International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

IOT-GUARD REAL-TIME SECURITY MANAGEMENT IN SMART HOME ENVIRONMENT

Mrs. D. J. Hani Mary Sheniha[1], V. Logeshwari[2], N. Brindha[3]

[1]*Assistant Professor, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Tamil Nadu, India*
[2]*Student, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Tamil Nadu, India*
[3]*Student, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Tamil Nadu, India*

Abstract - *A security management system is designed to provide complete safety from robbery, destruction, and intrusion by monitoring the internal and external Smart Home Environment (SHE), using surveillance cameras. Various cyber-physical systems widely adopt the use of intelligent video surveillance, for automatic and accurate identification of crime events and objects in a crime scene. Intelligent Video Surveillance enables video analytics to predict and interpret the activity of a scenario without human intervention. Protective services and authorities often fail to reply to crime incidents efficiently. An efficient crime predictive system could enable robust security management in a Smart Home Environment by identifying preventative procedures. Instead of gathering information from the crime scene after the crime, it can be stopped before happening by proper computing and quick action.*

***Key Words*: Smart Home Environment, crime, surveillance, IoT, motion detection, object detection, fog computing, cloud computing.**

1. INTRODUCTION

A smart home environment (SHE) consists of varied applications of present computing that integrates smartness into dwellings for comfort, healthcare, safety, security, and energy conservation. SHE is monitored by close intelligence to provide context-aware services and to facilitate safety and security management. A security management system is meant to supply complete safety from theft, sabotage, exploitation and intrusion by watching the inner and external SHE. Various digital physical frameworks broadly receive the utilization of Intelligent Video police work (IVS) for programmed and legitimate recognizable proof of occasions and articles during an objective scene. IVS permits video analytics to predict and interpret the activity of a state of affairs without human intervention. Meanwhile, with the assistance of AI (AI) and machine learning (ML), police work applications and security procedures are being improved with increased functions and as per the Uniform Crime Reports printed by the Federal Bureau of Investigation (FBI), the 2017 statistics show that in USA, burglaries of residential properties accounted for 67.2 % of all felony offenses, and therefore the victims of these offenses suffered associate calculable $3.4 billion in property losses. Additionally, 15.5 you look after all robberies in 2017 occurred at industrial properties whereas residences knowledgeable Sixteen Personality Factor Questionnaire. Due to this rise in property crime, the analysis community is listening to sensible home security protecting services and authorities usually fail to retort to crime incidents efficiently. They need an inclination to follow a reactive approach that depends totally on witness reports or electronic circuits and CCTV footages once the crime takes place. Therefore, in most cases, once an event happens, authorities visit things of the incident, retrieve the content manually from the camera to identify relevant footage either by watching the entire length of the video or by process it through specialized video analytics algorithms. Therefore, reactive approach is in fact inefficient for preventing crimes. An efficient crime prophetic system may change sturdy security management in associate SHE by identifying preventative procedures. Thus, the authorities may crop crime incidents and losses. Additionally, trendy multimedia police work systems comprise an outsized vary of sensors, distributed over multiple sites. The video television in associate SHE consists of the various cameras which will end up an oversized quantity of police work information, each icon and video. This might end in serious network congestion and impose sophisticated process load on individual devices and systems.

1.1 Internet of Things

IoT is that the ability for things that contain embedded technologies to sense, communicate, interact, and collaborate with alternative things, so making a network of physical objects. Problems associated with privacy and confidentially area unit for the most part highlighted within the business context. The neutral area unit unlikely to adopt IoT solutions if there are not any surety in terms of information confidentiality, genuineness and privacy. Knowledge confidentiality indicating the confirmation that solely explicit entities have the correct to realize and manipulate knowledge, whereby knowledge could represent associate degree quality to be protected to secure the fight.

Reasonable house is a living arrangement furnished with innovation that improves security of patient's gathering and screen their wellbeing conditions. so as to confirm confidentiality and privacy in information management system, varied access management techniques are projected, which incorporates Role-Based Access management (RBAC) that greatly used as a fortunate different to traditional discretionary and necessary access management. **Internet application development demand is very high.** So IoT may be a major technology by which we will produce various useful internet applications. Basically, IoT may be a network during which all physical objects are connected to the web through network devices or routers and exchange data. IoT permits items to be controlled remotely across existing system foundation. IoT may be an excellent and intelligent technique which reduces human effort also as quick access to physical devices. This technique also has autonomous control feature by which any device can control with none human interaction. The connectedness of various devices of different fields with Internet and exchange of data between them represents the connectivity of world through various technologies.

