Provisional Application for United States Patent

TITLE: The technology to improve protection of private data for using in visual surveillance systems in which data are transmitted through the Internet or other publicly accessible networks.

INVENTOR(S): Dmitry Morozov

FIG. 1

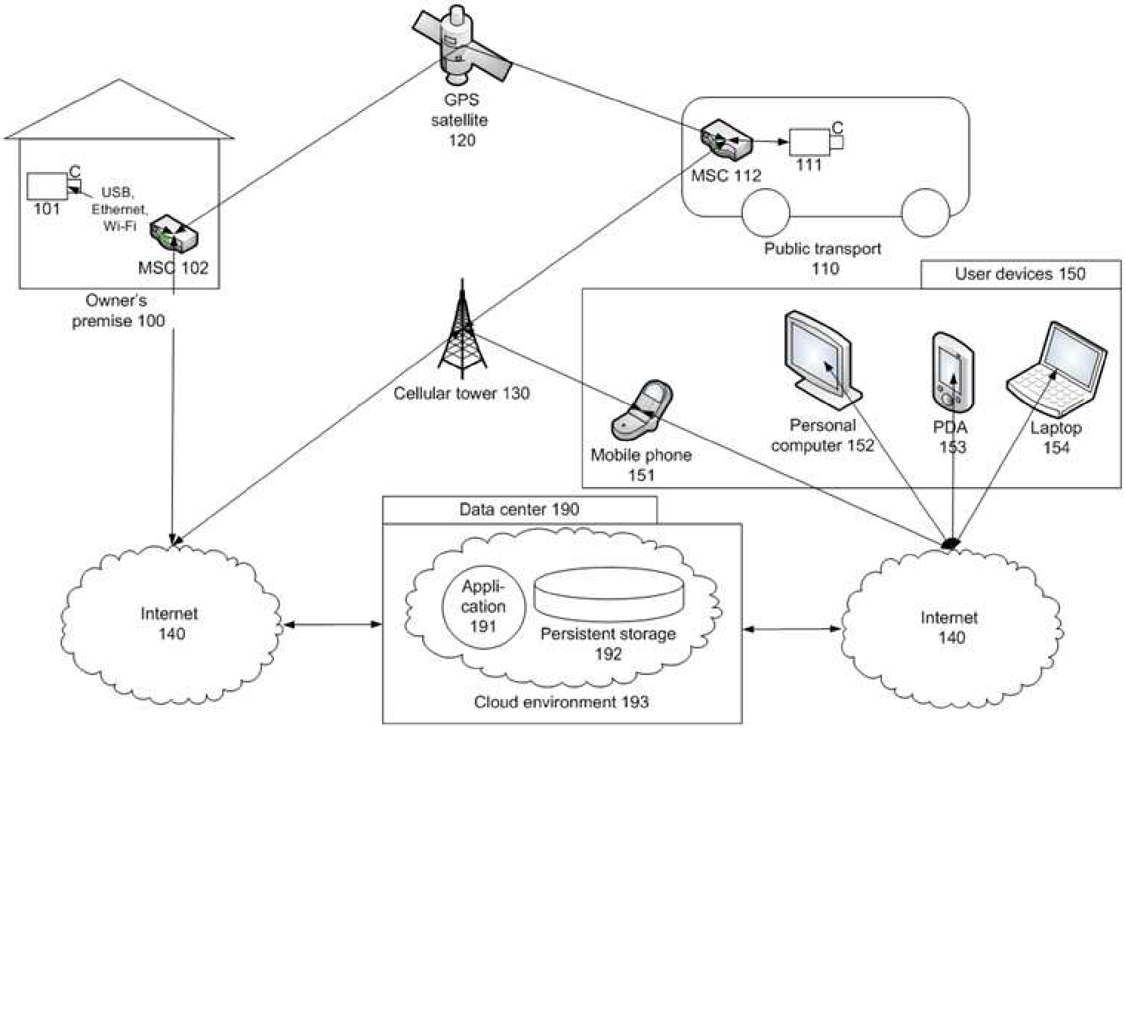


FIG. 2

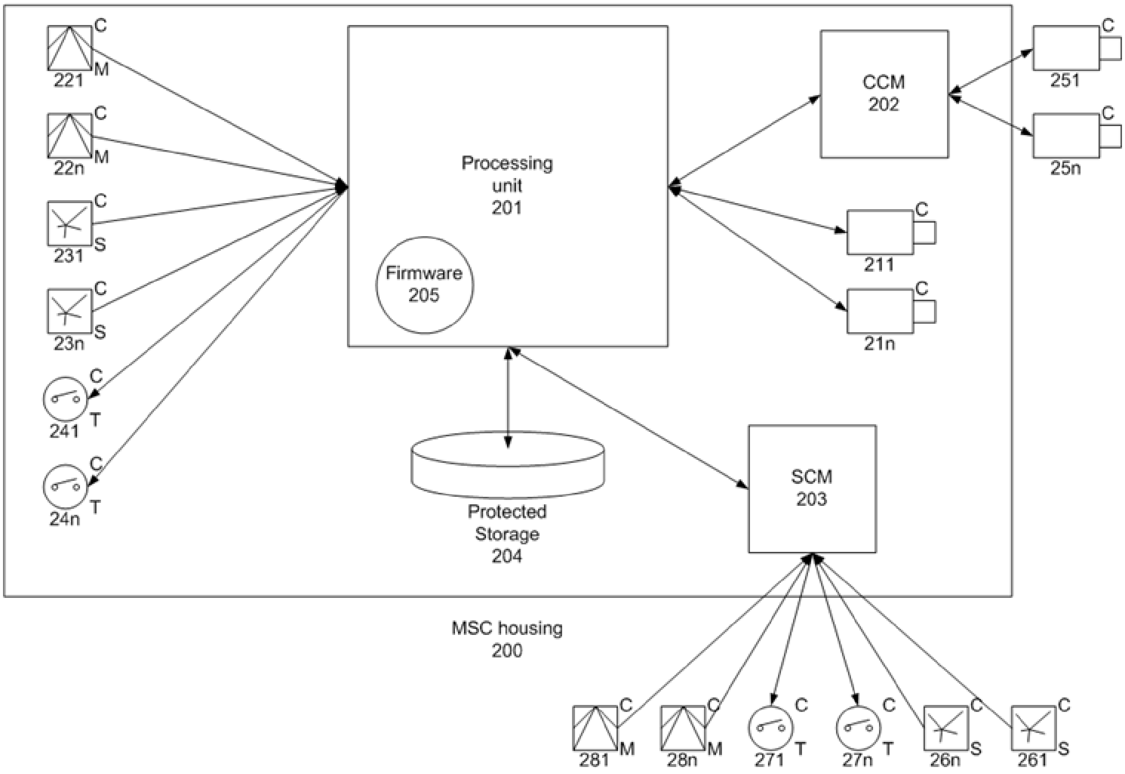

Processing unit 201
Firmware 205
CCM 202
SCM 203
Protected Storage 204
MSC housing 200
221 C M
22n C M
231 C S
23n C S
241 C T
24n C T
211 C
21n C
251 C
25n C
281 C M
28n C M
271 C T
27n C T
26n C S
261 C S

