PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2024)**, 2024, **pp**. 24–38
ISSN: 3078-3186

Research Article

Development of Smart Video Surveillance Systems: Technical and Security Challenges in Urban Environments

Suhaib Qassem Yahya Al-Hashemi[1,*], Majid Salal Naghmash [1] , , Ahmad Ghandour [1],

[1] *Islamic University Of Lebanon Faculty Of Engineering*

ARTICLE INFO

Article History

Received 20 Dec 2023

Revised: 2 Feb 2023
Accepted 1 Mar 2024
Published 22 Mar 2024

Keywords

Video surveillance systems, cyber security, activity analysis, real-time data processing, video compression.

ABSTRACT

Video surveillance schemes have become a critical tool for safeguarding urban and industrial services, thanks to the rapid advancement in object recognition, tracking, and human activity analysis technologies. The achievement of these systems relies on background analysis, motion detection, and innovative solutions for real-time data processing and storage. These schemes have transitioned from analog setups to IP-based systems, offering more flexibility and remote control capabilities. However, they face important cybersecurity challenges, such as data breaches, bandwidth consumption, and high processing demands. This research explores the technological advancements in video surveillance systems, focusing on the security challenges and analytics in urban environments. Furthermore, it discourses strategies for optimizing system efficiency through modern compression algorithms and real-time human activity analysis.

1. INTRODUCTION

The active area of research in recent time is the video surveillance [1]. Objects recognition and track in video surveillance system is frequently base on background estimations a subtraction [2]. The main focus of today video surveillance system performance is the applications of video compress technologies to powerful multiplexing or storage image from a big number of cameras to mass store device [3].

Since the viewpoint of real-time threats detections, it is known that humans visual attentions drop under acceptance level, when train personal and assign to the tasks of visual surveillance [4]. In addition, the video analysing technology could be apply to advance the smart surveillances system that could be assistance the humans' operators in real-time threats detections [5]. Exactly, multi scales track technology is the subsequent steps in apply automatic video analysisto surveillance system.

Visual surveillance application including car and ordinary traffics monitor, humans' activities surveillance for infrequent activities detections, persons counted [6]. The classic surveillance applications consist of three building block include motion detection, objects track and high level motions analysing. The multimedia system could be providing surveillance coverage across a wide area, ensure objects visibilities over largest variety if depth which could be employ to disambiguation obstruction. The technique that addressed handover am ong camera, in configuration with shearing or separate view are hence becomes gradually important [7]. The event of interested identify as move objects and persons should be coordinate in the multi views systems and event of specialist interesting should be track through the scenes. Numerous video surveillance product is obtainable on the markets for offices and homes security and remote surveillances. They monitoring of homes, an office, or any position of concern, captured motions event by use webcam or camcorder and distinguish abnormality [8]. In webcams case, the visual information is saved in compress or un-compress videos clip, and the systems triggering several alert like send an e-mails. The unavoidably of working with complex scene characterize by high variance, require the use of specific and sophisticate algorithm for video acquisitions, cameras calibrations, noises filtering and motions detections that is capable to learn and adopts to change scenes.

Work with scene characterize by reduced structures require the usage of robust patterns recognitions.

*Corresponding author email: sq.al.hashemi@gmail.com
DOI: https://doi.org/10.70470/SHIFRA/2024/004

2. URBAN SURVEILLANCES VIDEO SYSTEMS

The systems comprise the functions of objects detections, track, recognitions and classifications. The problems of object detections has been tack by use statistic model of the background images, frames difference technique or a combinations of all [9]. Numerous technique have been use for objects track in videos sequence to cope with multiple interact target. Objects recognitions and classifications are perform by use statistic patterns recognition and neural networks. Numerous feature, which explores the specific conditions of the problems, could be used. This includes geometric feature like bound boxes aspects ration, motion pattern and colour histograms [10].

3. VIDEO SURVEILLANCE SYSTEM DESCRIPTIONS

Surveillance systems implementing could be view as four independents, nonetheless interact module include detection, track, classifications and recognitions as illustrated in figure 1 in order to performs the detections tasks, a real-time algorithms.

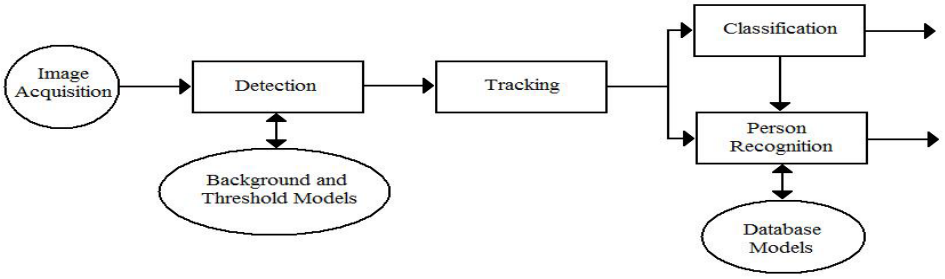

Fig. 1. Surveillance system diagram

This suggestion use two adaptive background image, per-pixel adaptive threshold and a regions group algorithms. The track algorithms determine the overlapping among detected region in consecutive frame to linked them, in case of no ambiguity exist.

The linked of an dynamic regions in consecutive frame originate a stroked, which describe the evolutions of the mass centres over times. The cataloguing tasks are performs every frames for wholly dynamic regions detecting, and the classification of a stroked is performs by determine the furthermost voted classes [11].

4. DETECTIONS PROCESSING

The key difficult of any approach lie in controlling environment, the background undergoes changes, classically use to the existences of lighting variation and distracter. The healthiness toward light variations of the scene is achieve by use adaptive background model and adaptive per-pixel threshold. The usage of multiple background and the grouping techniques contributing to the robustness of the algorithms toward unwanted distracter.

The system could be implementing by use two grays scales backgrounds model, create throughout a train stage. The ideas are to have lowest and a highest pixel values, contemplate this method to variation of no targeting pixel in the scenes. The per-pixel thresholds are then initialize to be above the differences among the two background. Events detection, detect and track object is a critical aptitude for surveillances. From the viewpoint of a humans intelligences analysis, the most critical challenges in videos base monitoring is interpret the automatics analyzing information to detecting event of concern and identifying trend. The challenge here is by use the knowledge of times and disposition condition to advance videos analysing by use geometrics model of the environments and other objects and activities model to understand event and using, learn technique to improved systems performances and detecting unusual event.

Objects detections are the first phase in furthermost track system and serve as a mean of focused attentions. There is two approach to objects detections include background subtraction and salient motions detections. Backgrounds subtraction assume a motionless backgrounds and treat wholly change in the scenes as object of interesting, whereas salient motions detections assuming that a scenes will have numerous different type of motions of which some type is of interested from a surveillances perspectives.

5. TRACK PROCESSING

The tracking purpose is to determining the spatial-temporal data of every targets presents in the scenes. Meanwhile the visual motions of target is constantly smaller compared to their spatial extend, no position predictions is required to constructing the stroke [12]. The region suggestion and their classifications are depended on a binary associations matrix compute by test the overlapping of region in consecutive frame. When there is a matched, the strokes are update. In addition,

the track of interact with the detections target stop in the scenes for a certain quantity of times, the trackers merge the targets in the backgrounds.

