)
20. Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., Bilal, M.: Smart home security: challenges, issues and solutions at different IoT layers. J. Supercomput. **77**(12), 14053–14089 (2021)
21. Ali, W., Dustgeer, G., Awais, M., Shah, M.A.: IoT-based smart home: Security challenges, security requirements, and solutions. In: 2017 23rd International Conference on Automation and Computing (ICAC), pp. 1–6. IEEE (2017)
22. Yu, Z., Song, L., Jiang, L., Sharafi, O.K.: Systematic literature review on the security challenges of blockchain in IoT-based smart cities. Kybernetes **51**(1), 323–347 (2022)

23. Ray, A.K., Bagwari, A.: IoT based Smart home: Security Aspects and security architecture. In: 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), pp. 218–222. IEEE (2020)
24. Wahyuni, R., Rickyta, A., Rahmalisa, U., Irawan, Y.: Home security alarm using Wemos D1 and HC-SR501 sensor-based telegram notification. J. Robot. Control (JRC) **2**(3), 200–204 (2021)
25. Gokaraju, B., Yessick, D., Steel, J., Doss, D.A., Turlapaty, A.C.: Integration of intrusion detection and web service alarm for home automation system using 'ARM' microprocessor. In: SoutheastCon 2016, Norfolk, VA, pp. 1–2 (2016) https://doi.org/10.1109/SECON.2016.7506717
26. Mahmud Rana, G.M.S., Mamun Khan, A.A., Hoque, M.N., Mitul, A.F.: Design and implementation of a GSM-based remote home security and appliance control system. In: 2013 2nd International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, pp. 291–295 (2013). https://doi.org/10.1109/ICAEE.2013.6750350
27. Tiong, P.K., Ahmad, N.S., Goh, P.: Motion detection with IoT-based home security system. In: Arai, K., Bhatia, R., Kapoor, S. (eds.) Intelligent Computing: Proceedings of the 2019 Computing Conference, Volume 2, pp. 1217–1229. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-22868-2_85
28. Radzi, S.A., Alif, M.M.F., Athirah, Y.N., Jaafar, A.S., Norihan, A.H., Saleha, M.S.: IoT-based facial recognition door access control home security system using raspberry pi. Int. J. Power Electron. Drive Syst. **11**(1), 417 (2020)
29. Hoque, M.A., Davidson, C.: Design and implementation of an IoT-based smart home security system. Int. J. Netw. Distrib. Comput. **7**(2), 85–92 (2019)
30. Shirisha, E.: IoT based home security and automation using google assistant. Turkish J. Comput. Math. Educ. (TURCOMAT) **12**(6), 117–122 (2021)
31. Pirbhulal, S., et al.: A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors **17**(1), 69 (2017)
32. Kodali, R.K., Jain, V., Bose, S., Boppana, L.: IoT-based smart security and home automation system. In: 2016 International Conference on Computing, Communication, and Automation (ICCCA), pp. 1286–1289. IEEE (2016)
33. Alani, S., Mahmood, S.N., Attaallah, S.Z., Mhmood, H.S., Khudhur, Z.A., Dhannoon, A.A.: IoT based implemented comparison analysis of two well-known network platforms for smart home automation. Int. J. Elect. Comput. Eng. (IJECE) **11**(1), 442 (2021). https://doi.org/10.11591/ijece.v11i1.pp442-450
34. Pirbhulal, S., Wu, W., Muhammad, K., Mehmood, I., Li, G., de Albuquerque, V.H.C.: Mobility enabled security for optimizing IoT-based intelligent applications. IEEE Netw. **34**(2), 72–77 (2020)