US Patent & Trademark Office
Patent Public Search | Text View

METHODS AND SYSTEMS FOR ROUTING MEDIA

Abstract

A method for routing media in a surveillance system comprises, at a gateway device placed on a local network deployed at a location being surveilled and having network connectivity to a cloud computing device, detecting networked device(s) placed on the local network, the networked device(s) comprising media device(s) each configured to generate media stream data as the location is being surveilled, determining a level of interest associated with the media stream data, obtaining, based on the detecting, at least one rule indicative of when the media stream data is to be routed, based on the level of interest, via the gateway device and when the media stream data is to be routed directly to the cloud computing device for processing, and instructing, based on the level of interest, at least one of the networked device(s) to route the media stream data according to the at least one rule.

Related U.S. Application Data

parent US continuation 18376412 20231003 parent-grant-document US 12284234 child US 19097002
parent US continuation-in-part 17976131 20221028 parent-grant-document US 11799934 child US 18376412

Publication Classification

Int. Cl.: **H04L65/61** (20220101); **G08B13/196** (20060101)

Background/Summary

CROSS-REFERENCE TO RELATED APPLICATIONS [0001] This patent application is a continuation of U.S. application Ser. No. 18/376,412 filed on Oct. 3, 2023, which is a continuation in part of U.S. application Ser. No. 17/976,131 filed on Oct. 28, 2022, the entire contents of which are incorporated herein by reference.

FIELD
[0002] The improvements generally relate to surveillance systems, and more particularly to routing media stream data in a surveillance system.
BACKGROUND
[0003] Surveillance systems are typically composed of a variety of different devices connected by a local network deployed at the site being surveilled. Many surveillance systems include cameras or other devices which capture images or video data used in performing surveillance of the site. Increasingly, modern surveillance systems are beginning to employ cloud-aware or other connected devices which can allocate their workload between local processing, within the connected device, and remote or cloud-based processing, available for instance via a remote or cloud server.
[0004] These cloud-aware devices may reside on the same local network as other non-cloud-aware devices, including legacy internet protocol (IP) cameras, local storage devices, and the like. A surveillance system or network which is configured to employ both local (also known as "on-premises") resources and cloud-based resources is known as a hybrid deployment. However, because existing cloud-aware devices are typically programmed to solely communicate with the remote or cloud server, the cloud-aware devices are also typically unaware of the other devices or resources potentially available to them on the local network. Existing cloud-aware devices are also vulnerable to unreliable or faulty internet connectivity disrupting their sole channel of communication to the remote or cloud server.
[0005] While existing surveillance systems are suitable for their purposes, there remains room for improvement.
SUMMARY
[0006] The following presents a simplified summary of one or more implementations in accordance with aspects of the present disclosure, in order to provide a basic understanding of such implementations, without limiting the embodiments presented within the present disclosure. While existing surveillance systems and networks effecting hybrid deployments are suitable for their purposes, existing cloud-aware devices in such deployments—media devices such as cloud cameras, cloud microphones, etc. —are typically unaware of the other devices present on the local network. As a result, the cloud-aware media devices are not equipped to leverage the resources available to them on the local network. This is particularly salient when it comes to providing alternative routes for media produced by the cloud-aware media devices in the event of loss of connectivity or network unreliability.
[0007] To this end, the present disclosure provides methods, systems, and computer-readable media for routing media in a surveillance system, which may be performed by the remote or cloud server, or by any suitable device on the local network, including by any media device on the network (whether cloud-aware or otherwise), by a gateway device on the network, or the like. Network detection is performed to detect the other devices present on the local network, including other media devices, other gateway devices, and the like. Based on what other network devices are

detected, one or more rules are obtained which indicate when media stream data, produced by the media devices, are to be routed by the gateway device(s), and when the media stream data is to be routed directly to the cloud server, based on a level of interest associated with the media stream data. The media stream data is then routed according to the at least one rule, based on the level of interest.

[0008] In accordance with one aspect, there is provided a method for routing media in a surveillance system, the method comprising, at a gateway device placed on a local network deployed at a location being surveilled, the gateway device having network connectivity to a cloud computing device, detecting one or more networked devices placed on the local network, the one or more networked devices comprising one or more media devices each configured to generate media stream data as the location is being surveilled, determining a level of interest associated with the media stream data, obtaining, based on the detecting, at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the gateway device and when the media stream data is to be routed directly to the cloud computing device for processing, and instructing, based on the level of interest associated with the media stream data, at least one of the one or more networked devices to route the media stream data according to the at least one rule.

[0009] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises conducting a media content analysis of the media stream data and generating one or more metadata items based on the media content analysis, the level of interest associated with the media stream data being determined based on the one or more metadata items.

[0010] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises receiving from the one or more media devices one or more metadata items related to the media stream data, the level of interest associated with the media stream data being determined based on the one or more metadata items.

[0011] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data satisfying a time restriction.

[0012] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of determining that the one or more media devices generated the media stream data during a target timeframe.

[0013] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data satisfying a location restriction.

[0014] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data satisfying at least one of a time restriction and a location restriction.

[0015] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of determining that the one or more media devices generated the media stream data in response to occurrence of a trigger event related to a status of the surveillance system.

[0016] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of detecting, based on the media content analysis, a presence of one or more objects in a field of view of the one or more media devices.

[0017] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of determining that a number of the one or more objects exceeds a threshold.

[0018] In at least one embodiment in accordance with any previous/other embodiment described

herein, the media stream data is determined to be of interest as a result of detecting, based on the media content analysis, a displacement of one or more objects in a field of view of the one or more media devices.

[0019] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises determining a speed of the one or more objects, wherein the media stream data is determined to be of interest as a result of determining that the speed of the one or more objects exceeds a speed threshold.

[0020] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises determining a direction of motion of the one or more objects, wherein the media stream data is determined to be of interest based on the direction of motion.

[0021] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of determining that the direction of motion of the one or more objects breeches a predefined boundary.

[0022] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises monitoring one or more parameters associated with at least one of the local network and an environment of the location being surveilled to determine whether the at least one rule is satisfied, wherein the at least one of the one or more networked devices is instructed to route the media stream data according to the at least one rule when the at least one rule is satisfied.

[0023] In at least one embodiment in accordance with any previous/other embodiment described herein, monitoring the one or more parameters comprises monitoring at least one of a performance of the local network, a performance of the cloud computing device, a time of day, a current weather at the location, a visibility at the location, a field of view of the one or more media devices, and a positioning of the one or more media devices within the environment.

[0024] In accordance with another aspect, there is provided a method for routing media in a surveillance system, the method comprising, at a cloud computing device, detecting one or more networked devices placed on a local network deployed at a location being surveilled, the one or more networked devices comprising one or more media devices and one or more gateway devices, each media device configured to generate media stream data as the location is being surveilled, and each gateway device having network connectivity to the cloud computing device, determining a level of interest associated with the media stream data, obtaining, based on the detecting, at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the one or more gateway devices and when the media stream data is to be routed directly to the cloud computing device for processing, and instructing, based on the level of interest associated with the media stream data, at least one of the one or more networked devices to route the media stream data according to the at least one rule.

[0025] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises conducting a media content analysis of the media stream data and generating one or more metadata items based on the media content analysis, the level of interest associated with the media stream data being determined based on the one or more metadata items.

[0026] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises receiving from the one or more media devices one or more metadata items related to the media stream data, the level of interest associated with the media stream data being determined based on the one or more metadata items.

[0027] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data satisfying a time restriction.

[0028] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data

satisfying a location restriction.

[0029] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data satisfying at least one of a time restriction and a location restriction.

[0030] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of determining that the one or more media devices generated the media stream data in response to occurrence of a trigger event related to a status of the surveillance system.

[0031] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of detecting, based on the media content analysis, a presence of one or more objects in a field of view of the one or more media devices.

[0032] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of determining that a number of the one or more objects exceeds a threshold.

[0033] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of detecting, based on the media content analysis, a displacement of one or more objects in a field of view of the one or more media devices.

[0034] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises determining a speed of the one or more objects, the media stream data being determined to be of interest as a result of determining that the speed of the one or more objects exceeds a speed threshold.

[0035] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises determining a direction of motion of the one or more objects, the media stream data being determined to be of interest based on the direction of motion.

[0036] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises monitoring one or more parameters associated with at least one of the local network and an environment of the location being surveilled to determine whether the at least one rule is satisfied, the at least one of the one or more networked devices being instructed to route the media stream data according to the at least one rule when the at least one rule is satisfied.

[0037] In accordance with yet another aspect, there is provided a method for routing media in a surveillance system, the method comprising, at one of a plurality of media devices placed on a local network deployed at a location being surveilled, detecting one or more networked devices placed on the local network, the one or more networked devices comprising remaining ones of the plurality of media devices and one or more gateway devices, each media device from the plurality of media devices configured to generate media stream data as the location is being surveilled, and each gateway device having network connectivity to a cloud computing device, determining a level of interest associated with the media stream data, obtaining, based on the detecting, at least one rule from at least one of the cloud computing device and the one or more gateway devices, the at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the one or more gateway devices and when the media stream data is to be routed directly to the cloud computing device for processing, and routing, based on the level of interest associated with the media stream data, the media stream data according to the at least one rule.

[0038] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises conducting a media content analysis of the media stream data and generating one or more metadata items based on the media content analysis, wherein the level of interest associated with the media stream data is determined based on the one or more metadata

items.

[0039] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data satisfying a time restriction.

[0040] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data satisfying a location restriction.

[0041] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest based on the media stream data satisfying at least one of a time restriction and a location restriction.

[0042] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of determining that the plurality of media devices generated the media stream data in response to occurrence of a trigger event related to a status of the surveillance system.

[0043] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of detecting, based on the media content analysis, a presence of one or more objects in a field of view of the one or more media devices.

[0044] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of determining that a number of the one or more objects exceeds a threshold.

