Original Research Paper

IoT-Fog based Smart-Building Security System Design and Performance Evaluation

Maha Medhat, Khaled El-Shafey and Ali Rashed

Department of System and Computer Engineering, AL-Azhar University, Cairo, Egypt

Abstract: This paper aims to develop a smart building-security system utilizing fog technology. Fog computing is an innovative solution to reduce latency and network congestion, in which the cloud is extended to the edge of the network. The proposed system can detect an intruder, fire and water leakage. It is implemented using Raspberry Pi, Arduino, Pi-camera and different sensors. The sensors are installed on Arduino and Pi-camera is mounted on Raspberry Pi. The Raspberry Pi is used as a fog node to fit the time-sensitive nature of the system. The performance was evaluated through the iFogSim toolkit. Fog reduces 33.26 and 46.8% average latency and sensor delay as compared to the cloud. Also, the value of the network usage decreases by 71% in the case of fog-based even with increased network load. Finally, the iFogSim was evaluated by measuring the simulation time, which gave acceptable results of about 8.5 sec.

Keywords: Fog Computing, iFogSim Simulator, Smart-Building Security, IoT, Raspberry Pi

Introduction

Internet of Things is a network of interconnected electronic devices capable of sending data without interference or with minimal human intervention. This technology has been widely used for emergency applications such as smart city applications, health monitoring and smart building security. The smart building-security system becomes one of the critical issues that require research and study to protect people's lives and properties where any type of delay could be life-threatening (AlHammadi *et al*., 2019).

Fog is a complementary technology to cloud computing aiming to meet time-sensitive application requirements represented in low latency and an acceptable value of network usage to avoid congestion and further delay. This new technology decreases the volume of data that needs to be transferred to the cloud (Mukherjee *et al*., 2018; Khakimov *et al*., 2018).

In this study, an IoT-Fog based building security system is proposed and simulated to take the advantages offered by both fog computing and the Internet of Things. The system is implemented for monitoring the presence of intruders using the combination of motion detection and sound detector, early detection of fire using three different types of sensors and protects the building from water leakage.

The system also utilizes the capability of a door open sensor and glass break detector to detect any suspicious activity. The system is implemented on Raspberry Pi 3 and Arduino. Raspberry Pi was chosen as the system control unit to employ as a fog node (Lavassani *et al*., 2018). The system is expected to recognize the emergency type and report the exciting situation to the relevant emergency department. The system is also equipped with a feedback mechanism that warns the house owner who can cancel the false alarm within 10 sec to avoid false positive alarm.

To show a preference for fog computing compared to traditional cloud computing, the system performance was evaluated using the iFogSim toolkit. The evaluation includes the measurement of system latency and network usage. The results showed a significant decrease in their values in the case of fog computing. Finally, the iFogsim toolkit was evaluated by measuring the execution time.

The structure of the paper is organized as follows: Section II comprises some related work that has been done by researchers in this field. Section III gives details about the proposed system design approach. Section IV, presents system evaluation, simulation results and discussion. The summary of the paper is concluded in section V.

Related Work

Various technologies used in the proposed system were presented and discussed in this section.

A. Fog Computing

Fog computing is an emerging and evolving technology that bridges the cloud and the Internet-of-Things (IoT) world. It acts as a layer between them to allow computing in a decentralized manner (Cisco Systems, 2015). It provides a promising approach for processing a huge amount of data generated and consumed by billions of devices connected to the Internet of Things at the edge of the network (Naha *et al.*, 2018; Habibi *et al.*, 2020).

In the last few years, researchers have developed several emergency response systems based on fog technology. Paul *et al.* (2018) have proposed a fog computing-based IoT for a health monitoring system to help patients who suffer from chronic diseases. The proposed system reduces the amount of data that is transferred between the cloud and sensor networks. It also overcomes a data center failure bears with it.

Dar *et al.* (2018a) has presented an automated accident detection and response system which makes use of fog computing to decrease response time. System evaluation by iFogSim toolkit is introduced in (Dar *et al.*, 2019; 2018b).

Sarkar and Kumar (2019) have developed and simulated a fog based intelligent security system using the PTZ controller. Also, (Peng *et al.*, 2020) proposed a traffic analysis system using broad learning which supports traffic-intensive applications utilizing fog computing to save bandwidth resources by offloading the traffic data uploading tasks to the fog nodes.