6. CLASSIFICATIONS MODULE

In the task of classifications, three key question have to be answered including of which class must be consider which feature finest separated. This class and which classifier best adapted to the previous choice?
The foremost objective of the classifier is to realize minimizing classification error though considered a varied spectrums of class. In the same time, the objective was not to considered time-dependents feature, limited the classifiers wholly geometrics property. In this technique, the result of classifiers could be usage in different machine, as it is independents of the achieve frame-rates [13].
The class that comprised numerous merge target cannot be describe via a Gaussian distribution over the features spaces. This could assuming several different configurations, which made them harder to parameterizing. This suggest the select of a non-parametric classifiers, such as K-Nearest Neighbor algorithms. The classifications tasks interact with the trackers in every frames, elective for the classes of every detecting targets. The last class is selected for every strokes as being the greatest voted ones. Within many surveillances' application, determined the types of object are critical.
The videos track-based system use statistic about the appearances, shapes and motions of moving object to rapidly distinguished persons, vehicles, door open or close, tree move. The Image-based system like faces, pedestrians, or vehicles detections, find objects or definite types without previous knowledge of the images position or scales. This system tended to be slow than videos track base system that leveraged existing track information to located and segments the objects of concern [14].

7. RECOGNITIONS TECHNIQUES

Similar to classification modules, no time data is use to performs the recognitions tasks. The recognition processing is intended at recognize in a short terms duration which is a target that becomes occlude for a few seconds or target that merges for a few seconds and then splitting for a second time. The model is characterize by the PDF estimate of the selected features spaces, in this colour cases [15].

8. ACTIVITIES ANALYSING

The humans activities understanding is one of the greatest difficult open problem in the areas of automating video surveillances. Detect and analyze humans motions in real time from videos images has lately becomes feasible with algorithm.
This algorithm represents a respectable first steps to the problems of recognize and analyse human, nonetheless they still have certain drawback. Consequently the humans subjects should dominated the images frames thus that the individually body component could be dependably detecting [16].

9. OBJECTS MODELLING

The purpose of video surveillance systems is to monitoring the activities in a specify indoors or outdoors areas. Since the images are generally capture by a fixed cameras, it is easy to detected a still backgrounds than moved objects. Meanwhile the camera use in surveillance is classically fixed, a straight forward method to detecting the moving object is to compared every newest frames with a references frames, represented in the best conceivable method the scene backgrounds [17]. The related subtractions are high-level processing module for objects track, event detections and scenes understand purpose use the result of this processing. Effective background subtraction play a important roles in find dependable result in the high levels process task [18]. Background modelling is usually carry out at pixel levels. In every pixels, the set of pixel features, collect in a numbers of frame, is use to build an suitable models of the local backgrounds [19].
Feature use for strength or colour, local base like edge, difference or depths and regions base, like the block correlations. The finest method to builds such a background models will be to captured the blank scenes for a numbers of frame and take the regular frames as the assessed backgrounds. Inappropriately, like this scenarios are harder to be putting in practices in numerous application like the surveillances at an airports terminals, metro stations or on highways. The improved method to modeled the statics backgrounds are over a random variables or a random vectors with an associating possibility compactness functions. In certain case, like tree wave in the backgrounds or a rotated fans, more than just one adjustable must be usage to appropriate backgrounds modelling [20].

10. ALTERATION DETECTIONS

In the surveillance applications consideration, the video camera captured image of a static scenes, with light change, furthermost of the times. The arrival of an intruders into the scene could thus be detect through the change it cause. The

change detections subdivisions algorithms could be used with the changed area characteristically correspond to intruder. The changing detection algorithms implement a statistic hypothesis tests to decide whether a given pixels has change, or not change as in [21].

Additionally, the threshold steps make additional consideration about the difference among the changing and unchanging area variation, and on the sizes of the change areas, to realize a better behavioural for the threshold operations [22]. The foremost module of the changed detections segmentations is as follow:

1. Threshold process: pixels classification as changing or not changing resulting from the threshold process of the difference among consecutive image. The threshold values is robotically computing, depend on the videos sequences characteristic, without any manual configurations.
2. Combinations with memories: The threshold outputs is combine with the segmentations mask from a memories, to made the changing detections resulting more steady. This could improve segmentations result in case of the motions of a given objects temporarily stop.
3. Smoothing: Isolating pixel is remove and smallest hole in object has occupied to made the changed detections division results in more smooth.
4. Memories updating: The last step contains in the automatic adjustments of the memories content, depend on the observe sequences characteristic.

The memories store the data about the changing area detect in past time instant, being indispensable to keeps tracking of object even when they temporal stopping move, to ensures an improved temporal stability of changed regions. Though, by use a extended memory might have the unwanted effects of create segmentations mask for the moved object that is largest than the actual object. The algorithms memories lengths controlled parameters represent number of time instances in the pixel classifications as change must be kept. These parameters are automatic adjusting depend on the sequences characteristic, covered to zeros when a considerable quantity of motions is detecting, and to the maximum allows values when only slow motion is detecting [23].

11. TRACKING SYSTEMS SOLUTION

The tracking system purposes are to obtain data about objects in the checked spaces at numerous scale in a unified frameworks. The systems use a mixture of energetic camera and multi scales model to addressed the issues of scale variation in the visual track application. The videos from the static camera is use to detecting and tracking multiple object in either two or three dimensions. The static cameras image could be use to extracting extra data about at a courses levels like objects classes or objects attribute.

The data from the courses and fine scales analyse is joint in the internal scenes representations. The concepts use numerous key technique, include detection of the moved object in the videos track in two or three dimension. Similarly, the systems use a mixture of energetic camera and multi scales model to addressed the issues of scale variation in the visual track application [24].

12. COMPRESSION AND ENCODING OF VIDEOS

The furthermost commonly kinds of video encode employing in video surveillances system are MPEG-4 and M-JPEG. The M-JPEG type codify every frames as a JPEG pictures, without exploit any inter frames predictions. In this manners, the result videos streams contains of independents frame. The advantage of this approaches is relate to the lower process powers needed in compress and decompress the videos stream. Furthermore, the M-JPEGs type is selected in case of trials indication is a goal of record. The M-JPEGs type could divide up to separated frame which could analyse freely of the earlier and succeeding frame. Additionally, meanwhile JPEGs frame is themselves compression, and the M-JPEG formatting could be adjusting to save bandwidths.

Though, with M-JPEGs there is no utilization of the inherent correlations among many frame. For these reasons, difference encodings algorithm, in specific belong to a MPEG formats, are increased replace M-JPEG because of their high bandwidths effectiveness, as they takes advantages of the static natures of the scenes shot through the routines camera operation.

This effective transcode technique is obtainable to translating MPEG flow into M-JPEG in an effective manners. In this direction, the MPEGs flow could achieve the requirements of derive statics picture from the videos flows, to be usage as trial evidences. In subsequent details on the greatest current one, an MPEGs-4, major of CCTVs system run MPEG-4 and alike differentials encoded algorithm extend the applicable of the early standards MPEG-1 and the more current formats MPEG-2 is exactly targeting at higher-definitions televisions application. In specific, MPEG-4 provide supporting for lower bits rates encoded and for 3D contents and complex videos or audios object. In this technique, MPEG-4 could be say to extended the provision of effectual coding for videos flow cover the entire ranging from lower bits rate active to HDTVs and elsewhere.

Analogy to MPEG1,2,4 decompose a videos flows exploit redundancies predictions mechanism. Though, different from MPEGs-1 and 2, a units of representations non named a frames, nonetheless a video objects. In simple cases, to lower bits

rate, the entire scenes might single video objects. Every video object is layer into video objects layers such as possibility to have one base layers and numerous enhancements layer.
The Video object layers are order sequence of snapshot in times, refer to as video objects plane. In every video object plane, the encoders process the shapes, motions, and textures characteristic.
The shapes data is encode via bound the video objects and rectangle boxes and divided a bounded boxes to macros block. Every MBs is classify divers depend on the positions and then shapes coding. The textures coded is same to frame base standard like MPEG-1 or H.263, using video object as frame that classify as interceding. Additionally, the forwards predicting or bidirectional predicting.

