Security management in smart home environment

Mary Gladence (marygladence.it@sathyabama.ac.in)
Sathyabama University https://orcid.org/0000-0002-6767-6537
Maria Anu V
Sathyabama Institute of Science and Technology
Revathy S
Sathyambama Institute of Science and Technology: Sathyabama Institute of Science and Technology
Jeyanthi P
Sathyambama Institute of Science and Technology: Sathyabama Institute of Science and Technology

Research Article

Keywords: IoT, edge, fog, video surveillance, real-time security

Posted Date: April 6th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-323709/v1

Version of Record: A version of this preprint was published at Soft Computing on July 28th, 2021. See the published version at https://doi.org/10.1007/s00500-021-06054-z.

Security Management in Smart Home Environment

L.Mary Gladence, V.Maria Anu, S.Revathy, P.Jeyanthi

Associate Professor, Sathyabama Institute of Science and Technology, Chennai

lgladence@gmail.com, mariaanu18@gmail.com, revathy@gmail.com

Abstract: A Smart Home Environment (SHE) comprises various luxurious things which makes us very comfortable to live our lives happily and securely. The only problem that smart homes are facing is **"SECURITY".** Security for smart homes is the biggest task to achieve. For this purpose, this work is to build a product that provides the security for the smart homes automatically when the crime is going to happen. In general case, if any crime had taken place in any smart home, the general procedure of investigation will take place i.e. the people will complain to the police and the police will visit the place and after that he will observe the surroundings clearly. In order to pull up the clues if any, he will watch the CCTV footage, consult the nearby people in-order to draw some facts and then FIR will be filed.In order to get rid of this time-consuming process, the automatic crime detection is proposed. Here malware practices are identified, when a person attempts crime activity. This type of automatic process of detection of crime will ensure a complete security for the smart homes. We will track the CCTV camera pictures when the thief is trying to commit a crime and the information along with the pictures will be sent to the fog server and the fog server will analyze whether the person is doing crime or not. In case if a fog server had identified the person as a crime person or a thief then it automatically sends the information to the near- by police station and as well as owners of the house and then provides security for the smart homes.

Key Words: IoT, edge, fog, video surveillance, real-time security

I. INTRODUCTION

A smart home comprises various things which involves comfort, social insurance, security. SHE is observed by surrounding cameras to give mindful administrations and to encourage wellbeing and security for the smart homes[1]. A security is a board framework that is intended to guarantee from burglary, harm, and interruption by checking the inner and outside surroundings of smart homes by utilizing observation cameras[2]. Different frameworks generally include the utilization of clever video observation (IVS)[3-4] for programmed and exact distinguishing proof of occasions and articles in an objective scene. IVS empowers video analytics to detect the crimes without human intervention[3]. In the meantime, with the advancement of man-made discoveries in Artificial Intelligence (AI) and Machine Learning (ML), reconnaissance implementation and hide techniques are being made better with upgraded capacities and precision[5]. As indicated by the Uniform Crime Reports distributed by the Federal Bureau of Investigation (FBI), the 2017 measurements show that in the USA, robberies of private properties represented 67.2 percent of all robbery offenses, and the casualties of these misfortunes. What's more, 15.5 percent of all thefts in 2017 happened at business properties. Because of this ascent in property, the examination network is focusing on keen home security Protective administrations and specialists frequently neglect to react to crime occurrences effectively. They will follow the general receptive methodology which depends for the most part on witness reports or TV

(CCTV) film after the theft happens. Hence, as a rule, when an occasion happens, specialists visit the area of the occurrence, recover the substance physically from the camera, and afterwards they continue to recognize important film or by preparing it through specific video investigation calculations [7]. Generally receptive methodology is normally useless to stop violations[8]. An effective framework could empower security in a SHE by distinguishing precaution strategies. In this manner, the specialists could diminish wrongdoing episodes and misfortunes. Furthermore, present day mixed media observation frameworks include a wide scope of sensors, circulated over various destinations.

The video observation framework in a SHE comprises numerous cameras that can deliver a lot of reconnaissance information, both photograph and video. This may bring about substantial system clog and force muddled handling load on singular gadgets and frameworks[10]. Right now, we will talk about a non-integrated smart video observation structure to give a powerful answer for this issue. Things used in IOT combination of the books, virtual items, live creatures, investigation, and system availability that permits these items to gather and trade information over a web based framework[11]. This connection with different networks empowers progressed IOT applications (e.g., condition checking, keen city, clever transportation and for any medical services, reconnaissance, and brilliant homes)[12]. The IOT releases one type of to cut the edge for development to encourage present day collaborations and gives new chances to foundations and administrations that improve personal satisfaction. Consequently, an IoT-based smart surveillance framework can be adjusted to diminish the crime percentage, particularly in a shrewd structure. Despite the fact that cloud-based IoT models are utilized for handling and putting away basic observation information [9], they have issues in regards to transfer speed which require IoT hubs close to the wellspring of visual information to meet their postpone necessities 11,21. Mist processing of cloud and edge gadgets, gives a decentralized figuring foundation to play out a generous measure of correspondence, control, stockpiling, and the board[14]. It might use at least one IoT end gadgets or close client edge gadgets cooperatively.