[0045] In at least one embodiment in accordance with any previous/other embodiment described herein, the media stream data is determined to be of interest as a result of detecting, based on the media content analysis, a displacement of one or more objects in a field of view of the one or more media devices.

[0046] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises determining a speed of the one or more objects, the media stream data being determined to be of interest as a result of determining that the speed of the one or more objects exceeds a speed threshold.

[0047] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises determining a direction of motion of the one or more objects, the media stream data being determined to be of interest based on the direction of motion.

[0048] In at least one embodiment in accordance with any previous/other embodiment described herein, the method further comprises monitoring one or more parameters associated with at least one of the local network and an environment of the location being surveilled to determine whether the at least one rule is satisfied, the media stream data being routed according to the at least one rule when the at least one rule is satisfied.

[0049] In accordance with yet another aspect, there is provided a system for routing media. The system comprises a cloud computing device, one or more networked devices placed on a local network deployed at a location being surveilled, the one or more networked devices comprising one or more media devices each configured to generate media stream data as the location is being surveilled, and a gateway device placed on the local network and having network connectivity to the cloud computing device, the gateway device configured for detecting the one or more networked devices placed on the local network, determining a level of interest associated with the media stream data, obtaining, based on the detecting, at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the gateway device and when the media stream data is to be routed directly to the cloud computing device for processing, and instructing, based on the level of interest associated with the media stream data, at least one of the one or more networked devices to route the media stream data according to the at least one rule.

[0050] In accordance with yet another aspect, there is provided a system for routing media. The system comprises a cloud computing device and one or more networked devices placed on a local network deployed at a location being surveilled, the one or more networked devices comprising one or more media devices and one or more gateway devices, each media device configured to generate media stream data as the location is being surveilled, and each gateway device having network connectivity to the cloud computing device, the cloud computing device configured for detecting the one or more networked devices placed on the local network, determining a level of interest associated with the media stream data, obtaining, based on the detecting, at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the one or more gateway devices and when the media stream data is to be routed directly to the cloud computing device for processing, and instructing, based on the level of interest associated with the media stream data, at least one of the one or more networked devices to route the media stream data according to the at least one rule.

[0051] In accordance with yet another aspect, there is provided a system for routing media. The system comprises a plurality of media devices placed on a local network deployed at a location being surveilled, each media device from the plurality of media devices configured to generate media stream data as the location is being surveilled, a cloud computing device, and one or more networked devices placed on the local network, the one or more networked devices comprising remaining ones of the plurality of media devices and one or more gateway devices, each gateway device having network connectivity to the cloud computing device, one of the plurality of media devices configured for detecting the one or more networked devices placed on the local network, determining a level of interest associated with the media stream data, obtaining, based on the detecting, at least one rule from at least one of the cloud computing device and the one or more gateway devices, the at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the one or more gateway devices and when the media stream data is to be routed directly to the cloud computing device for processing, and routing, based on the level of interest associated with the media stream data, the media stream data according to the at least one rule.

[0052] Many further features and combinations thereof concerning embodiments described herein will appear to those skilled in the art following a reading of the instant disclosure.

Description

DESCRIPTION OF THE FIGURES
[0053] In the figures,
[0054] FIG. **1** is a schematic diagram illustrating a system for routing media, in accordance with an illustrative embodiment;
[0055] FIG. **2** is a schematic diagram detailing a network and the cloud-based computing infrastructure of the system of FIG. **1**, in accordance with an illustrative embodiment;
[0056] FIG. **3** is a flowchart illustrating an example method for routing media in a surveillance system, in accordance with an illustrative embodiment.
[0057] FIG. **4** is block diagram of an example computing device, in accordance with an illustrative embodiment.
[0058] It will be noticed that throughout the appended drawings, like features are identified by like reference numerals.
DETAILED DESCRIPTION
[0059] Described herein are methods and systems for routing media. In one embodiment, the systems and methods described herein may be used for monitoring and surveillance, and more specifically for routing media stream data generated within an area monitoring system (also

referred to herein as a "surveillance system"). It should however be understood that the methods and systems described herein may be used for a variety of applications and other embodiments may therefore apply.

[0060] FIG. **1** illustrates an example system **100** for routing media. The system **100** may be a surveillance system. It should however be understood that, while reference is made herein to a system **100** used for security purposes, the system **100** may be used for any other suitable purpose, such as for monitoring public transport or traffic, etc. The system **100** may also be implemented in any suitable environment, such as, but not limited to, a home, a business, or the like.

[0061] The system **100** comprises a number (N) of local networks **102**.sub.1, **102**.sub.2, . . . , and **102**.sub.N each deployed at a location (or site) being surveilled. For instance, a first network **102**.sub.1 may be deployed at a first geographical location and a second network **102**.sub.2 may be deployed at a second geographical location different from the first geographical location. Any suitable number of networks **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N may apply. In some embodiments, only one network as in **102**.sub.1 is provided. In other embodiments, the system **100** is a distributed system comprising more than one network **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N. Each network **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N may comprise any suitable network including, but not limited to, a Personal Area Network (PAN), Local Area Network (LAN), Wireless Local Area Network (WLAN), Metropolitan Area Network (MAN), or Wide Area Network (WAN), or combinations thereof. In one embodiment, each network **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N is a LAN having a plurality of networked devices **104** placed thereon. In addition, each network **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N is communicatively coupled to a cloud-based computing infrastructure **106** which is configured to provide one or more cloud computing services to one or more components of the system **100**, as will be described further below.

[0062] It should be understood that the system **100** may comprise a wide variety of different network technologies and protocols. Communication between the networked devices **104** may occur across wired, wireless, or a combination of wired and wireless networks. In addition to the networked devices **104** described below with reference to FIG. **2**, the system **100** may include any number of devices such as routers, modems, bridges, hubs, switches, and/or repeaters, among other possibilities.

[0063] Referring now to FIG. **2** in addition to FIG. **1**, in one embodiment, the plurality of networked devices **104** comprises a first plurality (X) of media devices **202**.sub.1, **202**.sub.2, . . . , and **202**.sub.X, and a second plurality (Y) of media devices **204**.sub.1, **204**.sub.2, . . . , and **204**.sub.Y. It should be understood that any suitable number of media devices may apply and that the number of first media devices **202**.sub.1, **202**.sub.2, . . . , and **202**.sub.X may be the same as, or different from, the number of second media devices **204**.sub.1, **204**.sub.2, . . . , and **204**.sub.Y. It should however be understood that, in some embodiments, the system **100** may only comprise second media devices **204**.sub.1, **204**.sub.2, . . . , and **204**.sub.Y and no first media devices **202**.sub.1, **202**.sub.2, . . . , and **202**.sub.X may be provided. The opposite may also apply.

[0064] As will be described further below, the second plurality of media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y have direct network connectivity (i.e., are configured to directly connect, through the communication link **205**) to the cloud-based computing infrastructure **106** while the first plurality of media devices **202**.sub.1, **202**.sub.2, . . . , and **202**.sub.X are not configured to have such direct network connectivity and may only access the cloud-based computing infrastructure **106** via one or more other networked devices **104**, namely via one or more gateway devices **206** to which they are connected. The first plurality of media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X may therefore be referred to as "traditional" cameras and the second plurality of media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may be referred to as "cloud cameras".

[0065] The media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may be used to monitor objects, events, places, and/or people of interest within the location under surveillance. As a result of such monitoring, the media devices **202**.sub.1, **202**.sub.2,

. . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y generate media streams, which may include image and/or video data (e.g., metadata, compressed video data, and/or uncompressed video data) and/or audio data, all referred to herein as "media stream data". In one embodiment, the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y comprise digital video cameras (e.g., fixed cameras, dome cameras, pan, tilt, and zoom—or PTZ—cameras, panoramic and multi-sensor cameras, and the like) disposed within the location under surveillance. Such video cameras may comprise Internet Protocol (IP) cameras configured to send the media stream data via the network **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N they are placed in, which may, in this case, comprise an IP network. The media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may also (or alternatively) comprise any suitable surveillance device including, but not limited to, radars, audio microphones, video and/or audio encoders connected to analog device(s) or appliance(s), sensors, door stations, intercoms, and the like.

[0066] Furthermore, the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may provide the media stream data in real-time or non-real time. The media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may comprise local storage. In embodiments in which the media stream data is provided in non-real time, the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may comprise devices, such as network-attached storage media having media stream data recorded therein. It should therefore be understood that while reference is made herein to the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y being video cameras, this is for illustrative purposes only and any other suitable media device may apply. It should also be understood that each group of media devices (i.e. the first media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and the second media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y) may comprise devices of different types. In addition, the first media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X may be of a different type than the second media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. For example, the first media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X may comprise video cameras and the second media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may comprise microphones. Other embodiments may apply.

[0067] When the system **100** comprises several media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, these may be located in close proximity to one another, for instance in the same building or on the same city block, or they may be remote from one another, for instance, located in different parts of the same city or in different cities altogether. Embodiments involving clusters of media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may also be considered, where media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, and **204**.sub.1, **204**.sub.2, . . . **204**.sub.Y belonging to one of a number of clusters may be geographically proximate to one another while the clusters themselves may be remote from one another.

[0068] Still referring to FIG. **2** in addition to FIG. **1**, in one embodiment, the plurality of networked devices **104** further comprises one or more gateway devices **206** communicatively coupled to the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and/or **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. Although the gateway device(s) **206** are illustrated as being connected to the media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y (which have direct network connectivity to the cloud-based computing infrastructure **106**), it should be understood that this is for illustrative purposes only and, in some embodiments, there may be no direct connection between the gateway device(s) **206** and the media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. In addition, although the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, the media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, and the gateway device(s) **206** are illustrated as being provided on the same (i.e. common) local network **102**.sub.1, it may, in some embodiments, be suitable for only the media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y and the gateway device(s) **206** to be on the same

local network as in **102**.sub.1. Therefore, in some embodiments, the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, may be provided on a local network different from the local network **102**.sub.1 on which the media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, and the gateway device(s) **206** are provided. Each gateway device **206** is configured to provide a connection (and allows communication and data flow) between the networks **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N and the cloud-based computing infrastructure **106**, which have different network protocol technologies.

