PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2024)**, 2024, **pp**. 17–23
ISSN: 3078-3186

Research Article

Improving IP Video Surveillance Systems: The Shift to Digital Networks and Security Challenges

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 Nov 2023
Revised: 9 Jan 2023
Accepted 10 Feb 2024
Published 2 Mar 2024

Keywords
Video Surveillance,
IP-based Systems,
Internet Protocol,
Cybersecurity,
Bandwidth.

ABSTRACT

In the numerical era, video surveillance schemes have fast evolved from analog technologies to IP-based systems, enabling widespread deployment in various environments such as streets, train stations, workplaces, factories, and homes. The incorporation of intelligent applications like facial recognition, object tracking, and event detection has expanded the utility of surveillance networks, allowing for the management of thousands of cameras across large geographic areas. This change has been facilitated by advancements in Internet Protocol (IP) technology, shifting surveillance from analog systems using coaxial cables to packet-switching systems in IPv6 and IPv4 networks. However, the extensive adoption of IP-based systems has introduced several challenges, including increased vulnerability to cyber attacks, bandwidth demands, processing power requirements, and network security issues. This research discovers the evolution of video surveillance systems, the technical and security challenges posed by IP-based networks, and potential solutions for improving their efficiency and security.

1. INTRODUCTION

In current time, video surveillance system could be establish universally like street, train station, workplace, factory, and at home also [1]. Intellectual application make largest surveillances network applied to managing an utilized. As an examples, the technology for face recognitions, identify threat, event-detections, tracking object, and quickly investigate incident, could be scale to thousands of camera over largest geographical area. In the last decade, the surveillance technology have evolve from analog system to packet switching system within IPv6 and IPv4 networks [2]. The analogy system used camera transmitting analogy signal classically over a coaxial cable to a record unit [3]. The attack on this system is renunciation of services by cut wire, video injections via intercept the cables, and recorded interfering over physical interacted with the record units. The IP-based system have varied topology and technology to make them remote more complex and that result in much large attacks surfaces [4]. Additionally, this system is expose to the internet enable attacker to unceasingly attacks them nevertheless newest vulnerability is discover daily. Irrespective, IP-based videos surveillances system have becomes reasonable because of the common and universal Internet of Thing (IoT). The markets of security device in connecting home have developed by a factor of 17 over the last few year [5]. Because of their convinces, expediency, and affordability, videos surveillances system has become omnipresent in our time. Though, as expect, this system and their component have been the goal of many cyber attacking. This system has employed into botnet to performs nefariousness task. Early 2015, the infamousness mire botnets targeting surveillances system, and infection over 600,000 devices international [6].

Usually, the monitoring methods established in a large number of rooms by manpower while in existing time the surveillance systems could be set up by means of online networks [7]. The online monitoring of videos is less consumption of time and could reduce the manpower numbers with more elasticity to watch their property where they desire as long as they have internet networks. The properties and life security are an aspect of life which could not piddle with the individuals and governments desired to recognize the situations of their highly appreciated things each moment of being although the actuality that these things positioning in diverse places diagonally the worldwide [8]. The observation is to observe the behavior and activities normally of human for the purpose of influencing, protecting, and directing. The surveillance could provide the observation of groups or personality by government association while could also be related to illness monitoring which monitors the development of illness in the society as not in a straight line observed individually. The monitoring word might apply to observe as of are serve in terms of electric devices such as internet protocol (IP) camera or electrically transmission the data such as internet traffic and mobile phone call. Different kinds of monitoring techniques are available in the market such as telephone, biometric monitoring, computer monitoring, data mining human operative and social networks . The response and effectiveness of operators are widely depending on his vigilance rather than the technology