An edge gadget (otherwise called a terminal/end), then again, will in general be restricted to processing at the corner of the system. The data generating sensors and IoT gadgets are situated at or close to an edge hub. Haze hubs can decrease trouble on asset compelled edge gadgets[11], conquer data transfer capacity limitations for incorporated administrations, and meet dormancy prerequisites of deferral delicate applications. Having registering has the capacity of reacting rapidly, and in this manner gives on-request benefits by putting away and preparing information locally. This measure urges scientists to coordinate to improve ongoing crime counterattack. In contrast to the old-style approach, where the camera sensors stay dynamic paying little heed to the nearness of target occasions or abnormalities, an occasion driven methodology can give better reconnaissance benefits by observing examples and observation action in the field of view. Right now, the end/edge hub will advance the observation information to the haze at whatever point it distinguishes an occasion in the information streams.

This methodology can essentially be used for reducing vitality utilization and transfer speed because of the negligible measure of information transmission to the mist . Edge figuring empowers this occasion driven methodology in an objective IOT observation application by assigning straightforward handling to camera-associated**,** IOT -edge-hub gadgets[15]. Haze registering, then again, empowers AI into the framework to settle on choices dependent on recently accumulated data or earlier sources of information which have made the framework progressively computerized[16]. Profound learning (DL), otherwise called profound organized learning, various leveled learning, profound element learning, and deep representation learning[17]. DL calculations are more mainstream than the old ML calculations, particularly, in the zone of PC vision (i.e., object acknowledgment, driverless vehicles, and AI gaming). Incorporating DL in the any identifying for any members AI into the haze hub will empower it to foresee potential occasions, and choose to follow up on its own, which is important for actualizing a prescient recognizable proof of wrongdoing occasions and in the long run to evade wrongdoing occurrences at a

SHE. In view of the considerable number of conversations above, we propose IOT guard, an occasion driven edge-mist coordinated video reconnaissance structure, to perform constant security of the executives by helping in wrongdoing anticipation and foreseeing wrongdoing occasions at a SHE. The proposed IOT -monitor approach gives a three-layer structural system that organizes occasion driven for the gadgets to the edges in a smart home and Data load-executed mist processing hubs to address expanding human security concerns. The framework additionally gives an alarm by sending the wrongdoing information in a split second to the police or defensive help, and in this way, it guarantees a fast reaction. The principal commitments of the proposed framework are: (I) an asset proficient savvy edge-hub execution to recognize human interruption and start mist preparing; (ii) a mist empowered foundation for the location and affirmation of a wrongdoing; and (iii) an occasion driven wrongdoing information detailing administration to the police headquarters to manage an identified wrongdoing. Hence, the proposed structure incorporates picture preparing, AI PC vision, and system specialized strategies for continuous wrongdoing occasion identification, guaranteeing asset proficiency and great appropriation of the handling load in an IoT-based video observation framework.

II. RELATED WORK

Discovery framework for observing a structure with the assistance of a picture-based profundity sensor and a programmable container[18]. A gadget free inhabitant action detecting framework utilizing Wi-Fi connections- empowered IOT gadgets for brilliant house.[19-20] Consider an on-street person on foot following framework over different moving cameras and in another article, built up a system for vehicle following and restriction dependent on 3-D compelled numerous pieces following. Quality-of content-depends on joint one another to another source and channel coding framework for distinguishing people in a versatile observation cloud[4]. proposed in architecture that enhances security by using information from exclusive camera,videos. Cloud-based IOT structures are utilized for preparing and putting away basic observation information where every camera/hub sends the information legitimately to a cloud for a wide range of basic leadership[5].

The creators talked about the commitment of innovation and its verified reconciliation into IoT designs. Structure for a sight and sound reconnaissance framework that supports the preparing over-burden, access, details and security, and protection in huge scale observation settings. These examinations uncover the ability of distributed computing to fulfill numerous Internet of things prerequisites (e.g., observing, sensor stream preparing, and perception assignments). The huge measure information sent by the end gadgets utilizing rapid fiber systems prompts a high system sending cost[3]. In spite of the fact that the circumstance has changed as of late, issues in regards to transfer speed, vitality, and inertness progressively video observation applications[8]. Therefore, mist registering worldview rose and mist – based arrangements would now be able to encourage continuous preparing and quick reaction time, and diminish dormancy issues, in this manner expanding distributed computing and administrations closer to the finish of the system[8]. Mist, can be recognized from the cloud by its closeness to the end clients, the geological dissemination, and its versatility supported[9].

