International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

IoT based Smart Home Security

Dr. C Priya[1], Devahariharan B[2], Thamarai Kannan A[3], Lokesh M[4], Gokul Seshanth P[5]

[1]*Assistant Professor, Dept. of Electronics and Instrumentation Engineering, Sri Sairam Engineering College, Tamil Nadu, India*
[2,3,4,5] *Student, Dept. of Electronics and Instrumentation Engineering, Sri Sairam Engineering College, Tamil Nadu, India*

---***---

Abstract - In this paper, the structure and execution of expanded Internet of Things (IoT) called IoT based smart home security, for an efficient, asset proficient, and constant real-time security management framework is done. The framework, comprising of edge-fog computational layers, will help in criminal avoidance and foresee criminal acts in an intelligent home condition. The IoT based Smart Home Security will distinguish and affirm criminal activities in real-time, utilizing Artificial Intelligence (computer based intelligence) and an event driven way to send criminal information to defensive administrations and police units causing quick activity while monitoring the activities. In this investigation, an IoT based Smart Home Security testbed model is executed and assessments performed on outcomes show better performance by the proposed system in terms of resource efficiency, agility, and scalability over the traditional IoT surveillance systems and state-of-the-art approaches.

Key Words: IoT, edge-fog computational layers, Artificial Intelligence

1.INTRODUCTION

An Intelligent Home Condition (IHC) consists of various applications of ubiquitous computing that integrates smartness into dwellings for comfort, healthcare, safety, security, and energy conservation. An IHC is monitored by ambient intelligence to produce context-aware services and to facilitate safety and security management. A security management system is meant to produce complete safety from robbery, sabotage, and intrusion by monitoring the interior and external IHC, using surveillance cameras. Various cyber-physical systems widely adopt the utilization of intelligent video surveillance, for automatic and accurate identification of events and objects in a very target scene. IVS is used to predict and interpret the activity of a scenario without any human intervention. Protective services and authorities often fail to retort to crime incidents efficiently. Therefore, in most cases, when an occasion occurs, authorities visit the situation of the incident, retrieve the content manually from the camera, and so proceed to spot relevant footage either by watching the complete length of the video or by processing it through specialized video analytics algorithms. Thus the reactive approach is, of course, inefficient for preventing crimes. An efficient crime predictive system could enable robust security management in an IHC by identifying preventive procedures. The video closed-circuit television in an IHC consists of the many cameras that may produce an outsized amount of surveillance data, both photo, and video. This might lead to heavy network congestion and impose complicated processing load on individual devices and systems. This paper is to discuss on the IoT integrated intelligent video surveillance framework to produce a good solution to the present problem.

2. LITERATURE SURVEY

2.1 An Intelligence System for Video Surveillance in IoT Environment

The main objective of this project is to share visual information on collision detection, location of accident and traffic information with nearby hospitals and police station. Here the camera sends the video automatically to a cloud-based network for multiple access by individual cloud customers. In this project, the camera is continuously monitoring the events and is connected to the cloud network via the internet. It is easy to access the information stored in the cloud network by others to control the traffic flows and handle emergency situations as and when they arise in near real-time. Employing this, the response time can be reduced.

2.2 A robust occupancy detection and tracking algorithm for the automatic monitoring and commissioning of a building

The focus of this study is that the 24hours daily monitoring of buildings for commissioning purposes. The proposed monitoring system enables the continual detection and tracking of the occupants with the help of an image-based depth sensor and a programmable pan-tilt-zoom (PTZ) camera, even under dim lighting conditions. The SVM-based observation measurement provides a more reliable tracking performance. This paper presents a sturdy day-and-night people tracking and counting algorithm. The function of large-scale field monitoring is realized by employing a PTZ camera network instead of a typical fixed camera. Furthermore, supported the depth image sensor, the contour information of the occupant is visiting be applied for more accurate activity recognition. The positive results of the occupancy detection and therefore the tracking algorithms are applied to count the quantity of individuals and to observe a building in the experiment.