To facilitate the fog based system evaluation, there have been some studies for the edge and fog computing simulator. Gupta *et al.* (2017) conducted a study entitle " iFogSim: A Toolkit for Modeling and Simulation of Resource Management Techniques in Internet of Things, Edge and Fog Computing Environments ". It introduced an open-source simulator for edge and fog computing to evaluate the IoT environment scenarios in terms of latency, network congestion, energy consumption and cost.

The iFogSim depends on sensor-actuate architecture as illustrated in (Mahmud and Buyya, 2019). In this architecture, data is initially collected from sensors then broadcasted to local fog server either in an event or periodic manner. Subsequently, local fog nodes process the received data. Lastly, necessary reactions are directed back to actuators.

The cloud-only placement and Fog-based scenarios are modeled in the simulator. The cloud-only is based on the traditional cloud-based where all modules of an application run in the data center. Sensors transmit the sensed data to the cloud where it is processed. While for the fog placement, the data is processed at the fog server.

B. Building Security System

There have been several previous studies on IoT based building-security system. Tanwar *et al.* (2017) conducted a study entitled "An Advanced Internet of Thing based Security Alert System for Smart Home". It describes inexpensive home security systems. The hardware used was Raspberry Pi, Infrared (PIR) and, modules to minimize delays during e-mail alerts. PIR sensors are used as a motion detector and Raspberry Pi as the control unit.

Another research was conducted by (Kumbhar *et al.*, 2018) entitled "IoT Based Home Security System Using Raspberry Pi-3". It proposed IoT enabled security system to send an email to the owner of the home once an intrusion is detected in front of the door. Raspberry pi controls the whole system where an image is captured by pi-camera. The motion is detected by using a motion sensor, Ultrasonic sensor and microphone.

The third study was conducted by (Rani *et al.*, 2018) entitled "IoT Based Home Security System Using Raspberry Pi with Email and Voice Alert". It proposed a security system using raspberry pi which sends a real-time SMS alert to authorize person through WAY2SMS which is connected through the internet. The image of the intruder is then sent via g-mail after motion detection.

Taryudi and Budi (2018) conducted a study entitled "IoT-based Integrated Home Security and Monitoring System". This study discusses the design of a monitoring system to detect the room temperature and humidity to detect the stove's fire. The system is controlled by NodeMCU ESP8266.

The fifth study was conducted by (Surantha and Wicaksono, 2019) under the title "An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients". This research discusses the design and implementation of a home security system with human detection capability using Raspberry Pi 3 and Arduino. The webcam is mounted on the Raspberry Pi and the PIR sensor is installed on Arduino. The movement around the sensor is detected by the PIR sensor which activates the webcam to capture a picture. The author proposed a Histogram of Oriented Gradients (HOG) and Support Vector Machine (SVM) to detect the suspicious object. The alarm then is activated and a warning email is sent to the owner. This system is very good because it can detect the intruder with an accuracy of 90% as illustrated by authors.

Al Rasyid *et al.* (2018) proposed a smart home system using raspberry pi as a main centralized controller. The system has several end nodes using Arduino and can work in two modes of access that is a local mode (intranet) and internet to facilitate the use of a large scale.

Saheed *et al.* (2019) proposed a fire prevention and surveillance security system as an efficient means of controlling intruders, fire-outbreak as well as serving as a surveillance system. It consists of a gas sensor, PIR

sensors, buzzer, Global System Mobile (GSM) module, Liquid Crystal Display (LCD) and RGB Light Emitting Diode (LED). All components were connected to the Arduino Mega microcontroller.

C. Fog and Cloud-based Smart System

There have been a limited number of studies that combine IoT smart system and cloud-fog based technology. The author in (Yuan, 2015) conducted a study entitled "Study of Smart Home System Based on Cloud Computing and the Key Technologies". This study proposed a new smart home system that is based on the combined development of cloud computing and the Internet of Things. The proposed system is greatly shortens processing time when compared to ordinary intelligence lives.

Another research was conducted by (Stojkoska and Trivodaliev, 2017) entitled "Enabling internet of things for smart homes through fog computing". Through simulation on thereal smart meter dataset, the result showed that fog computing based on predictive filters can reduce the number of transmissions and minimize smart home network traffic.

Dutta and Roy (2017) have conducted a study under the title "IoT-fog-cloud based architecture for smart city: Prototype of a smart building". It aims to improve the standard of living at home and in-office with newly improved working facilities where the whole system will be automatic, efficient and will be under the control of the user via his/her smartphone done by the integration of IoT, fog and cloud.