[9]clarified the design, highlights, and job of mist registering. Circulated and productive item discovery engineering in edge processing for continuous reconnaissance application[11]. The creators clarified an edge-figuring system to empower helpful video preparation on asset plenteous cell phones for delay-touchy media framework for identifying and receiving mixed media transmission blunders in an observation IoT condition is portrayed[14].

A DL-based person on foot discovery and face acknowledgment procedure for reconnaissance application for the unforgettable IoT condition demonstrated the plan of a novel overloading methodology to upgrade internet DL applications with an edge-registering condition. depicted the

structure of a self-enhancing, setting driven, IoT remote sensor hub for reconnaissance applications[15]. A haze system for canny video reconnaissance to improve wrongdoing help and wellbeing in open one place to one place is displayed **[18]**depicting some perception instrument which wires multimedia data for enormous scale savvy video observation, using an occasion driven methodology. The creators depicted the basic application necessities of a productive brilliant observation framework, for example, continuous and precise recognition of an occasion, solid and spry expectation of wrongdoing occasions, and superior assistance organization. Asset proficient methodologies are used in the IOT-based video reconnaissance models on account of the ever-expanding same observation hubs[11]. A BW-and vitality mindful video pressure calculation for IoT-based video reconnaissance applications[23]. Nonetheless, to send an asset proficient and proactive reconnaissance framework, the recently talked about recommendations might be lacking. It likewise accomplishes huge proficiency contrasted with SoA or customary observance structures.[21-22]

III. PROPOSED FRAMEWORK

To Design a Home with a Smart Home Environment which protects the people in the home from any kind of robbery, crime, sabotage. Which safeguards by monitoring the events and the moments happening.

*To protect home from any kind of crime activities.

*To provide a secure environment to the people living in the home.

In existing frameworks different digital physical frameworks generally embrace the utilization of wise video reconnaissance, for programmed and precise-ID of occasions and articles in an objective shown in the scene. IVS empowers video examination to predict to have decipher the ongoing situation for a human without any mediation. In the meantime, with the advancement of computerized reasoning (AI) and (ML), observation implementation and hiding for methodology are being improved with upgraded capacities and exactness. Defensive administrations and specialists frequently neglect to react to wrongdoing episodes effectively. Along these lines, much of the time, when an occasion happens, specialists visit the area of the episode, recover the substance physically from the camera, and afterwards they distinguish significant film. Based on the observation which are stated earlier, there are few drawbacks such as

- Protective administrations and specialists regularly neglect to react to wrongdoing occurrences effectively.

- Authorities visit the area of the episode, recover the substance physically from the camera. Manual examination will take a lot of time.

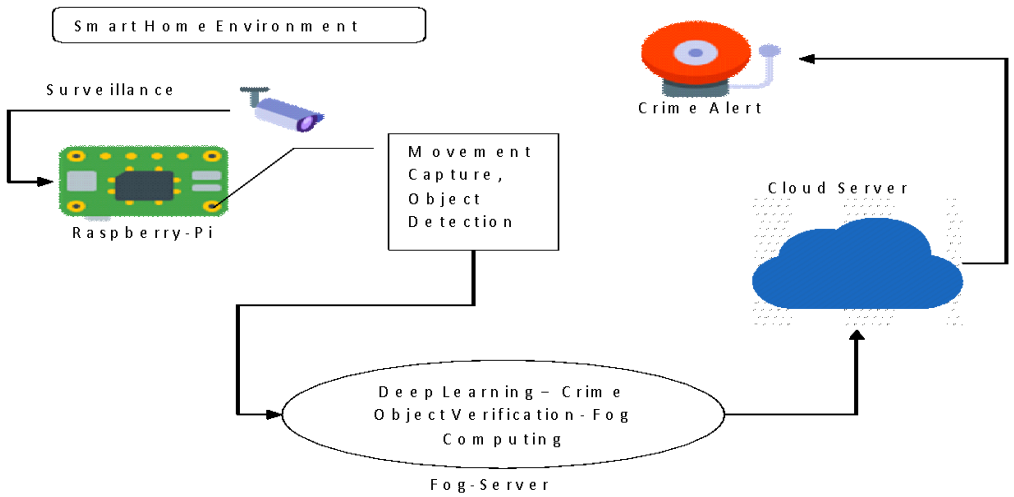

Fig. 1. Overview of the Proposed System

To avoid the drawbacks which are said in the existing system are rectified using proposed work, going to actualize IoT-monitor, an occasion driven edge-haze coordinated video observation system, to perform ongoing security on the board by helping in wrongdoing anticipation and predicting wrongdoing occasions at a SHE. The proposed methodology to protect the approach given in a three-layer compositional system that organizes in the occasion for the given gadgets in the drivenedge inthe smarthome and DL implemented mist figuring hubs to address expanding human security concerns. The framework likewise gives an alarm by sending the wrongdoing information in a split second to the police or defensive help, and in this manner, it guarantees a speedy reaction. Overview of proposed work is illustrated in Figure 3.1. The Proposed System is aSmart Home Environment in which the surveillance cameras are installed at a place, and these surveillance cameras are connected to the Raspberry – pi kit through which the movement captured and the object detection are processed to the fog server and this fog server performs the algorithm proposed on the objects captured and verifies whether the object is a dangerous one or not if it detects a harmful object then it sends the authentication alert message to the respective authority and alert them through the notification. This proposed work detects the below activities such as

- Detection of wrongdoing objects within the time-frame.
- Automatic and precise recognizable proof of wrongdoing occasions.