2.3 Choice of Application Layer Protocols for Next Generation Video Surveillance Using Internet of Video

Video surveillance has become appearing due to the increasing security requirements in each and every moment of life. The next-generation video television (VSS) possesses great challenges in various applications, like intelligent urban surveillance systems and smart cities. In these applications, we'd wish to cater to the fast-growing number of surveillance nodes which introduce several constraints, example, high latency, high bandwidth, high energy consumption, and CPU and memory usage. To accommodate these issues, the internet of video things (IoVT), which is taken into consideration to be a component of the net of Things (IoT), are often a solution. The IoVT consists of visual sensors (i.e., cameras) connected to the net. Unlike conventional systems, under an IoVT framework, the VSS provides multiple layers (i.e., edge, fog, cloud) of communication and deciding by capturing and analyzing rich contextual and behavioral information. Since an appropriate application layer protocol (ALP) can help in alleviating the challenges of future VSSs, the selection of ALPs is incredibly important for IoVT-based systems. Therefore, this paper presents a generic architecture of an IoVT-based VSS and a comparative analysis of several ALPs, like MQTT, AMQP, HTTP, XMPP, CoAP, and DDS, with real-time experimentation. This analysis will assist the users to make a decision on the suitable ALPs in various surveillance applications and determine their suitability at different nodes of the IoVT framework.

3. PROPOSED SYSTEM

This paper is to implement IoT based Smart Home Security, an event-driven edge-fog-integrated video surveillance framework, to execute real-time security management by helping in criminal act prevention and predicting crime events at an Intelligent Home Condition. The proposed IoT based Smart Home Security approach provides a three layer architectural framework that orchestrates event-driven edge devices in an IHC and DL-implemented fog computing nodes to address increasing human security concerns. The system also gives an alert by sending the criminal data instantly to the defensive force or protective service, and thus, it ensures a quick response.

This section describes the security management framework of the proposed IoT based Smart Home Security. The system gives criminal act detection and proactive alerts using edge- and fog-integrated approaches. Fig.-2.1 illustrates the architecture of the system for security management at an Intelligent Home Condition. Camera connected several edge nodes are placed at various points to cover the in and out of a residential unit. The event driven feature deployed in every single edge nodes keeps them on standby unless any appropriate movement from the human intrusion is detected. If movement is recognized, the edge node will take motion-detected pictures and forward those pictures and its own location to a fog node. A single fog node controls multiple edge nodes within one single unit or building. Multiple fog nodes to cover a complete residential area comprising of multiple buildings.

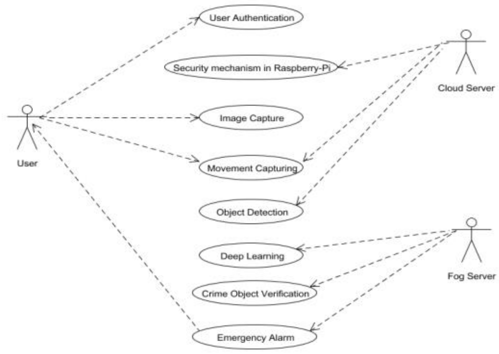


Fig-2.1: Flow of process

The above figure gives the flow of the process, the communication between the servers and image processing hardware and software. With the help of Artificial Intelligence, each fog node can distinguish and recognize a possible criminal activity function and criminal activity object by processing the motion-captured pictures sent by an edge node. If a fog node recognizes and confirms the presence of human and weapons, it will differentiate the types of weapon and immediately dispatch criminal act event information (i.e., a labeled image and location) to the nearest criminal act prevention force (i.e., defensive or protective service in that area) instantly. Each fog node is also able to dispatch criminal act data simultaneously in the form of a cell phone alert notification. Using the criminal act data sent by the fog node, the criminal act prevention force can ensure real-time criminal act prevention before the crime actually happens. The Artificial Intelligence enabled event-driven fog node also neglects any false positive result registered by the edge node. Each criminal act prevention force may receive a crime notification from multiple fog nodes covering a household area. All the fog nodes maintain bidirectional communication with a centralized cloud server within a smart city for reception system updates, criminal act event data mining, statistical analysis, and timely information storage.

The above figure gives the diagrammatic representation of the flow in which the process flows. The algorithm used here is Convolutional Neural Network. This uses Raspberry Pi for the computational process which runs on the software coded with Python. Python is a widely used programming language. It was first introduced in 1991 by Guido van Rossum and developed by Python Software Foundations. It was designed and developed with priority for increasing on code readability, and its syntax allows programmers to share their ideas in lesser lines of code.