The fourth study was proposed by (Shah, 2017) entitled "A Mobile Ad hoc Cloud Computing and Networking Infrastructure for Automated Video Surveillance System". It introduced a mobile automated video surveillance system that requires a vast quantity of computing and storage resources. The author built the Surveillance System based on mobile ad hoc network cloud computing. The proposed system has been implemented on a group of Wi-Fi Direct enabled Samsung mobile devices.

From the literature review, there have been few researchers who focus on the fog, smart building system. However, there has been no researcher specifically discussing fog-based intruder detection and fire prevention. Also, several studies did not compare the fog based system to traditional cloud computing. Therefore, in this research, the design is proposed to minimize system latency and network traffic. The research also compares the important network parameters in the case of designing the system with fog or only-cloud technology.

The Architecture of the Proposed System

Based on the fog technology advantages, a fog-based building-security system is introduced. The system design approach is discussed in this section. The general fog-based system architecture is shown in Fig. 1. It consists of three layers, sensors layer, fog layer and cloud layer.

The system is implemented on Raspberry Pi 3, Arduino microcontroller (Surantha and Wicaksono, 2019), Pi camera and, several sensors. The Raspberry Pi is chosen as the control unit because it can be implemented as a fog node where all sensors data is processed over it near the source. Arduino is used to integrating all the electronic devices into one environment.

A. General System Design

To ensure the complete safety of people's life and property, the system has been designed to detect three main emergencies. The proposed system can early detect if there is an intruder, a water leakage, or a fire (Fig. 2).

For early fire detection, the system will continuously monitor the surrounding temperature, the level of carbon monoxide in the air and, the presence of thick smoke. If any of these signs are presented, a fire warning is sent to the user's smartphone and the nearest fire station.

In this research, we assume the system is designed for a private building. The PIR sensor reads every movement that passes through the detection range of the PIR sensor, i.e., around 4-7 m. The PIR sensor reads continuously until a movement is found. If there is a movement, then the system will check the sound detector. The system then sends an alarm to the owner's mobile. If the alarm notification did not cancel in 10 sec, the Pi Camera is activated to capture the intruder picture and to record the theft video.

A door open sensor and a glass break detector are used to detect any suspicious activity to confirm the home attack situation and inform the nearest police station. The proposed system also protects the building from drowning with water through a water sensor. The complete system workflow is shown in Fig. 2.