[0069] In one embodiment, and as will be discussed further below, one or more of the gateway devices **206** are configured to instruct at least one of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y on the manner in which the media stream data generated by the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y is to be routed within the system **100** for subsequent data management and processing. The gateway device(s) **206** may be used to provide to the first plurality of media devices **202**.sub.1, **202**.sub.2, . . . , and **202**.sub.X connectivity to the cloud-based computing infrastructure **106**. The gateway device(s) **206** may further cause the media stream data generated by the media device(s) **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y to be stored (i.e. archived) in storage media **214**, the memory **210**, and/or in the cloud-based computing infrastructure **106** for subsequent use.

[0070] Each gateway device **206** comprises at least one processor **208**, at least one memory **210**, and at least one input/output (I/O) interface **212**, the processor **208** being communicatively coupled to the memory **210** and the I/O interface(s) **212**. The processor **208**, the memory **210** and the I/O interface(s) **212** may be linked via bus connections. The processor **208** may be a general-purpose programmable processor. In the example of FIG. **2**, the processor **208** is shown as being unitary, but the processor **208** may also be multicore, or distributed (e.g. a multi-processor).

[0071] The memory **210** stores program instructions and data used by the processor **208** to implement the data routing and/or storage functions described further below. The memory **210** may also store locally media stream data, acting as a local database, as well as store information regarding the media device(s) **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y that are accessible to the gateway device **206**. For example, the memory **210** may store the identity, IP address, and configuration (e.g., type, transmission capability, reception capability, connectivity capabilities to the cloud-based computing infrastructure **106**, etc.) of the media device(s) **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y. The memory **210**, though shown as unitary for simplicity in the example of FIG. **2**, may comprise multiple memory modules and/or caching. In particular, the memory **210** may comprise several layers of memory such as a hard drive, external drive (e.g. SD card storage) or the like and a faster and smaller Random Access Memory (RAM) module. The RAM module may store data and/or program code currently being, recently being or soon to be processed by the processor **208** as well as cache data and/or program code from a hard drive. A hard drive may store program code and be accessed to retrieve such code for execution by the processor **208** and may be accessed by the processor **208** to store and access data. The memory **210** may have a recycling architecture for storing, for instance, occurrence records, data source and/or database coordinates, where older data files are deleted when the memory **210** is full or near being full, or after the older data files have been stored in memory **210** for a certain time.

[0072] The I/O interface(s) **212** may comprise a network interface and may be a wired or wireless interface for establishing a remote connection with, for example, a remote server, an external data source (not shown), the client device **110**, etc. For instance, the I/O interface(s) **212** may be an Ethernet port, a WAN port, a TCP port, etc. The I/O interface(s) **212** may be used for communication with the media device(s) **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y, client device(s) **216**, and/or storage media **214** which may be one or more external database(s), one or more external systems, for example, having one or more

databases, that are accessible via Application Programming Interface (API) calls, and/or one or more local databases that are part of the gateway device **206**.

[0073] The storage media **214** may be used to archive (e.g., alternatively or in addition to the memory **210**) the media stream data received from the media device(s) **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y via the gateway device(s) **206**, for subsequent use including, but not limited to, data processing and real-time or delayed access by authorized user(s) of the surveillance system **100**). The storage media **214** may be accessible to the gateway device(s) **206**, the media device(s) **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, and the media device(s) **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. The storage media **214** may comprise a medium (i.e. a computer-readable medium) configured for storing data in a format readable by a processor or other computing device. The storage media **214** may, in some embodiments, be one or more servers comprising one or more databases. In such embodiments, the one or more servers may have processing and/or analytics capabilities and may have their own connection to the cloud-based computing infrastructure **106**, thus also serving as gateway device(s).

[0074] Still referring to FIG. **2** in addition to FIG. **1**, in one embodiment, the plurality of networked devices **104** further comprises client device(s) **216** in communication with the one or more media device(s) **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y, as well as with the gateway device(s) **206**. One or more client devices **216** may be provided, in close proximity to one another, for instance located in the same office or data center, or remote from one another, for instance located in different offices and data centers dispersed across the same city or in different cities altogether. Each client device **216** may be a remote computing device (i.e. functioning as a client) that comprises a plurality of components interconnected via bus connections and the like. In the illustrated example, each client device **216** comprises I/O interface(s) **218**, at least one processor **220**, at least one memory **222**, I/O device(s) **224** (e.g., a keyboard, a mouse, a touchscreen, etc.), and at least one display device **226** (e.g. a screen, a tactile display, etc.). The client device **216** may be a desktop computer, a laptop, a smartphone, a tablet, etc. The processor **220**, the memory **222** and the I/O interface(s) **218** may be similar to the processor **208**, the memory **210** and the I/O interface(s) **212**, respectively.

[0075] A client application program may be stored in the memory **222** of each client device **216**, the client application program providing the user with an interface to interact with a gateway device **206**. In some embodiments, the gateway device **206** may be connected to at least one client device **216**, where, for instance, the connection between the gateway device **206** and the client device **216** may be a wired connection. In some embodiments, the functionality of the gateway device **206** and the client device **216** may be implemented on a single computing device.

[0076] The client device **216** may be operated by authorized user(s) to access, view, process, edit and/or analyze information associated with the media stream data generated by the media device(s) **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y. The information may comprise video information, such as a video feed, as well as any other relevant information obtained from the gateway device(s) **206**. The client device **216** may be configured to launch a video playback application, a web browser, or a web application (not shown) that renders a graphical user interface (GUI) on the display device **226**. The GUI may be used to display outputs and accept inputs and/or commands from user(s) of the client device **216**. The GUI may further provide user(s) with the ability to view and/or edit video feeds, as well as be presented information of interest related to the video feeds.

[0077] Still referring to FIG. **2** in addition to FIG. **1**, in one embodiment, the cloud-based computing infrastructure **106** is configured to run part of the workload of components of the video surveillance system **100** in the cloud. In particular, the cloud-based computing infrastructure **106** may provide any suitable cloud computing service(s) related to management of the video surveillance system **100** including, but not limited to, processing of media stream data, cloud archiving or storage of media stream data, storage of video indexes, off-network live video requests

and viewing, video analysis, indexing and persisting metadata for applications such as forensic search, live video camera health monitoring, alert scheduling, bandwidth management, or other form of processing and/or management related to the media stream data. For this purpose, in one embodiment, the cloud-based computing infrastructure **106** comprises a cloud computing device (referred to herein as a cloud computing server) **228** communicatively coupled to cloud-based storage media **230**. The cloud computing server **228** may comprise one or more virtual processors configured to process the media stream data upon receipt thereof and cause the cloud computing service(s) to be provided.

[0078] As previously noted and as can be seen in FIG. **2**, the gateway device(s) **206** and the second plurality of media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y have connectivity to the cloud-based computing infrastructure **106**. Each gateway device **206** may have direct connectivity to the cloud-based computing infrastructure **106** (e.g., via communication link **232**) or indirect connectivity thereto (e.g., via one or more other gateway devices **206**). In other words, the gateway device(s) **206** and the second plurality of media devices **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y are configured to directly communicate with the cloud computing server **228** and/or the cloud-based storage media **230** via communication links **232** and **205**, respectively. In contrast, the first plurality of media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X do not have direct network connectivity to the cloud-based computing infrastructure **106** and may only communicate with (e.g., transmit media stream data to) the cloud computing server **228** and/or the cloud-based storage media **230** via the gateway device(s) **206**, as will be described further below.

[0079] It is proposed herein to route the media stream data generated by the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and/or **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y within the system **100** dynamically, based on one or more rules (also referred to as "policies"). The rules ensure that the routing is performed correctly and the rules may vary depending on the configuration of the system **100** and on the type of networked devices **104** present on the networks **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N. As such, in one embodiment, routing of the media stream data within the system **100** is performed subsequent to detecting the networked devices **104** placed on the network (e.g., the LAN) as in **102**.sub.1 deployed at the location being surveilled. The networked devices **104** as detected may comprise one or more of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, the gateway device(s) **206**, the storage media **214**, and/or the client device(s) **216**.

[0080] The detection of the networked devices **104** may be performed by any suitable computing device (also referred to herein as a "detection device") provided as part of the system **100** and configured to perform the detection. In some embodiments, the detection device is a given gateway device **206**. In other embodiments, the detection device is a given media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, and more particularly a given second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y. In yet other embodiments, the detection device is a given first media device **202**.sub.1, **202**.sub.2, . . . , or **202**.sub.X.

[0081] The detection may be performed at the detection device actively, i.e. by the detection device itself. In one embodiment, active detection may be performed by a detection device (e.g., the given gateway device **206** or the given second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y) already placed on the network as in **102**.sub.1. In particular, a device located on the network **102**.sub.1, such as one or more of the gateway device(s) **206** or one or more of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, may discover other networked devices **104** belonging to the same network **102**.sub.1. For example, the gateway device(s) **206** may detect one another. A second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y may also be configured to detect the first media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X placed on the network **102**.sub.1 (and vice versa). A second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y may also be configured to detect the gateway device(s) **206** placed on the network **102**.sub.1 (e.g., the gateway device **206** positioned at a shortest distance to the media

device's location), and the gateway device(s) **206** may in turn detect the second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y. The gateway device(s) **206** may also detect the storage media **214** and/or detect the client device(s) **216** placed on the network **102**.sub.1. It should be understood that the detection may be performed by any other suitable networked device **104** placed on the network **102**.sub.1.

