applied sciences

MDPI

Review

Attacks and Preventive Measures on Video Surveillance Systems: A Review

Preethi Vennam [1], Pramod T. C. [2], Thippeswamy B. M. [3], Yong-Guk Kim [4,*] and Pavan Kumar B. N. [4,*]

[1] Department of Computer Science & Engineering, Dayananda Sagar University, Bengaluru 560078, India; preethivennam@gmail.com
[2] Department of Computer Science & Engineering, Siddaganga Institute of Technology, Tumakuru 572103, India; tcpramodhere@gmail.com
[3] Department of Computer Science & Engineering, Adama Science & Technology University, Adama 1888, Ethiopia; thippeswamy.b@astu.edu.et
[4] Department of Computer Engineering, Sejong University, Seoul 05000, Korea
* Correspondence: ykim@sejong.ac.kr (Y.-G.K.); pavanbn8@gmail.com (P.K.B.N.)

Abstract: Video surveillance systems are widely deployed with large systems for use in strategic places such as home security, public transportation, banks, ATM centers, city centers, airports, and public roads, and play a vital role in protecting critical infrastructures. As various attacks are possible in these systems, identifying attacks and considering suitable security measures are essential. In this paper, we present a detailed review of existing and possible threats in video surveillance, CCTV, and IP-camera systems. This provides insight for the better identification of the security risks associated with the design and deployment of these systems and promotes further research in this emerging field. We also present countermeasures to prevent and protect the surveillance systems from various security attacks.

Keywords: video surveillance system (VSS); closed-circuit television cameras (CCTV); Internet of Things (IoT); security attacks

Citation: Vennam, P.; T. C., P.; B. M., T.; Kim, Y.-G.; B. N., P.K. Attacks and Preventive Measures on Video Surveillance Systems: A Review. *Appl. Sci.* **2021**, *11*, 5571. https://doi.org/10.3390/app11125571

Academic Editors: Juan Francisco De Paz Santana and Gianluigi Ferrari

Received: 10 February 2021
Accepted: 10 June 2021
Published: 16 June 2021

1. Introduction

Surveillance systems have become more and more popular in recent times. Government and private organizations, residential societies, and commercial and public spaces, are using these systems to keep a check on various activities for security and safety purposes. In French, the word "sur" means "from above" and "veiller" means "to watch". Surveillance means monitoring movements, activities and behavior in order to manage, control, and protect people. Surveillance systems have the advantage of remote and continuous monitoring. To view events as they occur and to monitor activities in any area at a later time, closed-circuit television systems (CCTV) technology is being used. Increasing thefts and criminal activities demand the usage of CCTV cameras in both commercial and residential sectors for security purposes. CCTV cameras are available in different forms: non-IP (Internet Protocol), IP CCTV cameras and wireless CCTV cameras. Due to the features of technology, flexibility, ease of use, and affordability, the usage of IP-based wireless CCTV cameras is becoming a trend in the present scenario. As it is being used in many applications all over the world, the market for CCTV is widely expanding. Figure 1 shows the forecast of the wired and wireless cameras market in the coming years. The size of the security camera market was valued at USD 3.71 billion in 2019 and is expected to grow at a compound annual growth rate (CAGR) of 15.7% from 2020 to 2027 [1].

The virtue of IoT is that it gives new look for the upcoming video surveillance systems. Instead of capturing footage and visualizing it later in order to detect theft, violence or vandalism, there is a need for cameras to self-detect the abnormal events and interpret the same to other systems for necessary actions. To cater to this, cameras are becoming

smart, with the integration of the latest technologies. The smart cameras have exploited the benefits of computer vision, machine learning and automation. IoT helps to connect network-enabled cameras with other devices and systems and thus transforms secure surveillance into smart security surveillance systems.

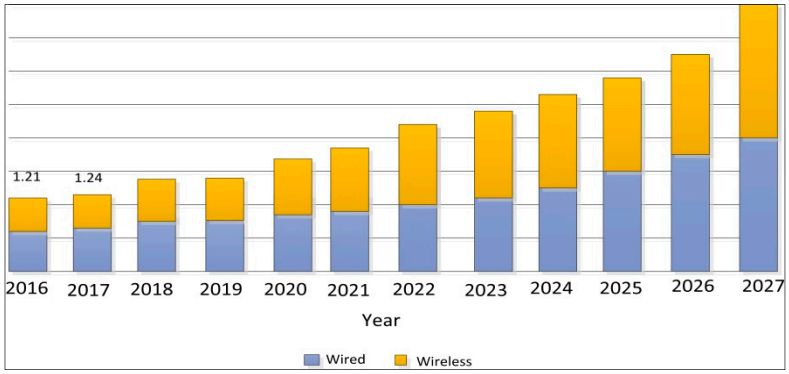

Figure 1. Security camera market size.

Overview of VSS: Video surveillance systems are widely used in cyber-systems such as healthcare, traffic analysis, wildlife monitoring, environmental monitoring, weather forecasting and public safety. In VSS, security cameras are available in a wide range of styles and features. A wireless VSS source node consists of cameras, a transceiver, storage unit, microprocessor and power supply. Each node performs video compression, data transmission and video capturing as the basic function. The data processing unit and data transmission unit at each wireless node process a large amount of video data without degrading information and security, which is a most challenging task in video surveillance applications [2]. The general architecture of a functional VSS is illustrated in Figure 2.

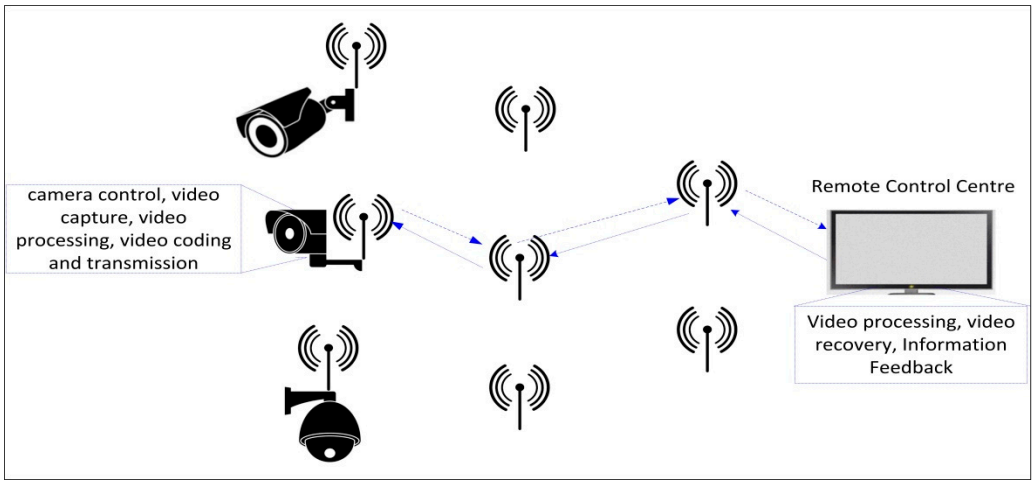

Figure 2. Overview of video surveillance system.