B. Hardware Design

The hardware layout is outlined in this section. That involves the selection of the electronics parts and the integration of all the components. Figure 3 shows the hardware design for our building-security system.
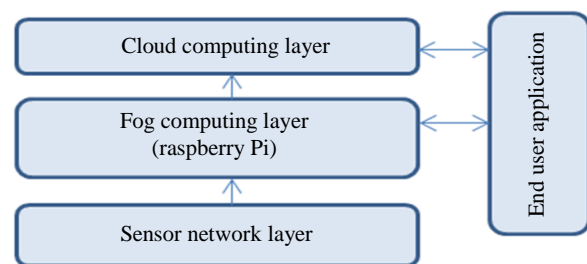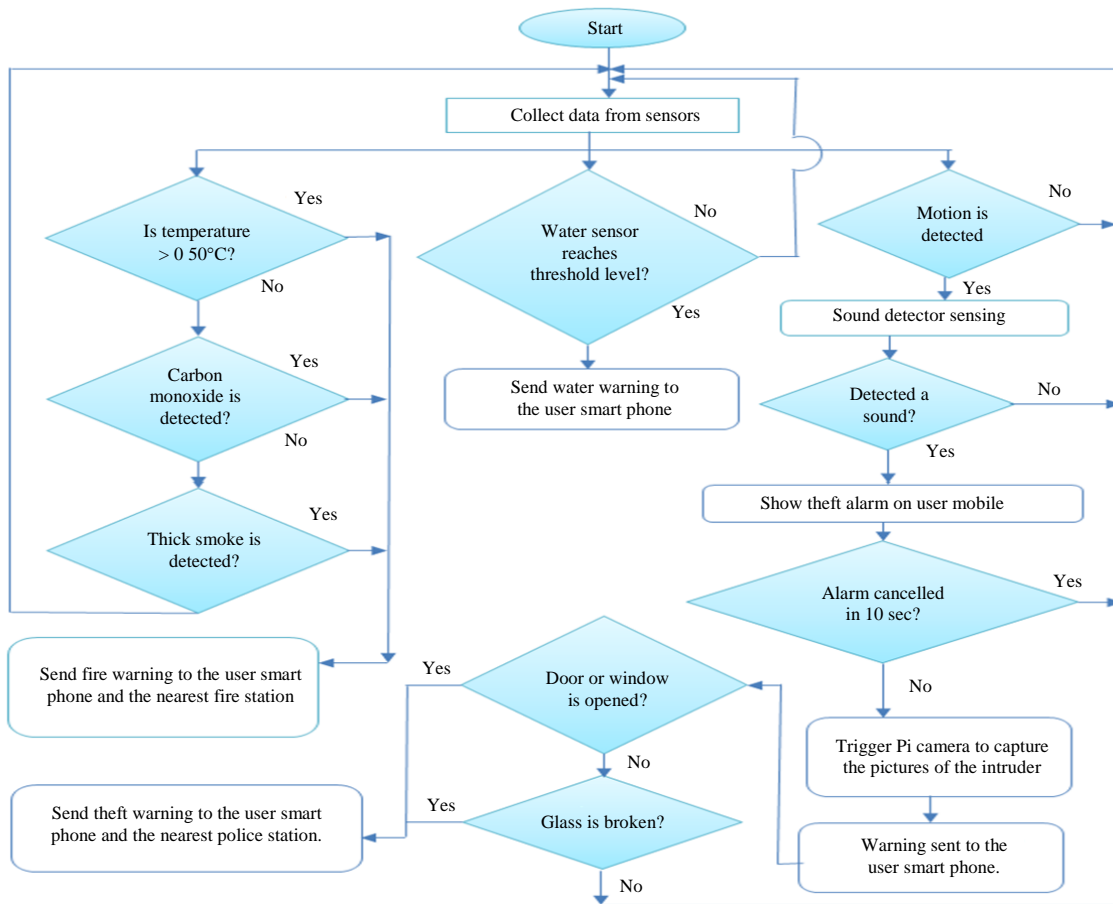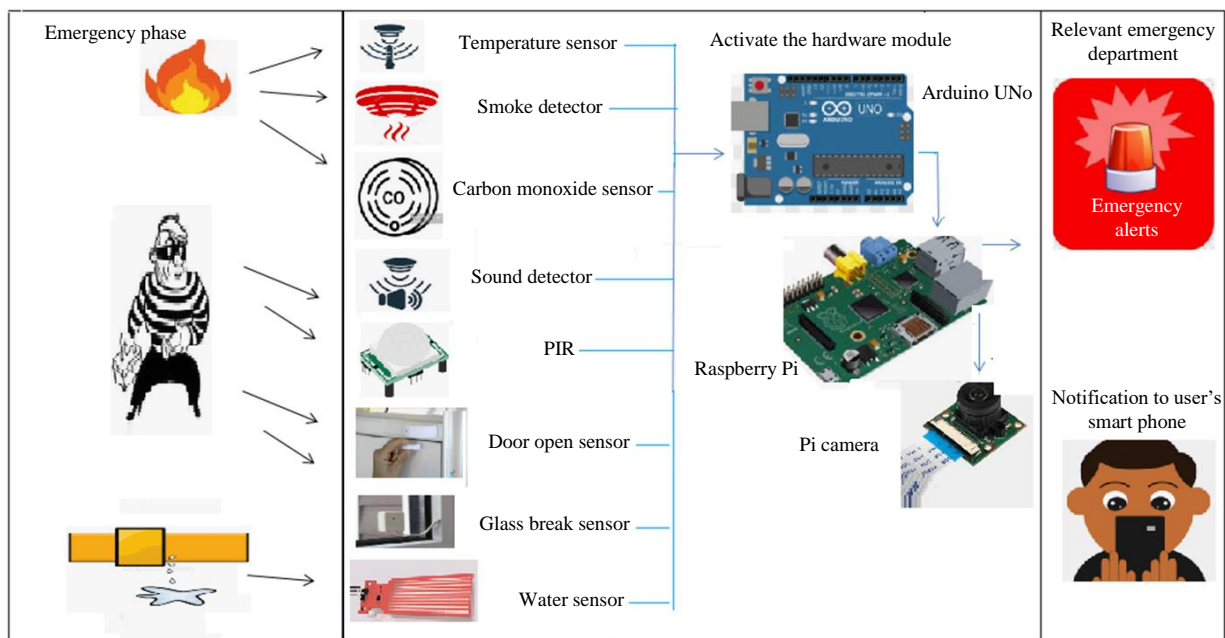