13. RESEARCHES CHALLENGES

The TCP/IPs technologies and relate IP-base network non intend to provision the severe requirement in term of bandwidths and systems reliabilities that essential by a security systems. Hence, important point should be taken into accounts and numerous issue, often in contrasts with each other, arises when employ these technologies in the field of video surveillances include:

1. network bandwidth.
2. higher process capabilities require to encoded, decoded and recorded many videos stream.
3. networks security protocol, algorithms and policy for guarantee the privacy and authenticities of the videos stream.
4. encoded algorithm design for live streams which offers bandwidths efficiencies, lower process power requirement which outputs could be use indication in lawful trial.
5. mechanism detected with reaction to Denials of services attack and guaranteeing services in faults situation.

Because of the number of stream involve video streams and, in particulars, video surveillances are amongst the furthermost critical applications in term of bandwidths requirement. Each video cameras ordinarily require among one and ten Mb/s for a highest qualities streams with a frames rates of 25 frame per seconds and an images resolutions of 640×480 pixel. Commonly enterprises and municipals network is not design to supports ten or even hundreds of stream due to the majorities of current install LAN only provide a full bandwidths of 10/100 Mb/s. The mid-size shop mall may easy to needs among 100 and 300 camera. Though for information transmissions purpose a commonly 100 Mb/s LAN is passable for maximum shop mall, to streams highest resolutions videos flow for 1 Gb/s networks is hardly adequate and a 10 Gb/s infrastructures are clear sensible.
Three main approach and technique to cope with the bandwidths requirement of videos security application. Firstly, over provision of network resources could be introduce at the networks designing stages. Deployed a higher bandwidths network by mean of 1 Gb/s Ethernet standards must be a commonly solutions for LAN. Backbone at 10 Gb/s will be required to guaranteeing a good interconnections amongst the LAN segment. Secondly, the videos compression ration could be increase by use additional effectual videos compressions algorithm. Though, the high compression ratio, the slow algorithms to decoded the videos and, thus, the highest computational power. Lastly, implements of smart and effectual context aware videos adaptations algorithm in the cameras which dynamic switches from the idle to videos transmissions status in case of situations interested is detect.
Fairly interestingly, in numerous videos security system, the real bottlenecks are not bandwidths but the process difficulty. Though the migrations to differential video encoding algorithm (e.g., MPEG-4) has importantly decrease the bandwidths require per videos streams, the more complexity compress scheme have dramatic increasing
the process requirement and, thus, the cost of hardware accomplished of simultaneous decoded many higher resolutions video stream.
Equally, the video surveillances are frequently use in crime preventions, networks security, privacy and detections of fault situation is very important topic. Besides, guarantee the video surveillances services to be always obtainable is greatly important than for other type of service. Definitely, the video surveillances infrastructures should be robust against DoS attack and prompt reporting any problems to the controlling rooms with as detail as conceivable data in locations issues rose. Liability to DoS is an inherent problems of other services provision systems were event should be process to determined their validities. By way of prank telephones call or pleasant of doors bell of last time, an active means of avoiding DoS attacks to occurred in identifications of attackers. These are only fundamentals solutions, specified the inherent weakness of services provision system to DoS. When the physicals sources of DoS traffics could be identify, formerly at the smallest the invaded network elements could be isolate or shutting down and, in some instance, the attacker identities could be more traced backs. The video surveillance systems might be assumed deal to DoS by mean of both practical and sensitive countermeasure. In specific, routes base packets filter solution might be use to this conclusion. Definitely, observing that the system insulating from the external network, the only gateways being the controlling rooms, which is assume to be dependable enough. Therefore, intrusions from external networks could be easy identifying and filter at the controlling rooms terminal. Malicious information sent to the cameras over the wireless link could instead be counteract by mean of the surveillances systems itself. Indeed, the directional grids antenna is use in the surveillance system that is not easily to blockage or malicious distorted unless an external devices are putting in lines of sights of transmitter

and receiver. Though, this will be probable detect in the surveillances systems itself, therefore enable the detections of the intrusion and maybe also identify the intruders.

14. RELATED WORKS

14.1 The IP-Based Video surveillance security System

The video surveillance system have becomes a portion of the internet of Thing (IoT) in last few dedicate. This surveillance system currently protecting industrials facility, railway, gas station, and own homes. Inappropriately, such IoT system, there is inherent risks that could leads to important violation of a user privacies. The exploration of attacks surfaces of current surveillances system and the various way they could be compromise with real example have been proposed by [25] in 2020s. They identify a threat agent goals vectors, and the results consequence of successfully attack. Lastly, they presents existing countermeasure and best practice and discussed the threat horizons. Their reviews are to providing researcher and engineer by healthier understand of a modern surveillances system to hardens current system and developing the improve solution.

Several way on IP-based surveillances systems could be deploy. The networks topology could be centralize wholly camera connecting to a DVR or distribution the users connect to every individual cameras. In term of convenience, the systems could be straight available through the internets. Regarding to this, they identifies three category of availability as illustrated in figure 2.

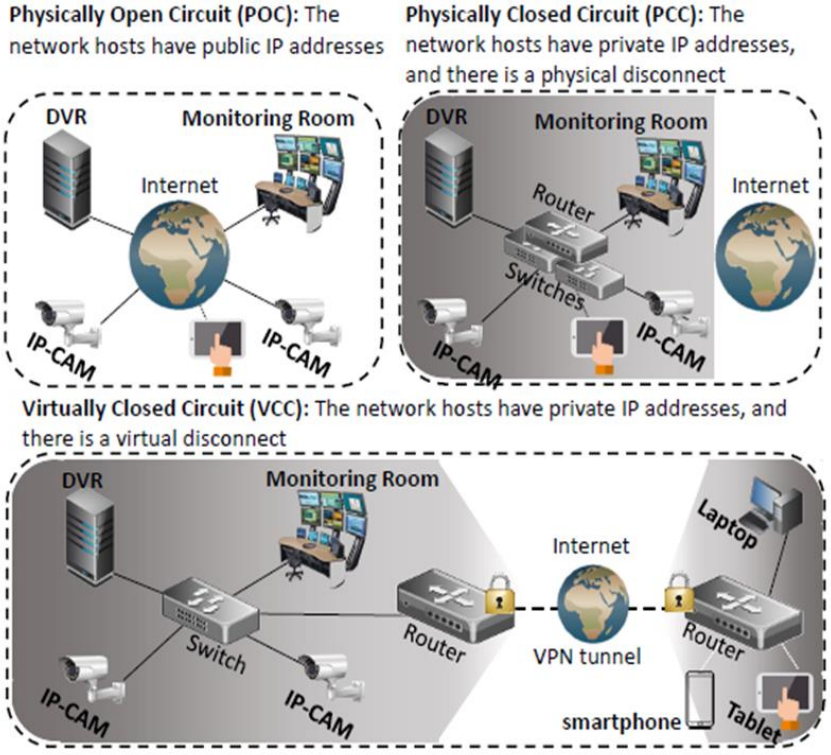

Fig. 2. Availability model for deploy avideo surveillance system

14.2 Recovery Optimizing of Surveillances Videos Storage Systems

The investigation and analysing the characteristic of videos information and put onward a campus surveillances videos storage systems with the universities of the specific applications environments have been proposed by [26]. Directing to the challenges that the contents-base videos retrievals responses time is too longs, the key-frames indexing sub-system is design. The main frames of the videos is reflected the key contents of the videos. They extract from their videos, the vital frame is associate with the meta data to establishing the storage indexing. The key-frames indexing is use in look up operation whereas query. This technique could great reducing the amounts of videos information read and efficiently improve the query competence. They modelled the storage systems through a stochastic petri nets and verifying the promotions of query performances by measurable analysing.