FIG. 3

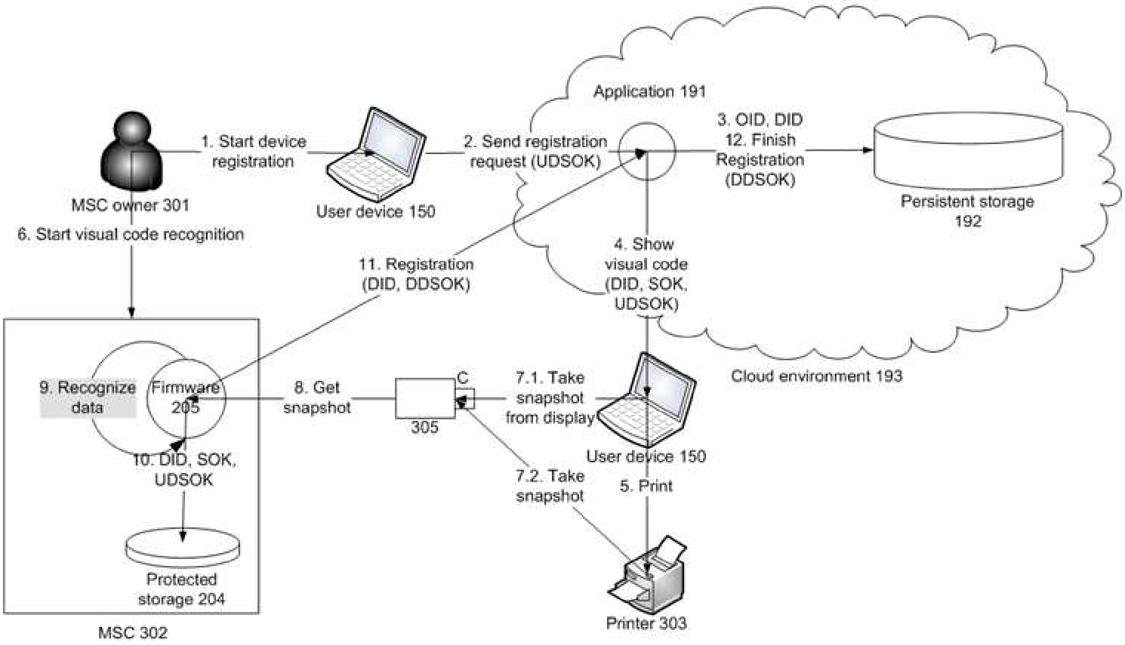

Application 191
MSC owner 301
1. Start device registration
User device 150
2. Send registration request (UDSOK)
3. OID, DID
12. Finish Registration (DDSOK)
Persistent storage 192
6. Start visual code recognition
4. Show visual code (DID, SOK, UDSOK)
11. Registration (DID, DDSOK)
Cloud environment 193
9. Recognize data
Firmware 205
8. Get snapshot
C
305
7.1. Take snapshot from display
User device 150
10. DID, SOK, UDSOK
7.2. Take snapshot
5. Print
Protected storage 204
Printer 303
MSC 302

FIG. 4

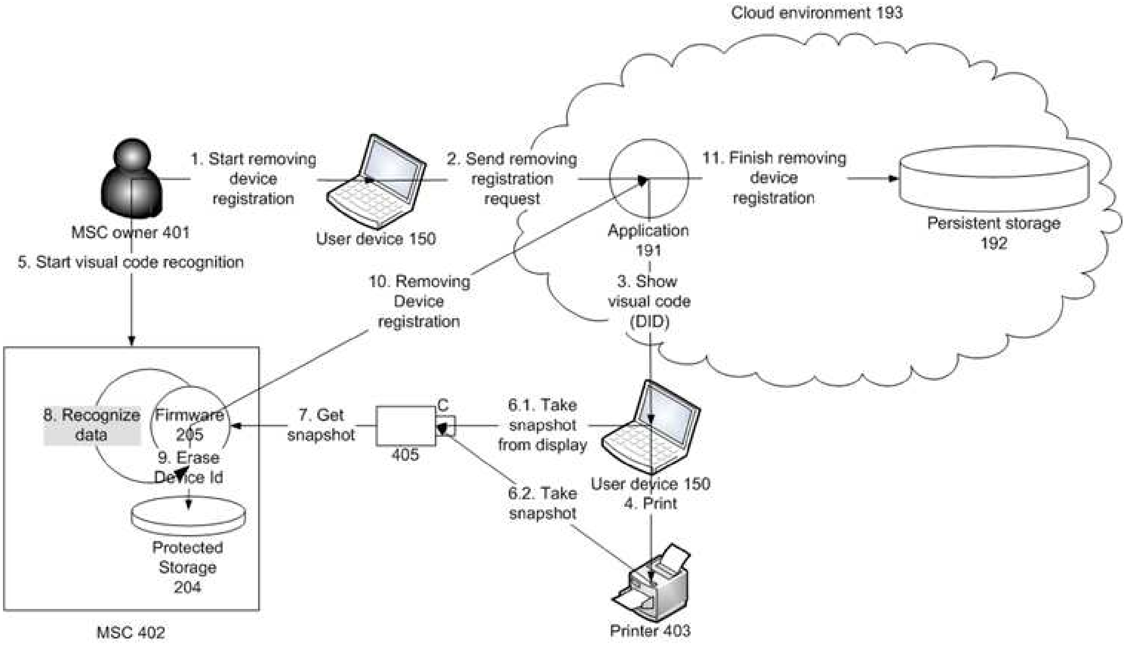

Cloud environment 193
1. Start removing device registration
2. Send removing registration request
11. Finish removing device registration
MSC owner 401
User device 150
Application 191
Persistent storage 192
5. Start visual code recognition
10. Removing Device registration
3. Show visual code (DID)
8. Recognize data
Firmware 205
9. Erase Device Id
7. Get snapshot
C
405
6.1. Take snapshot from display
6.2. Take snapshot
User device 150
4. Print
Protected Storage 204
MSC 402
Printer 403