Fig. 1: General topology representation of the proposed architecture

Fig. 2: System workflow

Fig. 3: Proposed system architecture

1328

Raspberry Pi 3 Model B was used as the processing module. We used a PIR motion sensor, sound detector, door open sensor and glass break detector to detect an intruder. Temperature sensors, a carbon monoxide detector and a smoke sensor were used for early fire detection. A water sensor is used to report the water leakage case. All sensors were connected to the Arduino for easy sensor data handling. Arduino is connected to the Raspberry Pi via the USB port. This is by far the easiest method that minimizes wiring and hassle. To capture an intruder picture, the Raspberry Pi Camera Module is connected to the RPi via the camera module port. For sending and receiving SMS text messages, a GSM modem is connected up to the Raspberry Pi. The Raspberry Pi 3 is also connected to the internet so that the system can send the picture and the theft video to be stored in the cloud.

C. Software Design

In this section, we show the most important points about the proposed system programming. The user starts activating the system in Raspberry Pi. A fire, a water leakage, or intruder detection are handled by the relevant sensors. Arduino sends the true or false sensed values to Raspberry Pi. Raspberry Pi 3 controls the Pi camera. Photo captured and video recording is triggered after Arduino sends the data. Raspberry Pi sends notifications to the user's smartphone and the relevant emergency department. After the execution of the emergency response plan, the important data regarding the accident is stored in the central cloud database.

The Raspberry Pi and Arduino are considered the ideal match for real-time applications. The Arduino IDE is already included in the raspbian properties. We can install it using the code "$ sudo aptget install arduino". More details can be found in (Debian, 2012). The Raspberry Pi Camera Module is connected to Raspberry Pi 3 via camera module port (Fig. 4). The camera is enabled from Raspberry Pi Configuration tool >> Interfaces.

To capture an intruder image, use the code "camera.capture('/home/pi/Desktop/image.jpg')" and "camera.start_recording('/home/pi/Desktop/video.h264')" to record the theft video.

Simulation and Result Discussion

To illustrate the importance of fog computing versus the traditional cloud computing, the simulation was done considering the anti-theft system that uses the PIR and the sound detector. Simulation has been done using the iFogsim toolkit to evaluate the system performance in the form of system latency, total network usage and simulator execution time. The structure of the topology used for the anti-theft system is shown in Fig. 4.

The system has been evaluated on several physical infrastructure configurations which differ in the number of Raspberry Pi and Arduino edge as shown in Table 1. Two placement policies have been evaluated in the physical topology cloud-only placement and fog-based placement. The sensor node is represented in the motion sensor and sound detector, while the smartphone and pi-camera are modeled as an actuator node.

The simulation configurations of the different devices (MIP-RAM-UP Link BW-Down Link BW-Busy and Idle power) are described in Table 2. While the Network latency between devices is tabulated in Table 3.

We conducted several simulation runs and the average results were computed to avoid the effect of the simulation time overhead and machine busy and idle power. The results are a clear demonstration of how the system works faster and performs better in the fog computing scenario. System latency and system delay comparison is illustrated in Table 4. Figure 5 and 6 show the comparison between cloud and fog-based on network usage and simulation time.

A. System Latency and System Delay

The Building-Security system is related to security and detection both, so latency is the most vital parameter to achieve a quick emergency response. The system latency and delay comparison between cloud and fog-based is given in Table 4. The average latency of the fog-based system is 62.8 ms where the latency in the case of the cloud scenario is 94.1 ms. Latency reduction is achieved through processing the gathered data on fog nodes. The simulation also shows lower values of the delay between the PIR sensor and the Raspberry Pi (emission of data, processing and then forwarding to gateway and Arduino to raspberry pi), where the delay is 47.5 and 89.3 ms for fog-based and cloud-only respectively.