*Corresponding author email: sq.al.hashemi@gmail.com
DOI: https://doi.org/10.70470/SHIFRA/2024/003

ability of the monitoring systems [9]. The human activity and events can be overlooked, and the operators' attentiveness level can significantly drop after 10 minutes of idleness in their monitoring tasks. The high-resolution digital IP monitoring cameras are connected through the internet to a remote security surveillance point, enabling a new approach that focuses on identifying events within the camera's field of view. Security system installers face numerous challenges when integrating this type of online video surveillance, as it requires operation in difficult settings and the recording and streaming of footage from hundreds of cameras .The security landscape, both in video and physical fields, is experiencing a massive shift from analog to digital broadcasting over IP networks. [10]. The video in analog form coming from coaxial cable to dynamic voltage restorer (DVR) are digitized and compacted by programming algorithms. Hence, the IP based approach needs to solve many issues to meet the human demands under high security and reliability. High bandwidth capacity requires transmitting and received hundreds of video streams concurrently as proposed by [11]. The requirements of processing power to encode and decode multiples streams have been suggested by [12]. The digital signal processing (DSP) techniques could be used to design many video monitoring systems from low end-to-end to high end-to-end from portable to plug in implementations. For high resolution, the video monitoring system over the internet protocol architecture and on-chip. Any digitalize videotape monitoring scheme could be separated into 3 module such as video monitoring, network boundary, and vital monitoring room modules .The surveillance word may applying to observed as of a standby in term of electric device such as internet protocols (IP) cameras or electrical transmissions the information such as internet traffics and mobiles phones calling [13]. Many types of surveillance technique is obtainable in the markets such as telephones, biometrics monitor, computers monitor, data mining humans operatives and social network [14]. The reaction and efficiency of operator is wide depended on his vigilance instead of the technology's capabilities of the surveillance system [15]. The humans activities and event can happen overlook and the concentration stages of operator drop have attentiveness ranks drops significantly after 10 minute of idleness in monitoring tasks [16]. high-resolution digital IP monitoring camera attain to connecting over the internets and remote security surveillances points and enable newest approaches that draws attentions to event identify in the scenes of cameras [17].

The installer of security system faced numerous challenges to integrating these types of online videos surveillances that must be operating in difficult setting, records and stream of hundreds of camera [18]. The video security and physical field is suffering an massive moving as of analogy to digital broadcasting over IP network [19]. The videos in analogy forms coms from coax cables to dynamics voltage restorers (DVR) is digitize and compacting by program algorithm [20]. Therefore, the IP base approaches need to solved several issue to meet the humans demand under higher security and consistency. Higher bandwidths capability required transmit and receive hundreds of videos stream concurrently as proposed by many approaches. The requirement of process powers to encoding and decoding multiple stream have been suggested by their suggestions.

Digital signal processing technique use to designing several videos surveillance system from lower end-to-end to higher end-to-end from portables to plug in implementation. For higher resolutions, the video surveillance systems over the internet protocols construction and on-chips. Any digitalization videotapes surveillance schemes can be separate into 3 modules like video streams, network boundaries, and monitoring room module [21]. The advantage and disadvantage of technical challenge and researches open issue of IP base approaches with respecting to traditional method has been investigate and develop as illustrated figure 1 [22]. The virtual diagrams of videos monitoring which has successful design and employ in the realizations stage. The modules of videos capture is normal collecting of camera group and video cassette encoder parts. The videos capture from cameras are process and compress as raw information through video coded. Formerly, the modules of networks interfaces processing the videos coding streams and deliver to the IP sections. The modules of central rooms provide important surveillances every videos and controlling the camera reaction.