The progressing of **video surveillance** systems with the digitals networks trends, is transform from innovative analogy signals transmissions, over the digitals signals transmissions, to networks digitals transmissions in existing. The disks videos recorders as illustrative of digitals surveillances systems is gradual replace by networks videos recorders.

The disk videos recorders combine videos controlling with videos storage to made the systems more integrating and more appropriate, nonetheless it could store information on the disks of the local computers, that limiting the sizes of the systems information. The NVR has a functions of receive IP camera information, videos codecs, storages, real-times displaying. They also forwards the store videos information to other storage system over the network as illustrated in figure 3.

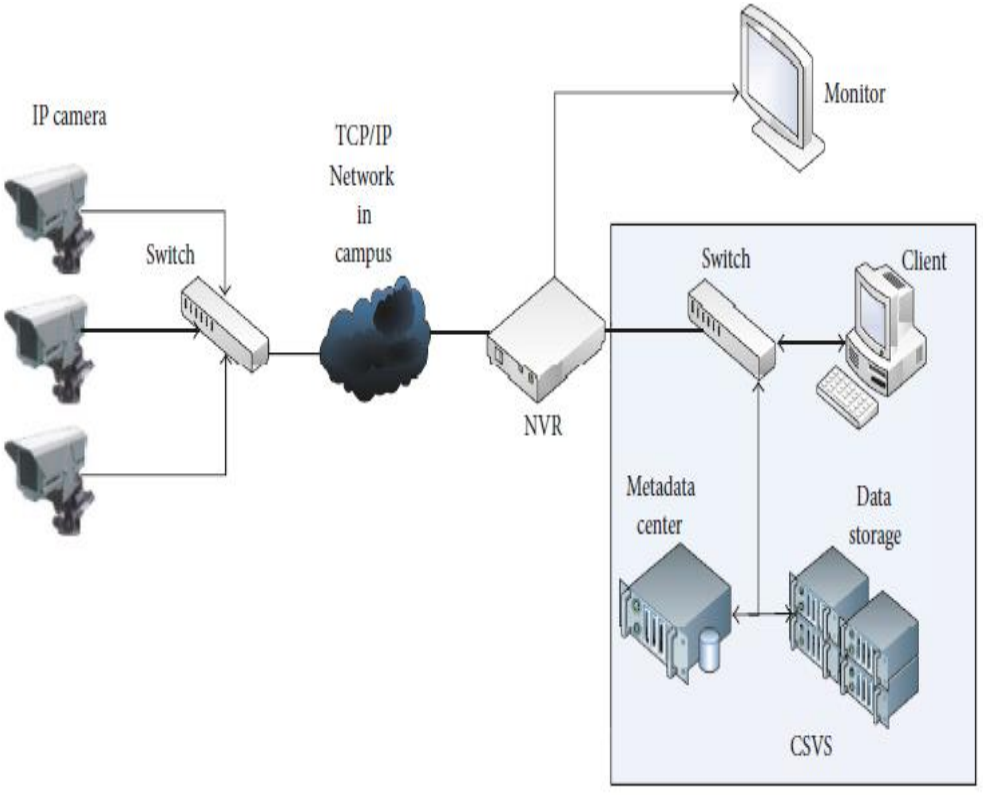

Fig. 3. Video surveillance systems deployment

14.3 Configurations, Interface and Networks of Wireless IP-Based Cameras for Surveillance System Design

Three methods for configuration, interface and networking of a wireless IP-based cameras for surveillance systems have been design and proposed by [27]. Their implementations technique suggested for configure, interface and networking the IP cameras are:

1. access the IP-based cameras by use the Wan scams vendors software.
2. access the IP-based cameras through Firefox® web browsers.
3. access the IP-based cameras through Simulink in MATLAB.

They demonstrate the interface and networking of the IP-base cameras with numerous computer by use an Ethernet switches. The live stream videos depend on their suggestion technique could be adapt for images detections, recognitions and track for real-time intelligent surveillance system designs. They installed the software over the WAN technology. In case of the CD is inserting into the hosts computers, the next option is itemize include:

a. Mobiles view software.
b. computers IE view via Ocx Setup.msi.
c. Searches tools.exe.

From these option, the Ocx Setup.msi has selecting, click and runs leads to the software installations. Afterward, their cameras powers before connected to the IP cameras host computers through the CAT5E cables with the RJ45 connectors at tips of the cables. Formerly, the Search too.exe is doubled clicking and runs to search for the IP of the connect IP at tips of the cables. Formerly, the Search too.exe is doubled clicking and runs to search for the IP of the connect IP cameras and this pages are loading as illustrated in figure 4.

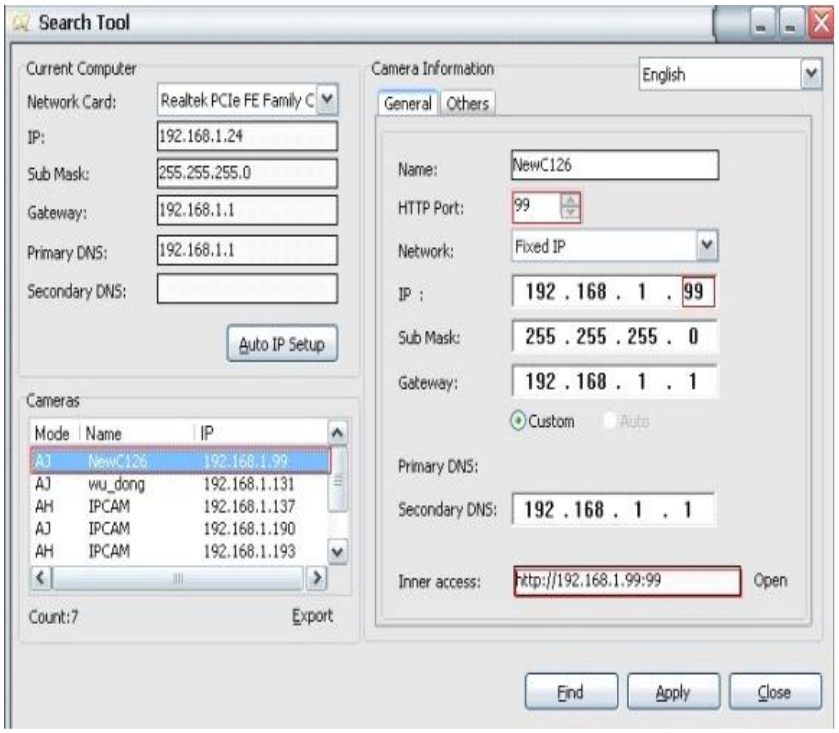

Fig. 4. Configure and networking of IP cameras by Wan scam vendors

14.4 Video surveillance System

The reviewing of numerous present video surveillance system have been published by [28]. The increasing of video monitoring become energetic the video surveillances systems to capable the support a personnel in monitor and track activity. The goal of the surveillances application is to detecting, tracking and classifying target. Their paper is defined the objects model, activities analysing and changing detections. They described a design of the video surveillance systems as illustrated in Figure 2.5. This work have videos outputs from CCD cameras. The videos outputs is divide into videos series that inputs for processor named pre-processing. To recognize the moving object on the backgrounds, head detection and luggage detections is used the trackers. Trackers contains the subsequent block:

1. Motions Detectors.
2. Heads Detectors.
3. Shapes Trackers.
4. Regions Trackers.

The outputs of tracking is recognize in recognitions blocks. Their systems used person tracking algorithms which was design by Nils Siebel. The read persons tracker is software for track persons in cameras image for visual surveillances purpose.