Motivation and Our Contribution

The usage of VSS is ubiquitous in today's scenario. As these systems are more beneficial and available at affordable cost, they are widely utilized to protect the public and private network systems. Attackers are continuously targeting these systems with new attacks and vulnerabilities. When we use an internet-connected camera from a computer or smartphone, there is a chance that someone else can access it. That person can be a "hacker" or an application to which we may have knowingly or unknowingly given access permission. For example, when a simple search word such as "webcamXP" is given on Shodan.io [3], an IoT search engine, one can access random video footage of retail stores,

city centers, boating docks, and domestic spaces. The large scale, restricted resources, outdated firmware, poorly secured IoT devices and inbuilt vulnerabilities have attracted bad actors to perform various attacks on the IoT ecosystem. Table 1 shows examples of real-time attacks that occurred on VSS.

Table 1. Attack incidents and vulnerabilities on VSS.

Attack and Vulnerability Events	Year	Place/Device Manufacturer	Remarks
DDoS attack—Mirai [4]	September, 2016	French web host OVH	It was the largest DDoS attack ever recorded at over 600 Gbps in size targeting IoT devices, including routers, IP cameras and digital video recorders.
Ransomware [5]	January, 2017	USA	The ransomware attack affected 123 of 187 network video recorders in a closed-circuit TV system for public spaces across Washington, D.C.
Privacy hack and defacing [6]	May, 2018	Yachiyo and Ageo, Japan	Hackers disabled more than 60 Canon security cameras officially.
DoS attack [7]	December, 2018	Bosch IP cameras (firmware versions: 6.32 and higher)	It is classified as "buffer overflow" vulnerability, situated in the RCP and parser of the web server. This would enable an attacker to reactivate disabled features (e.g., telnet) or bypass access credentials (username/password).
Command injection [8]	October, 2018	Yi Technology, a renowned Chinese organization closely connected with Xiaomi	Issues streamed from a data exposure vulnerability which existed in the mobile-to-camera communications of Yi Home Camera.
Brute-force attack [9]	March, 2018	South Korean firm Hanwha Techwin	Kapersky recognized almost 2000 vulnerable cameras that were accessible by means of open IP addresses on the internet.
Privilege escalation attacks [10]	March, 2018	Hanwha SmartCam	Due to a fault in the design, an interloper could obtain entrance through the cloud to all cameras and control them. The primary issue for this is the cloud architecture depended on the XMPP communications protocol.
Command and control attack [11]	June, 2018	Foscam security cameras	The attacker utilized stack-based buffer overflow vulnerability to crash the webService procedure and gain administrative access.
Command and control attack [12]	July, 2019	Delhi, India	Remote hacking and backdoor access to CCTV cameras.
Privacy attack—ransomware [13]	March, 2021	USA	150,000 security cameras at banks, jails, schools, carmaker Tesla, and other sites were hacked to expose "the surveillance state".

The reasons for above-mentioned attacks may be due to the usage of default login credentials, no access privileges and poor security and privacy features. The motivation for an attacker could be blackmailing, the ability to observe live video feed, access to video footage, access to VSS network, disabling video feeds, violating privacy, remotely disabling the connection, and performing DoS attacks, etc. As VSSs are used in important places, only authorized agents should have the access to monitor and control it. Privacy and security are the foremost concerns while using such systems. Considering all this, this paper first identifies the possible attacks on such systems and then discusses the measures that can be incorporated to prevent security attacks. Additionally, a comparison is carried out on existing VSS frameworks along with their advantages and disadvantages.

After the launch of the Mirai attack and its consequences in the year 2016, there has been a dramatic increase in studies related to attacks and vulnerabilities in the VSS domain. The articles have discussed the loopholes and flaws in the IoT networks. For our review, we have considered the peer-reviewed articles from the year 2016 to 2021. Keywords used for the literature survey are as follows: video surveillance systems, attacks on VSS, security frameworks for VSS, privacy issues with IP camera and botnet. To understand the security loopholes and possible solutions to mitigate the threats in VSS, this paper follows the following steps (Figure 3) to articulate the security issues of VSS.

Figure 3. Roadmap of the paper.

The rest of the paper is organized as follows: various types of attacks in VSS are given in Section 2. The security measures for VSS are summarized in Section 3. In Section 4, a detailed review and analysis of the latest advances in VSS frameworks are presented and tabulated. Concluding remarks are made in Section 5.

2. Attacks on VSS

In this section, we present all the possible types of active attacks at different layers of the video surveillance systems. The main issues are (a) privacy and security that concerns a surveillance system, (b) the uncertainty of not knowing what happens to your data when it is stored in the cloud and (c) how the user monitoring devices such as smartphones can also be a cause of the attack in the surveillance network [14–23].

In an attack scenario, the basic steps are: (a) information gathering, (b) assessing vulnerability, (c) launching attack, and (d) cleaning up. Some of the tools used by attackers at different steps are listed in Figure 4. Hoque et al. [24] present more elaborate details of information gathering and attack launching tools that can be used by attackers. M.Rytel et al. [25] presents details of different vulnerability databases available, attack surfaces and their details.

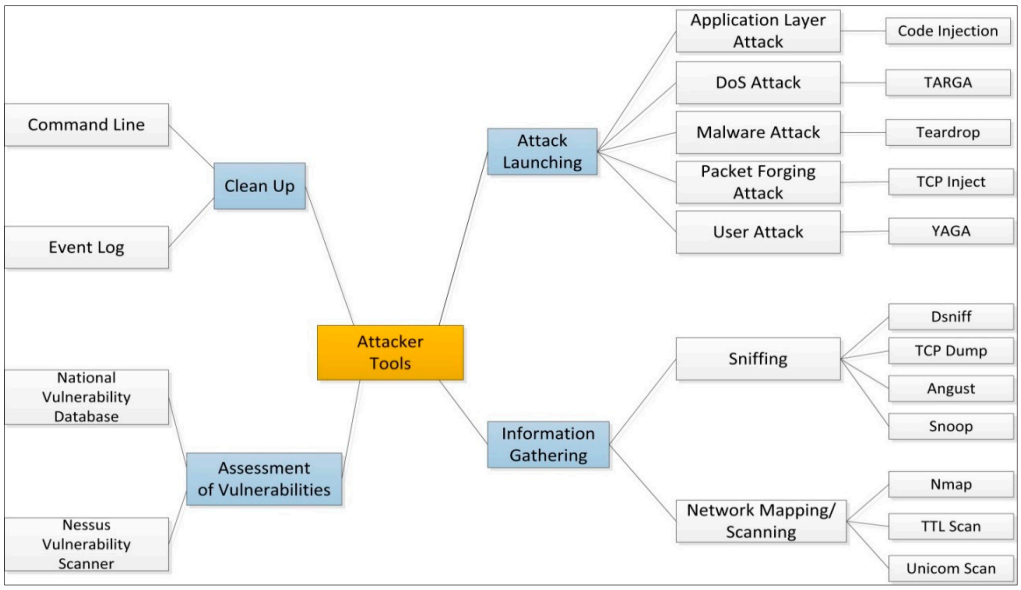

Figure 4. Common tools used by attackers.

