International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

Low Cost Energy Efficient Smart Security System with Information Stamping for IoT Networks

M. S. Venkata Chandrashekar[1], S. Bharath[2], Suhas P. Shetty[3], Suraj S. Kashyap[4], B. Tahir Naquash[5]
[1,2,3,4]*Student, Department of Computer Science Engineering, Alva's Inst. of Engg. and Tech., Moodbidri, India*
[5]*Assistant Profesor, Dept. of Computer Science Engineering, Alva's Inst. of Engg. and Tech., Moodbidri, India*

***Abstract*: A security system with CCTV and other network nodes in IoT deals with large amount of data, so the need for devices with larger storage space comes into the picture which is a bit costlier. Traditional security systems are more power consuming as it has to record for 24x7 with more throughput but less efficient. Thus need human in middle to upload into cloud is needed. In this work, we propose a low-cost energy efficient smart security system for CCTV with other network nodes. Whenever motion is detected by passive infrared (PIR) sensor, at that time only the camera and all other security sensor nodes in network are activated (Switched on), the captured video and information (sensor data) are stamped on the image using image processing techniques on Python platform. It will be stored in a local storage device, after certain threshold (based on sensitivity of the location) data will be uploaded into the cloud along with data log created during processing stage by Python programming model. In this way, we can reduce the amount of data to be stored (as no recording when idle), consumed power (as device is switched off when idle), maintenance cost (as fully programmed). No need for human in middle for uploading data into the cloud (as program will upload data in to cloud). Because of time, date and information (data from sensor nodes) stamping on each frame of video using python programming model video access becomes easier, as data log will be created.**

***Keywords*: IoT; PIR sensor; Storing in cloud; information stamping; Motion Detection.**

1. Introduction

Internet of every Things is a network of connected "Things" like vehicles, buildings, embedded systems, sensors, as well as people. IoT enables these things to collect, store and exchange data of interest to complete various tasks like security of buildings (CCTV), traffic control and monitoring, patient health monitoring, environmental monitoring, system condition prognostics and prediction, smart grid, smart buildings, smart cities, and so on as discussed in [1].

Specifically, IoT devices allow physical objects to store data and exchange data without the intervention of humans (Machine to Machine communication takes place) across the existing network, cloud infrastructures and take intelligent decisions results in improving accuracy, and economic benefit. Intel has estimated that the number of connected devices across worldwide will rise from 20 billion in2017 to 200 billion by 2020. IoT has a variety of applications in security, health, consumer, and military applications [2]. Therefore, itis significant to effectively and efficiently store the data produced by the IoT devices (sensor nodes). So that IoT devices can be adopted drastically towards a connected future with making the products cheaper by utilizing less storage space which in turn decreases the cost of device by the method discussed in this paper for Security cameras.

Due to increasing amount of data sources, advances in the Internet of Things and Big Data technologies and the availability of a wide range of machine learning algorithms offers new potential to deliver analytical services to citizens. However, there is still a gap in combining the current state of the art in an integrated framework that would help in reducing development, design costs and enable new kind of services [3].

In recent smart city applications there is a large scale deployment of cameras and other sensors around the globe these cameras act like an eye of a sensory network which includes smart transportation [4], lighting [5], health [6], environment [7], and disaster management [8]. Internet of Things architecture is a fundamental requirement in these applications, which prescribes a virtual platform for globally identifiable objects (each object having a unique IPv6 address) that have sensing and communication capability [9].Internet of Things architecture differs significantly from a traditional Wireless Sensor Network (WSN) because an IoT sensor can efficiently communicate to an IoT-cloud environment where the data can be acquired and transmitted virtually anywhere and processed in the cloud, which can be at any cognitive location. The IoT sensor networks use a different set of communication techniques like NB-IoT, LoRA, Sigfox etc., with message protocols like AMQP, COAP etc. Internet of Things treat each sensor as a "virtual object" with an abstracted hardware layer. While sensors can be deployed in the entire city, dedicated to a specific sensing task or a general sensing task, some of the sensing tasks can be outsourced to city residents by making them utilize their smart electronic gadgets. Even though both of these cases are treated as similar virtual objects in Internet of Things, we define a sensor as dedicated if it is used for

collecting data for a pre-specified task (e.g., sensors deployed to sense environment variables like pressure temperature etc. within a smart city infrastructure to measure O_2 and CO_2 levels [8]). Google's Science Journal application [10] and Tre sight [11] use embedded sensors available in the smartphones (e.g., accelerometer, gyroscope, GPS, microphone, camera) for sensing; we define these built-in sensors as non- dedicated because their users do not use them solely for one application.