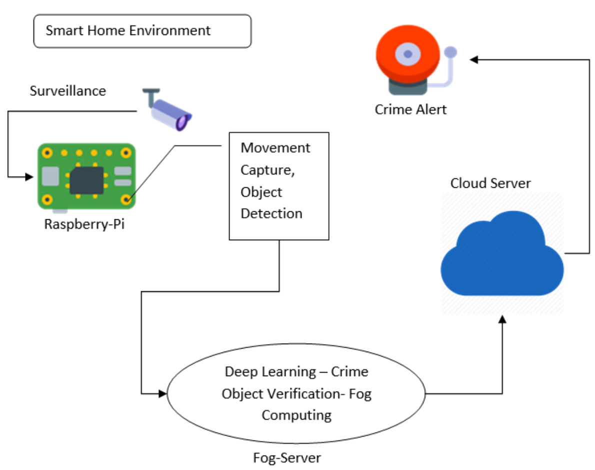


Fig-2.2: Architecture Diagram

The above figure gives the diagrammatic representation of the flow in which the process flows. The low level hardware setup of this project includes a camera connected to a Raspberry Pi. Python language is used for coding for the purpose of image processing for motion detection, weapon detection and for auto-generated mail and mobile application. This android application is developed for mobile phones which can be installed by the residents of the smart home environment and also an auto-generated email which carries the image captured from the camera whenever movement is detected. The mobile application displays the information of type of weapon and number of persons captured by the camera.

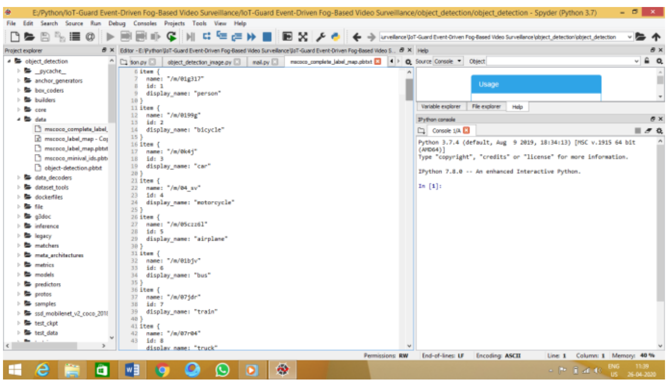
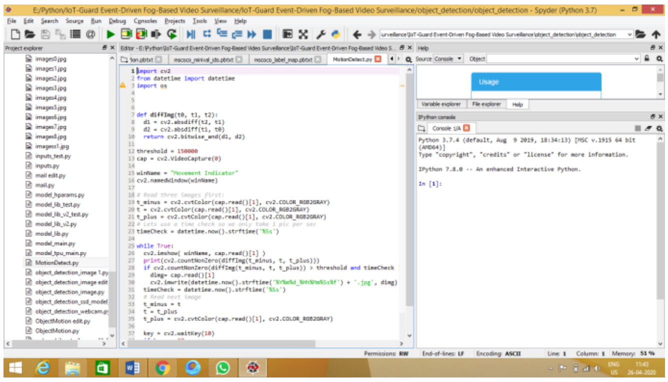


Fig-2.3: Training of Images

A set of images comprising of hundreds of pictures are trained initially for image processing to detect motion and objects. Fig-2.3 gives the trained images label list. The accuracy of this process depends on the number of images been trained.

The part of code done for motion detection is shown in the fig-2.4, which detects any movement and captures the image if any. This helps in implementing high level security.



Fig–2.4 : Code for Motion detection

As a future enhancement, additional features like automatic door and window sealing can be added. This feature will get enabled when there is a detection of human movement and when armed, also to detect other types of weapon.

3. RESULT

In this section, the result of the project implemented is discussed with the output obtained during the execution of the process. As said earlier, a set of images were trained for detection of human movement.

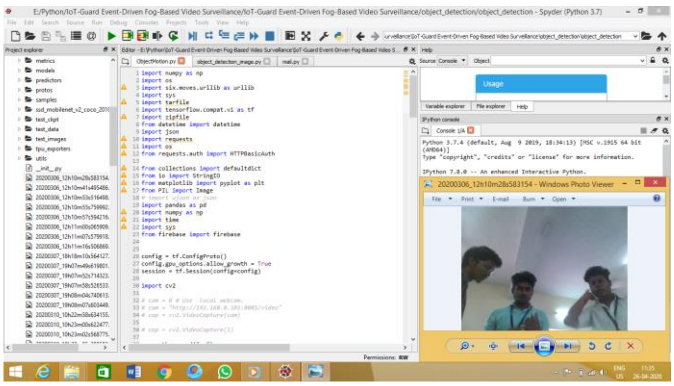
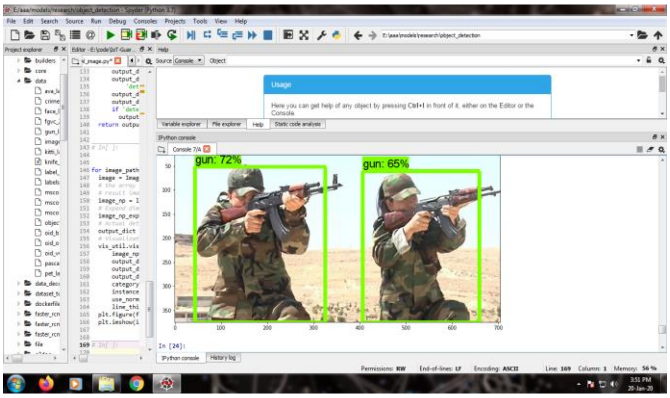