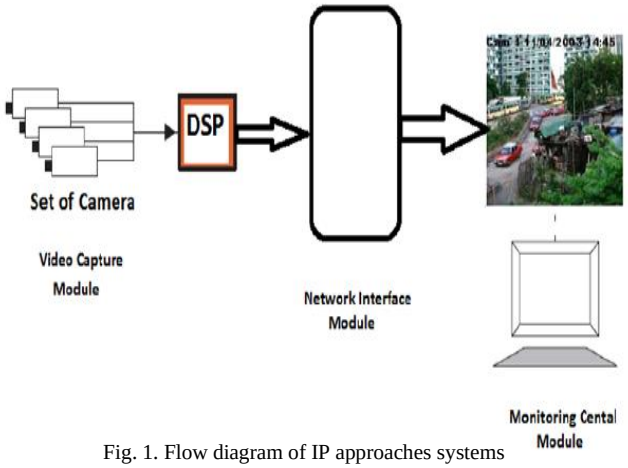

Fig. 1. Flow diagram of IP approaches systems

The system of video surveillance is common and widespread in several environment. The video surveillances become a key component in ensuring securities at airport, bank, casino, and correctional institution [23]. Lately, government agency, business, and school are turn toward videos surveillances as a mean to increased community security. With the propagation of inexpensive camera and the obtainability of higher-speed, broad-bands wireless network, deploy a larger number of cameras for security surveillances has becomes economical and technical possible [24].
Numerous important researches question continues to be address before relying on videos surveillances as an active tool for corruption preventions, crime resolutions, and crime protections [25]. Considerable of present researches in videos surveillance focus on algorithm to analysing videos and other media from multiples source to automatic detection important event [26]. As an examples application comprise interruption detections, activities surveillance, and ordinary calculating. The ability of extract moved object from a videos sequence is a fundamentals and vital problems of this vision system. In the system that use static camera, background subtractions is the technique typical use to segmentation moving region in the images sequence, by compare every frames to a models of the scene backgrounds [27].
In order to develop better understand of IP-based videos monitoring system, in figure 2 presents a taxonomy of their concept. Generally, the systems could be described in term of its purposes, implementations, topologies, and protections. The details of every of this aspect is create it, to start with a basics taxonomy that base on commonly knowledge and our experiences in cyber securities. Then, the changed of taxonomy based on inputs from monitoring systems engineer, security expert, and the papers, vulnerability disclosure, and report which be reviewing. The verifying of the information can be mapping to this taxonomy.

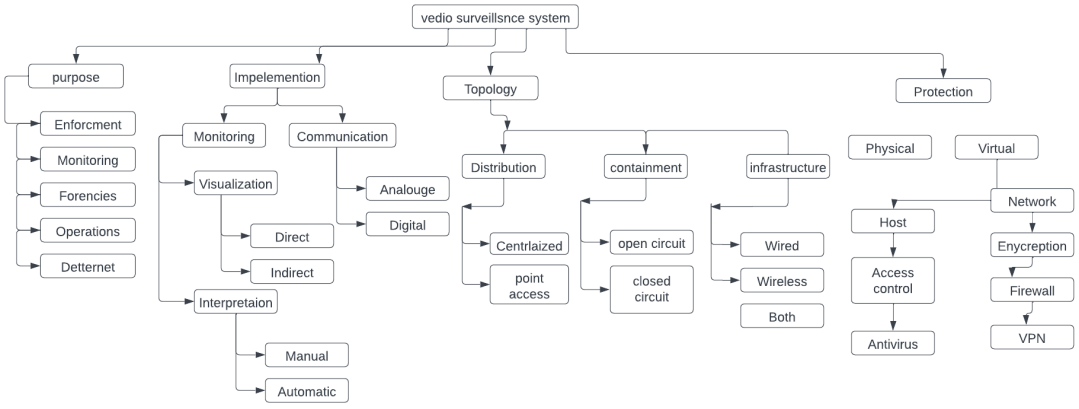

Fig. 2. video surveillance system overview

The upgrade of the smart cities, clever campus, and another project, the demand of video surveillance systems deployments is becomes further fine-grain and multi points. The progress tendencies of videos monitoring systems are move toward "digital, networks, highest-definitions, and intelligent [28]. The numbers of monitor device is increased the feature of videos is continual improved, and the durations time of the video retentions is extended.
This change increased the quantity of information produce through the video surveillance systems quickly. to effectively organized these mass monitor of videos data and to rapidly located the relevant videos in the post reifications is the important requirement of surveillances video storages systems. The growth of distributing file system and clouds store and a larger numbers of surveillance videos store system is base on the IP-SAN technology [29].
This technology ensured the systems scalability, loads balance, higher obtainability, information backup, and recoveries. Nevertheless this common storages technology design storage system focused on the writing effectiveness of storages. Preceding design disquiet the capability to write multiple videos information alongside as inquiry is lacks. Certain active videos association method is suggested with little considerations of the storage with larger amount of videos information. Though, the environments of video data surveillance has single applications characteristic.
The video data surveillance is a written-base data without spike or manger in the data generation. The monitor video data writing is successive. Data video is stream media information with larger file sizes; comparing to randomly write of smaller magnitude files, the speeds of videos information write is faster, due to there is not ample opening or closed operations.