FIG. 5

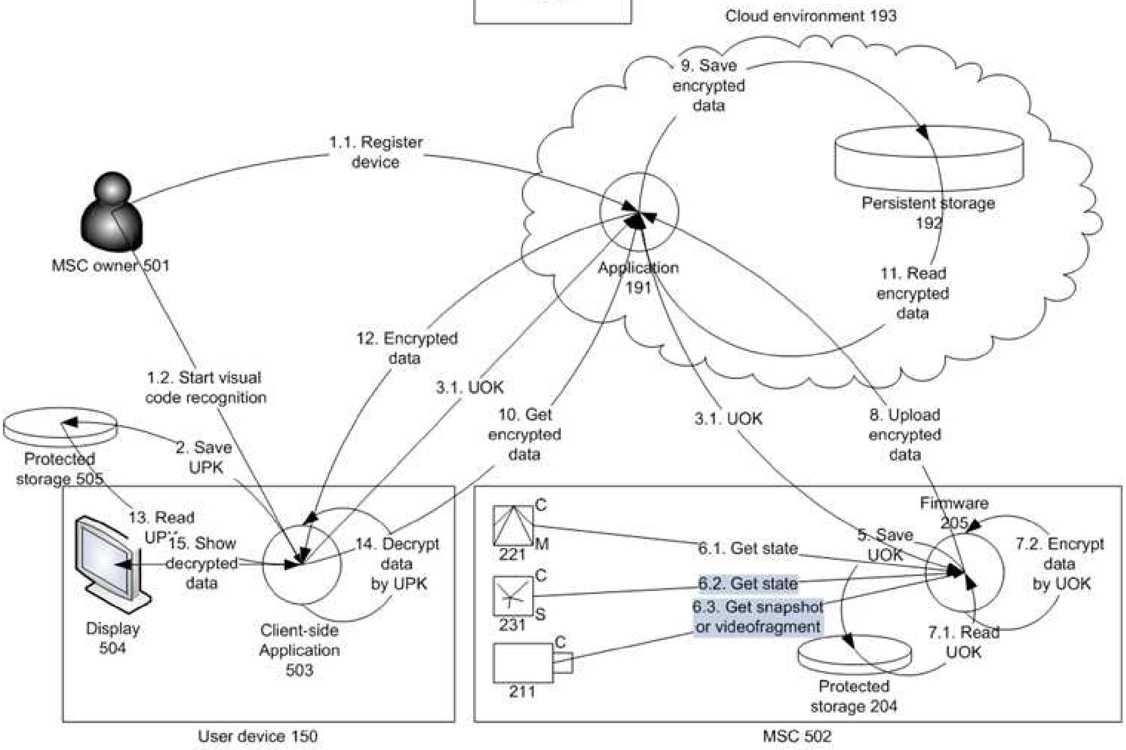
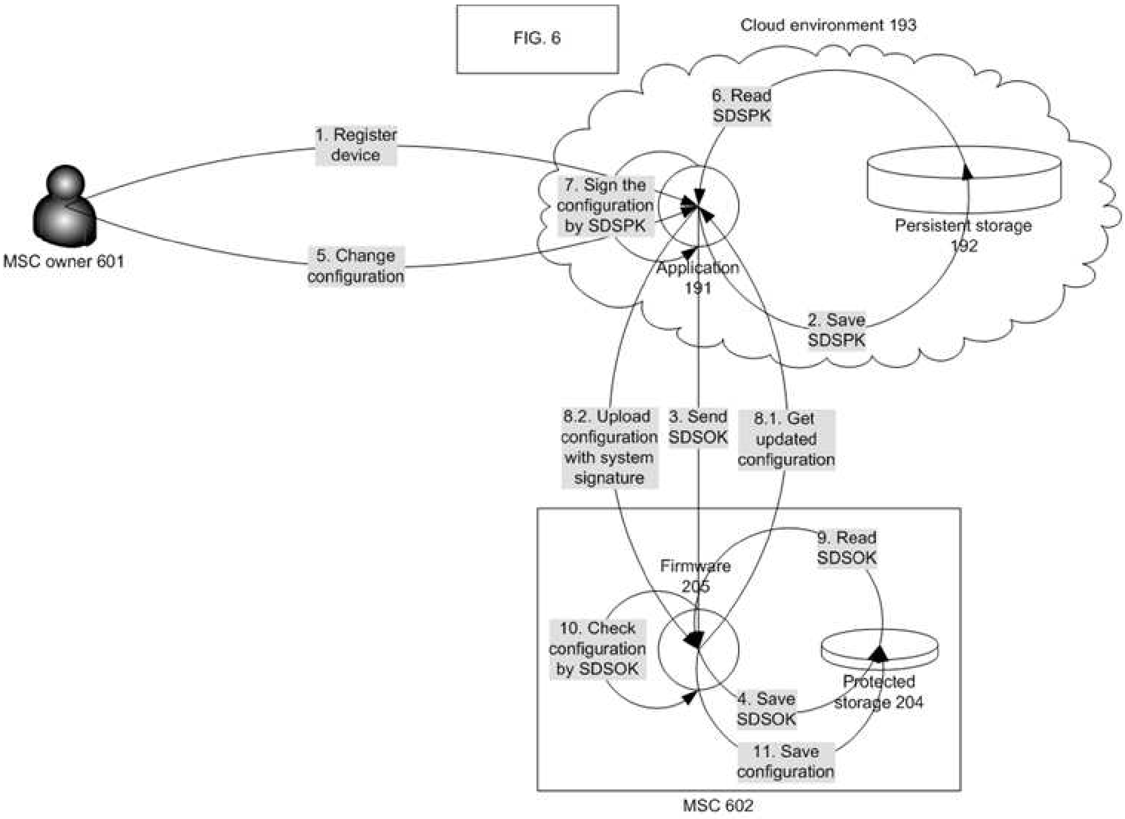
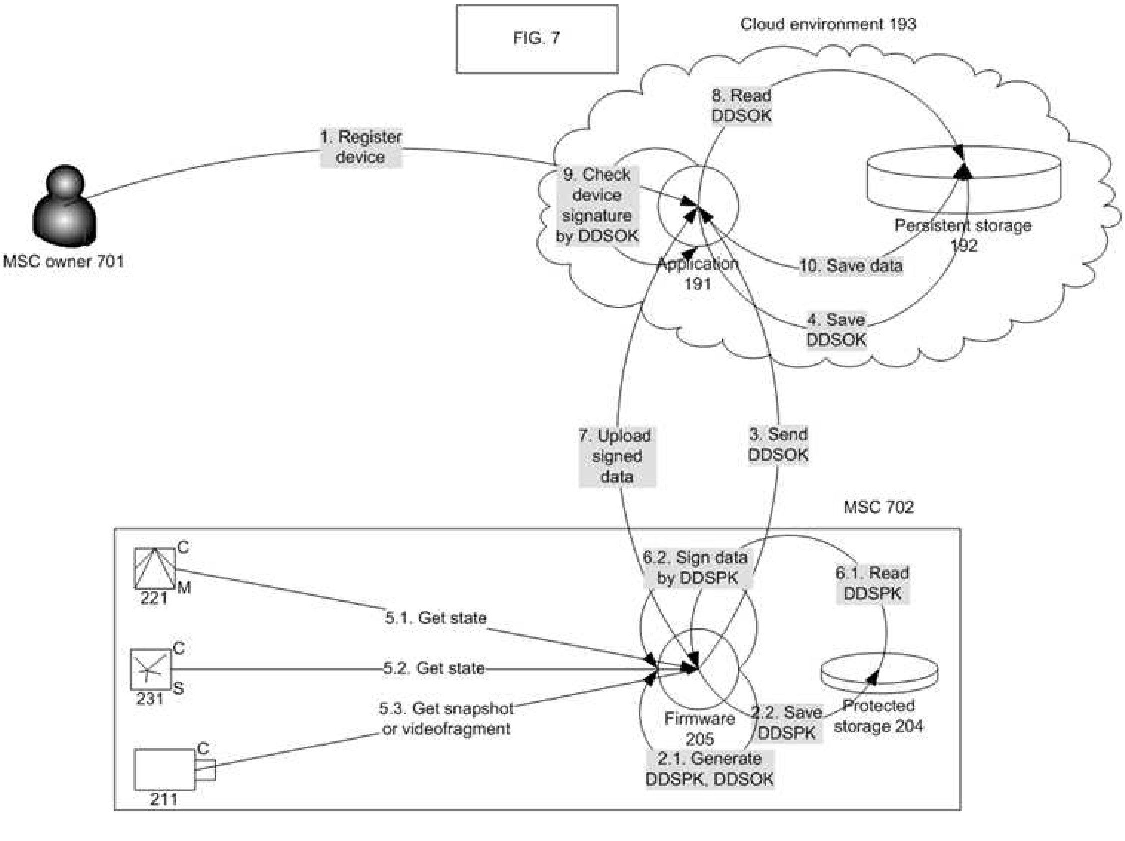