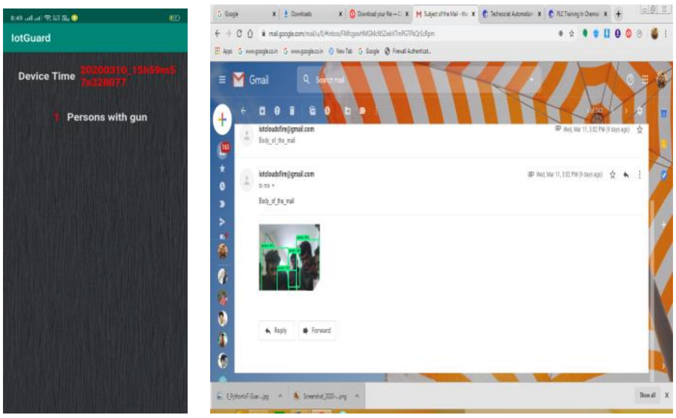
Fig-3.1: Motion detection and captured image

From fig-3.1, whenever there was a movement detected, the images were captured as shown. It also detects the type of weapon carried if any present within the range and also gives information on the type of weapon as shown in fig-3.2.



Fig–3.2: Detection of Weapon

Fig-3.3 (a) & (b) gives the information on the mobile application developed and the auto-generated mail respectively. This auto-generated mail is sent whenever a movement is detected and carries the image captured when the movement was detected.



(a) Mobile application (b) Auto-generated email

Fig-3.3

4. CONCLUSIONS

In this article, the design, deployment, and performance evaluation of the IoT based Smart Home Security, which is an event driven and fog-based smart-surveillance system for real-time criminal act detection and security management has been presented. The application targets security management within a smart home environment under the smart-city paradigm. The suitability and feasibility of the proposed system by deploying a laboratory testbed of the IoT based Smart Home Security and its performance was evaluated. The proposed architecture with and without a video compression algorithm and performance comparison between them along with other IoT based video surveillance architectures was implemented. This system gives highly efficient data output for effective analysis and transfer of information to the desired location. Although the video compression algorithm helped the proposed IoT based Smart Home Security architecture to save 20 percent more storage, it reduced its efficiency, notably in terms of energy and percentage of CPU usage. Therefore, the proposed system is far more efficient even without the video compression algorithm. Then, the auto-generated mail and application ads to the merit that the resident of that house would be able to immediately know when there is any anonymous activity happening around the house. The proposed system can be upgraded in the future by adding other types of crime objects or threat events to the model without changing the system configuration. Moreover, it can be further trained to detect more features in the future, for instance, utilizing transfer learning, and thus enabling it to differentiate between resident members and intruders using facial recognition features. This system could include smarter and services in the future for further video surveillance applications by usage of its efficient workload management ability.

REFERENCES

[1] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, ``A review of smart homes_Past, present, and future,'' *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 6, pp. 1190_1203, Nov. 2012.

[2] G. Kioumourtzis, M. Skitsas, N. Zotos, and A. Sideris, ``Wide area video surveillane based on edge and fog computing concept,'' in *Proc. 8th Int. Conf. Inf., Intell., Syst. Appl. (IISA)*, Aug. 2017, pp. 1_6.

[3] V. Gouaillier and A.-E. Fleurant, ``Intelligent video surveillance: Promises and challenges,'' CRIM Technopôle Defence Secur., Montreal, QC, Canada, Technol. Commercial Intell. Rep., Mar. 2009, vol. 456, p. 468

[4] T. Sultana, M. W. Alam, and K. A. Wahid, ``Reliability analysis of Io VT based intelligent video surveillance system,'' in *Proc. IEEE 20th Int. Workshop Multimedia Signal Process. (MMSP)*, Aug. 2018, pp. 1_4.