2.1. Visual Layer Attacks

VSSs are used by applications for the recognition of facial features, the automatic reading of license plates, scanning and reading QR codes and the compression of image data. VSS has an additional level of abstraction, i.e., the visual layer. This layer is prone to a few types of attacks as they involve imagery semantics and image recognition. The attacks are spread/injected in a multitude of ways, such as preinstalled malware in the system or through a firmware update or remote command insertion [26].

Malicious images can be embedded into the images taken by video cameras/sensors [27]. One of the most common attacks on a live feed from VSS is frame duplication attack. An attacker, once gaining access to a VSS system, can insert previously recorded "normal" looking frames in place of the live stream, to avoid the detection of ongoing suspicious activity. To detect these frame duplication attacks, spatial and temporal domain similarities between frames are extracted and analyzed using various correlation techniques. To achieve this, a massive database is required for storing a huge amount of data and an enormous amount of computation time is required to detect and prevent such attacks in real time.

2.2. Covert Channel Attacks

In this type of attack, informational objects between processes can communicate which normally should be blocked as per the security policy. These attacks are different from legitimate channel exploitations which attack semi-secured systems using techniques such as steganography, to disguise prohibited objects inside actual informational objects. Attackers can communicate with malware embedded inside a system using this type of attack. Based on criteria such as timing/storage, network/OS/hardware, and value/transition based, covert attacks can be classified into various types. Some examples of covert channel attacks [28,29] are:

- Manipulating CCTV/VSS infrared LEDs: by sending command/control data to the VSS cameras by using the infrared LED messages;
- A new type of optical covert channel named (VisisSploit) leaks data through a computer LCD display;
- Network-based covert channels can be created to coordinate distributed denial of service attacks, bypassing the user firewall. For example, the IPv4 header TTL field can be used to carry information into or out of a network domain.

2.3. Steganography Attacks

Steganography involves a method to use the unused or less important information bits of the user content (such as images, videos, network traffic). Two types of common steganography attacks are hiding the malicious code in the genuine application and by a command and control (C & C) communications channel [30,31].

A common technique in many malware droppers is to append data to the end of the file or utilize unused portions of the file format [32]. In any method of steganography, it is hard to detect malicious code coming through user files in a network. Malicious payloads can be embedded into a set of PNG files. The PNG files can then be compiled into a legitimate application, along with a function that would extract and drop the malware onto the system.

In command and control protocol attacks, the "Domain Name Server (DNS) and Hyper Text Transfer Protocol (HTTP)", can be used to embed the malicious code in response to a request from a client.

As an example, we consider User A (house or office owner) who approaches the IP camera. After it detects User A's face successfully, it stores the image and captures another image without a face (named a cover image). The steganography technique is now used to send a "stego image" (combined image where the actual image is hidden in the cover image). This "stego image" is stored in the home server, which then will be processed using the reverse steganography technique to retrieve the original image with the face.

Another User B (attacker) intercepts data transmission between the IP camera and the home server and captures all the data which have "stego image" along with other captured images. At this point, the attacker can perform three categories of attack; namely, stego-only attack, known cover attack and known message attack. Any image can be represented with a pixel value (a bunch of ones and zeroes). The cover image will also have a string of bits, but their sequence of bits will be different on the LSB or the MSB side when compared to the corresponding face image. Any change on the LSB bits of the face image will not alter it significantly, whereas changes in the MSB bits will significantly degrade the quality of the face image. An attacker can use statistical analysis for the detection of changes in LSB bits or human visual perception to detect the changes in the MSB bits to detect the face image from the cover image. User B can then use this decrypted face image to attack the home security system and gain access to the home or office.

2.4. Pan–Tilt–Zoom Attacks

Pan–Tilt–Zoom (PTZ) is a functional characteristic of a surveillance camera that can zoom in and out, and change the view of the camera to horizontal (right, left) and vertical (up, down) angles. Camera models utilize stepper motors built into them and employ PTZ data protocols to achieve this functionality. The PTZ data protocols use RS-422 or RS-485 links, as well as Ethernet and Wi-Fi channels. PTZ-capable cameras can be controlled by keyboard shortcuts or with a specially designed joystick using PTZ commands. A compromised PTZ camera can send data to the external attacker along with the PTZ coordinates [33]. When a user is using a mobile application to watch a live feed from the camera through a cloud server, then all the PTZ requests are routed through cloud servers to the camera. If this communication is carried out after an interval of every few seconds, an attacker who is intercepting this communication may not be able to decode the PTZ data but can precisely find the interval after which communication is happening. The attacker can then launch an attack that matches with the communication interval, thus avoiding detection [34].

2.5. Denial of Service and Jamming Attacks

Any action or series of actions that prevent any part of an information system from functioning is known as denial of service by jamming the communication network [35]. When monitoring important activities such as real time crimes, in many video surveillance systems, it is critically important to have an un-tampered and uninterrupted operation. DoS and jamming attacks with a very short duration of less than a few minutes can still make a VSS camera miss a fast-paced crime such as a bank robbery. A denial-of-service attack on a home surveillance camera will not have a major impact when compared to denial-of-service attacks on commercial surveillance systems, which may have a greater impact. These kinds of attacks must be taken into consideration during the early phases of the setup and testing of the surveillance system. For example, "BrickerBot is a malware that attacks IoT devices that run a specific version of the DropBear SSH server and target Linux devices running Busy box (usually IP cameras)".

DoS attacks can be classified into two types: flooding and logic attacks. Flooding attacks work by overwhelming the current network with a large volume of complex data packets to deplete their resources such as memory and bandwidth. Logic attacks exploit the known vulnerabilities in the system to attack the remote servers. Out of these two types of attacks, flooding attacks are more dangerous as it is difficult (resource-intensive, time-intensive and cost-intensive) to differentiate real data packets from the flooded data.

2.6. Malware Attack

Malware comes in different forms and types such as viruses, Trojans, ransomware and spyware. In a smartphone, users download mobile applications, and malicious code embedded into the application program can gain access to personal information which the attackers can then exploit for financial gain [36]. The Mirai malware that occurred in

2016 takes advantage of the IP addresses of the devices that are vulnerable in the Internet of Things (IoT), and then turns these devices into bots that can be used as part of botnets for large-scale network attacks. Another malware, BrickerBot, like Mirai malware, infects its target and gains access to the device and destroys it—"bricks it", i.e., the device is longer operable. In a surveillance network, no one wants to wake up and realize that their surveillance camera no longer works because it was intentionally destroyed by someone trying to "protect" it. Nor does anyone want a picture or video of their device or application storage that went viral on social media due to their camera (which can be a surveillance camera or smartphone camera) being hacked. There are significant security threats with a malware attack which enables an attacker to execute any command on a target machine or within a target process. Due to this, the attacker can have a different way to invade by performing malicious code injection, data leaks and also performing privilege escalation. Access control entry vulnerabilities have been discovered on IP cameras, DVRs, and VPN routers which are publicly listed in https://cve.mitre.org. Here, CVE stands for Common Vulnerability Exposure. (For example: CVE-2021-1131, CVE-2020-7848, CVE-2020-11624, CVE-2018-6414, CVE-2018-9156).