Table 1: Different simulation configuration

	NO. of raspberry Pi	No. of Arduino Edge
Configuration 1	1	2
Configuration 2	2	4
Configuration 3	4	8
Configuration 4	10	4

Table 2: Fog scenario simulation configuration

	Cloud	Fog device data center	Raspberry pi	Smart phone
MIP	44800	2800.000	2441.000	1000.00
RAM	40000	4000.000	1000.000	512.00
UP Link BW	100	10000.000	1000.000	1000.00
Down link BW	10000	10000.000	1000.000	100.00
Level	0	1.000	1.000	2.00
Busy Power	16*103	107.339	107.339	100.25
Idle Power	16*82.25	83.433	83.433	80.41

Table 3: Network latency between devices

Source	Destination	Latency (ms)
Cloud	FOG_DC	50
FOG_DC	Raspberry pi	4
Raspberry pi	Arduino Edge	2
Raspberry pi	Smart Phone	30

Table 4: System latency and system delay comparison

	Fog-based	Cloud-only
System latency (ms)	62.80465	94.1056
Message transfer (ms)	0.072917	0.048214
Motion Sensor (ms)	12.50575	13.80355
Motion Sensor to Raspberry (ms)	47.52673	89.29787
Sound detector (ms)	0.189427	0.202921
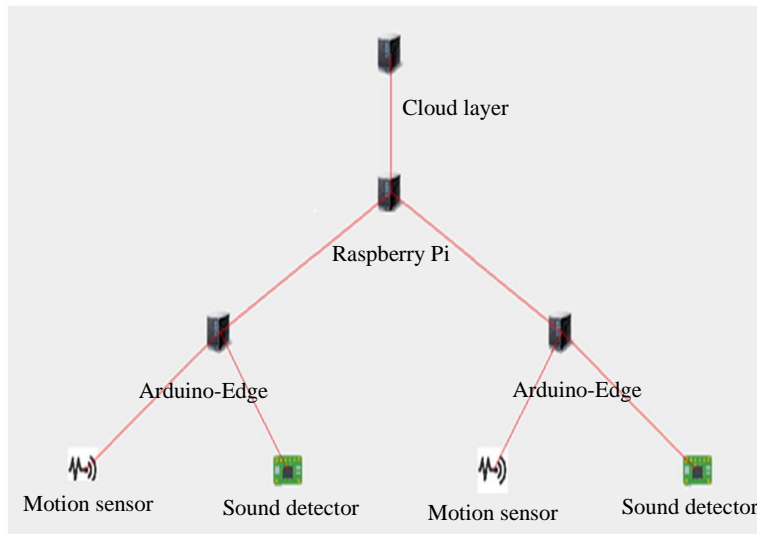
Fig. 4: Network topology for anti-theft system
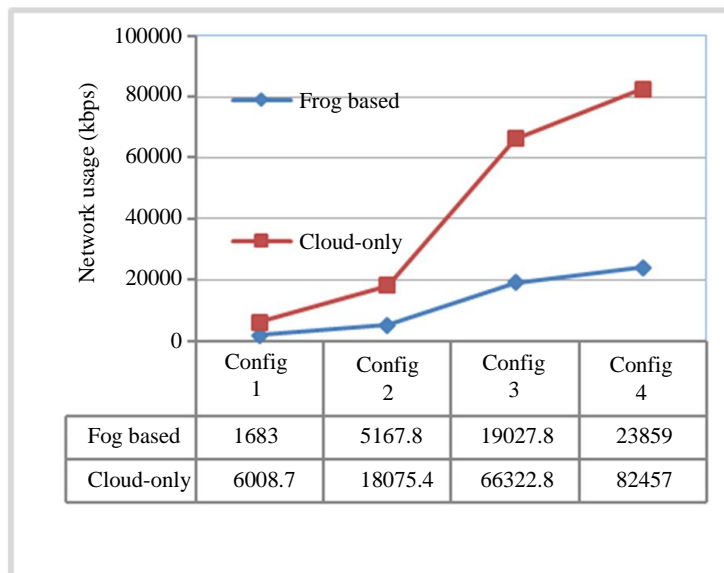
Fig. 5: Network usage for cloud and fog computing