A specific devoted and general camera for security systems acts as a sensor differs in terms of system price, performance, efficiency and security. A Dedicated camera sensors require high maintenance and installation costs, while general camera sensors do not need these costs because they are privately owned and maintained by the participants of the smart city who are taken in to position based on the demand [12]. However, volunteer participation is appreciated but it's a bit difficult [13] and the incoherent ad-hoc nature of then on-dedicated sensor networks necessitates more sophisticated data transmission/ allocation solutions, which can degrade application performance. Understanding their operational characteristics is crucial in assessing their performance when they become a part of the IoT virtual sensor network.

A security camera records and stores data on 24X7 basis but most of the data recorded by it during the ideal time (when the presence of human and motion of any other living beings is not there) is not useful to us, this leads to a lot of waste utilization of memory and is to be either manually deleted by the operator repeatedly and has to be uploaded to cloud again and again, since this type of classical system needs a lot of memory and manual work, as both of them are time consuming and costlier (pay for manual labour and storage space). If the thieves attack the secured area and destroy the local storage also then there will be no evidence to catch thieves and the entire purpose of security system is not fully utilized. Thus we propose an intelligent security system to solve this problem with increased efficiency. The objective of this work is designing a novel system for security cameras in IoT networks with event (presence of living being or motion of thing) driven system to store and record the data whenever an event occurs which reduces lot of unnecessary data to be stored in ideal time and also to decrease power consumption as system works only when driven by an event. This system uploads the data directly in to the cloud based on the threshold limit set by us. By this way as data is already in cloud even thief's destroy the local storage we can get it from cloud with the event log and can be analysed to catch them.

2. Related work

The design and implementation strategy of the Smart Security System has raised different works done earlier but we had implemented this work with higher efficiency, low cost, less power consumption, high throughput and less maintenance cost. In this section, we introduce notable previous work implemented.

Big Data: The development of enormous amount of data due to the Internet of things (IoT) is quickly increasing and affecting all areas of technologies and businesses by increasing the benefits for organizations and individuals. The growth of data produced via IoT has played a major role on the big data landscape. Big data can be categorized according to three aspects: volume, variety and velocity.

Security: Due to internet-connected, dynamic heterogeneous nature of IoT environments to be secured creates new security, authentication and privacy challenges. Security attacks in various environments have been identified and security requirements, solutions in all the environments is required based on several scenarios. Power Requirements: Low power consumption is essential in IoT networks due to the use of battery operated devices and the development of ultra-low-power (ULP) electronic devices has opened up opportunities for disruptive systems like the Internet of Things (IoT). By considering all these things into the design objective we have designed our system.

3. System architecture

The system architecture for this proposed work is as shown in Figure 1 it consists of multiple blocks that recognize the event, drives the event, information stamping and uploading the stored data to cloud IoT networks after the specified interval from the local storage device.

A. Event detection

Fig. 1. Block diagram of proposed security system

In this block air sensor is used to detect the activity surrounding (focal area of) the camera [14], similar type of work is adopted by us to detect the presence of living beings in the camera focal area and is used to trigger the camera and other sensor nodes in network which saves a lot of energy during ideal time (i.e. system is switched on only when needed) and also decreases the length of video by which we can decrease the storage space needed as less recording time, because of time stamping video is easily accessible. PIR sensors are more complicated than many of the other sensors explained in these tutorials (like photocells, FSRs and tilt switches) because there

are multiple variables that affect the sensors input and output. The PIR sensor itself has two slots in it, each slot is made of a special material that is sensitive to PIR. The lens used here is not really doing much and so we see that the two slots can 'see' out past some distance (basically the sensitivity of the sensor). When the sensor is idle, both slots detect the same amount of PIR, the ambient amount radiated from the room or walls or outdoors. When a warm body like a human or animal passes by, it first intercepts one half of the PIR sensor, which causes a positive differential change between the two halves. When the warm body leaves the sensing area, the reverse happens, whereby the sensor generates a negative differential change. The Figure 2 shows PIR sensor housed in a hermetically sealed metal can to improve noise/temperature/humidity- immunity. There is a window made of PIR transmissive material (typically coated silicon since that is very easy to come by) that protects the sensing element. Behind the window are the two balanced sensors [15]. This sensor produces an output voltage of 3.3v which is used to drive the load (the security system).