2. BACKGROUNDS

This part described in details the component of a videos monitoring systems. Firstly, the analysis of video surveillance applications scenario. Hence, this part focused on the details systems component and description their characteristic. Lastly, an investigation of the unusual feature of IP- base videos surveillance and reviewing the enable of IP technology for support IP videos streaming.

2.1 The Applications of Video Surveillance

The main application of video surveillance system decrease under the physical securities protection. Each physicals securities systems has to verifying the main objective of limitation, detections, and verifications. Usually, the video surveillances systems is adoption as a verification tools to decrease false positive upcoming outs of the interruption detections and accessing controlling system. Usual scenario is workplace building, bank, museum, parks lot and industrial plant. In another situation, like municipality and highway, video surveillances is not employ in conjunctions with a detections systems nonetheless it is somewhat a stands-alone systems managing thru the locals securities or policy workers. In the definite context, the close circuits televisions (CCTVs) systems play the roles of a restriction, detections and verifications mean in the same times. Through the previous few year, because of the increase adoptions of intelligent videos analyzing software, video surveillances system is becoming inactive verification system to completed detections solution. The analysis of video is capable to detecting the situation under automatic analyze the video stream.

As an example of such application is missing luggage detections in airport or the queues realization on highway.

The governments organization and enterprise are increase the numbers of camera on their premise to providing 24-hour videos-streaming recorded that help manage securities and obligation threat at the same times.

Appreciations to widespread and universal videos surveillances, many organizations is currently talented to reducing insurance premiums and, therefore, achieved more competence in ability managements. In this instance, casino is capitalizing huge budget in video surveillances by install system with thousands camera per casinos. The CCTV system assistance casino to increased securities, reduced fraud and solved numerous responsibility issue involve with betting, therefore, importantly satisfying the investee budgets.

Another essential application for video surveillances involved monitor specific industrials processing. Though, this application typically required special type of cameras equipment which exhibition different technologic challenge with respects to those for largest scales physical securities. As examples, productions plan in the pharmaceutical industries employment higher frames rates camera and hyper spectral image to monitors and certifying their processing. Though, this special industry application is not the main focusing of this thesis. Consequently, in the followings, we will mostly refers to the physical security applications and their researches challenge.

2.2 Video surveillances system component

every IP - based CCTV systems could be divided into 5 mains component include:

1. Video Capture.
2. Video Encode.
3. Video Transmissions.
4. Video Monitoring and Managements.
5. Video Record.

The first component of video capture of any CCTVs systems are the cameras, who's essential is the charge-coupled devices (CCDs) sensors that convert the lights signal into electrical signal. Conventional analog CCD is nowadays very often replaced with digital signal processing base CCDs. Additionally, camera typically has analogy outputs and a bayonets Neill-Councilman (BNCs) connectors to coax cables.

The second component is the encoder as the common of camera installing nowadays have digital DSP-based CCD nonetheless it is till now analog BNC outputs, the separated encoder devices are required to stream video over an IP network. The video encoder is essentially analog-to-digital converter that encoding an analogy videos streams comes from a coax cable to a streams of IPs packet typically compress within MPEG-4 or M-JPEGs. Videos encoder typically has BNCs inputs and IEEEs 802.3 Ethernets inputs or outputs. To controlling the motorize pan-tilt-zoom camera, numerous encoders is prepared with a sequential output that reported a telemetry reading of the electric engines. Lately, the increased succession of IP camera, where videos capture and video encoded component are integrate into the same devices, has reduce the necessity for separated video-encoder.