Cloud environment 193
9. Save encrypted data
1.1. Register device
Persistent storage 192
MSC owner 501
Application 191
11. Read encrypted data
12. Encrypted data
1.2. Start visual code recognition
3.1. UOK
10. Get encrypted data
3.1. UOK
8. Upload encrypted data
Protected storage 505
2. Save UPK
13. Read UPK
15. Show decrypted data
14. Decrypt data by UPK
Display 504
Client-side Application 503
User device 150
C
M
221
6.1. Get state
Firmware 205
5. Save UOK
7.2. Encrypt data by UOK
C
S
231
6.2. Get state
6.3. Get snapshot or videofragment
C
211
7.1. Read UOK
Protected storage 204
MSC 502

FIG. 6



Cloud environment 193
6. Read SDSPK
1. Register device
7. Sign the configuration by SDSPK
Persistent storage 192
MSC owner 601
5. Change configuration
Application 191
2. Save SDSPK
8.2. Upload configuration with system signature
3. Send SDSOK
8.1. Get updated configuration
9. Read SDSOK
Firmware 205
10. Check configuration by SDSOK
Protected storage 204
4. Save SDSOK
11. Save configuration
MSC 602

FIG. 7



Cloud environment 193
8. Read DDSOK
1. Register device
9. Check device signature by DDSOK
Persistent storage 192
MSC owner 701
Application 191
10. Save data
4. Save DDSOK
7. Upload signed data
3. Send DDSOK
MSC 702
C
221
M
6.2. Sign data by DDSPK
6.1. Read DDSPK
5.1. Get state
C
231
S
5.2. Get state
5.3. Get snapshot or videofragment
Firmware 205
2.2. Save DDSPK
Protected storage 204
2.1. Generate DDSPK, DDSOK
C
211

FIG. 8

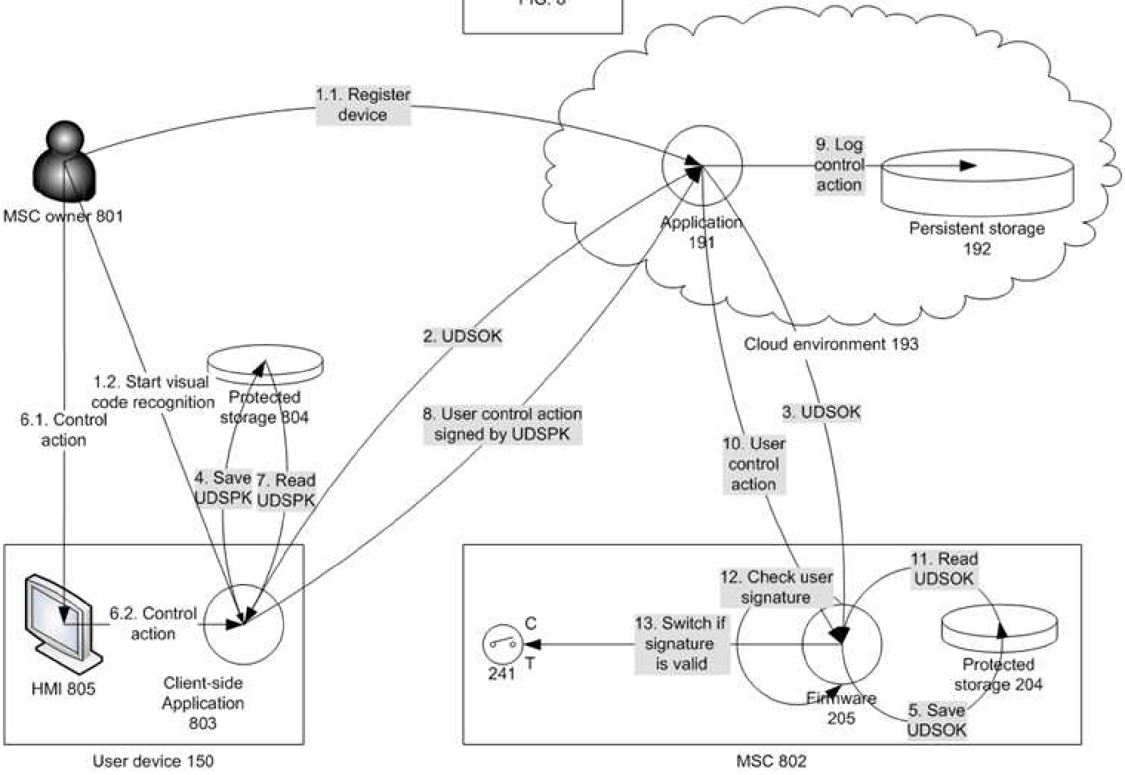
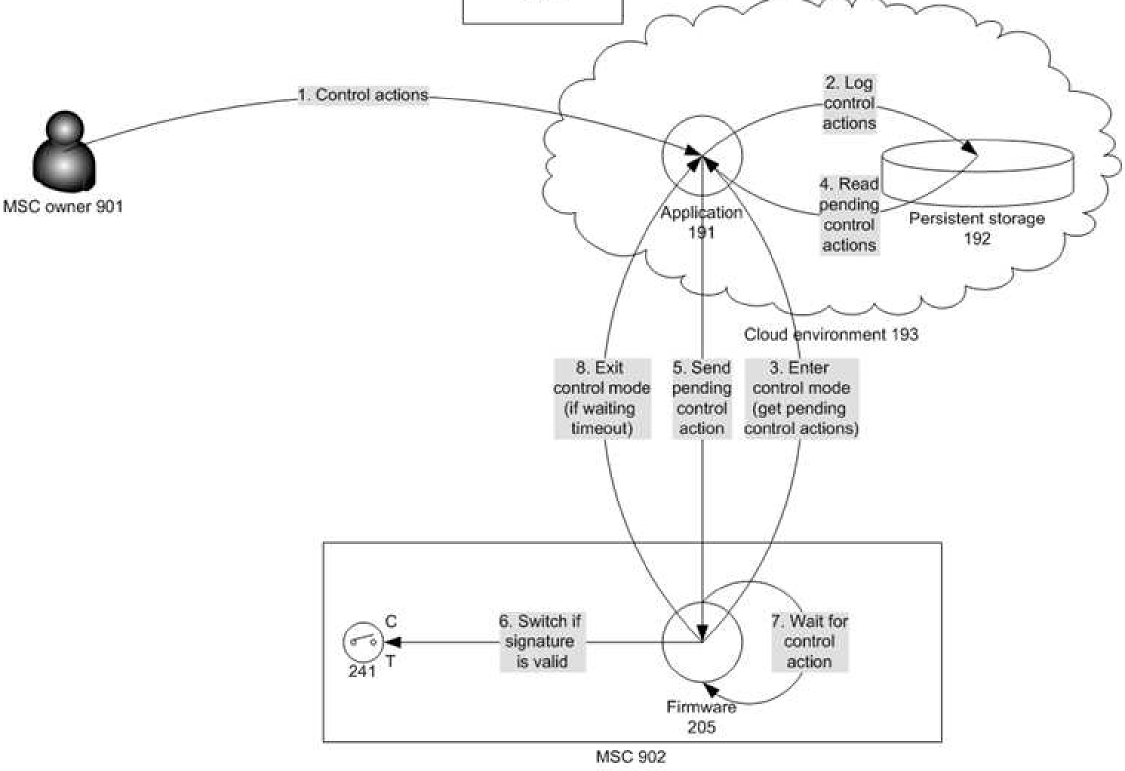