Its originate from researcher works on persons track for automatic visual surveillances system for crime detections and preventions as illustrated in Figure 5.

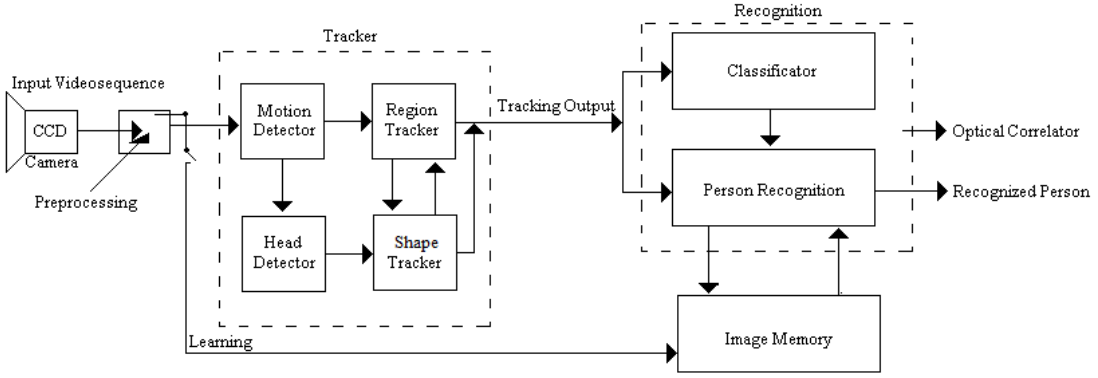

Fig. 5. Flow diagram of IP based approaches systems

14.5 Video surveillance System Designs

The description of the step involve in design of a video surveillance systems have been published by [29]. They discuss the theories of video surveillances categories, component involve, select the finest component, and a detailed virtual designs. The introduction of the video surveillance system idea is follow by the details discussions of design consideration and the design verifications. The systems are design to monitoring a bank floors where the monitors display the wanted outputs from a simulation implementing of the systems. The system could be sets up as illustrated in figure 6 The DVRs is connecting to the routers by use LAN cable.

1. The subsequent should be note about the connections:
2. The IP address is randomly assign.
3. The computers is set up the DVRs through the user interfacing that is available through the LANs connections.
4. The ADSLs modems provide internets accessing to the systems.

Two camera is indicating to be connecting here though this is determine thru a numbers of port obtainable at the DVRs.

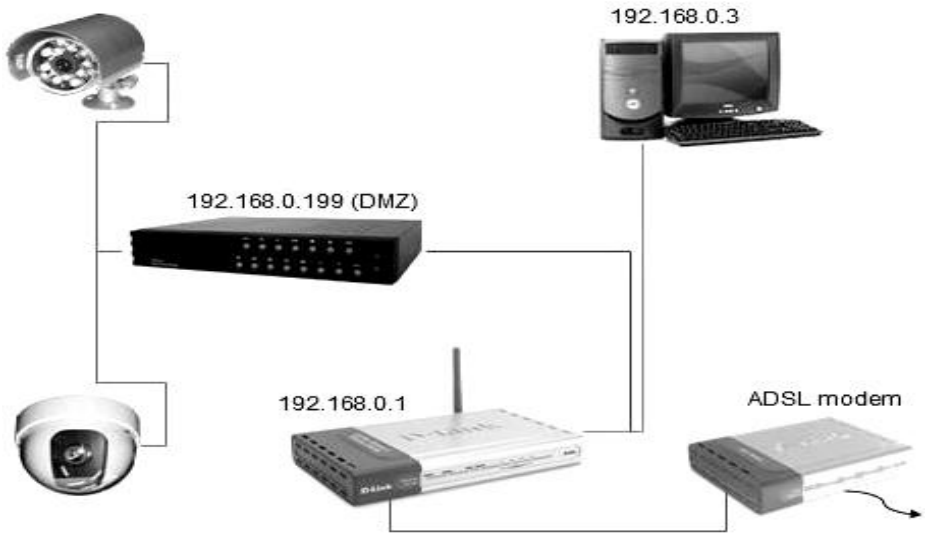

Fig. 6. Setup of DVRs cameras

14.6 The Characteristic and Advantages of IP Camera Videos Monitoring

The overviews and characteristic of IP cameras video surveillances system have been proposed by [30] that compare to systems with other kind of camera. Their study deal with the basic characteristic of the IP camera use in video surveillances system with real compression them with the analog one. The comparisons among IP and analog cameras characteristic is make when they use in operations of one video surveillances systems. The system of IP video surveillances multi views functions model is also study. Additionally, their study dealts with the IP cameras powers charging principle in the video surveillance systems through Ethernet case with and without PoEs switches. Their overviews include the basic characteristic of four types of IP camera contains:

1. Cubes.
2. Domes.
3. Boxes.
4. Given Bullets.

These characteristics offer the users a opportunity to easily and securely combined suitable camera and PoEs companionable device on the networks. The standards provide up to 15.4W on the switches or middle spans, that transfer concentrated powers of 12.9 W to the placed with a devices or cameras, power over Ethernet (PoE) for external camera as well. Figure 7 provides the principles of IP cameras network with and without lively splitters, using mid spans.

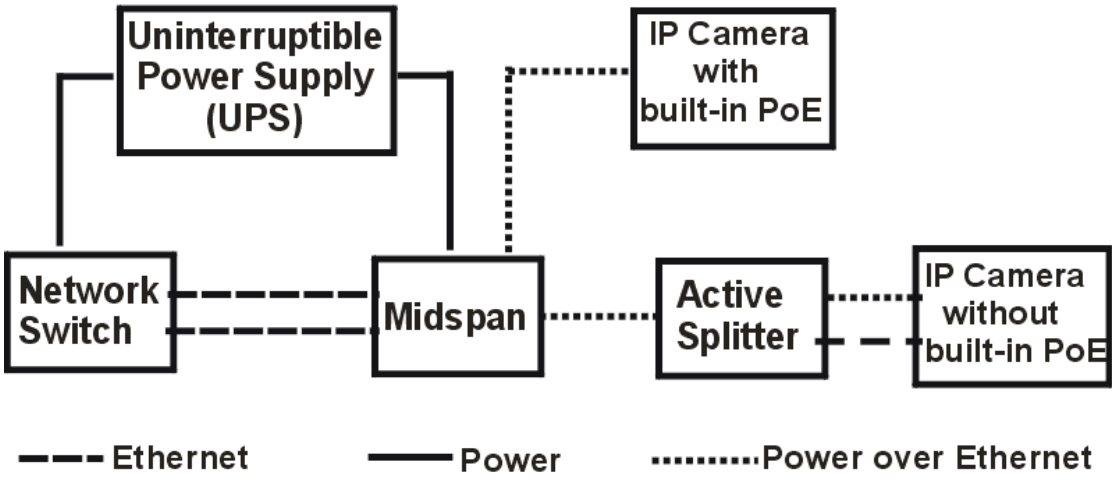

Fig..7. Principle of connected IP cameras with in video surveillances

14.7 Real-Time Systems For Videos Transmissions Over IP Network

The end-to-end servers-clients systems for higher-resolutions videos transmissions over IP network have been proposed by [31]. Their systems support communications of compress data, users operation over a full functional users interfaces and detections with track of move object and persons.