The third component is video transmissions section. In the conventional video surveillances system, the video streams were conveyed toward the controlling rooms over analog transmissions on coax cable such as unshielded twisted pairs cable or multi-modes and single-modes fibres optics. Though, in the last period, middle to larger scales video surveillances system are migrate to supported IP-based networks, further lately, to wireless infrastructure appreciations to progressively lowers instalments and managements costs of IP network. For instance, the narrows middle of internets, a IPs protocols itself is helped the videos surveillances worlds in integrated diverse transmissions technology composed. Furthermore, packets switch network allow multi video stream to be convey on the same cables by share the obtainable transmissions capability and leverage the infrastructures cost with other information of video and voices flow the transmissions media such as Coppers, Fibbers, and wireless. In the construction of IP-network, mostly base on coppers and fibres as transmissions mediums. Equally, larger outdoors environment is typically cover by WAN. The WAN is generally provide through larger internet services suppliers through higher capability lease line or wireless technology. The foremost challenges in usage

lease-lines and WANs technologies for videos surveillances is because of the highest bandwidths required per videos streaming that intensely carry up the lease and operating cost.

The fourth component is the video monitor and managing part. The videos monitoring and managements systems are the users' interfaces that allow the operators to choice different video stream and watch the real times and recording videos. Videos monitor and managements system are frequently software-base and runs on generics workstations hardware. The final bottlenecks of large video surveillance systems are the process powers needed by the videos monitoring workstations to decoded the larger numbers of video stream acquire.

To provide the connectivity for many and varied application has constantly amongst the philosophical basis internets and IPs network in universal.

The IP networks are multipurpose in its natures. Therefore, it is conceivable to used exist off-the-shelf technologies for the need of our services, even they are rather specialize which mean instantiate the transports flow to carry video stream. Additionally, present networks structure deploy for information or Internet-relate application could comes in handy when videos flow generated from security camera needs to be transmitting across a buildings or even across an whole cities. Furthermore, appreciations to the presence of largest WAN and the internets, remote monitor of camera hundreds of mile away are allows without required every dedicate infrastructures. Lastly, by use IP flow is better of the points views of information retrievals and storages.

From construction viewpoint, the migrations of a videos security systems to IPs network mean that intellect and capability moved from the controlling rooms toward the camera. Comparing to a conventional analogy CCTV camera, IP cameras are more complex embed compute systems, where the optical, videos, encoder, and transmissions component are integrating. Up-to-date IP camera very often included also a Web-servers which allow the users to displayed the videos streams through the Web-browsers. Furthermore, numerous IP camera today implementing advanced artificial intelligence algorithms that make them controlled how and when to streams the videos.

The view and record process could be performs in a spread manners. Exactly, we could have many views station in many physical location, every of those with different data access privileges. In addition, every cameras could locally recording the video streams, in order to save bandwidths and to increase the consistency and resiliencies of complete securities systems.

Lastly, migration to IPs network allow to select the greatest suitable transmissions technologies for every video streams and visibly switch transmissions media along the paths that the video streams take to reached the controlling rooms. By this techniques, the IP protocols become also the commonly denominators along the paths of every videos stream.

On the other hand, it should be observe that the use of an all-IP structures, distribution the process capacity all over the networks, could leads to increase cost and susceptibility of the network. For concern the costs increasing, this is till clear compensate by the advance feature. Giving the increased concerns about physical security, it is sensible to assumed that this extra expenditure is tolerate as it go with improve services. Because of the weighty hardware requirement, numerous customs solutions at a hybrid hardware-plus-software levels is obtainable to reducing the issue relate to unsuitable or inadequate universal purposes hardware or software. The fourth component is a videos record that work very often in conjunctions with the videos managements systems and sometime runs even on the equivalent servers. The video recording components are typically refer to networks videos recorders and tend to generics servers and higher hard disks capability or connecting to storages array such as like storage areas networks or networks attach storage technology Typically, this recorder does not required very higher process capability because it does not decompressing the videos stream nonetheless it merely indexing the videos and recorded the videos on the networks storage systems. The fifth components is the video surveillances over IP. Depend on these details, the identifying the subsequent keys advantage of video stream over IP networks with respecting to conventional solution: control exist network and infrastructure a. distributed intelligence, record and view capability b. enhance the system flexibilities in expand networks with many transmissions mediums. Concern to occurs the increasing safety protections require via further costly IPs terminal again physicals damages and vandalisms. Since the points of views networks securities or vulnerabilities, the challenge is unlike in same times, other interesting and mostly involved the networks managements itself. These points are stronger for wirelesses network, and posture extra issue of developer together with certain designed guideline.