2.7. Privilege Escalation Attack

In a multiple user architecture of any application or device network, access permissions to its users are restricted. Users at different levels have different permissions. In Android user applications or surveillance applications, components such as service, content provider, broadcast receiver and activity may be able to use privilege escalation to receive more permissions than required or desired. Two variants of privilege escalation are Vertical Privilege Escalation and Horizontal Privilege Escalation.

Vertical Privilege Escalation: bugs and design flaws can be applied to allow the smartphone user to execute higher level applications or functions. Even a process, for instance, may use a bug in the system kernel and run functions with system privileges. There must be at least one process running with system rights to enable another lower-level process to escalate.

Horizontal Privilege Escalation: the user and applications are located at the same permission level. Privilege escalation takes place if a user or an application can access data or functions of another user or application.

One of the Android built-in security features is the Android application sandbox. It is a technique to manage and separate the user applications from the critical system resources and applications. Privilege escalation attack bypasses sandbox restriction by running malicious code at run time [37]. An application which is "non-privileged" can still access files of "privileged" system applications such as geo-location, user passcode, battery status, camera permission, etc.

Similarly, in a video surveillance system, an attacker can exploit the firmware default port and login information and access the device as a user with privileged rights [38]. In such a scenario, companies could do nothing but recommend their customers apply newer firmware and use stronger passwords.

The prevalent attacks on different parts of the VSS infrastructure are outlined in Figure 5. Table 2 gives information on different types of attacks, their description and examples of how such attacks are conducted by the attackers.

Table 2. VSS architecture layers, attacks and their examples.

Layer	Attacks	Threats	Description	Examples
Perception Layer	Device attack	Physical Attacks, impersonation, malicious code injection	Someone takes advantage of a bug or inherent vulnerability to gain access to the infrastructure.	Physical access to a security surveillance camera and modifying the design settings.
	IoT botnet	DoS attacks, routing attacks	Group of hacked computers, smart devices, and appliances connected to the Internet are known as an IoT botnet.	The Mirai malware is seen as a milestone in the threat landscape and exploits security holes in IoT devices and launches attacks.
Network Layer	Attacks on Wifi/Ethernet	Routing attacks, data transit attacks	Numerous malicious activities can be performed on devices if an attacker gains physical access to the local network wirelessly.	In the network level attacks, cybercriminals are able to redirect network traffic; for example, Address Resolution Protocol poisoning (ARP) or by changing the Domain Name System (DNS) settings.
	Reconnaissance	DoS attacks, routing attacks	The aim is to collect data about an infrastructure, including the network services and devices that are running.	This can be achieved by scanning network ports and packet sniffers.
	Man-in-the-middle attack	Data transit attacks	It is a type of eavesdropping attack. This attack could permit the attacker to secretly relay and possibly alter the communications between two IoT devices.	Attackers can use a network packet analyzer, i.e., Wireshark for analyzing network traffic. If communications are not encrypted or authenticated, an attacker can easily steal the data.
Application Layer	Cloud infrastructure	Data leakage, DoS attacks, malicious code injection	An IoT device interconnects with back-end cloud services. IoT cloud services might permit the client to select simple passwords.	A lot of cloud services have a logical weakness, which is actually the permission of cloud to a cybercriminal to obtain sensitive information of the customer and also access to the device without any authentication.
	Privilege escalation	Data leakage, malicious code injection	The attacker takes advantage of programming errors or software flaws to permit cybercriminals to elevate access to an IoT infrastructure.	Grant the cybercriminal elevated access to the IoT ecosystem and its associated data and applications.
	Server-side denial of service (DoS)	DoS attacks, Malicious Code Injection	Electronic devices and its connected devices are deactivated or changed by a cybercriminal, via physical or remote access to the IoT sensors.	An attacker can deny the sensors to send and receive communications. Another example could be battery abuse, device disabling, or device bricking.

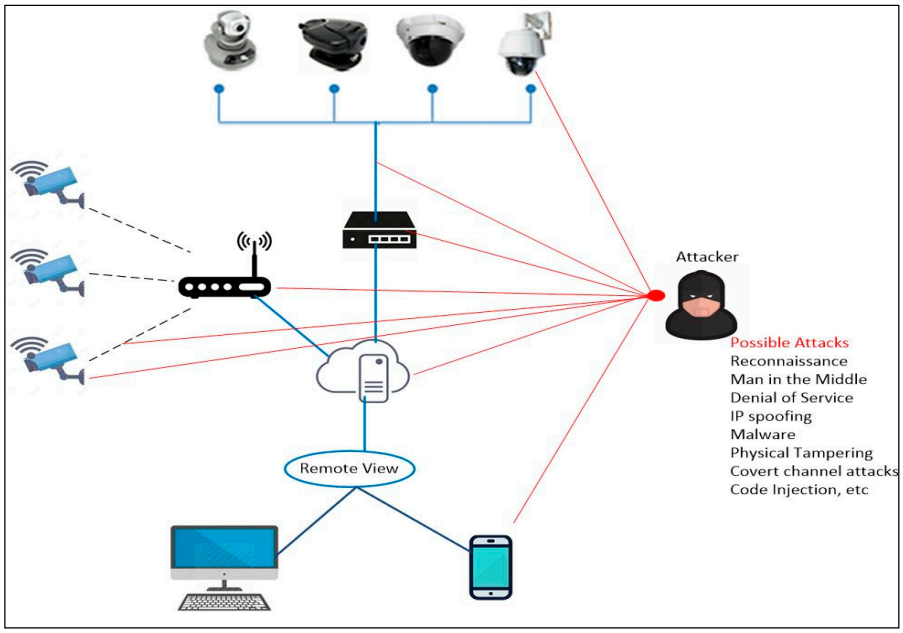

Figure 5. Pervasive attacks on VSS.

3. Security Measures for VSS

The security of the hardware, firmware and network communications of video surveillance systems can be enhanced by following the guidelines summarized in this section. Preventing attacks against connected devices requires effort from both the industry and users. Vendors must adopt good practices for built-in security measures, such as secure remote access, basic encryption, and patching all known vulnerabilities [39–47]. Without proper safeguarding, IP-connected cameras are vulnerable to hacking, which can lead to the compromise of millions of security cameras and video recorders. The security mechanisms that can be used to prevent different types of attacks is tabulated in Table 3. To protect from security attacks, the security measures that are suitable at different layers (perception layer, network layer and application layer) are summarized in Figure 6.