[0082] The detection may alternatively be performed passively. In this case, the detection device may receive information indicative of the presence of the networked devices **104** on the network as in **102**.sub.1. The information may be received from a device already placed on the network as in **102**.sub.1 and communicatively coupled to the other networked devices **104**, from the given gateway device **206** or from the given second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y, or the like) having performed the active detection. In one embodiment, passive detection may be performed by a detection device (e.g., the cloud computing server **228**) that is not already placed on the network as in **102**.sub.1. For example, the cloud computing server **228** may be configured to instruct the gateway device **206** (or any other device placed on the local network **102**.sub.1) to monitor the network **102**.sub.1. The gateway device **206** may in turn generate at least one detection signal indicative of the presence of the other networked devices **104** placed on the network **102**.sub.1, and communicate the at least one detection signal to the detection device (e.g., to the cloud computing server **228**) via any suitable means. It should however be understood that a device placed on the network as in **102**.sub.1 may also be configured to perform passive detection.

[0083] The detection of the networked devices **104** present on the network **102**.sub.1 may be performed by the detection device periodically, i.e. at predetermined time intervals. Alternatively, the detection may be performed in response to the detection device receiving a user-initiated command, upon a user providing (e.g., via the I/O device(s) **224** of their client device **216**) instructions to detect the presence of the networked devices **104**. In other embodiments, the detection may be performed in response to the detection device receiving a system-initiated command, which may automatically generated once one or more of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y are placed on the network **102**.sub.1. For example, the detection may be configured to be part of an initialization process when a media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y is added to the network **102**.sub.1. The detection may also be performed programmatically or via a system policy.

[0084] In one embodiment, active detection involves performing, at the detection device, a network discovery routine to locate the devices **104** present on the network **102**.sub.1. In some embodiments, the outcome of the network discovery routine is sent (e.g., by any device present on the local network **102**.sub.1) to the cloud computing server **228**. Any suitable network discovery routine may be performed. In one embodiment, the detection device may send, using any suitable communication means, at least one broadcast message over the network **102**.sub.1. Upon receipt of a broadcast message, each networked device **104** placed on the network **102**.sub.1 may generate a response message indicative of the presence of the networked device **104** placed on the network **102**.sub.1. Each response message may contain information (e.g., IP address, configuration, etc.) uniquely identifying the networked device **104**. In addition to indicating the presence of networked devices **104** on the network **102**.sub.1, the detection process may therefore allow to determine the IP address and configuration of the detected devices **104**. As used herein, the term "configuration", when relating to the networked devices **104**, refers to one or more parameters indicative of a device's type, transmission capability, and/or reception capability. For example, determining the configuration of the networked devices **104** present on the network **102**.sub.1 comprises determining that the networked devices **104** comprise at least one second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y configured to directly access the cloud-based computing infrastructure **106**. Determining the configuration of the networked devices **104** may further (or alternatively) comprise determining that the networked devices **104** comprise at least one first

media device **202**.sub.1, **202**.sub.2, . . . , or **202**.sub.X configured to access the cloud-based computing infrastructure **106** via one or more gateway devices **206**. In some embodiments, determining the configuration of the networked devices **104** may also comprise determining that a given device is already enrolled in a given system (e.g., on the local network **102**.sub.1). In this manner, it may be possible to avoid attempting to re-enroll the given device with the given system.

[0085] Once the networked devices **104** have been detected, one or more rules (also understood to be "routing rules") based on which routing of the media stream data is to be performed are obtained. Each rule ensures proper routing of media stream data within the system **100**, from a source to a destination. The rules may be determined using any suitable means or technique, in order to achieve any desired objective in relation to the system **100**. In one embodiment, the rules are set in order to optimize costs, network usage, system reliability, and resiliency to disconnection.

[0086] As used herein, the term "reliability", when referring to the system **100**, refers to the fact that one can depend (or rely) on the system **100** to operate as expected. For a video-surveillance system, such as the system **100**, reliability may encompass several aspects including, but not limited to, ensuring that video is recorded and available at all times or ensuring proper management of the network bandwidth. In the present disclosure, the term "logically continuous", when used in association with a change of destination in the media stream data, refers to a media stream data where little to no data is lost when the destination of the media stream data is changed. However, in some examples, some (but little) data may still be lost due to the transition. As used herein, the term "resiliency to disconnection" refers to the fact that recording gaps in the media stream data are avoided even in the event of disconnection of the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y generating the media stream data. For example, if a media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y (e.g., a video camera) continuously streams data to the cloud-based storage media **230** and loses network (e.g., Internet) connectivity, recording gaps in the video archive can be avoided by relying on local storage provided at the local networks **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N. In particular, the local storage (e.g., the storage media **214** or storage within the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y) may act as a buffer that allows for the system **100** to fill any gaps in cloud storage when network connectivity is restored.

[0087] A rule may only be applicable under certain circumstances (i.e. when certain condition(s) are met) and may not be applicable under others. In some embodiments, when the condition(s) are met, the rule is said to be satisfied and it can be applied (i.e. implemented or followed) to route the media stream data within the system **100**. The condition(s) may relate to the networks **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N, an environment of the location under surveillance by the system **100**, components of the system **100**, a level of interest in the media stream data, or the like. As will be discussed further below, in some embodiments, one or more parameters may therefore be monitored and/or the level of interest associated with the media stream data determined in order to assess whether the conditions are met and whether the rule is applicable. In some embodiments, only one rule is satisfied, and therefore applicable, at any given time. In other embodiments, more than one rule may be satisfied, and therefore applicable, at any given time.

[0088] In some embodiments, a rule may indicate that the media stream data should remain available at all times or most (e.g., 99%) of the time. In other embodiments, a rule may indicate that the media stream data is to be stored (using the same or different quality) in a redundant manner: locally (e.g., in storage media **214**), in the memory **210** of the gateway device **206**, and in the cloud-based storage media at all times for subsequent viewing by a client device **216**.

[0089] As another example, in order to comply with governmental regulations, a rule may indicate that the media stream data (e.g., uninterrupted or continuous video footage) is to be archived for a predetermined time period. This may be the case, for instance, in certain jurisdictions where certain businesses are required to maintain at all times at least a predetermined number of days (e.g., 30, 90, or 180 days) of archived video records for all video cameras on their premises or face potential

fines.

[0090] As another example, a rule may indicate that a given analysis (e.g., video analysis) is to be performed on the media stream data prior to storage thereof (e.g., in the cloud-based storage media **230**). As yet another example, in order to optimize network usage, a rule may indicate that the analysis of the media stream data is to be performed at a given time of day (e.g., in the evenings or during business hours), during off-peak periods (e.g., on the weekends), or the like. As yet another example, a rule may indicate that, in order to minimize costs, local resources (e.g., the processor **208** of the gateway device **206**, rather than the cloud computing server **228**) are to be used to decode and analyze video streams generated by the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. For instance, a rule may indicate that the media stream data is to be sent to the gateway device **206** where processing (e.g., video transcoding, decoding, and/or re-encoding) of the media stream data is to be performed prior to the media stream data being sent to the cloud-based storage media **230**.

[0091] As another example, a rule may indicate that, in order to minimize computational costs, media stream data having a different (e.g., lower) quality is to be sent to the gateway device **206** where computationally intensive analytics are to be performed. As yet another example, a rule may indicate that the media stream data is to be sent to the gateway device **206** so that the latter can control the bandwidth used between the networks **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N and the cloud-based computing infrastructure **106** and, if needed, degrade the quality of some of the media stream data based on predefined criteria.

[0092] In some embodiments, a rule may indicate the manner in which the media stream data is to be routed within the system **100** (e.g., via the gateway device(s) **206** or directly to the cloud-based computing infrastructure **106**), based on a level of interest associated with the media stream data. As used herein, the term "level of interest" may relate to the degree to which the media stream data is of interest (e.g., deemed pertinent for an investigation or search that may be in progress), or suspected to be of interest (e.g., by the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y capturing the media stream data, by a further downstream device, etc.), to user(s) of the surveillance system **100** (e.g., security personnel). The level of interest associated with the media stream data may be determined subsequent to obtaining the one or more rules. For example, any component of the system **100** (e.g., the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, the one or more gateway devices **206**, and/or the client device(s) **216**) making decisions on routing the media stream data may be provided (e.g., by another component of the system **100**) with one or more rules for use in determining whether the media stream data is of interest. It should however be understood that, it may be possible, in some embodiments, for the level of interest to be determined prior to obtaining the one or more rules. In other embodiments, the level of interest may be determined in parallel with (e.g. simultaneously to) obtaining the one or more rules. The system component making decisions on routing the media stream data may indeed be provided with one or more rules indicating condition(s) to evaluate in order to determine whether the media stream data is of interest and the manner in which to route the media stream data of interest. For example, a rule such as "If you see a blue car, route this video to the cloud" (which indicates that blue cars are of interest and that routing is to be done to the cloud computing server **228** if the media stream data depicts blue cars) may be provided.

[0093] As will be described further below, various criteria may be evaluated, separately or in combination, to determine whether the media stream data is of interest. This determination may be performed by any suitable component of the system **100** (e.g., the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, the one or more gateway devices **206**, and/or the client device(s) **216**). In other words, different devices within the system **100** may be responsible for determining whether a particular media stream data is of interest or not. In some instances, a given media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . ,

204.sub.Y may be responsible for this determination while, in other instances, a given gateway device **206**, a client device **216**, or another device present on the local network **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N or part of the cloud-based computing infrastructure **106** may be responsible for this determination.

[0094] In some embodiments, a first component of the system **100** may make a first level (or preliminary) determination (e.g., based on a first set of conditions or rules) as to whether the particular media stream data is of interest or not and may send the particular media stream data, along with the first level determination, to a second component of the system **100** which may evaluate additional conditions or rules to complete the determination (i.e. may a second level or final determination). Indeed, the rules that determine which media stream data is of interest may have multiple conditions that are to be evaluated. For example, the media stream data may be considered to be of interest if the media stream data corresponds to video captured at night and indicative of motion of more than a given number of objects, for a time period exceeding a given amount of time. The first system component may then be a media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y that evaluates whether the particular media stream data is indicative of motion of one or more objects present within the media device's field of view, or whether the particular media stream data was captured at a time of day of interest (e.g., in the evenings or during business hours). The second system component may be a gateway device **206** that further evaluates, from the particular media stream data, whether the detected motion indicates that the one or more objects are of interest, or whether the number of objects present within the media device's field of view exceeds a given threshold. In some embodiments, the determination as to whether the media stream data is of interest may be optimized by, using the first level determination, to identify certain media stream data as not being of interest based on one condition (amongst the multiple conditions to be evaluated) not being met. For instance, the first system component may determine that the particular media stream data is not indicative of any motion, causing the particular media stream data to be flagged as not being of interest.