They rely on a communications sub-system that has been develop for real times transmissions of MJPEGs or MJPEG2000s compression videos data over out-of-order packets local and wider areas network. The image is at the HDTVs standards resolutions. The servers grab frame from a cameras-links sensors, encode the raw videos, place the encoding bits streams to the packet and transmit them over networks.

The clients receive and reorder the packet and then display the videos information. Every user could requested different focusing window from the servers depend on the viewpoints of interesting. Every encoder frames is fill with restarting marker to faces up the cases of a frames been losted. The communications systems contains of the transmissions protocols for the server raw information, send the packet over networks and re-order the packet as they arrived to the clients.

In addition, the supporting of errors corrections algorithms that is use in cases of lost packet. Figure 8 shows the TCPs servers-clients communications Block diagram.

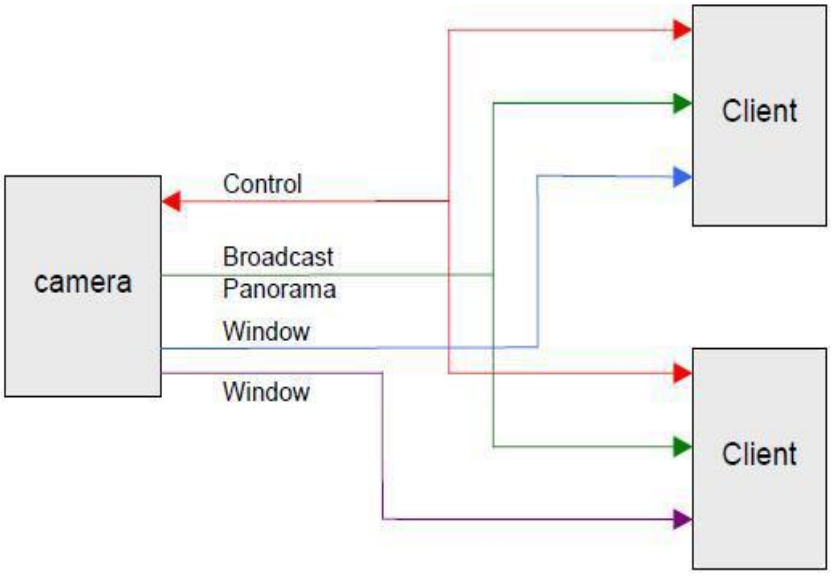

Fig. 8. TCP Servers - clients communications Block diagram

14.8 Video Transmission over Wireless IP Network

The dissemination of the contributions a simulation environment for video transmission over the wireless network in Fedora environment because the Cygwin in window-xp environment has been proposed by [32]. The over objective is to evaluate

the video transmission of an MPEG stream and considering average PSNR for the interaction of bandwidth 1 to 24 Mb and queue size 10 to 100. The simulation result graph is shown in figure 9.

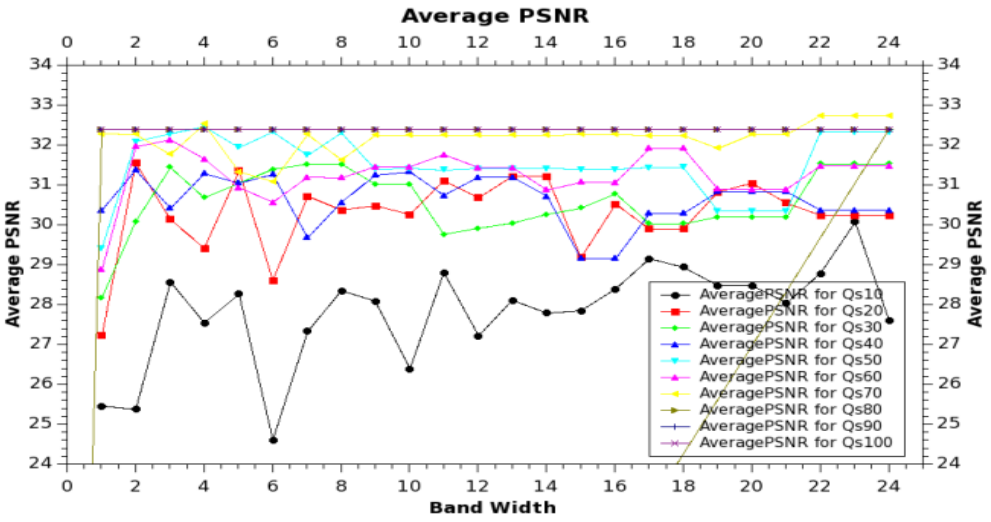

Fig. 9. Simulation results[33]

15. SECURITY PROBLEM IN THE LAYER

Meanwhile the wireless networks utilize broadcasting communication, the data could leaks and destroy on every different protocols layer, meaning that the physical layers, links layers, networks layers, transports layers, and applications layers. Then, the inspect possible attack on every of this layer could explain here.

15.1 Physical Layers

The foremost security problem on the physicals layers is mostly jamming and physical node security. The jamming attacks includes transmit interferences in the similar radios frequencies ranges use by the node. Frequency hops and codes spreads is two classic solution to resisting the jamming. Though, since the utilize commercial obtainable service wireless interface, the interface of this device is not proficient of utilize frequencies hopping or spread code to combats the determined jammers. Nevertheless, brute forces jamming is rather straights forwards to detecting and one could appeal laws enforcements to addressed this jamming. Aimed at the securities of the node that needs to offer the node with certain sorts of physical securities like affixing them into places, and utilize tamper-resistant package to protects the crypto graphics key and other information saved in the node.

15.2 Links Layers

In case of two Wi-Fi device trying to transmitting at the similar times, their signal will interferes, causes a collisions. These collisions might destroyed the transmitting frames. Consequently, the media accessing and controlling protocols incorporated a back off and collision avoidance mechanisms. In addition, one could use errors correction code to reduces these problems and by use discerning retransmissions resend frame that are not acknowledge by the receivers. Though, an attackers could mounts the collisions attacks to deliberately causes collision on the links layers. In same idea, an attackers could merely continuous transmitting frame, therefore utilize larger proportions of the link capacities, these will induced resourced exhaustions. Though, this might trying to limits the information rates of node to slowly down an internal attackers, a determine internals attackers could sends frame with every of the identity that it has compromises. Meaning that, this attackers could masquerade as multiple legitimate nodes, thus utilize the sums of the limit rate of wholly of this node.

15.3 Networks Layers

Numerous attack on the networks layers were found such as deceived routings data, discerning forward, sinkholes, Sybil, wormholes, HELLOs flood attacks, and acknowledgements spoof. Though, this attack will **not** be relevant to us when constraining the networks topologies to be a single hopping Wi-Fi networks, which wholly communications are direct among the router and other node. Assumed that the costs of a wireless routers or Wi-Fi accessing points need to be lower to suits the homes markets, when give cameras is out of ranges, hence, this will assumed the introductions of an extra wireless routers or Wi-Fi accessing points to maintains a single wireless hopping topologies.