	Config 1	Config 2	Config 3	Config 4
Fog based	3509	6284.667	12243.33	12828
Cloud-only	4229.333	7429.667	12376	13583
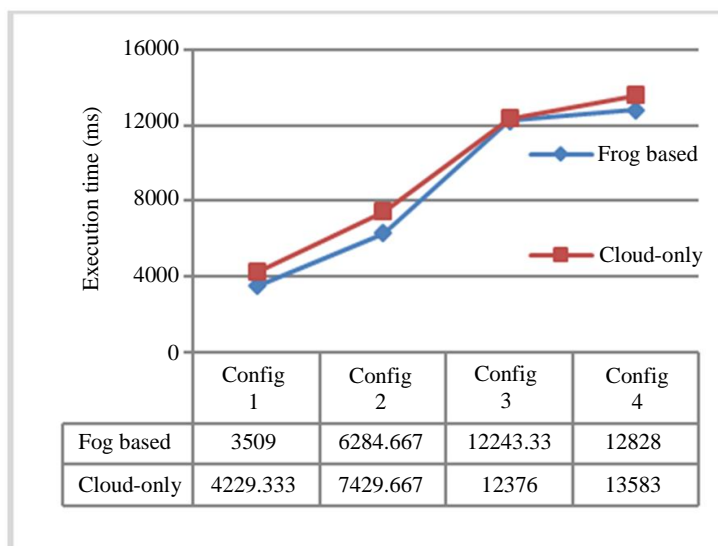
Fig. 6: Simulation time for cloud and fog-based

B. Network Usage

As shown in Fig. 5 the total network usage is significantly less in the case of fog computing. Where network congestion and slow speed transmission occur when only-cloud computing is used due to the increased traffic. The average network usage for cloud-only and fog-based is 43215 and 12434 kbps respectively. Figure 5 also demonstrates that as the number of devices connected to a network increase, the difference between network usage values of the two scenarios increases. For the first configuration, the difference is 4325 and for configuration 2, 3 and 4, the difference in the network usage values was 12908, 47295 and 58598 respectively. Thus, we can conclude that the increased number of connected devices can demonstrate the importance of using fog computing as it increases throughput and transmission speed.

C. Simulation Time

Execution time for various configurations was measured and illustrated in Fig. 6. The simulation time increases as the number of connected devices increase. The increase in simulation time is almost linear for both fog-computing and traditional cloud computing scenarios. The simulation time varies from 3.5 sec to 12.8 sec for the fog scenario and from 4.2 to 13.5 sec for cloud computing. We can conclude that simulation can be run in an acceptable time about 8.5 sec even if a considerable number of devices are added.

Conclusion

This paper has proposed a smart-building security system based on IoT and fog technology. The proposed system consists of Raspberry Pi 3, Arduino, several sensors and a Pi camera. The novelty of this system is using the raspberry as a fog node to allow efficient and localized processing of data.

The performance of the proposed system is evaluated using the iFogSim toolkit. The simulation shows that the average latency is 94.1 and 62.8 ms for cloud-only and fog-based scenarios respectively, which decreased by 33.26%. Also, the value of the delay between the PIR sensor and the Raspberry Pi has been decreased by 46.8% in the case of fog-based.

The simulation also illustrates on average, the network usage decreases by 4325, 12908, 47295 and 58598 for the different tested configurations. The network usage reduction is about 71% in the case of fog-based.

Finally, the iFogSim has been evaluated by measuring the simulation time, which proves that simulation can be run in an acceptable time of about 8.5 sec. In the future, this model will be verified in a real fog environment for practical realization.

Acknowledgment

Author's Contributions

Maha Medhat: Conducted the research, performed the simulation, compared the results and wrote the manuscript.

Khaled El-Shafey: Reviewed the simulation results and ensured their validity.

Ali Rashed: Conceived of the presented idea and designed the research plan.

Ethics

The authors declare that there are no competing interests, the final version of this manuscript have approved by the authors and all the content of this article is original and never been published anywhere else.

References

Al Rasyid, M. U. H., Saputra, F. A., & Prasetiyo, A. (2018, October). I-ON Smart Controller: Portable Smart Home Solution Based on Arduino And Raspberry Pi. In 2018 International Conference on Applied Science and Technology (iCAST) (pp. 161-164). IEEE.

AlHammadi, A., AlZaabi, A., AlMarzooqi, B., AlNeyadi, S., AlHashmi, Z., & Shatnawi, M. (2019, March). Survey of IoT-Based Smart Home Approaches. In 2019 Advances in Science and Engineering Technology International Conferences (ASET) (pp. 1-6). IEEE.

Cisco Systems. (2015). Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are.

Dar, B. K., Shah, M. A., Islam, S. U., Maple, C., Mussadiq, S., & Khan, S. (2019). Delay-aware accident detection and response system using fog computing. IEEE Access, 7, 70975-70985.