[0095] In some embodiments, media stream data may be considered to be of interest retroactively, based on any of the indicators described herein. In such a case, part or all of media stream data which was not previously considered to be of interest is, at a later time, considered to be of interest based on the occurrence of any of the indicators described above. Indicating that the media stream data is now of interest can involve setting a metadata flag or similar variable associated with the media stream data to an appropriate value indicating that the media stream data is of interest. This may occur at any location within the surveillance system **100** at which the media stream data is stored, whether temporarily or permanently. By way of an example, first media stream data may capture imagery of a storefront, and second media stream data may capture imagery of a parking lot adjacent to the storefront. When an altercation occurs in the parking lot, the second media stream data is deemed of interest based on any number of existing parameters (e.g., the presence or number of vehicles after closing hours, the speed of movement of the vehicles, the actions of persons, etc.). Although the scene depicted in the first media stream data may not itself be of interest—for instance, the number of vehicles or persons, their speed or actions, etc., may not result in the video being initially deemed of interest—the second media stream data being deemed of interest may cause the first media stream data to retroactively be deemed of interest. In this example, the first media stream data may be deemed of interest to facilitate determining the comings and goings of individuals and/or vehicles involved in the altercation depicted in the second media stream data. The level of interest in the first media stream data may therefore be dependent or conditional on the level of interest in the second media stream data. The preceding example should be considered to be one illustrative example, and not limiting of the ways by which a particular media stream data is retroactively determined to be of interest.

[0096] The component of the system **100** which is responsible for determining whether the particular media stream data is of interest may process (e.g., conduct a video analysis or any other

suitable analysis) the media streams (e.g., the media stream data) generated by each media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. The level of interest associated with the media stream data may then be determined based on an outcome of the processing (e.g., video analysis). Processing (e.g., conducting an analysis) of the media stream data may result in generation of metadata that may comprise, but is not limited to, metadata items about the media stream itself (e.g., data format, resolution, time of capture, location of capture, media device used for capture, and the like) or metadata items about the contents of the media stream, including metadata items relating the presence of object(s) in the media stream (e.g., object type, object color, object location in the field of view of the media device, object direction of movement, object speed of movement, and the like), metadata items relating environmental factors visible in the media stream (e.g., weather type, lighting conditions, disaster elements, and the like), or other metadata items. Some metadata items may be used to derive other metadata items. For example, a succession of object location metadata items (i.e. successive locations of an object in the media device's field of view over a given period of time) may be used to determine the object's speed of movement.

[0097] While reference is made herein to metadata being generated based on the analysis of the media stream data, it should be understood that each media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may (instead or additionally) be configured to directly provide the metadata to the component of the system **100** that is configured to determine whether the media stream data is of interest. The metadata may be provided by each media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y along with (e.g., as part of) or separate from the media streams generated by the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. The system component may then be configured to obtain the metadata (e.g., extract the metadata from the media streams) and determine based thereon whether the media stream data is of interest. In other cases, each of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may be configured to provide an indication that the generated media stream data is of interest. Such an indication may, for instance, be provided (e.g., contained) in the media streams generated by the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. As a result, the need for performing a video analysis of the media stream data may be alleviated.

[0098] It should however be understood that, in some embodiments, the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may only be configured to generate part of the metadata used to determine whether the media stream data is of interest. In yet other embodiments, the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may not be configured to generate any of the metadata. This may be the case, for example, when the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y have limited processing power or do not have the necessary tools (hardware and/or software) to produce analytics and generate metadata. In this case, the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may then provide the media stream data they have generated, alongside any metadata they may be able to produce, to another device present on the local network **102**.sub.1, **102**.sub.2, . . . , **102**.sub.N (e.g., another media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, a gateway device **206**, or a client device **216**). The other device may then analyze (e.g., perform video analysis of) the media steam data to generate metadata relating to the content of the media stream data.

[0099] Any suitable component of the system **100** (e.g., the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, the one or more gateway devices **206**, and/or the client device(s) **216**) may then use the metadata to determine whether the media stream data is of interest. It should be understood that the evaluation of the metadata and the evaluation of the level of interest in the media stream data may both be performed at the same time (i.e.

concurrently) and/or by a same component of the system **100**, which may result in an optimization.

[0100] In one embodiment, the media stream data may be considered to be of interest based on the metadata satisfying a time restriction. In particular, the media stream data may be considered to be of interest if it is determined (e.g., based on the time of capture metadata item) that the media stream data was generated during a target timeframe (i.e. a time period of interest), such as during business hours, during off-peak periods (e.g., on the weekends), in the evenings, or the like.

[0101] In another embodiment, the media stream data may be considered to be of interest based on the metadata satisfying a location restriction. For example, the media stream data may be considered to be of interest if it is determined (e.g., based on the location of capture metadata item) that the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . **204**.sub.Y that generated the media stream data is positioned at a specific location deemed to be of interest to the user(s) of the surveillance system **100**. This may be the case when the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y is a mobile camera (e.g., a body-worn camera or "bodycam") that uses a positioning system or device (e.g., a Global Position System-GPS-sensor incorporated therewith) to determine that the camera is at a particular location which makes the video captured by the camera of interest. In another example, the media stream data may be considered to be of interest depending on the regions or zones depicted by the media stream data (e.g., if it is determined, based on the metadata, that the media stream data depicts a doorway or other zone or region deemed to be of interest to the user(s)). The location may be determined by way of a global positioning system (GPS) or similar technology, by recognition of certain landmarks or the like visible in the media stream data, or by proxy. For example, a camera name, IP address, or other information may indicate that the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y is looking at a door, an entrance, or the like, and may be used as the location, region, or zone associated with the media data stream.

[0102] In another embodiment, the media stream data may be considered to be of interest based on the status of the surveillance system **100**. For example, the media stream data may be considered of interest if it is determined (e.g., based on the metadata) that the media stream data was generated by the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and/or **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y in response to occurrence of a trigger event, which may or may not be an isolated event. The trigger event may include, but is not limited to, a system-initiated command, a user-initiated command (e.g., upon a user providing via the I/O device(s) **224** of their client device **216** instructions for the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y to generate the media stream data), an alert or alarm (e.g., indicative of a threat level) was triggered by a component of the surveillance system (e.g., by client device(s) **216**) or a third-party system (e.g., a system configured to manage the surveillance system **100**), a trigger event associated with one or more of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and/or **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, or the like. For example, a motion sensor disposed within an establishment may be armed upon closing of the establishment. When the motion sensor is later tripped by the presence of an unauthorized person within the establishment, this may raise an alarm within the broader security system at the establishment, which includes the surveillance system **100**. In response to the alarm being raised, all video captured by media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and/or **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y may be treated as video of interest.

[0103] In yet another embodiment, the media stream data may be considered to be of interest based on an analysis of the content present in the field of view of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X and/or **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. For example, the media stream data may be considered to be of interest upon identifying one or more objects in the devices' field of view. Any suitable technique may be used to identify the one or more objects present in the device's field of view. The identified object(s) may also be classified (e.g., into different categories such as person, vehicle, building, and the like) using any suitable technique. Such classification may either

be performed by a given media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, such that the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y sends the media stream data along with object classification metadata associated therewith. Alternatively, the media stream data may be received from the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y without any object classification metadata and the object classification analysis may then be performed by a device (e.g., at the gateway device **206** or at the cloud computing server **228**) other than the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y having generated the media stream data. For example, an object detection algorithm may be used to produce metadata relating to the presence and action of objects detected in part or all of the media stream data (the metadata may be structured according to a particular metadata standard, for instance ONVIF® Profile M). Such an object detection algorithm may be provided in the component of the system **100** (e.g., the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, the one or more gateway devices **206**, and/or the client device(s) **216**) configured to generate metadata which may then be used to determine whether the media stream data is of interest. As such, any one of the components of the system **100** may be provided with suitable computational resources and software capabilities for implementing the object detection algorithm. The detection of any suitable object may result in a video being determined as being of interest, and the one or more detected objects may be objects being queried (e.g., under investigation by user(s) of the surveillance system **100**) or not. The objects may, for example, include vehicles having given attribute(s) (e.g., type, color, make, model, etc.) and/or being vehicles of interest (e.g., license plate identifier matches a hitlist). The objects may also include persons performing specific action(s), exhibiting specific behavior(s), fitting a given description, and/or having given attribute(s) such as physical characteristic(s) (e.g., height, hair color, eye color, etc.), physical appearance (e.g., type of clothing, color of clothing, type of shoes, colors of shoes, glasses, tattoos, scars, carried objects, and any other identifying mark), or the like. The objects may also include registered persons of interest (e.g., registered criminals). Other embodiments may apply.

[0104] The media stream data may further be considered to be of interest upon detection of a given number of objects in the devices' field of view. The number of objects may be determined using any suitable counting (e.g., people counting) or estimation technique. The media stream data may be considered to be of interest if the number of objects present in the devices' field of view is beyond (e.g., exceeds) a predetermined threshold. This may be applicable, for instance, when the allowable number of objects is limited by regulations, governmental or otherwise. For example, the media stream data may be considered to be of interest upon detection that a number of individuals (e.g., attendees at an event) present at a given location (e.g., a room or venue) at a given point in time exceeds the location's occupant capacity (e.g., the location's legal or expected maximum occupancy).