1.1. Register device
MSC owner 801
9. Log control action
Application 191
Persistent storage 192
Cloud environment 193
2. UDSOK
1.2. Start visual code recognition
Protected storage 804
6.1. Control action
8. User control action signed by UDSPK
3. UDSOK
10. User control action
4. Save UDSPK
7. Read UDSPK
11. Read UDSOK
12. Check user signature
6.2. Control action
13. Switch if signature is valid
C
T
241
HMI 805
Client-side Application 803
Protected storage 204
Firmware 205
5. Save UDSOK
User device 150
MSC 802

FIG. 9


1. Control actions
2. Log control actions
MSC owner 901
Application 191
4. Read pending control actions
Persistent storage 192
Cloud environment 193
8. Exit control mode (if waiting timeout)
5. Send pending control action
3. Enter control mode (get pending control actions)
6. Switch if signature is valid
7. Wait for control action
C
T
241
Firmware 205
MSC 902

[0001] BACKGROUND

[0002] This invention relates to visual surveillance systems and in particular to visual surveillance systems in which private data are transmitted through the Internet or other public network and stored in storages of any type maintained by the company providing visual surveillance services or by any third party.

[0003] The invention relates to surveillance data gathering devices, especially those with capabilities of remote control.

[0004] The invention relates to applications for surveillance data storage and fetching.

[0005] The invention relates to user devices for surveillance data representation communicating with the application for surveillance data storage and fetching through the Internet or other public networks.

[0006] The invention relates to methods of protection of private surveillance data and to methods of protection from intrusion in operation of visual surveillance system.

[0007] Prior art surveillance systems were designed to protect surveillance data on the way from the data gathering device to the data storage and on the way from the storage to the user device, but not to protect data from being accessed by the staff of company, which provides visual surveillance services for private persons.

[0008] Prior art devices for visual surveillance data gathering and applications for storage and representation of surveillance data were developed independently, therefore these devices and applications do not provide common procedures necessary for maximum protection of private data.

[0009] Prior art visual data gathering devices intended for data transmission through the Internet often have software components providing direct remote access to data gathered by the device, for example, HTTP-servers. These parts often have potential vulnerabilities. Also these components require credentials to provide access to surveillance data. There are difficulties with managing and securing these credentials for more than a few visual data gathering devices.

[00010] **BRIEF SUMMARY OF THE INVENTION**

[00011] In accordance with one aspect of the exemplary embodiment, a visual surveillance system includes plurality of devices for surveillance data gathering.

[00012] In accordance with another aspect of the exemplary embodiment, a visual surveillance system includes plurality of user devices for surveillance data representation and for user interaction with the surveillance system.

[00013] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system includes one or more data centers. For the purposes of this invention it is enough to specify that the data center provides necessary resources to run the application and also has the persistent storage of any type. These resources are referred hereinafter as “cloud environment”. Functions of the application related to scope of this invention are storage and fetching of surveillance data. The persistent storage is intended to store all surveillance data and all data necessary for the application to provide its functionality.

[00014] In accordance with yet another aspect of exemplary embodiment the application running in the cloud environment is programmed to exchange surveillance data between gathering devices, user devices and the persistent storage.

[00015] In accordance with yet another aspect of exemplary embodiment the application, the gathering device and the user device are operatively connected through the Internet or other public network.

[00016] In accordance with yet another aspect of exemplary embodiment the surveillance data gathering device can have capabilities for remote control, including remote control of external apparatus.

[00017] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system allows marking some attributes of surveillance data as owner’s private data.

[00018] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system realizes end-to-end encryption of surveillance data attributes marked as owner’s private data. Thanks to this process owner’s private data are stored in the persistent storage in encrypted form and are inaccessible to unauthorized persons including the staff of the company providing visual surveillance services.

[00019] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system verifies owner’s digital signature in receiving of control action. This procedure protects the visual surveillance system from execution of control action by unauthorized persons.

[00020] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system realizes the procedure of remote control in which the surveillance data gathering device periodically requests the application running in the cloud environment about pending control actions. This method excludes potentially vulnerable server parts from device software.

[00021] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system realizes the procedure of configuration data in which the surveillance data gathering device periodically requests the application running in the cloud environment about pending configuration data. This method excludes potentially vulnerable server parts from device software.

[00022] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system verifies digital signature in uploading of configuration data into the surveillance data gathering device. This procedure protects the configuration from intentional falsification.

[00023] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system uses verification of digital signature of surveillance data. This procedure protects the visual surveillance system from falsification of surveillance data.

[00024] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system uses connectionless protocol with total encryption of surveillance data in the process of surveillance data transmission from the surveillance data gathering device to the application running in the cloud environment.

[00025] In accordance with yet another aspect of exemplary embodiment, a visual surveillance system transmits registration attributes to the surveillance data gathering device by means of matrix bar code. This allows simplifying the registration procedure.