Dar, B. K., Shah, M. A., Shahid, H., Fizzah, F., & Amjad, Z. (2018a, September). An Architecture for Fog Computing Enabled Emergency Response and Disaster Management System (ERDMS). In 2018 24th International Conference on Automation and Computing (ICAC) (pp. 1-6). IEEE.

Dar, B. K., Shah, M. A., Shahid, H., & Naseem, A. (2018b, November). Fog computing based automated accident detection and emergency response system using android smartphone. In 2018 14th International Conference on Emerging Technologies (ICET) (pp. 1-6). IEEE.

Debian. (2012). Arduino and RasPi Get Connected! https://www.raspberrypi.org/magpi-issues/MagPi07.pdf

Dutta, J., & Roy, S. (2017, January). IoT-fog-cloud based architecture for smart city: Prototype of a smart building. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 237-242). IEEE.

Gupta, H., Vahid Dastjerdi, A., Ghosh, S. K., & Buyya, R. (2017). iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. Software: Practice and Experience, 47(9), 1275-1296.

Habibi, P., Farhoudi, M., Kazemian, S., Khorsandi, S., & Leon-Garcia, A. (2020). Fog Computing: A Comprehensive Architectural Survey. IEEE Access, 8, 69105-69133.

Khakimov, A., Muthanna, A., & Muthanna, M. S. A. (2018, January). Study of fog computing structure. In 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 51-54). IEEE.

Kumbhar, D., Singh, D., Abbas, M., Alex, M., & Yadav, A. (2018). IoT Based Home Security System Using Raspberry Pi 3. International Journal of Innovative Research in Computer and Communication Engineering, 6(4), 1-8.

Lavassani, M., Forsström, S., Jennehag, U., & Zhang, T. (2018). Combining fog computing with sensor mote machine learning for industrial IoT. Sensors, 18(5), 1532.

Mahmud, R., & Buyya, R. (2019). Modelling and simulation of fog and edge computing environments using iFogSim toolkit. Fog and edge computing: Principles and paradigms, 1-35.

Mukherjee, M., Shu, L., & Wang, D. (2018). Survey of fog computing: Fundamental, network applications and research challenges. IEEE Communications Surveys & Tutorials, 20(3), 1826-1857.

Naha, R. K., Garg, S., Georgakopoulos, D., Jayaraman, P. P., Gao, L., Xiang, Y., & Ranjan, R. (2018). Fog Computing: Survey of trends, architectures, requirements and research directions. IEEE access, 6, 47980-48009.

Paul, A., Pinjari, H., Hong, W. H., Seo, H. C., & Rho, S. (2018). Fog computing-based IoT for health monitoring system. Journal of Sensors, 2018.

Peng, X., Ota, K., & Dong, M. (2020). A broad learning-driven network traffic analysis system based on fog computing paradigm. China Communications, 17(2), 1-13.

Rani, R., Lavanya, S., & Poojitha, B. (2018). IoT Based Home Security System Using Raspberry Pi with Email and Voice Alert. International Journals of Advanced Research in Computer Science and Software Engineering ISSN, 119-123.

Saheed, A., Adeoye Adeyinka, O. M. & Zulikha, A. (2019). Access control, fire prevention and surveillance security system. Journal of Mechatronics and Robotics, 3(1), 563-570.

Sarkar, I., & Kumar, S. (2019, July). Fog Computing Based Intelligent Security Surveillance Using PTZ Controller Camera. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.

Shah, S. C. (2017). A Mobile Ad hoc Cloud Computing and Networking Infrastructure for Automated Video Surveillance System. Journal of Computer Science, 13(12), 767-780.

Stojkoska, B. R., & Trivodaliev, K. (2017, November). Enabling internet of things for smart homes through fog computing. In 2017 25th Telecommunication Forum (TELFOR) (pp. 1-4). IEEE.

Surantha, N., & Wicaksono, W. R. (2019). An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients.

Tanwar, S., Patel, P., Patel, K., Tyagi, S., Kumar, N., & Obaidat, M. S. (2017, July). An advanced internet of thing based security alert system for smart home. In 2017 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 25-29). IEEE.

Taryudi, D. B. A., & Budi, W. A. C. (2018). Iot-based integrated home security and monitoring system. In IOP Conf. Series: Journal of Physics: Conf. Series (Vol. 1140, p. 012006).

Yuan, L. (2015, December). Study of Smart Home System Based on Cloud Computing and the Key Technologies. In 2015 International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 968-972). IEEE.