[0105] In addition, the media stream data may be considered to be of interest if movement has been detected in the devices' field of view (i.e. upon detection of moving objects). The media stream data may also be considered to be of interest based on a path or direction of travel of the objects present in the devices' field of view. For example, the media stream data may be considered to be of interest if the metadata is indicative that a vehicle is entering a parking lot at a given time, that an individual is entering a store through the exit rather than through the entrance, or that an individual is walking on a highway or other non-pedestrian road. The media stream data may also be considered to be of interest based on a speed, acceleration, and/or direction of movement of the objects detected in the devices' field of view (e.g., based on the speed being beyond a speed threshold, direction of movement breeching a predefined perimeter or boundary, etc.). For this purpose, once moving objects are detected in the devices' field of view, the speed of the detected objects may be determined. For example, the media stream data may be considered to be of interest upon detection of cars traveling above or below authorized speed limitations for a given location.

[0106] Furthermore, the media stream data may be considered to be of interest upon detection (e.g., based on the metadata and/or analysis of the media stream data) of tampering with the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X and/or 204.sub.1, 204.sub.2, . . . , 204.sub.Y. For example, the media stream data may be considered to be of interest if the metadata and/or the media stream data is indicative of physical vandalism, damage, or theft one or more of the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y. For example, the media stream data may indicate that the field of view of one or more of the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y has been moved or blocked, or that the image or video generated by the one or more media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y has been altered. The metadata and/or media stream data may also be indicative of device downtime or outage, i.e. that the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y are or have been offline (e.g., disconnected from the local network 102.sub.1, 102.sub.2, . . . , 102.sub.N and/or the cloud-based computing infrastructure 106) for a given period of time. In some cases, the field of view of a media device 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y may be determined by comparing an expected background of the image with a current background or image: when a current background or image departs from an expected background by a certain amount, for instance for a duration of time exceeding a particular threshold, or the like, this may indicate an attempt to block the field of view of view of the media device 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y. Other approaches are also considered.

[0107] It should be understood that the examples of rules provided herein are for the purpose of illustration and that other embodiments may apply, depending on the application. For example, in some embodiments, the determination of certain media stream data as being of interest is based on deviation of the content of the media stream data from expected content or from relevant past content. For instance, when media stream metadata indicates motion within the field of view of the media device 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y capturing the media stream data at certain times of the day, at certain locations, or the like, this may be unexpected and thus be indicative of the media stream data being of interest. In another instance, when media stream metadata indicates a number of persons within the field of view of the media device 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y capturing the media stream data far exceeding an average number of people captured in previous media streams from the same media device 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y (e.g., more than a predetermined number of standard deviations beyond the average), this may be a deviation from the past video and thus be indicative of the media stream data being of interest.

[0108] In one embodiment, the rule(s) are stored in the cloud-based storage media 230. The cloud computing server 228 may therefore access the cloud-based storage media 230 to retrieve the rule(s) and determine the routing to be performed based on evaluation of the rule(s). For example, the cloud computing server 228 may be configured to evaluate rules such as whether media stream data is considered to be of interest, whether a network storage (e.g., storage media 214) is full, whether the connection between the cloud-based computing infrastructure 106 and the second media devices 204.sub.1, 204.sub.2, . . . , or 204.sub.Y is of low quality, and the like. It should however be understood that, in some embodiments, it may be beyond the configuration of the cloud computing server 228 to evaluate rules specific to the local 102.sub.1 network. For example, the cloud computing server 228 may not evaluate rules related to whether there is congestion on the local network 102.sub.1. Alternatively, when routing is performed by a networked device 104 placed on the network 102.sub.1 (e.g. by the gateway device 206 or a second media device 204.sub.1, 204.sub.2, . . . , or 204.sub.Y), the networked device 104 may send a request for the rule(s) to the cloud computing server 228. The cloud computing server 228 retrieves the rule(s)

from the cloud-based storage media **230** and transmits the retrieved rule(s) to the requesting entity (e.g. the gateway device **206** or second media device **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y) which then applies the rule(s) to determine the routing to be performed.

[0109] In another embodiment, the rule(s) are stored in memory or storage placed on the local network **102**.sub.1 and may be obtained (i.e., retrieved) by a networked device **104** placed on the network **102**.sub.1 (e.g. by a given gateway device **206** or a second media device **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y). For instance, the rule(s) may be stored in the memory **210** of a given gateway device **206**, in local storage of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, or in the storage media **214** accessible to the given gateway device **206** and to the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. The given gateway device **206** may then access the memory **210**, the storage media **214**, or the memory **222** to obtain (i.e. retrieve) the rule(s). The given gateway device **206** may then evaluate the rule(s) to determine the routing to be performed. In embodiments where an entity other than the given gateway device **206** (e.g., a second media device **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y) is configured to evaluate the rule(s) to determine the routing, the given gateway device **206** may then transmit (using any suitable communication means) the retrieved rule(s) to this entity.

[0110] In yet other embodiments, the rule(s) may be stored in storage media (not shown) accessible to a device placed on the local network **102**.sub.1 (e.g., a gateway device **206**, or a second media device **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y) and the given local device may access the storage media to retrieve the rule(s), which are in turn transmitted (using any suitable communication means) to the entity (e.g., the cloud computing server **228**, a given gateway device **206**, or a second media device **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y) configured to evaluate the rule(s) for implementation of the routing. A request for the rule(s) may therefore be sent (e.g. by the cloud computing server **228**, the given gateway device **206**, or the second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y) to the given local device and the given local device may in turn transmit the rule(s) in response to the request.

[0111] Once the at least one rule has been obtained, the gateway device **206**, the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y, or the cloud-computing server **228** assesses whether the at least one rule is satisfied and applies the at least one rule (when satisfied) for routing the media stream data according to the rule. For any given device of the system **100** (e.g. the cloud computing server **228**, the given gateway device **206**, or the second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y), applying a rule may entail actively routing the media stream data from its source to its final destination or sending instructions to another component of the system **100** to cause the media stream data to be routed. For example, the second media device **204**.sub.1, **204**.sub.2, . . . , or **204**.sub.Y may be configured to actively route its media stream data (or that generated by one or more other media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y) to its final destination in order to apply the at least one rule. The cloud computing server **228** and the given gateway device **206** may be configured to instruct a media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y to route its media stream data (or that generated by one or more other media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y) to its final destination in order to apply the at least one rule.

[0112] In some embodiments, to assess whether the at least one rule is satisfied, the gateway device **206**, the media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, and/or the cloud-computing server **228** monitors one or more parameters associated with the networks **102**.sub.1, **102**.sub.2, . . . , and **102**.sub.N, with the cloud-based infrastructure **106**, and/or with the environment of the location being surveilled. The parameters associated with the network **102**.sub.1 and the cloud-based infrastructure **106** include, but are not limited to, performance which may encompass bandwidth, latency, error rate, and other measures indicative of network quality

and connectivity, as well as cost-consideration parameters and parameters associated with cloud provider agreements, such as a monthly cloud data cap, a current capacity of cloud resources (e.g., evaluated in real-time), cloud-metering parameters, and the like. The parameters associated with the environment include, but are not limited to, a time of day, a current weather at the location, a visibility level at the location, a positioning of the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y within the environment, and a field of view of the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y.

[0113] In some embodiments, to assess whether the at least one rule is satisfied, the gateway device 206, the media device 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y, and/or the cloud-computing server 228 monitors metadata associated with the media stream data to determine whether the media stream data is of interest. This may be based on the presence of one or more objects (e.g., individuals, vehicles, or the like) within the field of view of the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y, the degree and/or type of motion of the objects present within the field of view of the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y, the detectability of environmental factors within the field of view of the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y, or any other number of factors. For example, a rule indicating that the analysis of the media stream data is to be performed at a given time of day (e.g., in the evenings or during business hours) is only satisfied when the time of day parameter is met. By way of another example, a rule indicating that media stream data should be stored redundantly based on the presence of a certain number of persons visible in the field of view is only satisfied when video analytics determine that the threshold of number of persons visible in the field of view is met.

[0114] When it is determined, based on monitoring the parameter(s) described herein, that the at least one rule is satisfied, the at least one rule is applied (e.g., by the cloud computing server 228, the given gateway device 206, or the second media device 204.sub.1, 204.sub.2, . . . , 204.sub.Y) to route the media stream data. For example, applying the at least one rule may involve transmitting the media stream data to the gateway device(s) 206 for buffering in the local storage media 214. Applying the at least one rule may alternatively involve transmitting, via the gateway device(s) 206, the media stream data to the cloud computing server 220 for storage in the cloud-based storage media 230. In yet other embodiments, applying the at least one rule may involve transmitting the media stream data directly to the cloud computing server 220 for storage in the cloud-based storage media 230. For example, the media stream data may be sent directly from one or more of the media devices 204.sub.1, 204.sub.2, . . . , 204.sub.Y to the cloud-based computing infrastructure 106. The media stream data may also be sent directly from the gateway device(s) 206 to the cloud-based computing infrastructure 106. In some embodiments, applying the at least one rule may involve sending the media stream data to both the local storage media 214 and the cloud-based storage media 230 for redundant archiving. In other embodiments, applying the at least one rule may involve continuously transmitting the media stream data (e.g., in real-time) to the local storage media 214 and/or the cloud-based storage media 230 for storage over a pre-determined time period.

[0115] Applying the at least one rule may further involve pre-processing the media stream data prior to transmission thereof (e.g. to the local storage media 214 and/or the cloud-based storage media 230 for archiving). Such pre-processing may be performed using any suitable technique and may include, but is not limited to, modifying a quality of the media stream data, video transcoding the media stream data, decoding the media stream data, re-encoding the media stream data, applying at least one overlay on the media stream data, applying a privacy mask on the media stream data, digitally signing the media stream data, encrypting the media stream data, performing color correction on the media stream data, adding metadata to the media stream data (e.g., to indicate a time at which the media stream data was generated), and identifying, based on the media

stream data, one or more objects present in a field of view of the one or more media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y that generated the media stream data. For example, pre-processing may involve modifying the quality of the media stream data such that a different quality stream is sent to the gateway device 206. The at least one rule may further indicate that such intensive video analytics may only be required when an object detection algorithm (built in the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y) detects an object of interest in the media stream data. As previously noted, according to one rule, the object detection algorithm may be used to determine whether the media stream data is of interest prior to routing thereof. Similarly, other rules based on other metadata associated with a media stream may also dictate how certain media stream data are routed. As also previously noted, video footage may be sent to the gateway device 206 so that the gateway device 206 may control the bandwidth used between the local network 102.sub.1 and the cloud-based computing infrastructure 106 and, if needed, degrade the quality of some video streams based on predefined criteria. Moreover, video footage may be sent to the gateway device 206 for the latter to perform video transcoding and/or perform any other activity that would involve decoding and/or re-encoding of the stream (e.g., applying overlays or a privacy mask or digitally signing the video before it leaves the premises). Other embodiments may apply.