1.2 Edge node

In edge computing, data is processed by the device itself or by an area computer or server, instead of being transmitted to a knowledge center. Edge computing enhances web gadgets and web applications by carrying registering nearer to the wellspring of the information. This limits the requirement for long separation interchanges among customer and server, which diminishes inertness and transmission capacity utilization. The word edge up this context means literal geographic distribution. Edge computing is computing that's done at or near the source of the info, rather than counting on the cloud at one among a dozen data centers to try to do all the work. It doesn't mean the cloud will disappear. It implies the cloud is coming to you. The clients should confirm with the Cloud Server for sanction this security system. The registration of user includes a basic kind to induce all basic details of the user. This info is going to be keep in cloud server. So users will enter into the net portal to envision the police investigation statistics. The sting node contains a Raspberry-Pi which can be connected with cluster of cameras around good Home surroundings. We have a tendency to area unit about to interface one camera with the sting node (Raspberry-Pi). Once any movement captured in police investigation camera then edge node can spot the movement captures the image and analyzes if any object is there then sending the snap to Fog node for any computing.

1.3. Fog node

Fog node identifies and confirms the presence of a personality's and weapon; it'll classify the sort of weapon and like shot dispatch crime event info to the closest crime hindrance unit instantly. Every fog node is additionally able to dispatch crime information at the same time within the style of a movable alert message. Mistreatment the crime information sent by the fog node; the crime hindrance unit will guarantee period of time crime hindrance before the crime really takes place. The AI enabled event-driven fog node conjointly nullifies any false positive result registered by the sting node. Every crime hindrance unit might receive a criminal offense notification from many fog nodes covering a dominion and send them to Cloud Server. All the fog nodes maintain bi-facial communication with a central cloud server at intervals a wise town for receiver updates, crime event data processing, applied math analysis, and periodic info storage. Supported the prediction result the alert or notification progressing to beware triggered to the represent authority in-order to forestall the crime before it's going to present itself.

1.4. Deep learning

It can be thought-about as a set of machine learning. It a field that's supported learning and up on its own by examining laptop algorithms. Whereas machine learning uses easier ideas, deep learning works with artificial neural networks, that area unit designed to imitate however humans suppose and learn. Till recently, neural networks were restricted by computing power and therefore were restricted in complexness. However, advancements in massive information analytics have allowable larger, refined neural networks, permitting computers to watch, learn, and react to advanced things quicker than humans. Deep learning has power-assisted image classification, language translation, speech recognition. It may be accustomed solve any pattern recognition drawback and while not human intervention.

Artificial neural networks, comprising several layers, drive deep learning. Deep Neural Networks (DNNs) area unit such kinds of networks wherever every layer will perform advanced operations like illustration and abstraction that be of pictures, sound, and text. thought-about the fastest-growing field in machine learning, deep learning represents a really turbulent digital technology, and it's being employed by progressively} more corporations to make new business models. Deep learning systems need giant amounts of knowledge to come correct results; consequently, data is fed as immense information sets. Once process the info, artificial neural networks area unit ready to classify information with the answers received from a series of binary true or false queries involving extremely advanced mathematical calculations. For instance, an identity verification program works by learning to notice and acknowledge edges and features of faces, then additional important components of the faces, and, finally, the representations of faces. Over time, the program trains itself, and also the chance of correct answers will increase. During this case, the identity verification program can accurately determine faces with time.

Let's say the goal is to own a neural network acknowledge photos that contain a dog. All dogs don't look specifically alike – contemplate a sheepdog and a poodle dog, as an example. What is more, photos show dogs at completely different angles and with varied amounts of sunshine and shadow. So, a coaching set of pictures should be compiled, together with several samples of dog faces that any individual would label as "dog," and footage of objects that aren't dogs, labeled (as one may expect), "not dog." the photographs, fed into the neural network, area unit born-again into information. These information moves through the network, and varied nodes assign weights to completely different components. The ultimate output layer compiles the ostensibly disconnected data – furred, contains a snout, has four legs, etc. – and delivers the output: dog.