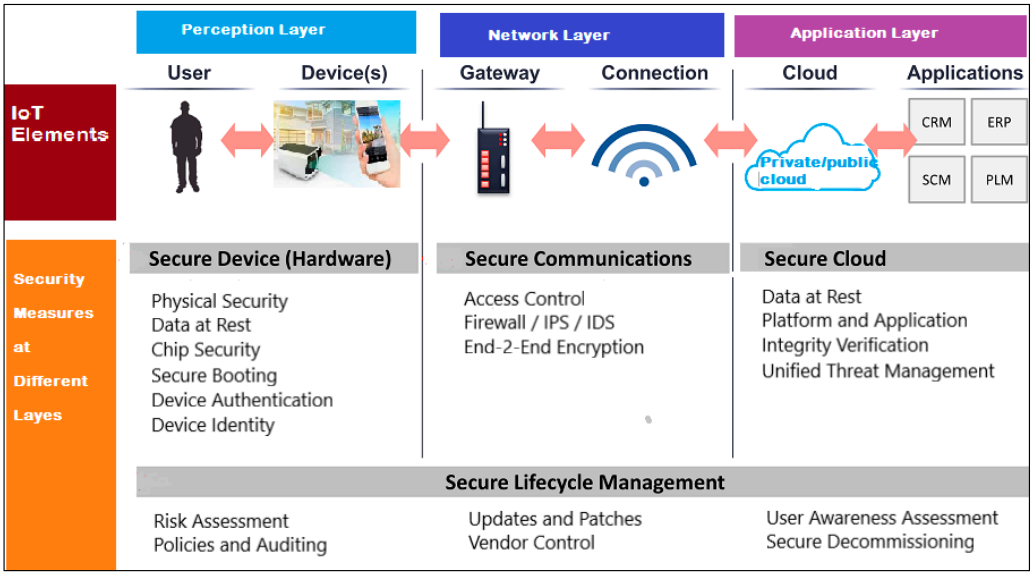

Figure 6. Summarizing the security measures at different layers.

Table 3. Summary of security mechanisms.

Type of Attacks	Mechanisms that Help to Prevent Attacks	Description
Spyware and malware	Anti-virus solution	Commercially available anti-virus solutions can scan system and cache files, messages and emails as well as website URLs. They can also prevent spyware and malware by preventing access to a suspected phishing website.
IP spoofing	Firewall	Firewall stops unauthorized inward or outward connections. It can prevent various types of network attacks by blocking unauthenticated wireless networks.
Man-in-the-middle, visual layer attacks.	Secure API	Cryptography-based API can provide various secure functionalities to the application developer.
Malware, DoS, covert channel attacks.	Access control	Access control not only limits the access of processes but also limits the user to resources and/or services, thus limiting risk from malicious applications.
Covert channel attacks, DoS, spyware, cross-site scripting attack.	Authentication	The user can login to a device only after being authenticated to prevent its unauthorized use.
Covert channel attack, spyware.	Spam filter	Spam filtering applications block unwanted calls, messages and emails. They can also prevent spam from reaching to the user's inbox.
Covert channel attacks, malware attacks, privilege escalation attack.	Pre-testing	Pre-testing can ensure application security by preventing malware. It can also validate applications and give proper access authority to application developers.
All types of attacks.	Regular update	Smartphone applications can prevent various types of attacks by regularly updating from various manufacturer-provided platforms.

The basic and necessary steps to avoid video surveillance camera attacks are as follows:

1. Installation and regular updating of the anti-virus application is the foremost step to defend against malicious attacks.
2. Network topology and configuration of a system is critical in maintaining the security of IP-based cameras, as there are multiple entry gateways through which it can be attacked. Configuration access is the key to provide security to the system. A local network system with a firewall and virtual private network (VPN) software for remote access is always safe. A secure, encrypted connection is a barrier for any attackers before they can go through a firewall. An alternative solution could be to use a cloud-connected IP security camera. In this type of locally connected system, rather than relying on a password to gain access to the firewall of a camera system, cloud-connected IP security cameras will communicate with a secured cloud-based server over an encrypted connection. Users can gain access by linking up their devices with those servers. Cloud-connected devices have the added advantage of continuous monitoring over locally connected systems.
3. Using a unique, lengthy and unpredictable password for each camera is a good starting point. This is especially critical for a port forwarding system. However, if a system employs VPN, having a single secured password for all connected cameras is enough. As a rule, changing passwords every 90 days is recommended.
4. Priority should be given to provide cybersecurity training to all employees who may have access to a central video surveillance system and all personnel must be made aware of cyber security guidelines.
5. In case of security breaches, a cybersecurity incident response team can be constituted to respond to such emergencies.

6. All latest software/firmware updates must be promptly applied as and when they are released by the manufacturers.
7. If a cloud-based system is deployed, only authentic verified vendors should be chosen.
8. One must be aware of all the latest cyber security standards being adopted as well as study all recent attacks to gain a better understanding of new techniques employed by attackers.

4. Review and Analysis of Existing VSS Frameworks

Yalon, the director of security research at Checkmarx [48] has explained a critical Android vulnerability CVE-2019-2234: the attacker can access the camera peripheral of popular smartphone devices such as Samsung and Google. The attacker can exploit this vulnerability and can access the victim's location, take photos of them and their surroundings, and record audio and video without the user's knowledge or consent. Additionally, the attacker can access the memory of the phone even when it is locked, the mobile screen is turned off or when the user is using another app such as call or browsing.

Subramanian et al. [49] demonstrate the two methods to hack into a camera application and take photos of the users without their consent. These malicious applications use background services and are able to capture the images and store them temporarily on the device using standard compression techniques.

Sanjana Prasad et al. [50] present a smart optimized surveillance system integrated with a smartphone or laptop using Raspberry Pi and a PIR sensor. The paper used an algorithm named ViBE (Visual Background Extractor) for detecting unwanted movement. The system transmits the video stream to smartphones or laptops for monitoring. They used a blowfish encryption and decryption algorithm to provide security for the transmission of video files between the source and destination.

Deypir et al. [51] studied the concept of criticality in Android permissions by analyzing the exploitation of permissions by known malware applications and their legal usage by useful applications. To measure the security risks of those malware applications, a new security model is proposed based on this analysis and the definition of large numbers of malware and benign apps. Computed risk values are most affected by the informative permissions and in turn, it gives rise to more security concerns. Two new datasets have been constructed from malicious and non-malicious Android apps and were analyzed against existing datasets to evaluate the proposed criterion. Usage pattern permissions of Android apps are changed over time to analyze the performances. A new risk measurement named "entropy-based risk score (ERS)" is introduced where entropy values are calculated from user applications based on the definition. As the security risk of giving permission is obtained, which can be similarly computed for Android calling as a security risk of giving permission.

Anagnostopoulos et al. [52] present the architecture of two different methods of DDoS attacks that can be carried out by botnets. The first method is completely based on a mobile botnet which takes advantage of the open Wi-Fi networks and a loophole in the mobile security which cannot blacklist the IP address which is frequently changing in the case of mobile devices. The second scenario consists of both mobile and PC, where a PC acts as a bot and acts as a proxy machine only because it has high computational ability compared to a smartphone. In both the methods and architecture, where the user presents the analysis of DNS amplification and/or TCP flooding how the proxy is initialized, mitigation, recovered and used to attack, Kambourakis et al. [53] explain the basic idea of Mirai's bot attack and the steps for executing the attack. An overview of its variants such as BrickerBot and Hajime botnet are presented.

Wu et al. [54] focused on security issues of frames captured by the surveillance camera by applying a background bootstrapping method, which eliminates background motion and allows for the precise estimation of salient motion. Salient motion estimation features can be measured by computing the block-level changes in current and reference frames. This motion estimation algorithm can detect even small background changes by using

image-based temporal gradients for salient motion. VSSs capture videos in the combination of Red, Green, and Blue (RBG) format using pixel sensors with a high resolution and frequency. The author proposed a randomized capturing approach, which makes it impossible for attackers to extract original information data from the encoded frames. This denies information required by the attackers for building a crypto-analysis model. This algorithm is secure as an attacker obtains any meaningful information from the encoded image. The bootstrapping method reduces the bandwidth, transmission and storage cost as well as gives ample time for the security analysts to detect any suspicious activity.