A. User Authentication with Surveillance System

The client needs to validate with the Cloud Server for empowering this security component. The enrollment of the client incorporates a fundamental structure to get every essential detail of the client. This data will be put away in a cloud server. With the goal that clients can go into the web-based interface to see the observation insights.

B. Object Detection with Edge Node

The edge hub contains a Raspberry-Pi which will be associated with gathering of cameras around Smart Home Environment. We are going to interface one camera with the edge hub (Raspberry-Pi). At the point when any crime actions caught in Surveillance cameras at that point edge hub will recognize the crime actions, catch the picture and examine the event that any article is there, at that point it will send the snap to Fog hub for additional figuring which is shown in "Figure.2". Based on this technology below activities are observed

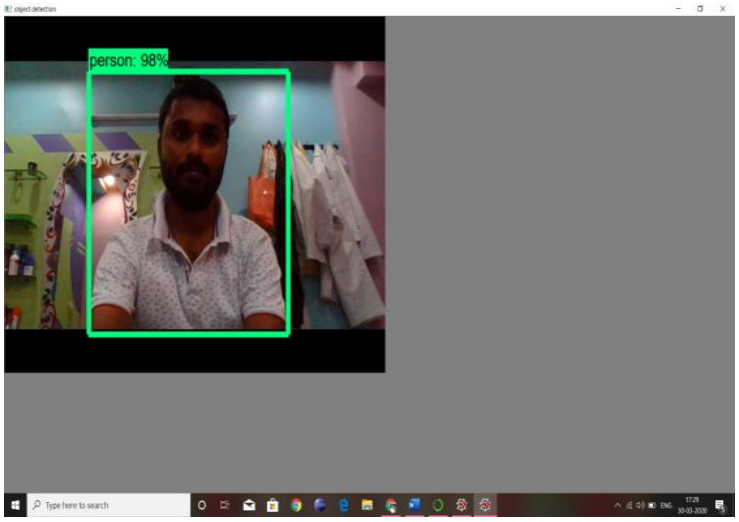

Fig. 2 Object detection with edge node

- Verifying the weapons like guns which will be carried by any human.
- Verified images are shown in the console.
- Verified images are shown by comparing with the dataset which is already stored in the trained dataset. Observations of above said activities are shown in "Figure. 3".