[00026] **BRIEF DESCRIPTION OF THE DRAWINGS**

[00027] **Figure 1.** Figure 1 shows a schematic view of exemplary embodiment of a visual surveillance system. The visual surveillance system includes plurality of surveillance data gathering devices, plurality of user devices, and one or more data centers. Surveillance data gathering devices, user devices and data centers are connected through the Internet or other public network.

[00028] **Figure 2.** Figure 2 illustrates a schematic view of the surveillance data gathering device. The device gathers surveillance data from plurality of external or internal video cameras and sensors of different types. The device can have plurality of external or internal control apparatus. Because of this functionality the device hereinafter referred as the “multifunctional surveillance controller”.

[00029] **Figure 3.** Figure 3 presents a schematic view of the process of registration of the multifunctional surveillance controller in the visual surveillance system. The process includes exchange of some special data between the user device, the multifunctional surveillance controller and the application running in the cloud environment.

[00030] **Figure 4.** Figure 4 shows a schematic view of the process of removing the registration of the multifunctional surveillance controller from the visual surveillance system.

[00031] **Figure 5.** Figure 5 shows a schematic view of the process of end-to-end encryption.

[00032] **Figure 6.** Figure 6 illustrates a schematic view of the process of uploading of configuration data from the application running in the cloud environment into the multifunctional surveillance controller with verification of digital signature.

[00033] **Figure 7.** Figure 7 shows a schematic view of the process of uploading of surveillance data from the multifunctional surveillance controller into the persistent storage with verification of digital signature.

[00034] **Figure 8.** Figure 8 shows a schematic view of the process of transmission of control actions from the owner to the multifunctional surveillance controller with verification of digital signature.

[00035] **Figure 9.** Figure 9 shows a schematic view of the process of transition of multifunctional surveillance controller into control mode.

[00036] DETAILED DESCRIPTION AND BEST MODE OF IMPLEMENTATION

[00037] Figure 1 shows a schematic view of exemplary embodiment of a visual surveillance system. The visual surveillance system includes plurality of multifunctional surveillance controllers such as **102** and **112** installed in owner's premises or in public transport respectively.

[00038] Multifunctional surveillance controllers **102** and **112** can receive GPS signal for determination of precision time and coordinates. In this case these data are automatically added as attributes to visual surveillance data transmitted by the multifunctional surveillance controller.

[00039] The visual surveillance system includes one or more data centers **190**. The data center provides necessary resources to run the application **191** and has the persistent storage **192** to store all surveillance data and all data necessary for the application **191** to provide its functionality. These resources are referred hereinafter as "cloud environment" **193**.

[00040] Multifunctional surveillance controllers exchange data with the application **191** through the Internet **140** or other public networks.

[00041] Multifunctional surveillance controllers **102** and **112** can be connected to wire or wireless networks of different types including, but not limited, Ethernet, WiFi, WiMAX, 3G and 4G.

[00042] The visual surveillance system includes plurality of user devices. By means of these devices the owner of multifunctional surveillance controller gets access to surveillance data and all functionality of the visual surveillance system. There are plenty of user device types including, but not limited, mobile phones **151**, personal computers **152**, PDA and tablet PC **153**, laptops **154**. In scope of given invention all these types hereinafter are referenced as “user device” **150**.

[00043] Multifunctional surveillance controllers **102** and **112** are programmed in such manner that can send notifications about events by means of SMS or MMS directly to the user mobile phone. In this case the SMS or MMS does not contain owner’s private data, but only the link to record, stored in the persistent storage **192**. The user device fetches private data associated with the event in accordance with procedures for maximum privacy protection which are described in following.

[00044] User devices **150** and the application **191** running in the cloud environment **193** are programmed to use for communications standard connection oriented protocols with data encryption, including, but not limited, HTTPS, SSL.

[00045] Figure 2 shows a schematic view of multifunctional surveillance controller (MSC).

[00046] The multifunctional surveillance controller has the protected storage **204**. This storage contains the firmware **205** and all data necessary for the firmware **205** to provide its functionality. These data include configuration information and keys which are used in processes of encryption and digital signature verification which are described in following.

[00047] The protected storage **204** can be of any type including, but not limited, FLASH, FRAM, SD-card, SSD, SATA and IDE. The protected storage **204** has software or hardware methods of data protection.

[00048] The multifunctional surveillance controller has the processing unit **201** that executes the firmware **205**.

[00049] The multifunctional surveillance controller can have plurality of sensors **221-22n**, **231-23n** of different types enclosed in the controller housing **200**.

[00050] The multifunctional surveillance controller can have plurality of sensors **261-26n**, **281-28n** of different types installed outside of the controller housing **200**.

[00051] Sensors **221-22n**, **231-23n** and **261-26n**, **281-28n** can be of any type including, but not limited, motion detectors, broken glass sensors.

[00052] The multifunctional surveillance controller can have plurality of control apparatus **241-24n** enclosed in the controller housing **200**.

[00053] The multifunctional surveillance controller can have plurality of control apparatus **271-27n** installed outside of the controller housing **200**.

[00054] The multifunctional surveillance controller can have one or more video cameras **211-21n** enclosed in the controller housing **200**.

[00055] The multifunctional surveillance controller can have one or more video cameras **251-25n** installed outside of the controller housing **200**.

[00056] The multifunctional surveillance controller can have a few camera communication modules (CCM) **202** to communicate with visual cameras **251-25n** installed outside of the controller housing **200**.

[00057] Video cameras installed outside of the controller housing **200** can be connected by means of a network. In this case the controller separates the trusted network of video cameras from an untrusted public network or the Internet.

[00058] The multifunctional surveillance controller can have a few sensor communication modules (SCM) **203** to communicate with sensors **261-26n**, **281-28n** installed outside of the controller housing **200**.

[00059] Depends on requirements or environmental conditions an industrial or domestic computer can be used as multifunctional surveillance controller.

[00060] Figure 3 shows a schematic view of process of registration of the multifunctional surveillance controller in the visual surveillance system.

[00061] The owner of the controller **301** starts the process of controller registration by interaction with the user interface of the application **191** by means of the user device **150**.

[00062] The user device **150** establishes bidirectional encrypted connection with the application **191** by means of one of standard protocols including, but not limited, HTTPS, SSL.

[00063] The application **191** generates the unique controller identifier (DID) and associates it with unique owner identifier (OID) and saves this pair in the persistent storage **192**.

[00064] The application **191** generates the pair consisting of the application open key (SOK) and the application private key (SPK) for encryption of data transmitted from the multifunctional surveillance controller **302** to the application **191**. This pair of keys is persisted until next time when the registration procedure will be executed.

[00065] The application **191** generates the matrix bar code containing registration information for uploading into the multifunctional surveillance controller **302**. This information includes, but is not limited, SOK, DID.

[00066] Matrix bar code can be of any type including, but not limited, QR-code.