[5] A. J. V. Neto, Z. Zhao, J. J. P. C. Rodrigues, H. B. Camboim, and T. Braun, ``Fog-based crime-assistance in smart IoT transportation system,'' *IEEE Access*, vol. 6, pp. 11101_11111, 2018.

[6] M. A. Hossain, ``Framework for a cloud-based multimedia surveillance system,'' *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 5, May 2014, Art. no. 135257.

[7] M. W. Alam, M. H. A. Sohag, A. H. Khan, T. Sultana, and K. A. Wahid, ``IoT-based intelligent capsule endoscopy system: A technical review,'' in *Intelligent Data Analysis for*

Biomedical Applications, 1st ed. New York, NY, USA: Academic, 2019, pp. 1_20.

[8] L. M. Vaquero and L. Rodero-Merino, ``Finding your way in the fog: Towards a comprehensive de_nition of fog computing,'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27_32, Oct. 2014.

[9] M. Chiang, S. Ha, C.-L. I, F. Risso, and T. Zhang, ``Clarifying fog computing and networking: 10 questions and answers,'' *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 18_20, Apr. 2017.

[10] B. Skrbic, D. Radovanovic, S. Tomovic, L. Lazovic, Z. Zecevic, and I. Radusinovic, ``A decentralized platform for heterogeneous IoT networks management,'' in *Proc. 23rd Int. Sci.-Prof. Conf. Inf. Technol. (IT)*, Feb. 2018, pp. 1_4.

[11] S. Wu, J. B. Rendall, M. J. Smith, S. Zhu, J. Xu, H. Wang, Q. Yang, and
P. Qin, ``Survey on prediction algorithms in smart homes,'' *IEEE Internet Things J.*, vol. 4, no. 3, pp. 636_644, Jun. 2017.

[12] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, ``State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traf_c control systems,'' *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2432_2455, 1st Quart., 2017.

[13] H.-C. Shih, ``A robust occupancy detection and tracking algorithm for the automatic monitoring and commissioning of a building,'' *Energy Buildings*, vol. 77, pp. 270_280, Jul. 2014.

[14] J. Yang, H. Zou, H. Jiang, and L. Xie, ``Device-free occupant activity sensing using WiFi-enabled IoT devices for smart homes,'' *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3991_4002, Oct. 2018.

[15] K.-H. Lee and J.-N. Hwang, ``On-road pedestrian tracking across multiple driving recorders,'' *IEEE Trans. Multimedia*, vol. 17, no. 9, pp. 1429_1438, Sep. 2015.

[16] K.-H. Lee, J.-N.Hwang, and S.-I. Chen, ``Model-based vehicle localization based on 3-D constrained multiple-kernel tracking,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 1, pp. 38_50, Jan. 2015.

[17] L. Li and M. K. H. Leung, ``Integrating intensity and texture differences for robust change detection,'' *IEEE Trans. Image Process.*, vol. 11, no. 2, pp. 105_112, Feb. 2002.

[18] O. Barnich and M. Van Droogenbroeck, ``ViBe: A universal background subtraction algorithm for video sequences,'' *IEEE Trans. Image Process.*, vol. 20, no. 6, pp. 1709_1724, Jun. 2011.

[19] J. Kang, D. V. Anderson, and M. H. Hayes, ``Face recognition for vehicle personalization with near infrared frame differencing,'' *IEEE Trans. Consum. Electron.*, vol. 62, no. 3, pp. 316_324, Aug. 2016.

[20] K. Simonyan and A. Zisserman, ``Very deep convolutional networks for large-scale image recognition,'' Sep. 2014, *arXiv:1409.1556*.

[21] R. Olmos, S. Tabik, and F. Herrera, ``Automatic handgun detection alarm in videos using deep learning,'' *Neurocomputing*, vol. 275, pp. 66_72, Jan. 2018.

[22] Z. Huang, Z. Pan, and B. Lei, ``Transfer learning with deep convolutional neural network for SAR target classi_cation with limited labeled data,'' *Remote Sens.*, vol. 9, no. 9, p. 907, 2017.

[23] A. Sammoud, A. Kumar, M. Bayoumi, and T. Elarabi, ``Real-time streaming challenges in Internet of video things (IoVT),'' in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2017, pp. 1_4.

[23] *CCTV Image of Man Wanted in Connection with Scunthorpe Armed Robbery Credit: Humberside Police*. Accessed: Jul. 17, 2019.