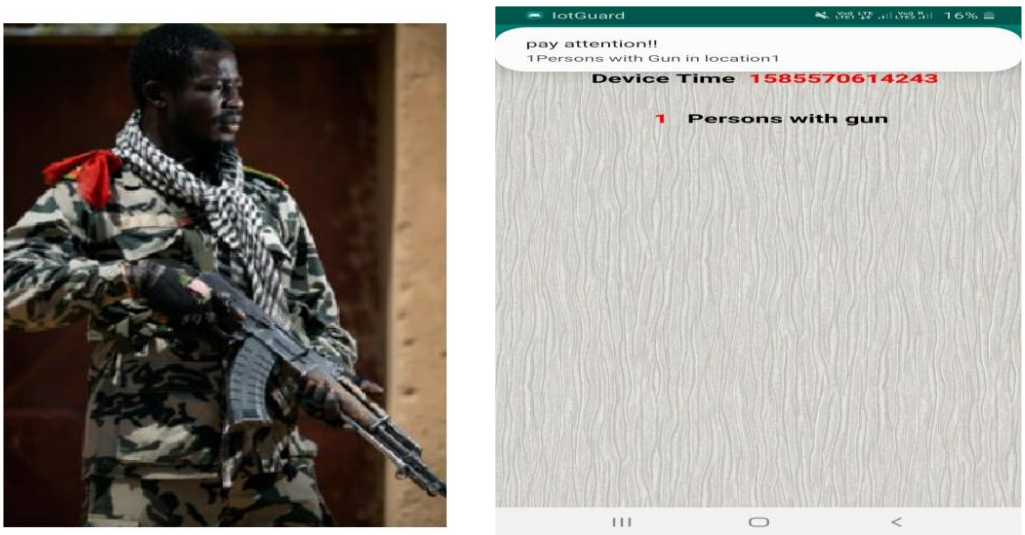

Fig. 3 Object verification and alert message

C. Fog Server Computation

Fog Computing distinguishes and claims the nearby human being and knives where it will number members to the sort of any harmful users and promptly, they shift themselves wrongdoing occasion data to the closest wrongdoing anticipation unit in a split second. Each haze hub is likewise ready to dispatch wrongdoing information all the while as a cell phone ready message. Utilizing the wrongdoing information sent by the mist hub, the wrongdoing avoidance unit can guarantee wrongdoing anticipation before the wrongdoing really happens. The AI empowered occasion driven mist hub likewise invalidates any bogus positive outcome enlisted by the edge hub. Every wrongdoing avoidance unit may get a wrongdoing notice from a few haze hubs covering a neighborhood and send them to Cloud Server. The convolutional neural network is implemented by forming layers based on convolution, where input data is convolved to a smaller area, detecting important partwithin that area. Each of the convolutional layers applies nonlinear activation functions and filters in the order of hundreds to thousands and combines their results to compute theoutput[17]. A fog node, controlling several edge nodes, receives motion-detected images from them. Using intelligent computational methods, it then applies an object detection algorithm using a pertained CNN model.

Therefore, we collected gun and knife datasets to train and build a CNN model thatis capable of detecting guns and knives. Hence, the CNN model running at a fog node detects and labels the images with the name of the crime objects having the highest probability, and saves those images. The fog node then assembles and sends crime data (i.e., the labeled image, crime event location, and camera position) to the nearest crime assistance or police unit and also sends an alert message to the protective service in real-time. On theother hand, the cloud is responsible for generating updated CNN crime data models (i.e.,by using transfer learning methods), so that the fog node can download them whenever they are available.

D. Surveillance Alert Mechanism

All the Fog Computing keeps up bidirectional correspondence with a focal cloud server inside a brilliant city for getting framework refreshes, wrongdoing occasion information mining, factual investigation, and intermittent data stockpiling. In light of the expectation result the alarm or notice will be activated to speak to experts so as to forestall the wrongdoing before it will happen. Flow diagram of surveillance alert mechanism is shown in “Figure. 4”

All the fog nodes maintain bidirectional communication with a central cloud server within a smart city for receiving system updates, crime event data mining, statistical analysis and periodic information storage. Based on the prediction result the alert or notification will be triggered to the represent authority in order to prevent the crime before it is going to take place. So with the help of this alert mechanism the respective authority can alert and take the necessary action or can stop the crime event before it happens.

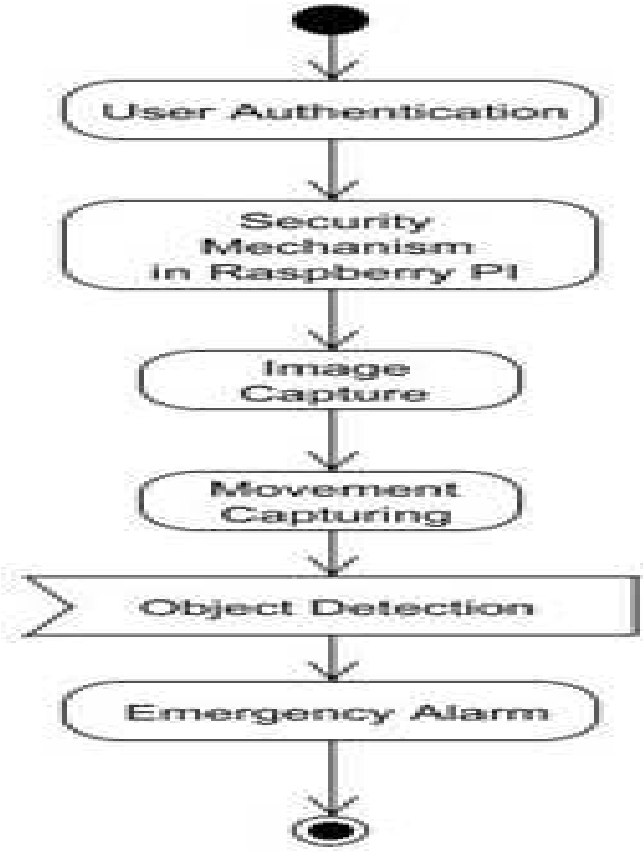

Fig. 4 Flow diagram of Surveillance Alert Mechanism

Name of the Node	Edge	Fog
Image detection time while in motion	Every fraction of second	Not Applicable
Object detection time(s)(Maximum)	Not applicable	13
%CPU utilization	18%	11%
Memory used	7%	2%
Energy Consumption	0.94	
Crime data (single imagetransition time(s))	0.35(Edge to Fog)	0.4(Fog to Police)
Crime image encoding time	0.03	0.028
Time required by the system(maximum)	17≈	

Table.1 clearly shows the performance of the proposed work. Even though this work is tested with lab setup which is available in our lab, this performance measure is pretty enough to appraise the proposed work. Based on this, easily report can be send to concerned authority to avoid the crime which happens within the proximity. In this way report can be send to nearby police station to avoid the crime which is going to happen in the houses. This is very useful for the disability persons. Based on this invention one who is staying alone without anyone's help can live their life happily. Through this one can clearly note that deep learning model requires high CPU one can clearly note that deep learning model requires high CPU and memory utilization in a IoT gadget. In addition to this very large computation reduces system performance, which lacks the efficiency of video surveillance