[00067] The application **191** shows generated matrix bar code by means of user device **150**. The owner **301** of the controller **302** can print this code by means of printer **303** in the case when this simplifies further procedures.

[00068] The owner **301** of the controller **302** places generated matrix bar code in view of one of video cameras **305** of the multifunctional surveillance controller **302**. The camera can be integrated or external in accordance with figure 2.

[00069] The multifunctional surveillance controller **302** is programmed to recognize information from matrix bar code generated by the application **191**.

[00070] The multifunctional surveillance controller **302** has means to activate the procedure of recognition of matrix bar code generated by the application **191**.

[00071] The owner **301** of the controller **302** activates the procedure of matrix bar code recognition.

[00072] The multifunctional surveillance controller **302** recognizes data from matrix bar code and saves obtained DID, SOK in the protected storage **204**.

[00073] The multifunctional surveillance controller connects to the application **191** by means of standard connection oriented protocol with data encryption and sends to the application **191** the command to register itself. The list of suitable protocols includes, but is not limited, HTTPS, SSL. The controller **302** identifies itself to the application **191** by means of the identifier (DID) obtained from matrix bar code.

[00074] The application **191** finishes the process of multifunctional surveillance controller **302** registration.

[00075] During process of registration the multifunctional surveillance controller **302** and the application **191** are exchanging information necessary for establishing of encrypted exchange of data. After the procedure of registration is finished, all surveillance data transmitted by the controller **302** are totally encrypted. The controller **302** uses connectionless protocol to transmit surveillance data to the application **191**. The controller can't be registered again until it will be unregistered as described in following.

[00076] Figure 4 shows a schematic view of process of removing the multifunctional surveillance controller from the visual surveillance system.

[00077] The owner of controller **401** starts the process of removing of controller registration from interaction with the user interface of the application **191** by means of the user device **150**.

[00078] The application **191** generates matrix bar code containing unique controller identifier (DID).

[00079] The application **191** shows generated matrix bar code by means of user device **150**. The owner **401** of the controller **402** can print this code by means of printer **403** in the case when this simplifies further procedures.

[00080] The owner **401** of the controller **402** places generated matrix bar code in view of one of video cameras **405** of the multifunctional surveillance controller **402**. The camera can be integrated or external in accordance with figure 2.

[00081] The multifunctional surveillance controller **402** is programmed to recognize information from matrix bar code generated by the application **191**.

[00082] The multifunctional surveillance controller **402** has means to activate the procedure of recognition of matrix bar code generated by the application **191**.

[00083] The owner **401** of the controller **402** activates the procedure of matrix bar code recognition.

[00084] The multifunctional surveillance controller **402** recognizes data from matrix bar code and extracts unique controller identifier (DID) for further operation.

[00085] If recognized DID coincides with DID stored in the protected storage **204** during registration process the multifunctional surveillance controller connects with the application **191** by means of standard connection oriented protocol with data encryption. The list of suitable protocols includes, but is not limited, HTTPS, SSL. After that the controller sends to the application command for removing registration data.

[00086] The application **191** finishes the process by removing registration data of the controller **402** from the persistent storage **192** and optionally removes all associated surveillance data.

[00087] The firmware **205** finishes the process by removing all data obtained during registration process from the protected storage **204**.

[00088] After the process of removing registration has been finished the visual surveillance system can get data from the multifunctional surveillance controller only after execution of new registration process. During this procedure the multifunctional surveillance controller will obtain a new unique identifier.

[00089] Figure 5 shows a schematic view of process of end-to-end encryption of private data in the visual surveillance system.

[00090] “Private data” are data marked as “private” by the owner of controller during process of controller configuration. By default “private” data are data directly related with an event registered by the visual surveillance system. List of types of “private” data includes, but is not limited, snapshots, visual fragments, state of sensors, coordinates. The application **191** and the firmware **205** are programmed to allow freely marking of any surveillance data attribute as “private”.

[00091] “Public data” are those not marked as “private”. List of types of “public” data includes, but is not limited, timestamps.

[00092] “Surveillance data” are all data which are transmitted by the multifunctional surveillance controller, namely “private data” together with “public data”.

[00093] End-to-end encryption operates only on private data and does not act on public data.

[00094] End-to-end encryption is optional and can be switched on by the controller owner **501** during process of controller registration.

[00095] End-to-end encryption starts from the procedure of registration of multifunctional surveillance controller **502** in the visual surveillance system. During registration procedure the controller owner **501** switches on optional end-to-end encryption and selects visual surveillance data attributes to be “private”.

[00096] During registration procedure the client-side application **503** running in the user device **150** generates pair of keys: owner private key (UPK) and owner open key (UOK). Subsequently UOK is used for encryption of owner's private data transmitted from the controller **502** to the application **191**. UPK is used for decryption of owner's private data obtained by the client-side application **503** from the application **191**. Thanks to this process owner's private data are stored in the persistent storage **192** in encrypted form.

[00097] The client-side application **503** saves created owner private key (UPK) in the protected storage **505**. The protected storage **505** can be the medium of any type including, but not limited, SD-card, USB-drive. This medium is stored in a place inaccessible to unauthorized persons.

[00098] The client-side application **503** transmits the owner open key (UOK) to the application **191**. In turn the application **191** transmits UOK together with other parameters to the controller **502** by means of matrix bar code in accordance with description of figure 3.

[00099] The multifunctional surveillance controller **502** saves UOK in the protected storage **204**.

[000100] Every time when the firmware **205** gathers private data from external or internal sensors or video cameras in accordance with description of figure 2, the firmware **205** reads UOK from the protected storage **204** and encrypts owner's private data by means of this UOK.

[000101] The multifunctional surveillance controller **502** transmits owner's private data in encrypted form to the application **191**.

[000102] The application **191** saves obtained owner’s private data in the persistent storage **192**.

[000103] The client-side application **503** requests owner’s private data from the application **191**.

[000104] The application **191** transmits owner’s private data encrypted by UOK to the client-side application **503**.

[000105] The client-side application **503** reads user private key (UPK) from the protected storage **505** and decrypts owner’s private data by means of this key.

[000106] The client-side application **503** shows decrypted owner’s private data by means of any available device including, but not limited, display, printer.

[000107] During process of registration an individual pair of keys is created for every multifunctional surveillance controller. This makes the system even more protected.

[000108] Thanks to the process of end-to-end encryption owner’s private data are protected from unauthorized access by staff of the company providing visual surveillance services.

[000109] The multifunctional surveillance controller **502** and the application **191** are programmed to transmit and receive surveillance data only by initiative of the controller **502**. This method excludes “server” parts from the firmware **205** of the controller **502** and associated vulnerabilities opening access to unencrypted owner’s private data for unauthorized persons.

[000110] Figure 6 shows a schematic view of process of uploading of configuration data in the multifunctional surveillance controller **602** with verification of digital signature.

[000111] The process starts from the procedure of registration of the multifunctional surveillance controller **602** in the visual surveillance system.