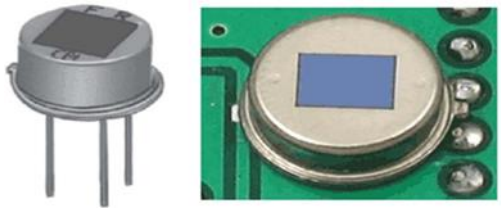

Fig. 2. A PIR Sensor

B. Information Collection

Smart cameras are real-time video acquisition and processing systems that combine on-board sensing, processing and communication capabilities and play an important role in several IoT applications [16]. However, security and privacy protection have become a major concern due to their widespread deployment, the sensitive nature of the captured data and the open infrastructure [17], [18]. Basic security objectives for a smart camera are thus (i) to prove the originality of images or video data (integrity), (ii) its origin (authenticity of the visual sensor) and (iii) to avoid third parties unauthorized access (confidentiality) throughout the entire lifetime of the data.

These smart cameras will be activated once the event is detected by the event detecting PIR sensors, the security camera network for surveillance is switched on and starts recording the video and each video is information stamped using PYTHON commands in the pre-processing stage and then sent for storage [19]. Here the storage may be local storage but the end will be cloud as for slow network connections it need time to upload data as IoT data be generated quite rapidly, the volume of data can be huge and the types of data can be various. In order to address these potential problems, this paper proposes a data storage method not only enabling efficient storing of massive IoT data but also integrating both structured and unstructured data (i.e. Data collected by sensors and camera) during the storage process by using intelligent(programmed) Raspy-Berry Pi module .As we are using the device for IoT networks the output interfacing must be a web based display, this is why we are using Raspy-Berry Pi module a system on chip, which has inbuilt Python platform, so it is easier to program and interface the local storage with cloud and upload the data.

C. Storage

In storage block there will be no special purpose except that it stores the recorded data and we have used the method [20] which is a motion estimation hardware model that is suitable to implement the circuit and cloud uploading. Different motion estimation configurations are considered. Supporting smaller block sizes is shown to impose significant memory cost in hardware although the coding gain achieved through supporting them is relatively smaller. Hence, depending on target encoder specifications, the decision can be made not to support certain block sizes. The general working and codec are discussed in [20].

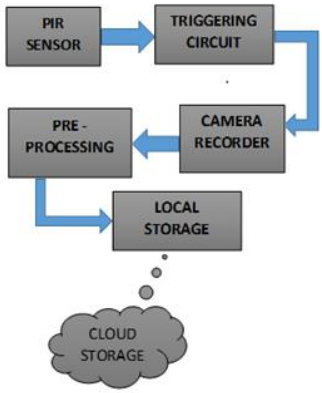

Fig. 3. Implementation of proposed Security System

4. Implementation

Design procedure and implementation are depicted by the flowchart as shown in Figure3. As already stated in the system architecture of this paper a PIR sensor is used to trigger the recording in the camera and activate any other sensor networks associated with it. The camera once activated circuit is powered up, recording continues until the activity of living being is there and once the activity of living being is null the trigger circuit starts discharging and after reaching certain value camera pauses/stops recording.

The part of PIR sensor and triggering circuit is as shown in Figure 4. The PIR led in Figure 4 once detects the thermal waves of a certain threshold (i.e. living being) it will switch on the BC547 transistor. The voltage will be transferred to the NO (open of relay) and this diode will trigger the positive voltage and load is connected to the AC mains thus camera recorder and the sensory network will be switched on, the recording starts and the data is stored. If PIR sensor has sensed null (below threshold i.e. no human being) it will stop giving sufficient voltage at Op pin and thus transistor BC547 is switched off and

NO will get to negative supply voltage thus the relay open and since no closed connection mains will be switched off. So the camera stops recording and all sensory network will also be switched off.

Figure 5 shows the pre-processed image with time and date stamped on it at the left top corner the time and date stamping can be done in MATLAB code but as we are using the RaspyBerry Pi module we have used PYTHON programming for information stamping on the video.

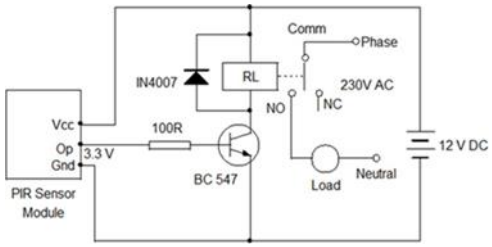

Fig. 4. PIR triggering circuit with system as load

Once date, time and information from other sensor nodes in the IoT network are stamped in the pre-processing stage then the recorded data is simply stored at the local storage device. The Raspy-Berry Pi module which is intelligent node checks the percentage of data stored in the local storage device, if it reaches certain percentage set by us then the recorded data is uploaded to cloud or based on the sensitivity of the location it will directly upload the data into the cloud (i.e. user can set the time range starting from 1sec or percentage of data in the local storage device).