Now, this answer received from the neural network are compared to the human-generated label. If there's a match, then the output is confirmed. If not, the neural system takes note of the mistake and modifies the weightings. The neural network tries to enhance its dog-recognition skills by repeatedly adjusting its weights over and once more. This coaching technique is termed supervised learning, that happens even once the neural networks don't seem to be expressly told what "makes" a dog. They have to acknowledge patterns in information over time and learn on their own.

2. RELATED WORK

Tanin Sultana and Khan A. Wahid [1] has proposed an appropriated Internet of Things (IoT) structure called IoT-watch, for a keen ongoing security the board framework. The framework, comprising of edge-fog computational layers, will help in wrongdoing counteraction and anticipate wrongdoing occasions during a smart home condition (SHE). A security the board framework is intended to supply total well-being from theft, harm, and interruption by observing the inside and outer SHE, utilizing reconnaissance cameras. Various cyber-physical systems widely adopt the utilization of intelligent video surveillance (IVS), for automatic and accurate identification of events and objects during a target scene. The internet of things (IoT) is that the internetworking of physical objects, virtual objects, living beings, analytics, and user interfaces, and network connectivity that allows these objects to collect and exchange data over an internet-based infrastructure. An IoT-based savvy reconnaissance framework can be adjusted to decrease the crime percentage, particularly in a keen structure. Although cloud-based IoT architectures are used for processing and storing essential surveillance data, they have issues regarding bandwidth and latency-sensitive video surveillance applications which require IoT nodes near the source of visual data to satisfy their delay requirements. Fog computing has been introduced to address these issues.

Tanin Sultana, Khan A. Wahid [2] proposed an IoVT framework for optimizing latency, bandwidth and energy consumption. Video observation has become pervasive expanding security necessities in each circle of life. The next generation video surveillance system VSS meets with great challenges in various applications, like intelligent urban surveillance systems and smart cities. In these applications, we'd prefer to influence the quickly developing number of observation hubs which present a few requirements, e.g., high inertness, high data transfer capacity, high vitality utilization, and CPU and memory use. To address these issues, the web of video things (IoVT), which is taken into account to be a neighborhood of the web of Things (IoT), are often an answer. The IoVT consists of visual sensors (i.e., cameras) connected to the web. In contrast to ordinary frameworks, the VSS under an IoVT structure gives numerous layers (i.e., edge, haze, cloud) of correspondence and choosing by catching and breaking down rich logical and conduct data. Since an appropriate application layer protocol (ALP) can help in alleviating the challenges of future VSSs, the choice of ALPs is critical for IoVT-based systems. Subsequently, this paper speaks to a conventional engineering of an IoVT-based VSS and a near examination of a few ALPs, as AMQP, MQTT, XMPP, HTML, DDS, and CoAP, with ongoing experimentation. This examination will help the clients to pick the appropriate ALPs in different observation applications and decide their fitness at various hubs of the IoVT system.

Jianbing, Kuan Zhang, Xiaodong Lin and Xuemin (Sherman) Shen [3] has proposed a technique to overcome the short comings of smart traffic lights, home energy management and augmented reality. Internet of Things (IoT) permits billions of physical items to be associated with assemble and trade information for offering different applications, as ecological observing, framework the board and private computerization. On the contrary hand, IoT has unsupported highlights (e.g., low idleness, area mindfulness and geographic circulation) that are basic for a couple IoT applications, including savvy traffic lights, home vitality the executives and increased reality. To support these features, fog computing is integrated into IoT to increase computing, storage and networking resources to the network edge. Unfortunately, it's confronted with various security and privacy risks, which raise serious concerns towards users. Right now, survey the design and highlights of fog registering and study basic jobs of fog nodes, including constant administrations, transient stockpiling, information dispersal and decentralized calculation. We also examine fog-assisted IoT applications supported different roles of fog nodes. At that point, we present security and protection dangers towards IoT applications and talk about the wellbeing and protection prerequisites in fog computing. Further, we show potential difficulties to make sure about fog processing and survey the

cutting-edge arrangements won't to address security and protection issues in fog registering for IoT applications. Finally, by defining several open research issues, it's expected to draw more attention and efforts into this new architecture.

Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kimb and Brij Guptac [4] has proposed a technique for the problems that rise due to the integration of cloud computing and IoT. Mobile Cloud Computing might be another innovation which alludes to a foundation where both the information stockpiling and handling work outside of the cell phone. Internet of Things may be a new technology which is growing rapidly within the field of telecommunications. The principle objective of the association and participation among things and items which sent through the remote systems is to fulfill the objective set to them as a consolidated element. Likewise, there's a quick advancement of the two advances, Cloud Computing and Internet of Things, respect the segment of remote interchanges. In this paper, we present a survey of IoT and Cloud Computing with attention on the safety problems with both technologies Finishing up, we present the commitment of Cloud. Along these lines, it shows how the Cloud Computing innovation improves the capacity of the IoT. Specifically, we combine the 2 aforementioned technologies (i.e., Cloud Computing and IoT) so as to look at the common features, and so as to get the advantages of their integration. Finally, we survey the safety challenges of the mixing of IoT and Cloud Computing.

Sola O. Ajiboye, Philip Birch, Christopher Chatwin and Rupert Young [5] has proposed a anatomy that licenses admission to abstracts from worst cameras, with the purpose of extending the ability and attention of accessible abundance masterminding, aegis activities, and accommodation aboveboard able systems that are maintained video composed acumen systems. There is growing assurance on video surveillance systems for exact surmising, appraisal and estimation of the advice adapted for anticipating, orchestrating, evaluating and active accessible prosperity. This is accessible from the gigantic cardinal of assay cameras beatific beyond accessible areas. For instance, in July 2013, British Aegis Industry Association (BSIA) appear that added than 4 actor CCTV cameras had been alien in Britain alone. The BSIA additionally acknowledge that aloof one .5% of those are accompaniment owned. The carefulness of after-effects got from government-possessed accessible aegis foundation would advance abnormally if absolute ascertainment frameworks 'uncover' applicative video-created metadata occasions, as activated alarms and along authorization catechism of a metadata archive. Subsequently, a policeman, for instance, with an adapted akin of arrangement permission can concern unified video systems beyond an outsized geographic breadth like a country to adumbrate the breadth of our proposed atypical hierarchical architecture, the Fused Video Surveillance Architectonics (FVSA). At the aerial level, FVSA comprises of an accouterment's framework that's accurate by a multi-layer absorption software interface. It presents video ascertainment frameworks as an adapted computational filigree of able administrations, which is abutting empowered to allocution with added absolute frameworks central the Internet of Things (IoT).

Shaoen Wu, Jacob B. Rendall, Matthew J. Smith, Shangyu Zhu, Junhong Xu, Honggang Wang, Qing Yang and Pinle Qin [6] proposed a address for home predictions. The apple has entered into a "smart" era. One breadth acceptable acute is the abode area we alive – homes. Acute homes are accepted to be able with abundant sensors to always monitor, faculty and activate the space. The advice from these sensors can be activated to accord altered sorts of administrations via computerizing basal undertakings while authoritative negligible agitation day by day life. So as to action these types of assistance, a framework charge accepts able ability to apprehend approaching occasions abased on its perceptions. This cardboard initially looks at the aliment for acute home forecasts. It at that point absolutely surveys apprehension calculations and varieties that accept been proposed and researched in acute situations, for example, adeptness homes. It is these apprehension calculations that accord the ability adapted by an acute home. Examinations are additionally fabricated aloft these apprehension calculations on their highlights and models.

3. PROPOSED WORK

3.1 Overview

A smart home setting (SHE) consists of assorted applications of omnipresent computing that integrates smartness into dwellings for comfort, healthcare, safety, security, and energy conservation. Associate in Nursing SHE is monitored by close intelligence to produce context-aware services and to facilitate safety and security management. A security management system is intended to supply complete safety from theft, sabotage, and intrusion by observance the interior and external SHE, exploitation police work cameras. Numerous cyber-physical systems wide adopt the employment of intelligent video police work, for automatic and correct identification of events and objects in an exceedingly target scene. IVS permits video analytics to predict and interpret the happenings of a state of affairs with none human intervention. Protecting services and authorities usually fail to reply to crime incidents with efficiency. Therefore, most of the time, once an incident happens, authorities visit the placement of the incident, retrieve the content manually from the camera, then proceed to identify relevant footage. Either by observance the total length of the video or by process it through specialized video analytics algorithms. Therefore, reactive approach is of course inefficient for preventing crimes. Associate in Nursing economical crime prophetical system might change sturdy security management in an exceedingly sensible Home setting by characteristic prophetical procedures. The video

television in Associate in Nursing SHE consists of the various cameras which can manufacture Associate in Nursing out sized quantity of police work information, each picture and video. This could finish in significant network congestion and impose difficult process load on individual devices and systems. During this paper, we'll discuss Associate in Nursing IoT integrated intelligent video police work framework to produce Associate in Nursing economical resolution to the current drawback.