Jeong et al. [55] have introduced a deep learning model to measure the classification accuracy of inserted malicious data as well as the side-channel attacks performed in a video surveillance system. An autoencoder and image-specific convolutional neural network (CNN) classification models were used, which are not limited to image datasets. NSL-KDD and an image dataset are first constructed in an adversarial sample with MNIST with a dataset that is first constructed. The samples were created using the "Jacobian-based saliency map attack (JSMA) method and the Fast Gradient Sign Method (FGSM)", in which autoencoder validation experiments and CNN-based classification models were created using the Tensor Flow and PyTorch libraries, to assess the risks of adversarial attacks. A predefined set of images is trained using the CNN algorithm and JSMA/FGSM is applied to extract the image dataset to determine side-channel attacks and image content alteration.

Rafik Hamza et al. [56] proposed a secure surveillance framework based on IoT systems by video streaming integration and the encryption of image algorithms. A highly efficient video encoding scheme is used to extract information from the frames using visual sensors to reduce redundant video processing. When an informative event is identified from key frames, a warning should be issued to concerned authorities autonomously. Event identification-based decision depends on the encoded key frames, but if modification occurs due to attacks during transmission, it can result in severe data losses. To overcome this issue, the author proposed a high speed and lightweight crypto algorithm for key frame encryption before transmission, which modifies the originality of key frames to break attacks, which in turn makes this highly suitable IoT-based systems.

Table 4 summarizes the existing methods optimizing the video stream with multiple nodes in the network architecture and methods used for securing VSS. Details such as methodology, issues addressed, advantages and disadvantages of each method are tabulated.

Table 4. Summary of literature review on VSS security and optimization methods.

Author(s)	Methodology	Issues Addressed	Advantages	Disadvantages
Wu et al. [54]	The background bootstrapping method is applied, which eliminates background motion and the need to precisely estimate the salient motion.	Visual attack	Proposed a randomized capturing approach, which makes it impossible for attackers to extract informative data or original data from the decoded frames.	Deals with large amount of surveillance data to decide about abnormal and suspicious activity detection.
Jeong et al. [55]	The adversarial attack method is used for finding vulnerability by employing a deep learning library for multimedia VSS.	Visual layer attack	The proposed experimental method measures the detected accuracy of the model and verifies the effect of adversarial samples.	Both the models used have a significant reduction in classification accuracy by using adversarial samples.

Table 4. *Cont.*

Author(s)	Methodology	Issues Addressed	Advantages	Disadvantages
Rafik Hamza et al. [56]	Proposed a secured surveillance framework based on the Internet of Things (IoT) system with intelligent integration of video summarization using key frames extraction algorithm and image encryption algorithm.	Visual attack	High speed and lightweight probabilistic key frames encryption algorithm is proposed for encrypting the key frames before they are transmitted about an event alert.	The final decision is based on event identification of encoded key frames.
Hossain et al. [57]	Summarizes several distinct issues of a cloud-based multimedia surveillance system and discusses the different design choices.	DoS attack and covert channel attacks	Presents significant issues related to cloud deployment architecture, media acquisition strategy, cloud storage, media processing, resource allocation, notification and sharing, big data analytics, security and privacy, and cloud-based system performance.	The device should be authenticated to each other before data transfer takes place.
Lubica et al. [58]	Analysis of the dictionary-based techniques for selecting the PIN (personal identification number).	Privilege escalation attack	The technique of the mitigated dictionary is useful for the selection of a secured PIN which is not prone to guessing attacks.	Application only works if a uniform PIN word is selected.
Alsmirat et al. [59]	Provides an end-to-end security framework for a cloud-based video surveillance system supported by a Mobile Edge Computing (MEC) server.	Visual layer attack	The proposed cloud-based VSS supports large number of cameras. An end-to-end security framework provides mutual authentication, data integrity as well as confidentiality and key management.	Key exchange is the major problem in proposed method.
Xu et al. [60]	A new model named video structural description (VSD) carries out the parsing of video content into text information by segmenting spatial and temporal data, selecting features, recognizing objects based on a semantic model.	Covert channel attack	Embedding video content into the text information reduces redundant frames processing.	The proposed approach is not tested with the attack model to check side-channel attacks.
Rahman et al. [61]	Sensitive data generated from visual sensors is secured by designing a system which identifies various privacy leakage channels in the distributed VSS.	Covert channel attack	Privacy-related problems of the leakage channels are mitigated at different levels.	When a secured privacy vault (obtained from distributed visual sensors) is stolen, information may be compromised.
Gaj et al. [62]	Geometric attacks are countered by using a compressed domain video watermarking scheme which embeds the watermark in the homogeneously moving object of a video sequence.	Visual layer attack	It can resist an RST (rotation, scaling and translation) attack without sacrificing the visual quality.	Not applicable for non-stationary backgrounds.

Table 4. *Cont.*

Author(s)	Methodology	Issues Addressed	Advantages	Disadvantages
Fadl et al. [63]	A new duplication detection algorithm is employed based on the standard deviation of residual inter frames.	Visual layer attack/ steganography attack	It is relatively effective in identifying inter-frame duplication forgery within an acceptable time.	It detects attacks in residual frames and is not possible for all types of intra-frame.
Lee et al. [64]	Blockchain technology is used to securely synchronize the CCTV video using the Secure Merkle-Tree method in all the authorized nodes of the system.	Malware attack	It enables deduplication to reduce storage costs. Additionally, the proposed method can synchronize CCTV video data safely without exposing the privacy of the object in the course of synchronization	It can have privacy violation due to the leakage of personal information from an object in a video, which may cause serious social issues.
Fitwi et al. [65]	The Lib-Pri system uses the blockchain technique for integrity checking, blurring mechanisms, and video access permissions.	Visual layer modification	Privacy-sensitive objects are detected and masked or blurred in the block chain network. Access permission for users is mentioned in a smart contract document. It ensures the regeneration of a masked image in an isolation storage if required for legal purposes.	The Lib-Pri system accuracy is crucial and applying a reversible mask to preserve privacy is an issue of concern.

5. Conclusions

In this paper, we have systematically presented various types of attacks on camera-based surveillance systems along with the prevention measures. The current developments of authentication methods to overcome the different attacks are outlined. Most of the methods reviewed attempted to provide security and methods of handling the video stream in video surveillance systems and smartphones. Existing security methods such as firewall, access control, and IDSs/IPS available for general network security may not be fully suitable for these environments. To mitigate the vulnerabilities and attacks, up-to-date security measures, tools and techniques are required. In the future, a comprehensive design will be proposed to mitigate the majority of the identified attacks in the video surveillance systems.

Author Contributions: Conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, P.V. and P.T.C.; writing—original draft preparation, writing—review and editing, P.V., P.T.C., T.B.M., P.K.B.N. and Y.-G.K.; visualization, P.V. and P.T.C.; supervision, project administration, T.B.M., Y.-G.K. and P.K.B.N.; funding acquisition, Y.-G.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP), grant funded by the Korea government (MSIT) (No.2019-0-00231) as well as by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2020R1A6A1A03038540).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Available on request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report with respect to this paper.