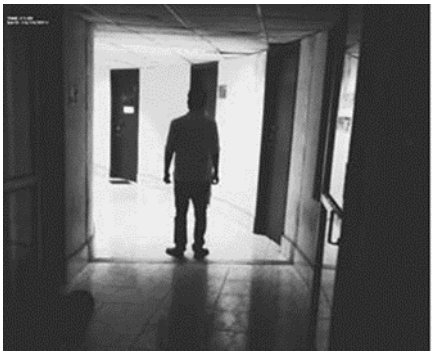

Fig. 5. Implementation of proposed Security System

The information stamping of the video frame, data uploading into cloud can be achieved in the pre-processing stage by using the algorithm as shown in Figure 6. In the pre-processing stage once the data is acquired when it is processed in the Python, if the event is detected then time and information are to be stamped on to the frame and if it reaches the storage limit or time limit set by user then the data will be uploaded into the cloud.

For uploading data into the cloud as we are dealing with the IoT networks the input and output nodes will be web-based application controllers for this work as we are using the Raspy-Berry Pi module we need to interface the nodes to the web application. The raspy-berry pi module acts as an intelligent node for storing and uploading data into the cloud, by making intelligent decisions (according to the programme dumped in it).

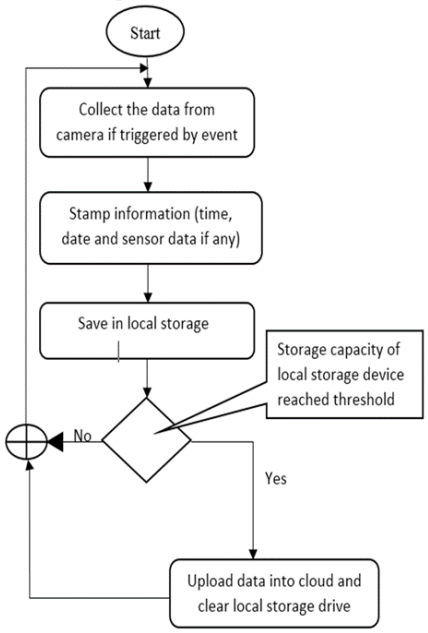

Fig. 6. Algorithm for data uploading and Pre-Processing

The implementation of the interface for Raspy-Berry pi with a smart camera and web server for data collection and data storage in the cloud can be done by python programming script as the python script is easier and widely available for all platforms with Inter-portability across different devices and platforms. The algorithm for the interfacing and uploading to cloud is as shown in Figure 5.

We have used the python programing model with deep learning platform jupyter notebook to upload the video in to the cloud and as already discussed the we have used python programming to information stamp every frame and maintain the data log at what times we are information stamping this will make sure that at the time event is being triggered the information is stamped on to the image. In IoT network the information stamped on the frame is not only the date and time but it contains the total information collected by the huge sensory nodes in the IoT network.

5. Result discussion

The Graph shows Activity Vs Power Consumption in mW (mille Watt) with respect to time for different security systems as shown in Figure 7. It compares the power consumption of the system on chip (SoC) smart camera with respect to the normal CCTV camera which has a power rating of 160mW as the normal camera is always switched on and no triggering circuit its power consumption remains constant but for smart camera

because of triggering circuit the camera is switched OFF and ON. So the average power consumption decreases. Since the camera is recording at intervals of time (i.e. during presence of human activity) length of video decreases, Raspy- Berry Pi interface uploads data into the cloud which reduces the need for manual labor.

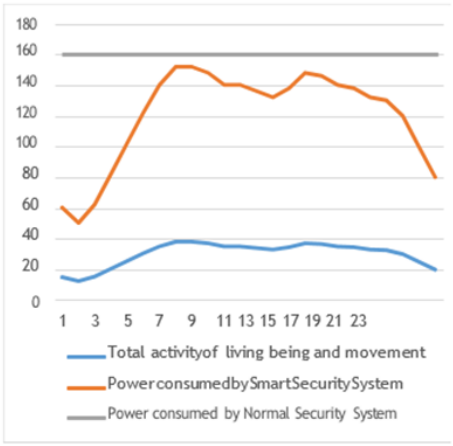

Fig. 7. Activity vs. Average Power Consumption per Hour in mille Watt with respect to time for different systems

6. Conclusion

In this paper a major problem faced by a security camera in IoT networks like more power consuming, data storing, need for storing long length videos, uneasy access of video data and need of manual labor work have been solved using a python programming model in Raspy-Berry pi. In this paper a special PIR motion detection sensor has been used to trigger security system, camera recorder and sensor network during the presence of living beings and any movement of other activity. So the recording length decrease which in turn decreases the required space for the video storage, decreases the length of video, power consumption and also due to time stamping on each frame during pre-processing makes the video more accessible to the user, saves lot of power, storage space and also automatic uploading of data into cloud storage makes the system more efficient. As the IoT era is being run only M2M (Machine to Machine) Communication occurs this type of system can be put in living being restricted areas for both safety and security by adding a piezo electric buzzer with Wi-Fi to the system as an alarming sound for detection of activity of living being in living being restricted areas.