IV. CONCLUSION

Right-now actualized IoT-monitor, an occasion driven fog computing coordinated video reconnaissance system. This will help the executives by wrongdoing anticipation and foreseeing wrongdoing occasions at a SHE. IoT guard observation is adjusted to decrease the crime percentage particularly in brilliant structures. Right now use edge-hubs, mist registering, cloud based IoT, observation ready systems. The prescient methodology is essential for programmed and precise ID of wrongdoing occasions and to stay away from wrongdoing occurrences at SHE. Thus, an alarm or warning will be sent to the owners or to the defense. AI system so as to forestall the wrongdoing before it will happen. Consequently, the proposed framework is unmistakably increasingly productive.This 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 deep learning, and thus enabling it to differentiate between resident members and intruders using facial recognition features. This system could include more intelligence and services in the future for other video surveillance applications by utilizing its efficient workload management ability.

Compliance with Ethical Standards

Conflict of interest: NIL
Ethical Approval: Not required for this study

Authorship Contribution

Author 1 & 2
Data Collection and problem defined, performed analysis to conclude the work. Literature review done.

Author 3 & 4
Data Analysis and performance evaluation, literature review done

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. ManCybern. Part C Appl. Rev., vol. 42, no. 6, pp. 1190–1203, Nov.2012.
2. T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, “How can heterogeneous internet of things build our future: A survey”, IEEE Commun. Surv. Tutorials, vol. 20, no. 3, pp. 2011–2027,2018.
3. V. Gouaillier, “Intelligent Video Surveillance: Promises and Challenges Technological and Commercial Intelligence Report,”2009.
4. T. Sultana, M. W. Alam, and K. A. Wahid, “Reliability Analysis of Io VT Based Intelligent Video Surveillance System,” in 2018IEEE 20th International Workshop on Multimedia Signal Processing (MMSP), 2018, pp. 1–4.

5. S. Din, A. Paul, A. Ahmad, B. B. Gupta, and S. Rho, "Service Orchestration of Optimizing Continuous Features in Industrial Surveillance Using Big Data Based Fog-Enabled Internet of Things", IEEE Access, vol. 6, pp. 21582–21591, 2018.
6. G. Kioumourtzis, M. Skitsas, N. Zotos, and A. Sideris, "Wide area video surveillance based on edge and fog computing concept",in 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA), 2017, pp. 1–6.
7. 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.
8. L. M. Vaquero and L. Rodero-Merino, "Finding your Way in the Fog," 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 2018 23rd International Scientific-Professional Conference on Information Technology(IT), 2018, pp. 1–4.
11. S. Wu et al., "Survey on Prediction Algorithms in Smart Homes," IEEE Internet Things J., vol. 4, no. 3, pp. 636–644, Jun. 2017.
12. H.-C. Shih, "A robust occupancy detection and tracking algorithm for the automatic monitoring and commissioning of a building," Energy Build., vol. 77, pp. 270–280, Jul. 2014.
13. 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.
14. C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," Futur. Gener.Comput. Syst., vol. 78, pp. 964–975, Jan. 2018.
15. M. A. Hossain, "Framework for a Cloud-Based Multimedia Surveillance System," Int. J. Distrib. Sens. Networks, vol. 10,no. 5, p. 135257, May 2014.
16. T. Sultana and K. A. Wahid, "Choice of Application Layer Protocols for Next Generation Video Surveillance Using Internet of Video Things," IEEE Access, vol. 7, pp. 41607–41624, 2019.
17. I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overviewofFog computing and its security issues," Concurr. Comput.Pract. Exp., vol. 28, no. 10, pp. 2991–3005, Jul. 2016.
18. J. Ren, Y. Guo, D. Zhang, Q. Liu, and Y. Zhang, "Distributed and Efficient Object Detection in Edge Computing: Challenges and Solutions," IEEE Netw., vol. 32, no. 6, pp. 137–143, Nov.2018.
19. C. Long, Y. Cao, T. Jiang, and Q. Zhang, "Edge Computing Framework for Cooperative Video Processing in Multimedia IoT Systems," IEEE Trans. Multimed., vol. 20, no. 5, pp. 1126–1139, May 2018.
20. Gladence LM, Anu VM, Rathna R, Brumancia E. Recommender system for home automation using IoT and artificial intelligence. Journal of Ambient Intelligence and Humanized Computing. 2020 Apr 19:1-9.
21. H. Li, K. Ota, and M. Dong, "Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing",IEEENetw., vol. 32, no. 1, pp. 96–101, Jan. 2018.
22. D. Kieran and W. Yan, "A Framework for an Event DrivenVideo Surveillance System," in 2010 7th IEEE International Conference on Advanced Video and Signal Based Surveillance, 2010, pp. 97–102.
23. S.Shanmuga Priya, A.Valarmathi,"The Personal Authentication Service And Security Enhancement For Optimal String Password" in Concurrency Computation Practice & Experience. Dec 2018.