References

1. Market Analysis Report. Available online: https://www.grandviewresearch.com/industry-analysis/smart-home-security-camera-market (accessed on 15 May 2021).
2. Yan, W.Q.; Zhou, L.; Shu, Y.; Yu, J. CVSS: A Cloud-Based Visual Surveillance System. *Int. J. Digit. Crime For.* **2018**, *10*, 79–91.
3. Shodan. Available online: https://www.shodan.io/ (accessed on 2 November 2020).
4. The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras almost Brought Down the Internet. Available online: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (accessed on 15 May 2021).
5. CyberScoop. Available online: https://www.cyberscoop.com/washington-dc-ransomware-dc-police-department/ (accessed on 15 May 2021).
6. Dozens of Canon Security Cameras Hacked in Japan. Available online: https://english.kyodonews.net/news/2018/05/91ec861ae24d-dozens-of-security-cameras-hacked-in-japan.html?phrase=ham%20fighters&words= (accessed on 15 May 2021).
7. Bosch IP Camera Vulnerability (CVE-2018-19036). Available online: https://psirt.bosch.com/security-advisories/bosch-2018-1202.html (accessed on 15 May 2021).
8. Vulners. Available online: https://vulners.com/talos/TALOS-2018-0565 (accessed on 15 May 2021).
9. Your Smart Camera May Have Been Spying on You. Available online: https://www.cnet.com/home/smart-home/your-smart-camera-may-have-been-spying-on-you/ (accessed on 15 May 2021).
10. Critical Flaw Lets Hackers Take Control of Samsung SmartCam Cameras. Available online: https://www.computerworld.com/article/3158204/critical-flaw-lets-hackers-take-control-of-samsung-smartcam-cameras.html (accessed on 15 May 2021).
11. Major Vulnerabilities and Exploit in Foscam Cameras. Available online: https://www.vdoo.com/blog/vdoo-has-found-major-vulnerabilities-in-foscam-cameras (accessed on 15 May 2021).
12. India Today. Available online: https://www.indiatoday.in/mail-today/story/installation-of-1-4-lakh-chinese-cctv-cameras-by-delhi-govt-sparks-row-1696032-2020-07-02 (accessed on 15 May 2021).
13. Kao, I.-L. *Securing Mobile Devices in the Business Environment*; IBM Global Technology Services–Thought Leadership White Paper; IBM: Armonk, NY, USA, 2011.
14. Becher, M.; Freiling, F.C.; Hoffmann, J.; Holz, T.; Uellenbeck, S.; Wolf, C. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In Proceedings of the 2011 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 22–25 May 2011; pp. 96–111.
15. McAfee Labs. *McAfee Threats Report: First Quarter 2013*; McAffe Press: San Jose, CA, USA, 2013. Available online: http://www.mcafee.com/us/resources/re-ports/rpquarterly-threat-q (accessed on 15 May 2021).
16. F-Secure Labs. *Mobile Threat Report January-March 2013*; F-Secure Labs: Helsinki, Finland, 2013. Available online: http://www.f-secure.com/static/doc/labs_global!Research/Mobile_Threat_Report_Q1_2013 (accessed on 15 May 2021).
17. Stites, D.; Tadimla, A. A Survey of Mobile Device Security, Threats, Vulnerabilities and Defences. 2011. Available online: http/afewguyscod-ing.com/2011/12/survey-mobile-device-security-threatsvulnerabilities-defences (accessed on 15 May 2021).
18. Enck, W.; Gilbert, P.; Chun, B.G.; Cox, L.P.; Jung, J.; McDaniel, P.; Sheth, A.P.; Droid, T. An Information on Tracking System for Real Time Privacy Monitoring on Smart-Phones. In Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation, Vancouver, BC, Canada, 4–6 October 2010; USENIX Association: Berkeley, CA, USA, 2020; pp. 1–6.
19. Franklin, J.; Brown, C.; Dog, S.; McNab, N.; Voss-Northrop, S.; Peck, M.; Stidham, B. Assessing Threats to Mobile Devices & Infrastructure NISTIR 8144. Available online: https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf (accessed on 15 May 2021).
20. Zheng, P.; Lionel, M.N. Spotlight: The rise of the smartphone. *IEEE Distrib. Syst. Online* **2006**, *7*, 3. [CrossRef]
21. Liranzo, J.; Hayajneh, T. Security and Privacy Issues Affecting Cloud-Based IP camera. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 458–465.
22. Hoque, N.; Bhuyan, M.H.; Baishya, R.C.; Bhattacharyya, D.K.; Kalita, J.K. Network attacks: Taxonomy, tools and systems. *J. Netw. Comput. Appl.* **2014**, *40*, 307–324. [CrossRef]
23. Rytel, M.; Felkner, A.; Janiszewski, M. Towards a Safer Internet of Things—A Survey of IoT Vulnerability Data Sources. *Sensors* **2020**, *20*, 5969. [CrossRef]
24. Costin, A. Poor Man's Panopticon: Mass CCTV Surveillance for the Masses. Available online: http://andreicostin.com/papers/poc2013_andrei.slides.pdf (accessed on 15 May 2021).
25. Mowery, K.; Wustrow, E.; Wypych, T.; Singleton, C.; Comfort, C.; Rescorla, E.; Halderman, J.A.; Shacham, H.; Checkoway, S. Security analysis of a full-body scanner. In *23rd USENIX Security Symposium USENIX Security 14*; USENIX Association: San Diego, CA, USA, 2014; pp. 369–384.
26. Jones, E.; Le Moigne, O.; Robert, J.-M. IP traceback solutions based on time to live covert channel. In Proceedings of the 2004 12th IEEE International Conference on Networks (ICON 2004) (IEEE Cat. No. 04EX955), Singapore, 19 November 2004; pp. 451–457.
27. Alcaraz, C.; Bernieri, G.; Pascucci, F.; Lopez, J.; Setola, R. Covert Channels-Based Stealth Attacks in Industry 4.0. *IEEE Syst. J.* **2019**, *13*, 3980–3988. [CrossRef]
28. Guri, M.; Hasson, O.; Kedma, G.; Elovici, Y. Visisploit: An optical covert-channel. *arXiv* **2016**, arXiv:1607.03946.
29. Sloan, T.; Hernandez-Castro, J. Forensic analysis of video steganography tools. *PeerJ Comput. Sci.* **2015**, *1*, e7. [CrossRef]