There are numerous multiple hop with the fixe LANs in the homes, nonetheless there will only be a single hopping overs a wireless links – and will be the only wireless hopping in the homes networks. Moreover, there might be a wide area

wireless networks from the homes to the internets, but this link is assume to be over a 3Gs networks . hence the frequencies will be license to the 3Gs operators and the securities of these links will be provide by the 3Gs securities mechanism.

15.4 Transports Layers and Applications layers

The transports layers carry applications layers data. When the cases of UDPs packet carry real-time protocols (RTPs) packet one could use secures RTPs (SRTPs) or another mean to provided encryption traffics. Moreover, SRTPs could provide authentications of each RTPs packets. When the cases of TCPs traffics one could use transports layers securities (TLSs) to offer confidential of the traffics. In case of the TLSs is use in conjunctions with publics keys cryptograph it is conceivable to implements mutual authentications of the device participate in a TCPs sessions. The TCPs is vulnerable to SYNs floods attack; so it may be desirables to use a more modern transports protocols like the Streams Controls Transmissions Protocols (SCTPs). The SCTPs avoid the creations of states which make a SYNs attacks likely.

Resynchronizations of a TCPs sessions might destroyed an current connections by prevents host from exchange data. The solutions are to authenticated wholly packet among the host. The important applications layers activity needs by the systems is key management.

16. INTEGRITIES

In the surveillances systems, the message integrity are an vital parts of the system securities. The messages integrity could protects alongside messages modifications. The secret keys systems could be use to produce a cryptographic checksums known as a message authentication codes. hence, when we want to sends a messages to Bs, the compute values using message authentication codes and share secret keys. Formerly the values are add on the messages sends to Bs. Once Bs receive these messages, it will computed the message authentication codes in the similar ways, and compared it to the values add to the messages. When the two value is similar, the messages could be consider unhampered with. Else, the messages has been modify.

Certain networks securities protocol, like SRTs, utilized the message authentication codes blocks to verifying the integrities of the messages. It must be note that these blocks are optional in SRTPs, nonetheless if it is presents it could be check to ensures the integrities of every messages. Digital signature is other ways to verifying integrities. The Digital signatures algorithms is depend on public keys cryptography. hash function could be used to produce a message authentication codes to protects the integrities in much the same ways as in secret keys cryptography. Though, this is not as secured as secret keys cryptography since the hashed functions is well-known.

17. KEY MANAGEMENT PROTOCOL

Key management is an vital issues for WSN. The establishments and managements of secrets key is vital element of communications securities, particularly over wireless link. Certain key management algorithm cannot be apply to WSN because of the constraint of the node; though, this is not an issues for our solutions as constraint on electric powers, CPUs performances, and obtainable memories is not so pertinent to our solutions. Consequently, we must be capable to more simply identifying a appropriate key management protocols for our systems. The Key management method use by WSN comprise random key pre-distribution scheme and pre-share keys distributions scheme for producing of key, pair-wise key management, and groups key management scheme. Moreover, there is a key management scheme base on spatial locations, a keys distributions centre (KDCs). Generally, the two basics key management scheme is a single key scheme with the multiple key schemes. The single key management schemes are a schemes where wholly node shared a single symmetric keys. This is the simple types of key management schemes. As examples of these schemes is Tiny Sec design by researcher at the University of California at Berkeley that use a single global key to encryption and authenticated traffics. The single key schemes has the high efficiency and it support utmost basic networks function, nonetheless the disadvantages is that if the keys is reveal, the securities of the completed systems is compromise.

Many key management scheme is more secured than single key management scheme, due to the different node used different key, therefore even if one nodes are compromise the system securities is not directly compromise. The Securities Protocol for Sensors Network (SPINSs) is an examples of a typical multiple key management protocols. It has two security modules: SNEPs and µTESLAs. The random keys distributions schemes is a good methods to decreased the risks when deliver the key. Each nodes could random stored key from a keys-pools, though maintains the probabilities of two node have similar keys above a some thresholds. When the two node shared a keys, then they could communicated with each other's.

The pre-shared key distribution schemes allow one keys to be share among two node, to enables nodes to nodes and nodes to bases stations communications. If we use many key management scheme, there should be at least one nodes performs the key management operation, as we have a routers in our topology we will used it to performs wholly of the key management function. The Key management protocol is design for many system conferring to their works pattern. The study of securities of WSNs due to the systems are same to WSNs, nonetheless un-like a WSNs, the system will sends many multimedia information; consequently, one could selected a key management protocols design for multimedia

transmission systems. The Multimedia Internets Keys (MIKEYs) is a protocols design for multimedia scenario; it could be used for peers-to-peers, one to many, and smaller sizes groups interaction. It could be used together with SRTPs, consequently certain multimedia session use this two protocol together to ensures communications securities. The MIKEYs together with SRTPs is typically utilize in Voice over IPs (VoIP's).

18. ROUTER BASE DEPLOYMENTS

Today, utmost homes surveillances system have three layer: front end device, networks transmissions, and central server. The fronts device typically collects and compressed image, status signals collections, and signals outputs. Split have to processing the image that is upload by the transmissions modules, and provided numerous service such as image analysing, alarms data storages, data and devices managements, users accessing controlling. The server provided application for numerous terminal. Some separated function from the server, and added this function to the routers. Consequently, the image from the camera could be analyse in the local router. The advantage of develop a routers deploy applications is obvious. The first advantages is reduces network traffic and save network resources via routers platforms to analysed data instead of upload this data to remote server. Also, the advantage is improve transmission speed, as the camera do not needs to uploaded wholly of the image wholly the times, but only those image that meets the user criteria needs to be upload to a remote server. User could controlled camera by an applications deploy on the routers. The deploy applications on the routers avoid the needs for a local servers while reduce the workloads of remote server. Though we can used other computer to realized these functions, the routers has the basic function we needs and wholly of the data from the local device would flows over the routers [34].

Hence, doing process on this data rather than just forward it to other processors to do the computation also reduce local networks traffics. Consequently the deploy of application on the routers, make the routers into a many functions tools to realized a home's surveillances networks. The routers we select is an open sources routers platforms; henceforth we could effortlessly developing newest function and extends current function. Furthermore, we need to made it convenient for user to downloaded a newer versions of the software for their routers.

19. COMMUNICATIONS CHANNELS FOR CAMERA

The camera and router have Wi-Fi module that could communicated straight to each other by Wi-Fi. Though, the camera could connecting to the routers mechanically, just as any other device which have a Wi-Fi modules, the special communications channels for camera; so that we could managed and Routers base Deployments controlling the camera straight to routers created a appropriate channels for used by camera, we must distinguishing camera from other Wi-Fi interfaces equipped device.

20. CHALLENGES:

High-resolution surveillance schemes require significant bandwidth, particularly in multi-camera setups, creation it crucial to establish a robust infrastructure to support the data flow. Video analytics in real-time also postures challenges due to the high computational power required for encoding, decoding, and processing multiple video streams simultaneously. Furthermore, IP-based surveillance schemes are susceptible to cyberattacks, such as Denial of Service (DoS) attacks and data gaps, which present serious risks to secrecy and security. Technically, these systems face complexities such as accurately detecting backgrounds under changing lighting situations and managing overlapping objects within the camera's ground of view, which requires advanced pattern recognition algorithms. Additionally, efficient data storage and organization systems are essential to handle the vast amounts of video data generated by continuous surveillance and the long retention periods needed.