Figures

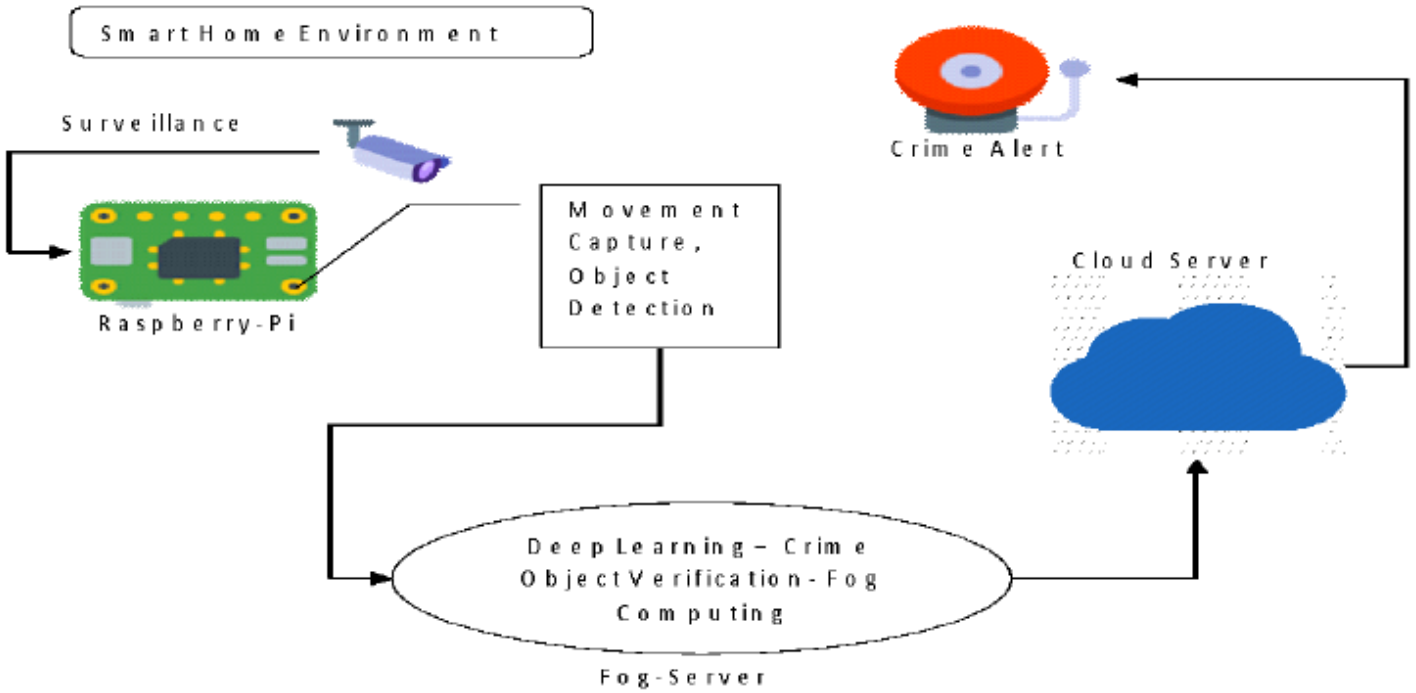

Figure 1

Overview of the Proposed System

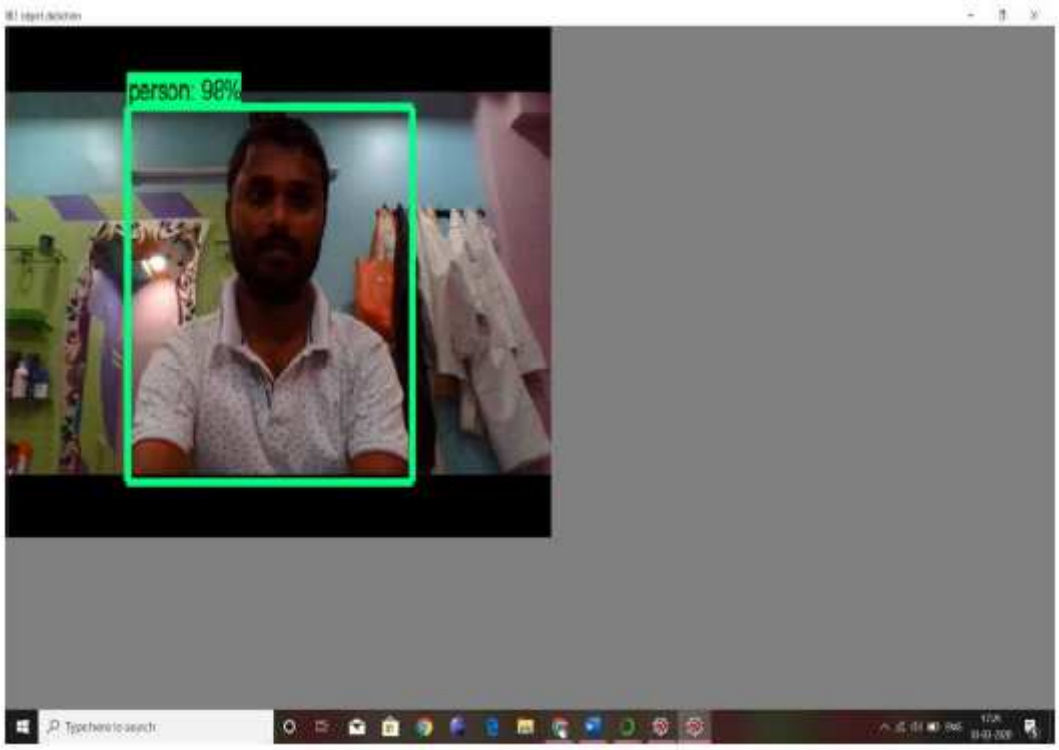

Figure 2