2.3. Video surveillances system Migrations and extensions to wireless network

A conception of utilize elastic wireless interconnection in a dynamics manner is no it elf newest. In 1990s, ad hoc network become widespread, appreciations to the diffusion of notebooks computer, open-sources software, and feasible communications equipment depend on radio frequencies and infrareds. The idea of ad hoc networks was establish for military applications, move to commerce civil scenario. In ten years, Wi-Fi network start to spreading, create a revolutions in internets services provision. By increase the approval and rises demands in additional Wi-Fi connection, implementations problem rosette. Indeed, Wi-Fi classically require extensively underwired infrastructures to accessing the backhauls networks, that costly to providing and relaxed to damaging, therefore violate the securities of data distribution.

The wireless mesh networks paradigm lately appeared as a valid alternative to wire connections, offered a relaxed and economic mean to provided broad bands wireless connectivity. The networks topology in advanced, which enable important

simplification in the managements of wireless communications mode. The distribution of centralize managements policies thus to avoiding inefficiency relate to distribution and random accessing. More guidelines will used is to limiting as much as possible multi hops relaying. These limitations are relevant for this studies, since it is reflecting in bandwidths limitation.

3. CONCLUSION

The change from analog to IP-based video surveillance schemes has revolutionized security monitoring across various sectors, enhancing capabilities for real-time surveillance, intelligent event detection, and system scalability. However, the change to IP-based technologies has also brought significant challenges, particularly in terms of network security, bandwidth, and processing power. The augmented exposure to the internet makes these systems vulnerable to cyberattacks, as demonstrated by incidents such as the Mirai botnet attack. Additionally, the essential for high bandwidth and computational power to handle multiple video streams simultaneously further complicates system implementation. Despite these challenges, the integration of IP-based technologies offers numerous advantages, including greater flexibility, scalability, and enhanced functionality. Moving onward, addressing security susceptibilities, optimizing bandwidth usage, and advancing processing capabilities will be essential in ensuring the continued development and reliability of IP-based video surveillance systems.

Funding:

The research was conducted without financial contributions from external funding bodies, foundations, or grants. The authors confirm that all research costs were covered independently.

Conflicts of Interest:

The authors declare no conflicts of interest in relation to this study.

Acknowledgment:

The authors acknowledge their institutions' substantial moral support and availability of research resources.