21. CONCLUSION:

Video surveillance schemes are a dangerous component of urban security substructure, with modern technologies such as object recognition and human activity analysis enhancing their effectiveness. Despite these technical advancements, several challenges remain, including high data processing demands, cyber security risks, and large storage requirements. Addressing these challenges needs innovative solutions, such as advanced video compression algorithms and scalable network substructures. By continuing to grow and refine these systems, a balance can be achieved between enhancing security and maintaining privacy.

Funding:

No external financial assistance or institutional funding was utilized for conducting this research. The authors assert that all research-related activities were self-financed.

Conflicts of Interest:

The authors declare that there are no competing interests associated with this work.

Acknowledgment:

The authors would like to thank their institutions for their steadfast encouragement and logistical support throughout this research journey.

References

[1] A. Almalawi et al., "Add-On Anomaly Threshold Technique for Improving Unsupervised Intrusion Detection on SCADA Data," Electronics, vol. 9, no. 6, p. 1017, 2020.

[2] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks," in 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), 2017, doi: 10.1109/HASE.2017.36.

[3] O. Koucham, "Intrusion Detection for Industrial Control Systems," Ph.D. dissertation, Universite Grenoble Alpes, 2018. doi: tel-02108208.

[4] J. Angseus and R. Ekbom, "Network-based Intrusion Detection Systems for Industrial Control Systems," M.S. thesis, Chalmers Univ. of Technol., 2017.

[5] Q. Lin, S. Verwer, R. Kooji, and A. Mathur, "Using Datasets from Industrial Control Systems for Cyber Security Research and Education," in CRITIS 2019.

[6] J. Wang and H. Shao, "Application of Wireless Sensor Network Technology in Security Control of Intelligent Buildings," Int. J. Online Eng., vol. 14, no. 5, pp. 93, 2018.

[7] M. Ghasemi-Varnamkhasti, S. S. Mohtasebi, and M. Siadat, "Discriminatory Power Assessment of the Sensor Array of an Electronic Nose System for the Detection of Non-Alcoholic Beer Aging," Czech J. Food Sci., vol. 30, no. 3, pp. 236–240, 2018.

[8] H. Xu et al., "A LCX-Based Intrusion-Detection Sensor Using a Broadband Noise Signal," IEEE Access, vol. 7, pp. 161928–161936, 2019.

[9] M. D. Azhar, N. Kuntoji, and P. Kumar, "Solar Based Security and Smart Irrigation System for Agriculture," Int. J. Adv. Res. Ideas Innov. Technol., vol. 4, pp. 1298–1300, 2018.

[10] Y. Shi, Y. Wang, and L. Zhao, "An Event Recognition Method for U-OTDR Sensing System Based on Deep Learning," Sensors, vol. 19, no. 15, p. 3421, 2019.

[11] R. W. Bello and O. M. Moradeyo, "Monitoring cattle grazing behavior and intrusion using global positioning system and virtual fencing," Asian J. Math. Sci., 2019.

[12] Y. S. Ma, Y. Han, Y. F. Shao, and K. Li, "Design of anti-theft tomb system based on wireless sensor network," in Artificial Intelligence Science and Technology: Proceedings of the 2016 International Conference (AIST2016), pp. 400–409, 2017.

[13] X. V. Wang, L. Wang, A. Mohammed, et al., "Ubiquitous Manufacturing System Based on Cloud: A Robotics Application," Rob. Comput. Integr. Manuf., vol. 45, pp. 116–125, 2017.

[14] D. He, S. Chan, and M. Guizani, "Security in the Internet of Things Supported by Mobile Edge Computing," IEEE Commun. Mag., vol. 56, no. 8, pp. 56–61, 2018.

[15] S. Shahriar, I. Zualkernan, M. Pasquier, A. Towheed, and S. Sujith, "An AIoT-based smart café system," SSRN, 2023.

[16] R. Hajovsky, M. Pies, and J. Velicka, "Monitoring the Condition of the Protective Fence Above the Railway Track," IFAC PapersOnLine, vol. 52, no. 27, pp. 145–150, 2019.

[17] X. Yao, "The Realisation of Goal-Driven Airport Enclosures Intrusion Alarm System," Int. J. Grid Util. Comput., vol. 8, no. 1, pp. 1–6, 2017.

[18] C. M. Niebuhr, M. Van Dijk, and J. N. Bhagwan, "Development of a Design and Implementation Process for the Integration of Hydrokinetic Devices into Existing Infrastructure in South Africa," Water SA, vol. 45, no. 3, pp. 434-446, 2019.

[19] M. Antonakakis et al., "Understanding the Mirai Botnet," in Proc. of the USENIX Security Symposium, Vancouver, Canada, Aug. 2017.

[20] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations," in Proc. of the 6th Int. Workshop on Trustworthy Embedded Devices, Vienna, Austria, Oct. 2016, pp. 45–54.

[21] M. Guri, B. Zadov, and Y. Elovici, "LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED," in Proc. Int. Conf. on Detection of Intrusions and Malware, and Vulnerability Assessment, Bonn, Germany, Jul. 2017, pp. 161–184.

[22] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, "Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition," in Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security, 2016, pp. 1528–1540.

[23] X. Li, W. Xu, S. Wang, and X. Qu, "Are You Lying: Validating the Time-Location of Outdoor Images," in Applied Cryptography and Network Security, Springer, Berlin/Heidelberg, Germany, 2017, pp. 103–123.

[24] R. Garg, A. L. Varna, and M. Wu, "Seeing ENF: Natural Timestamp for Digital Video via Optical Sensing and Signal Processing," in Proc. of the 19th ACM Int. Conf. on Multimedia, 2017, pp. 23–32.

[25] K. Muhammad, J. Ahmad, I. Mehmood, S. Rho, and S. W. Baik, "Convolutional Neural Networks Based Fire Detection in Surveillance Videos," IEEE Access, vol. 6, pp. 18174–18183, 2018.

[26] G. Goswami, N. Ratha, A. Agarwal, R. Singh, and M. Vatsa, "Unravelling Robustness of Deep Learning Based Face Recognition Against Adversarial Attacks," in Proc. of the Thirty-Second AAAI Conf. on Artificial Intelligence (AAAI-18), New Orleans, LA, USA, Feb. 2018.

[27] B. I. Reddy and V. Srikanth, "Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3)," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., 2019.

[28] M. Rogers and G. Eden, "The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures," Int. J. Commun., vol. 11, pp. 802–823, 2017.

[29] L. Munn, "Machine Readable Race: Constructing Racial Information in the Third Reich," Open Inf. Sci., vol. 4, no. 1, pp. 143–155, 2020.

[30] A. T. Markettos, C. Rothwell, B. F. Gutstein, A. Pearce, P. G. Neumann, S. W. Moore, and R. N. M. Watson, "Thunderclap: Exploring Vulnerabilities in Operating System IOMMU Protection via DMA from Untrustworthy Peripherals," in Proc. of the Network and Distributed Systems Security Symposium (NDSS), 2019.

[31] M. M. Jaycox, "No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333," Harvard Natl. Secur. J., vol. 12, p. 58, 2021.

[32] B. Jacobs, "Maximator: European Signals Intelligence Cooperation, from a Dutch Perspective," Intell. Natl. Secur., vol. 35, no. 5, pp. 659–668, 2020.

[33] N. Kalbo et al., "The Security of IP-Based Video Surveillance Systems," Sensors, vol. 20, p. 4806, 2020.

[34] S. Ma et al., "A Retrieval Optimized Surveillance Video Storage System for Campus Application Scenarios," Hindawi J. Electr. Comput. Eng., vol. 2018, Art. no. 3839104.