Object detection with edge node

Figure 3

Object verification and alert message

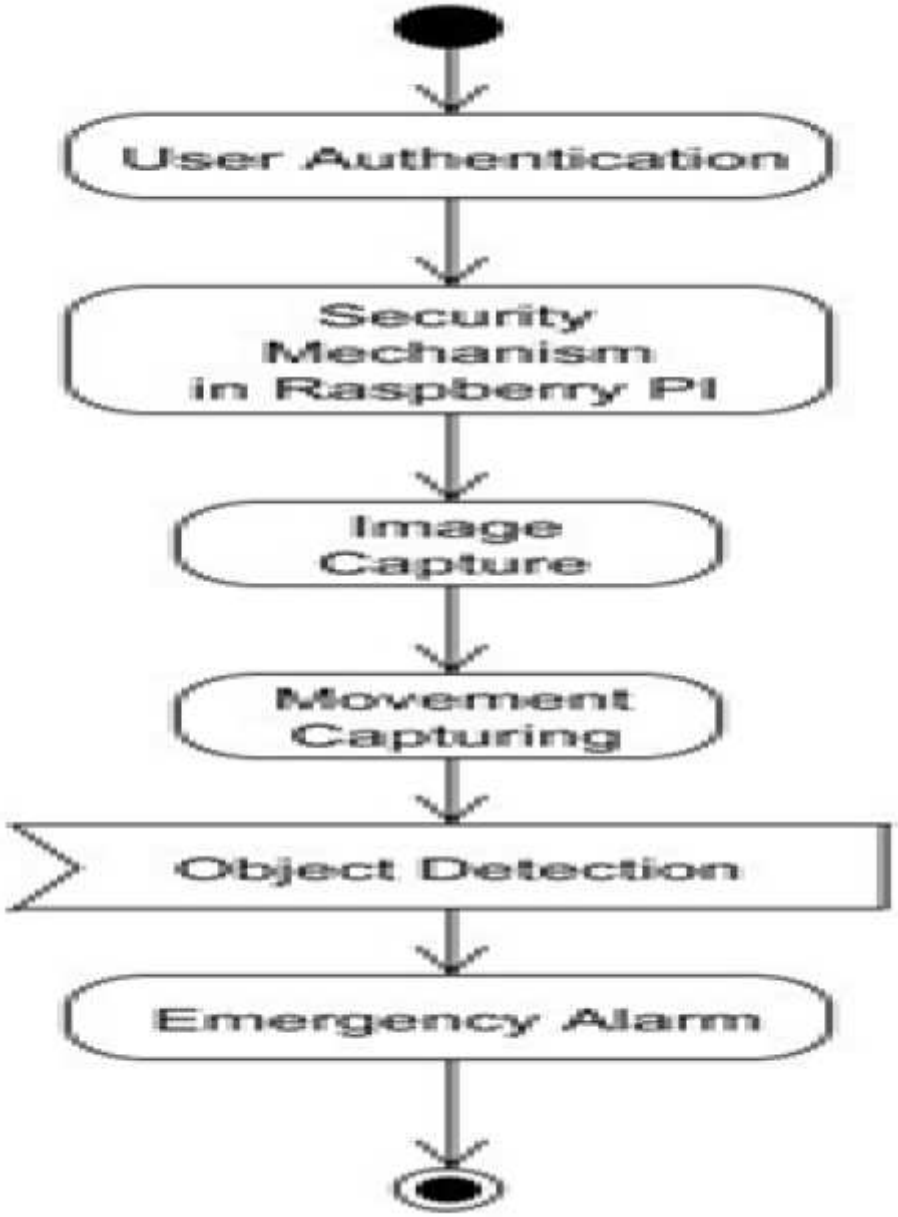

Figure 4

Flow diagram of Surveillance Alert Mechanism