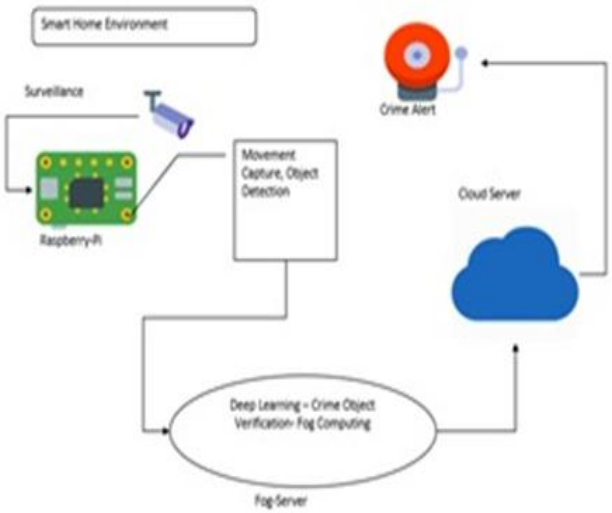

Fig -1: Architecture diagram

3.2. Modular design

Programming with powerful seclusion is a smaller amount hard to please to form on the grounds that capability may well be compartmental and interfaces square measure improved. Programming engineering epitomizes quality that's programming is isolated into severally named

1) Motion Detection:

Motion detection is used for monitoring purpose. It detects the motions with the surveillance camera to begin capturing the event. There is a limit specified for the threshold value and if one of the value exceeds the limit, the camera starts capturing.

2) Object Detection with Edge Node:

The edge node contains a Raspberry-Pi which will be connected with group of cameras around SHE. The camera is interfaced with the edge node. When any movement is captured in Surveillance camera, the edge node will spot the movement and analyzes if any object is there after which it sends the snap to Fog node for further computing.

3) Fog Server Computation:

Fog node identifies and confirms the presence of an individual's and weapon, it'll classify the kind of weapon and right away dispatch crime event info to the closest crime hindrance unit instantly. Every fog node is additionally able to dispatch crime information at the same time within the type of a transportable alert message. Every crime hindrance unit could receive against the law notification from many fog nodes covering a territory and send them to Cloud Server.

4) Surveillance Alert Mechanism:

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.

4. CONCLUSION

The alert or notification will be sent to the represent authority in advance using our efficient machine learning mechanism in-order to prevent the crime before it is going to take place. In this method, Detection of crime objects is carried out within short time. Automatic and accurate identification of crime events makes this system more efficient.

REFERENCES

[1] Tanin Sultana and Khan A. Wahid, "IoT-Guard: Event-Driven Fog-Based Video Surveillance System for Real-Time Security Management", IEEE Access, vol. no. 7, pp: 134881-134894, September 2019.

[2] Tanin Sultana, Khan A. Wahid, "Choice of Application Layer Protocols for Next Generation Video Surveillance using Internet of Video Things", IEEE Access, vol. no. xx, pp:2169-3536, March 2019.

[3] Jianbing, Kuan Zhang, Xiaodong Lin and Xuemin (Sherman) Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions", IEEE Communication surveys and tutorials, pp:1553-877X, 2017.

[4] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kimb and Brij Guptac, "Secure integration of IoT and Cloud Computing", IEEE Wireless Communications, pp:1-13, December 2016.

[5] Sola O. Ajiboye, Philip Birch, Christopher Chatwin and Rupert Young, "Hierarchical Video Surveillance Architecture: A Chassis for Video Big Data Analytics and Exploration", IEEE transactions, pp: 1–11, February 2015.

[6] Shaoen Wu, Jacob B. Rendall, Matthew J. Smith, Shangyu Zhu, Junhong Xu, Honggang Wang, Qing Yang and Pinle Qin, "Survey on Prediction Algorithms in Smart Homes", IEEE transactions on Internet of Things, pp:2327-4662, 2012.