30. Senthil, M. CCTV Surveillance System, attacks and design goals. *Int. J. Electr. Comput. Eng.* **2018**, *8*, 2072–2082. [CrossRef]
31. Maharjan, R.; Shrestha, A.K.; Basnet, R. Image Steganography: Protection of Digital Properties against Eavesdrop-ping. *arXiv* **2019**, arXiv:1909.04685.
32. Yin, J.; Fen, G.; Mughal, F.; Iranmanesh, V. Internet of Things: Securing Data using Image Steganography. In Proceedings of the 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS), Kota Kinabalu, Malaysia, 2–4 December 2015. [CrossRef]
33. Zhang, Y.-Y.; Li, X.-Z.; Liu, Y.-A. The detection and defence of DoS attack for wireless sensor network. *J. China Univ. Posts Telecommun.* **2012**, *19*, 52–56. [CrossRef]
34. Pan, J. Physical Integrity Attack Detection of Surveillance Camera with Deep Learning based Video Frame Interpolation. In Proceedings of the 2019 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), Bali, Indonesia, 5–7 November 2019; pp. 79–85.
35. Blasing, T.; Batyuk, L.; Schmidt, A.-D.; Camtepe, S.; Albayrak, S. An Android Application Sandbox system for suspicious software detection. In Proceedings of the 2010 5th International Conference on Malicious and Unwanted Software, Nancy, France, 19–20 October 2010; pp. 55–62.
36. Available online: https://www.cynet.com/network-attacks/privilege-escalation/ (accessed on 11 March 2021).
37. Hur, J.B.; Shamsi, J.A. A survey on security issues, vulnerabilities and attacks in Android based smartphone. In Proceedings of the 2017 International Conference on Information and Communication Technologies (ICICT), Karachi, Pakistan, 30–31 December 2017; pp. 40–46.
38. Cai, Y.; Tang, Y.; Li, H.; Yu, L.; Zhou, H.; Luo, X.; He, L.; Su, P. Resource Race Attacks on Android. In Proceedings of the 2020 IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER), London, ON, Canada, 18–21 February 2020; pp. 47–58.
39. Raveendranath, R.; Rajamani, V.; Babu, A.J.; Datta, S.K. Android malware attacks and countermeasures: Cur-rent and future directions. In Proceedings of the 2014 International Conference on Control, Instrumentation, Communication and Computa-tional Technologies (ICCICCT), Kanyakumari, India, 10–11 July 2014; pp. 137–143.
40. Wetherall, D.; ChoDnes, D.; Greenstein, B.; Han, S.; Homyack, P.; Jung, J.; Schechter, S.; Wang, X. Privacy revela-tions for web and mobile apps. In *13th Workshop on Hot Topics in Operating Systems HotOS XIII*; USENIX Association: Napa, CA, USA, 2011.
41. Jung, S.; Kwon, T. Automatic Smudge Attack Based on Machine Learning and Pattern Lock System Safety Analysis. *J. Korea Inst. Inf. Secur.* **2016**, *26*, 903–910.
42. Prema, S.; Pramod, T.C. Key Establishment Scheme for Intra and Inter Cluster Communication in WSN. In Proceedings of the 2018 Second. International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 15–16 February 2018; pp. 942–944. [CrossRef]
43. T.C., P.; G.S., T.; Iyengar, S.S.; Sunitha, N.R. CKMI: Comprehensive key management infrastructure design for Industrial Automation and Control Systems. *Future Internet* **2019**, *11*, 126. [CrossRef]
44. Wang, S.; Bie, R.; Zhao, F.; Zhang, N.; Cheng, X.; Choi, H. Security in wearable communications. *IEEE Netw.* **2016**, *30*, 61–67. [CrossRef]
45. Pramod, T.; Sunitha, N. Key pre-distribution schemes to support various architectural deployment models in WSN. *Int. J. Inf. Comput. Secur.* **2016**, *8*, 139. [CrossRef]
46. Pramod, T.C.; Sunitha, N.R. An approach to detect malicious activities in SCADA systems. In Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 4–6 July 2013; pp. 1–7.
47. Kalbo, N.; Mirsky, Y.; Shabtai, A.; Elovici, Y. The Security of IP-Based Video Surveillance Systems. *Sensors* **2020**, *20*, 4806. [CrossRef] [PubMed]
48. Android Camera Bug Under the Microscope. Available online: https://www.darkreading.com/vulnerabilities---threats/android-camera-bug-under-the-microscope/d/d-id/1339090 (accessed on 9 October 2020).
49. Malokar, N.K.; Subramanian, N.; Sriram, S.; Venkat, S.; Khan, Z.; Shrawne, S. Exploiting the Vulnerabilities of Android Camera API. *IARJSET* **2015**, *2*, 70–73. [CrossRef]
50. Prasad, S.; Mahalakshmi, P.; Sunder, A.J.C.; Swathi, R. Smart Surveillance Monitoring System Using Raspberry PI and PIR Sensor. *Int. J. Comput. Sci. Inf. Technol.* **2014**, *5*, 7107–7109.
51. Deypir, M. Entropy-based security risk measurement for Android mobile applications. *Soft Comput.* **2018**, *23*, 7303–7319. [CrossRef]
52. Anagnostopoulos, M.; Kambourakis, G.; Gritzalis, S. New facets of mobile botnet: Architecture and evaluation. *Int. J. Inf. Secur.* **2016**, *15*, 455–473. [CrossRef]
53. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and Other Botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
54. Wu, L.; Du, X.; Fu, X. Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *IEEE Commun. Mag.* **2014**, *52*, 80–87. [CrossRef]
55. Jeong, J.; Kwon, S.; Hong, M.-P.; Kwak, J.; Shon, T. Adversarial attack-based security vulnerability verification using deep learning library for multimedia video surveillance. *Multimed. Tools Appl.* **2019**, *79*, 16077–16091. [CrossRef]
56. Muhammad, K.; Hamza, R.; Ahmad, J.; Lloret, J.; Wang, H.H.G.; Baik, S.W. Secure Surveillance Framework for IoT Systems Using Probabilistic Image Encryption. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3679–3689. [CrossRef]

57. Hossain, M.A. Framework for a Cloud-Based Multimedia Surveillance System. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 1–11. [CrossRef]
58. Staneková, L.; Stanek, M. Analysis of dictionary methods for PIN selection. *Comput. Secur.* **2013**, *39*, 289–298. [CrossRef]
59. Alsmirat, M.A.; Obaidat, I.; Jararweh, Y.; Al-Saleh, M. A security framework for cloud-based video surveillance system. *Multimed. Tools Appl.* **2017**, *76*, 22787–22802. [CrossRef]
60. Xu, Z.; Hu, C.; Mei, L. Video structured description technology based intelligence analysis of surveillance videos for public security applications. *Multimed. Tools Appl.* **2015**, *75*, 12155–12172. [CrossRef]
61. Rahman, S.M.M.; Hossain, M.A.; Hassan, M.M.; Alamri, A.; Alghamdi, A.; Pathan, M. Secure privacy vault design for distributed multimedia surveillance system. *Futur. Gener. Comput. Syst.* **2016**, *55*, 344–352. [CrossRef]
62. Gaj, S.; Patel, A.S.; Sur, A. Object based watermarking for H.264/AVC video resistant to rst attacks. *Multimed. Tools Appl.* **2015**, *75*, 3053–3080. [CrossRef]
63. Fadl, S.M.; Han, Q.; Li, Q. Authentication of surveillance videos: Detecting frame duplication based on residual frame. *J. Forensic Sci.* **2018**, *63*, 1099–1109. [CrossRef]
64. Lee, D.; Park, N. Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. *Multimed. Tools Appl.* **2020**, 1–18. [CrossRef]
65. Fitwi, A.; Chen, Y.; Zhu, S. A Lightweight Blockchain-Based Privacy Protection for Smart Surveillance at the Edge. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 552–555.