[0116] In some embodiments, the media stream data is routed within the system 100 in real-time (i.e. at substantially the same time as it is generated by the media devices 202.sub.1, 202.sub.2, . . . , 202.sub.X and/or 204.sub.1, 204.sub.2, . . . , 204.sub.Y). In other embodiments, routing of the media stream data is delayed (i.e. the media stream data is not routed in real-time). For example, the system 100 may receive (e.g., from a user, via their client device 216) a request for video playback. In this case, one or more conditions (network, level of interest, etc.) described herein are evaluated to assess where the video playback is to be sourced from and the manner in which to route the video playback. Any suitable component of the system 100 (e.g., a media device 202.sub.1, 202.sub.2, . . . , 202.sub.X, 204.sub.1, 204.sub.2, . . . , 204.sub.Y, a gateway device 206, or the cloud computing server 228) may evaluate one or more parameters associated with the networks 102.sub.1, 102.sub.2, . . . , and 102.sub.N and/or with the cloud-based infrastructure 106, including, but not limited to, the transcode capacity or the resolution requested versus the resolution stored in memory. Additionally, in some cases the request for playback may also be associated with a level of interest (which may be an indication of the priority level of the user requesting playback, or the like) which may be used in determining how to treat the request. Based on the outcome of the evaluation (e.g., based on network conditions, or on other conditions), the system component may then retrieve the media stream data corresponding to the requested video playback from the appropriate source (e.g., from the memory 222, the memory 210, the storage media 214, and/or the storage media 230) for subsequent routing to the requesting entity.

[0117] It should be understood that both network conditions (or parameters) and interest level, as described herein above, in the media stream data may be used to determine the manner in which to route the media stream data. For example, the system 100 may determine that it has media stream data of interest that should be routed for additional processing to a gateway device 206. However, the network conditions may indicate that the gateway device 206 is currently operating at full capacity or is overloaded. In such a case, the routing rules may then dictate that the media stream data is to be routed to the cloud-based computing infrastructure 106 (e.g., to the cloud computing server 228) for processing there. Of course, other situations in which both network conditions and a level of interest in the media stream data are evaluated to affect routing decisions are also considered. For instance, the system 100 may be managing multiple different media stream data which place a certain strain on the system 100, and may prioritize routing of a first media stream data over another depending on the level of interest of the first media stream data, and how elements of the system 100 are occupied in routing and/or processing the other media stream data.

[0118] In some embodiments, when it is determined, based on monitoring the parameter(s), that the

at least one rule is not satisfied and is therefore not applicable, a default (or fallback) rule may be applied instead of the rule previously obtained. Default rules may apply to all devices on the network **102**.sub.1, **102**.sub.2, . . . , and **102**.sub.N and any suitable default rule may apply. For example, the rule previously obtained (e.g., retrieved) may indicate that the media stream data is to be archived for a predetermined time period in order to comply with governmental regulations. However, the outcome of the monitoring of the parameters associated with the networks **102**.sub.1, **102**.sub.2, . . . , and **102**.sub.N may indicate that the entirety of the media stream data cannot be archived for the predetermined time period (e.g., due to a change in quality of stored video, to the addition of new media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, to the fact that the local storage media **214** does not have sufficient storage capacity, or the like). In this case, the default rule may indicate that part of the media stream data is to be archived in the local storage media **214** and part of the media stream data is to be archived in the cloud-based storage media **230**. This would ensure that the media stream data is archived for the required time period. The default rule may also comprise instructions to output an alert (via any suitable communications means) to indicate the lack of sufficient local storage to meet the original requirements of the retrieved rule, to suggest to a user of the system **100** to expand the size of the local storage (e.g., of the local storage media **214**), and/or to get the user to consent to using the cloud-based storage media **230** to supplement the local storage. Other examples of default rules include, but are not limited to, always routing media stream data for storage in the local storage media **214**, storing a copy of all media stream data in the cloud-based storage media **230**, always retaining (i.e. storing) the media stream data for a predetermined number of days (e.g., 30, 90, or 180 days) required by local regulations, redundantly storing the media stream data, and performing a base level of video analytics on all media stream data to produce a base level of analytics-based metadata. It should be understood that other default rules may apply, depending on the application. It should also be understood that different default rules may apply depending on the time of day. For example, default rules may require to always run additional analytics on daytime video, save weekday video for a longer period of time, and the like. Moreover, different default rules may apply for different media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y, different media device locations, and the like. For example, a default rule may require to always run additional analytics on media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y positioned so as to be facing doors and other entryways.

[0119] Referring now to FIG. **3**, a method **300** for routing media in a surveillance system, such as the system **100** of FIG. **1**, will now be described in accordance with one embodiment. The method **300** may be performed by any one of the cloud computing server **228**, a gateway device **206**, or a media device **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , **204**.sub.Y. The method **300** may be performed upon running an application on an operating system (e.g., a mobile operating system such as Android) of a computing device (e.g., a client device **216** of FIG. **2**). The method **300** comprises, at step **302**, detecting one or more networked devices placed on a local network (e.g., network **102**.sub.1 of FIG. **2**) deployed at a location being surveilled. The one or more networked devices may comprise one or more media devices (e.g., video cameras or the like) and one or more gateway devices, each media device being configured to generate media as the location is being surveilled, and each gateway device having network connectivity to a cloud computing device (e.g., the cloud computing server **228** of FIG. **2**). In some embodiments, the method **300** may further comprise a step **303** of obtaining one or more metadata items associated with the media stream data. This may be achieved in the manner described herein above, by conducting an analysis of the content (referred to herein as a "media content analysis") of the media stream data and generating the metadata based on the analysis or by receiving the metadata items from the one or more media devices.

[0120] The method **300** further comprises, at step **304**, determining a level of interest associated with the media stream data. This may be achieved in the manner described herein above with

reference to FIG. **2**, by evaluating one or more criteria, separately or in combination. The level of interest may further be determined based on any metadata items obtained at step **303**. The method **300** then comprises, at step **306**, obtaining at least one rule indicative of when the media stream data is to be routed via the gateway device(s) and when the media stream data is to be routed directly to the cloud computing device, based on the level of interest associated with the media stream data. In some embodiments, the level of interest may be expressed as a binary value: media stream data may be of interest, or may not be of interest. In other embodiments, the level of interest may be expressed on a scale: a video may be of a default interest value, of high interest, of critical interest, etc. Other methodologies are also considered. While step **306** is illustrated and described herein as following step **304**, it should be understood that the order of steps **304** and **306** may be interchanged. Alternatively, steps **304** and **306** may be performed simultaneously. At step **308**, the method **300** comprises routing the media stream data according to the at least one rule based on the level of interest as determined at step **304**.

[0121] FIG. **4** is a schematic diagram of computing device **400**, which may be used to implement the method **300** of FIG. **3** (and/or one or more components of the system **100** of FIG. **1**). In certain embodiments, the computing device **400** is operable to register and authenticate users (using a login, unique identifier, and password for example) prior to providing access to applications, a local network, network resources, other networks, and network security devices. The computing device **400** may serve one user or multiple users.

[0122] The computing device **400** comprises a processing unit **402** and a memory **404** which has stored therein computer-executable instructions **406**. The processing unit **402** may comprise any suitable devices configured to implement the functionality of the method **300** such that instructions **406**, when executed by the computing device **400** or other programmable apparatus, may cause the functions/acts/steps performed by method **300** as described herein to be executed. The processing unit **402** may comprise, for example, any type of general-purpose microprocessor or microcontroller, a digital signal processing (DSP) processor, a central processing unit (CPU), an integrated circuit, a field programmable gate array (FPGA), a reconfigurable processor, other suitable programmed or programmable logic circuits, custom-designed analog and/or digital circuits, or any combination thereof.

[0123] The memory **404** may comprise any suitable known or other machine-readable storage medium. The memory **404** may comprise non-transitory computer readable storage medium, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. The memory **404** may include a suitable combination of any type of computer memory that is located either internally or externally to device, for example random-access memory (RAM), read-only memory (ROM), compact disc read-only memory (CDROM), electro-optical memory, magneto-optical memory, erasable programmable read-only memory (EPROM), and electrically-erasable programmable read-only memory (EEPROM), Ferroelectric RAM (FRAM) or the like. Memory **1004** may comprise any storage means (e.g. devices) suitable for retrievably storing machine-readable instructions **406** executable by the processing unit **402**.

[0124] In some embodiments, the systems and methods described herein may allow to leverage resources locates on premises and in the cloud to optimize costs, network usage, reliability, resiliency, or any other parameter relevant to a hybrid deployment. In particular, the systems and methods described herein may facilitate the opportunistic use of local network resources by cloud cameras, based on a provided set of rules used for dynamic routing of media stream data within a surveillance system. In this fashion, cloud-aware cameras which encounter network issues, local storage issues, or similar challenges that may not be easily resolved within the structure of the cloud-aware camera itself may instead rely on other elements of the local network, of which the cloud cameras were not previously aware.