References

[1] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The security of IP-based video surveillance systems," Sensors, vol. 20, no. 17, p. 4806, 2020.
[2] Z. Ling, K. Liu, Y. Xu, Y. Jin, and X. Fu, "An end-to-end view of IoT security and privacy," in GLOBECOM 2017-2017 IEEE Global Communications Conference, 2017, pp. 1–7.
[3] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.
[4] N. Akhtar and A. Mian, "Threat of adversarial attacks on deep learning in computer vision: A survey," IEEE Access, vol. 6, pp. 14410–14430, 2018.
[5] M. Guri and Y. Elovici, "Bridgeware: The air-gap malware," Communications of the ACM, vol. 61, pp. 74–82, 2018.
[6] E. Bertino and N. Islam, "Botnets and internet of things security," Computer, vol. 50, pp. 76–79, 2017.
[7] R. Schuster, V. Shmatikov, and E. Tromer, "Beauty and the burst: Remote identification of encrypted video streams," in USENIX Security Symposium, 2017.
[8] Y. Wang, T. Bao, C. Ding, and M. Zhu, "Face recognition in real-world surveillance videos with deep learning method," in 2017 2nd International Conference on Image, Vision and Computing (ICIVC), 2017, pp. 239–243.
[9] T. Li, H. Chang, M. Wang, B. Ni, R. Hong, and S. Yan, "Crowded scene analysis: A survey," IEEE Trans. on Circuits and Systems for Video Technology, vol. 25, pp. 367–386, 2014.
[10] P. V. Paul, S. Yogaraj, H. B. Ram, and A. M. Irshath, "Automated video object recognition system," in 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017, pp. 1–5.
[11] J. Chung and K. Sohn, "Image-based learning to measure traffic density using a deep convolutional neural network," IEEE Trans. on Intelligent Transportation Systems, vol. 19, pp. 1670–1675, 2017.
[12] Y. Mirsky and W. Lee, "The creation and detection of deepfakes: A survey," arXiv preprint arXiv:2004.11138, 2021.
[13] J. Valente, K. Koneru, and A. Cardenas, "Privacy and security in Internet-connected cameras," in 2019 IEEE International Congress on Internet of Things (ICIOT), 2019, pp. 173–180.
[14] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, pp. 80–84, 2017.
[15] M. Guri and D. Bykhovsky, "aIR-Jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR)," Computers & Security, vol. 82, pp. 15–29, 2019.
[16] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in Network and Distributed System Security Symposium (NDSS), 2018, vol. 5, no. 2.
[17] Y. Meidan et al., "N-BaIoT—network-based detection of IoT botnet attacks using deep autoencoders," IEEE Pervasive Computing, vol. 17, pp. 12–22, 2018.

[18] O. Mayer, B. Hosler, and M. C. Stamm, "Open set video camera model verification," in ICASSP 2020 - IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2020, pp. 2962–2966.
[19] P. W. Khan, Y. C. Byun, and N. Park, "A data verification system for CCTV surveillance cameras using blockchain technology in smart cities," Electronics, vol. 9, no. 3, p. 484, 2020.
[20] R. López-Valcarce and D. Romero, "Defending surveillance sensor networks against data-injection attacks via trusted nodes," in 2017 25th European Signal Processing Conference (EUSIPCO), 2017, pp. 380–384.
[21] N. Pitropakis, E. Panaousis, T. Giannetsos, E. Anastasiadis, and G. Loukas, "A taxonomy and survey of attacks against machine learning," Computer Science Review, vol. 34, p. 100199, 2019.
[22] W. Liu, M. Salzmann, and P. Fua, "Using depth for pixel-wise detection of adversarial attacks in crowd counting," arXiv preprint arXiv:1911.11484, 2019.
[23] C. Xiao et al., "Advit: Adversarial frames identifier based on temporal consistency in videos," in Proc. of the IEEE International Conference on Computer Vision, 2019, pp. 3968–3977.
[24] A. Castillo, S. Tabik, F. Pérez, R. Olmos, and F. Herrera, "Brightness guided preprocessing for automatic cold-steel weapon detection in surveillance videos with deep learning," Neurocomputing, vol. 330, pp. 151–161, 2019.
[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] C. Ding and D. Tao, "Trunk-branch ensemble convolutional neural networks for video-based face recognition," IEEE Trans. on Pattern Analysis and Machine Intelligence, 2017.
[27] A. Tambe, Y. L. Aung, R. Sridharan, M. Ochoa, N. O. Tippenhauer, A. Shabtai, and Y. Elovici, "Detection of threats to IoT devices using scalable VPN-forwarded honeypots," 2019.
[28] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici, "Game of drones-detecting streamed POI from encrypted FPV channel," arXiv preprint arXiv:1801.03074, 2018.
[29] E. Anthi, L. Williams, P. Burnap, and K. Jones, "A three-tiered intrusion detection system for industrial control systems," Journal of Cybersecurity, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyab006.