References

[1] A. Whitmore et. al. “The Internet of Things—A survey of topics and trends” in Information Systems Frontiers, Volume 17, Issue 2, pp 261–274, April 2015.

[2] S. Madakam et. al. “Internet of Things (IoT): A Literature Review” in Journal of Computer and Communications, Volume 3, pp 164-173, 2015.

[3] Martin Strohbac et. al. “Towards a Big Data Analytics Framework for IoT and Smart City Applications” in Modelling and Processing for Next-Generation Big-Data Technologies, pp 257-282, Jan. 2013.

[4] F. Calabrese, M. Colonna, P. Lovisolo, D. Parata, and C. Ratti, “Real-Time Urban Monitoring Using Cell Phones: A Case Study in Rome,” IEEE Trans. on Intelligent Transportation Systems, vol. 12, no. 1, pp.141–151, March 2011.

[5] A. Sevincer, A. Bhattarai, M. Bilgi, M. Yuksel, and N. Pala, “Lightnets: smart lighting and mobile optical wireless networks –A Survey,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp.1620–1641, 2013.

[6] R. Khatoun and S. Zeadally, “Smart Cities: Concepts, Architectures, Research Opportunities,” Communications of the ACM, vol. 59, no. 8, pp. 46–57, Jul. 2016.

[7] P. Rashidi, D. J. Cook, L. B. Holder, and M. Schmitter-Edgecombe, “Discovering Activities to Recognize and Track in a Smart Environment,” IEEE Trans. on knowledge and data engineering, vol. 23, no. 4, pp. 527–539, 2011.

[8] M. Habibzadeh, W. Xiong, M. Zheleva, E. K. Stern, B. H. Nussbaum, and T. Soyata, “Smart City Sensing and Communication Sub- Infrastructure,” in IEEE Midwest Symposium on Circuits and Systems, Boston, MA, Aug 2017.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, andM. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[10] Google, “Science Journal,” https://makingscience.withgoogle.com/science- journal.

[11] Y. Sun, H. Song, A. J. Jara, and R. Bie, “Internet of Things and Big Data Analytics for Smart and Connected Communities,” IEEE Access, vol. 4, pp. 766–773, 2016.

[12] M. Pouryazdan, B. Kantarci, T. Soyata, L. Foschini, and H. Song, “Quantifying User Reputation Scores, Data Trustworthiness, and User Incentives in Mobile Crowd-Sensing,” IEEE Access, vol. 5, pp. 1382–1397, Jan 2017.

[13] M. Pouryazdan, C. Fiandrino, B. Kantarci, D. Kliazovich, T. Soyata, and P. Bouvry, “Game-Theoretic Recruitment of Sensing Service Providers for Trustworthy Cloud-Centric Internet-of-Things (IoT) Applications,” in Globecom Workshops, Washington, DC, pp. 1–6, Dec 2016.

[14] C.Twumasi et al “Energy Saving System using a PIR Sensor for Classroom Monitoring” in IEEE PES-Power Africa, pp.347-351, June 2017.

[15] Adafruit “sensors” https://learn.adafruit.com/pir-passive-infrared-proximity-motion sensor/how-pirs-work.

[16] M. Reisslein, B. Rinner, and A. Roy-Chowdhury, “Smart camera networks [guest editors’ introduction],” Computer, vol. 47, no. 5, pp. 23–25, May 2014.

[17] T. Winkler and B. Rinner, “Security and privacy protection in visual sensor networks: A survey,” ACM Comput. The survey, vol. 47, no. 1, pp. 2:1–2:42, May 2014.

[18] E. Fernandes, J. Jung, and A. Prakash, “Security analysis of emerging smart home applications,” in Proc. IEEE Symposium on Security and Privacy (SP), pp. 636–654, May 2016.

[19] L. Jiang et al “An IoT-Oriented Data Storage Framework in Cloud Computing Platform” in IEEE Transactions on Industrial Informatics Volume: 10, Issue: 2, pp 1443-1451, May 2014.

[20] M. E. Sinangil et. al., “Memory Cost vs. Coding efficiency Trade-Offs for HEVC motion Estimation Engine” in 19th IEEE international conference on image processing, pp.1533-1536, Sept. 2012.