[0125] In some cases, employing the methods and systems described herein may result in reduced

data loss and/or improved data availability at any given time for a given cloud camera in a hybrid deployment. In some cases, employing the methods and systems described herein may facilitate data redundancy independently of the particular storage capability of a given cloud camera in a hybrid deployment. In some cases, employing the methods and systems described herein may facilitate adherence to legal or regulatory requirements for operators of a cloud camera in a hybrid deployment where the cloud camera itself would not have been capable of adhering to the requirements. In some cases, employing the methods and systems described herein may facilitate cloud streaming of media streams generated by the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y, or otherwise improve cloud availability of the media streams. In some cases, employing the methods and systems described herein may improve failover capabilities of the media devices **202**.sub.1, **202**.sub.2, . . . , **202**.sub.X, **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y. In some cases, employing the methods and systems described herein may assist operators of the surveillance system **100** in better managing costs by enabling the media devices **204**.sub.1, **204**.sub.2, . . . , and/or **204**.sub.Y to employ local resources they may otherwise not have otherwise been aware of.

[0126] The embodiments of the devices, systems and methods described herein may be implemented in a combination of both hardware and software. These embodiments may be implemented on programmable computers, each computer including at least one processor, a data storage system (including volatile memory or non-volatile memory or other data storage elements or a combination thereof), and at least one communication interface.

[0127] Program code is applied to input data to perform the functions described herein and to generate output information. The output information is applied to one or more output devices. In some embodiments, the communication interface may be a network communication interface. In embodiments in which elements may be combined, the communication interface may be a software communication interface, such as those for inter-process communication. In still other embodiments, there may be a combination of communication interfaces implemented as hardware, software, and combination thereof.

[0128] Throughout the foregoing discussion, numerous references have been made regarding servers, services, interfaces, portals, platforms, or other systems formed from computing devices. It should be appreciated that the use of such terms is deemed to represent one or more computing devices having at least one processor configured to execute software instructions stored on a computer readable tangible, non-transitory medium. For example, a server can include one or more computers operating as a web server, database server, or other type of computer server in a manner to fulfill described roles, responsibilities, or functions.

[0129] The foregoing discussion provides many example embodiments. Although each embodiment represents a single combination of inventive elements, other examples may include all possible combinations of the disclosed elements. Thus if one embodiment comprises elements A, B, and C, and a second embodiment comprises elements B and D, other remaining combinations of A, B, C, or D, may also be used.

[0130] The term "connected" or "coupled to" may include both direct coupling (in which two elements that are coupled to each other contact each other) and indirect coupling (in which at least one additional element is located between the two elements).

[0131] The technical solution of embodiments may be in the form of a software product. The software product may be stored in a non-volatile or non-transitory storage medium, which can be a compact disk read-only memory (CD-ROM), a USB flash disk, or a removable hard disk. The software product includes a number of instructions that enable a computer device (personal computer, server, or network device) to execute the methods provided by the embodiments.

[0132] The embodiments described herein are implemented by physical computer hardware, including computing devices, servers, receivers, transmitters, processors, memory, displays, and networks. The embodiments described herein provide useful physical machines and particularly

configured computer hardware arrangements. The embodiments described herein are directed to electronic machines and methods implemented by electronic machines adapted for processing and transforming electromagnetic signals which represent various types of information. The embodiments described herein pervasively and integrally relate to machines, and their uses; and the embodiments described herein have no meaning or practical applicability outside their use with computer hardware, machines, and various hardware components. Substituting the physical hardware particularly configured to implement various acts for non-physical hardware, using mental steps for example, may substantially affect the way the embodiments work. Such computer hardware limitations are clearly essential elements of the embodiments described herein, and they cannot be omitted or substituted for mental means without having a material effect on the operation and structure of the embodiments described herein. The computer hardware is essential to implement the various embodiments described herein and is not merely used to perform steps expeditiously and in an efficient manner.

[0133] Although the embodiments have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the scope as defined by the appended claims.

[0134] Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed, that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized. Accordingly, the examples described above and illustrated herein are intended to be examples only, and the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

Claims

1. A method for routing media in a surveillance system, the method comprising, at a gateway device placed on a local network deployed at a location being surveilled, the gateway device having network connectivity to a cloud computing device: detecting one or more networked devices placed on the local network, the one or more networked devices comprising one or more media devices each configured to generate media stream data as the location is being surveilled; determining a level of interest associated with the media stream data; obtaining, based on the detecting, at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the gateway device and when the media stream data is to be routed directly to the cloud computing device for processing; and instructing, based on the level of interest associated with the media stream data, at least one of the one or more networked devices to route the media stream data according to the at least one rule.

2. The method of claim 1, further comprising conducting a media content analysis of the media stream data and generating one or more metadata items based on the media content analysis, wherein the level of interest associated with the media stream data is determined based on the one or more metadata items.

3. The method of claim 1, further comprising receiving from the one or more media devices one or more metadata items related to the media stream data, wherein the level of interest associated with the media stream data is determined based on the one or more metadata items.

4. The method of claim 1, wherein the media stream data is determined to be of interest one of: based on the media stream data satisfying at least one of a time restriction and a location restriction; and as a result of determining that the one or more media devices generated the media stream data in response to occurrence of a trigger event related to a status of the surveillance

system.

5. The method of claim 2, wherein the media stream data is determined to be of interest at least one of: as a result of detecting, based on the media content analysis, a presence of one or more objects in a field of view of the one or more media devices; and as a result of detecting, based on the media content analysis, a displacement of the one or more objects in a field of view of the one or more media devices.

6. The method of claim 5, further comprising at least one of: determining a speed of the one or more objects, wherein the media stream data is determined to be of interest as a result of determining that the speed of the one or more objects exceeds a speed threshold; and determining a direction of motion of the one or more objects, wherein the media stream data is determined to be of interest based on the direction of motion.

7. The method of claim 1, further comprising monitoring one or more parameters associated with at least one of the local network and an environment of the location being surveilled to determine whether the at least one rule is satisfied, wherein the at least one of the one or more networked devices is instructed to route the media stream data according to the at least one rule when the at least one rule is satisfied.

8. A method for routing media in a surveillance system, the method comprising, at a cloud computing device: detecting one or more networked devices placed on a local network deployed at a location being surveilled, the one or more networked devices comprising one or more media devices and one or more gateway devices, each media device configured to generate media stream data as the location is being surveilled, and each gateway device having network connectivity to the cloud computing device; determining a level of interest associated with the media stream data; obtaining, based on the detecting, at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the one or more gateway devices and when the media stream data is to be routed directly to the cloud computing device for processing; and instructing, based on the level of interest associated with the media stream data, at least one of the one or more networked devices to route the media stream data according to the at least one rule.

9. The method of claim 8, further comprising conducting a media content analysis of the media stream data and generating one or more metadata items based on the media content analysis, wherein the level of interest associated with the media stream data is determined based on the one or more metadata items.

10. The method of claim 8, further comprising receiving from the one or more media devices one or more metadata items related to the media stream data, wherein the level of interest associated with the media stream data is determined based on the one or more metadata items.

11. The method of claim 8, wherein the media stream data is determined to be of interest one of: based on the media stream data satisfying at least one of a time restriction and a location restriction; and as a result of determining that the one or more media devices generated the media stream data in response to occurrence of a trigger event related to a status of the surveillance system.

12. The method of claim 9, wherein the media stream data is determined to be of interest at least one of: as a result of detecting, based on the media content analysis, a presence of one or more objects in a field of view of the one or more media devices; and as a result of detecting, based on the media content analysis, a displacement of the one or more objects in a field of view of the one or more media devices.

13. The method of claim 12, further comprising at least one of: determining a speed of the one or more objects, wherein the media stream data is determined to be of interest as a result of determining that the speed of the one or more objects exceeds a speed threshold; and determining a direction of motion of the one or more objects, wherein the media stream data is determined to be of interest based on the direction of motion.

14. The method of claim 8, further comprising monitoring one or more parameters associated with at least one of the local network and an environment of the location being surveilled to determine whether the at least one rule is satisfied, wherein the at least one of the one or more networked devices is instructed to route the media stream data according to the at least one rule when the at least one rule is satisfied.

15. A method for routing media in a surveillance system, the method comprising, at one of a plurality of media devices placed on a local network deployed at a location being surveilled: detecting one or more networked devices placed on the local network, the one or more networked devices comprising one or more gateway devices, each media device from the plurality of media devices configured to generate media stream data as the location is being surveilled, and each gateway device having network connectivity to a cloud computing device; determining a level of interest associated with the media stream data; obtaining, based on the detecting, at least one rule from at least one of the cloud computing device and the one or more gateway devices, the at least one rule indicative of when the media stream data is to be routed, based on the level of interest associated with the media stream data, via the one or more gateway devices and when the media stream data is to be routed directly to the cloud computing device for processing; and routing, based on the level of interest associated with the media stream data, the media stream data according to the at least one rule.

16. The method of claim 15, further comprising conducting a media content analysis of the media stream data and generating one or more metadata items based on the media content analysis, wherein the level of interest associated with the media stream data is determined based on the one or more metadata items.

17. The method of claim 15, wherein the media stream data is determined to be of interest one of: based on the media stream data satisfying at least one of a time restriction and a location restriction; and as a result of determining that the plurality of media devices generated the media stream data in response to occurrence of a trigger event related to a status of the surveillance system.

18. The method of claim 16, wherein the media stream data is determined to be of interest at least one of: as a result of detecting, based on the media content analysis, a presence of one or more objects in a field of view of the one or more media devices; and as a result of detecting, based on the media content analysis, a displacement of one or more objects in a field of view of the one or more media devices.

19. The method of claim 18, further comprising at least one of: determining a speed of the one or more objects, wherein the media stream data is determined to be of interest as a result of determining that the speed of the one or more objects exceeds a speed threshold; and determining a direction of motion of the one or more objects, wherein the media stream data is determined to be of interest based on the direction of motion.

20. The method of claim 15, further comprising monitoring one or more parameters associated with at least one of the local network and an environment of the location being surveilled to determine whether the at least one rule is satisfied, wherein the media stream data is routed according to the at least one rule when the at least one rule is satisfied.