[000112] During registration process the application **191** generates the system private key for digital signature (SDSPK) and the system open key for verification of the digital signature (SDSOK).

[000113] The application **191** saves the private key SDSPK in the persistent storage **192**.

[000114] The firmware **205** receives the open key SDSOK from the application **191** and saves it in the protected storage **204**.

[000115] The controller owner changes configuration of the multifunctional surveillance controller **602**.

[000116] The multifunctional surveillance controller **602** periodically requests the application **191** about updated configuration data with period specified during process of manufacturing or during previous process of configuration. The controller **602** sends request by means of one of standard encrypted connection oriented protocols including, but not limited, HTTPS, SSL.

[000117] If the configuration was changed from the moment of last request then the application **191** reads the private key SDSPK from the persistent storage **192**, signs configuration data by means of this key and then transmits configuration data to the controller **602**.

[000118] The multifunctional surveillance controller **602** receives updated configuration data, reads the open key SDSOK and verifies by means of this key the signature of obtained configuration data.

[000119] If the signature is valid then the controller **602** saves configuration data in the protected storage **204** and starts to use them.

[000120] This procedure protects configuration of the multifunctional surveillance controller **602** from intentional falsification.

[000121] Figure 7 shows a schematic view of process of uploading of data from multifunctional surveillance controller **702** with verification of digital signature.

[000122] The process starts from the procedure of registration of the multifunctional surveillance controller **702** in the visual surveillance system.

[000123] During registration process the firmware **205** generates the controller private key for digital signature (DDSPK) and the controller open key for verification of digital signature (DDSOK).

[000124] During registration process the firmware **205** transmits the open key DDSOK to the application **191** in accordance with figure 3.

[000125] The application **191** saves obtained open key DDSOK in the persistent storage **192**.

[000126] The firmware **205** saves the private key DDSPK in the protected storage **204**.

[000127] Every time when the firmware **205** gathers data from internal or external sensors or video cameras, it reads private key DDSPK from the protected storage **204**, signs obtained data by using this key and transmits signed data to the application **191**.

[000128] Every time the application **191** receives surveillance data from the controller **702**, it reads the open key DDSOK and verifies by means of this key the signature of obtained data.

[000129] If the digital signature is valid then the application **191** saves obtained data in the persistent storage **192**.

[000130] This procedure protects the visual surveillance system from intentional or occasional substitution of data inflowing from the multifunctional surveillance controller.

[000131] The multifunctional surveillance controller **702** is programmed to gather visual surveillance data from video cameras in different formats and to convert these data to unified format before transmission to the application **191**.

[000132] Figure 8 shows a schematic view of process of transmission of control actions from the controller owner **801** to the controller **802** with verification of digital signature.

[000133] The process starts from procedure of registration of the multifunctional surveillance controller **802** in the visual surveillance system.

[000134] During registration procedure the client-side application **803** running in the user device **150** generates the owner private key for digital signature (UDSPK) and the owner open key for verification of the digital signature (UDSOK).

[000135] The client-side application **803** saves obtained key UDSPK in the protected storage **804**.

[000136] The client-side application **803** transmits UDSOK to the application **191**. In turn the application **191** during registration procedure transmits UDSOK together with other parameters to the controller **802** by means of matrix bar code in accordance with figure 3.

[000137] The controller **802** saves obtained open key UDSOK in the protected storage **204**.

[000138] Every time when the controller owner **801** sends a control action to the controller **802** by means of the HMI **805** of the user device **150**, the client-side application **803** reads the private key UDSPK from the protected storage **804** and signs by means of this key data of the control action. The user device **150** can be of any type in accordance with figure 1.

[000139] The client-side application **803** transmits data of control action signed by means of the private key UDSPK to the application **191**.

[000140] The application **191** logs obtained control action in the persistent storage **192**.

[000141] The application **191** transmits the control action signed by means of the private key UDSPK to the firmware **205** of the controller **802**.

[000142] The firmware **205** reads the open key UDSOK from the protected storage **204** and verifies by means of this key the signature of obtained control action.

[000143] If the signature of obtained control action is valid then the firmware **205** of the controller **802** executes obtained action and switches state of corresponding external **271-27n** or internal **241-24n** control apparatus.

[000144] This procedure protects the visual surveillance system from execution of control action by an unauthorized person.

[000145] Figure 9 shows a schematic view of transition of the multifunctional surveillance controller into the control mode. This figure together with figure 8 shows the process of remote control by means of the multifunctional surveillance controller.

[000146] The controller owner **901** sends one or more control actions by means of user device **903** to the application **191** running in the cloud environment **193**.

[000147] The application **191** logs control actions in the persistent storage **192** and mark them as “pending”.

[000148] The multifunctional surveillance controller periodically, with the period given during manufacturing process or during previous configuration process, requests the application **191** about pending control actions.

[000149] The application **191** transmits pending control actions or sends the message designating that there are no control actions.

[000150] The firmware **205** receives control actions and executes them in accordance with description of figure 8.

[000151] After that the firmware **205** waits for the given period of time of arriving of new control actions.

[000152] If during this time no further control actions were received then the controller **903** disconnects from the application **191** until next time when the procedure will be executed.

[000153] This procedure increases security by exclusion of “server” components at the cost of latency in control.

CLAIMS

[000154] I claim:

1. The visual surveillance system comprising plurality of visual surveillance data gathering devices, one or more datacenters providing cloud environments, plurality of user devices.
2. The visual surveillance system according to claim 1 and comprising the application running in the cloud environment and transmitting surveillance data, configuration data and owner control actions between user devices, the persistent storage and surveillance data gathering devices.
3. The visual surveillance system according to claim 2 and comprising the persistent storage which stores surveillance data and also all data necessary for the application to provide its functionality.
4. The visual surveillance system according to claim 1 and comprising plurality of multifunctional surveillance controllers for surveillance data gathering.
5. The visual surveillance system according to claim 1 whenever it uses digital signature verification in process of uploading of configuration data into the multifunctional surveillance controller.
6. The visual surveillance system according to claim 5 whenever it is used for automatic configuration of plurality of multifunctional surveillance controllers.
7. The visual surveillance system according to claim 5 whenever the process of transmission of configuration data to the multifunctional surveillance controller starts from a request of the controller.
8. The visual surveillance system according to claim 1 whenever it uses verification of digital signature in the process of transmission of surveillance data from the

multifunctional surveillance controller to the application running in the cloud environment.

9. The visual surveillance system according to claim 1 whenever it uses connectionless protocol in process of surveillance data transmission from the multifunctional surveillance controller to the application running in the cloud environment.

10. The visual surveillance system according to claim **Ошибка! Источник ссылки не найден.** whenever it uses total encryption of data in process of surveillance data transmission from the multifunctional surveillance controller to the application running in the cloud environment.

11. The visual surveillance system according to claim 1 whenever it allows to mark attributes of visual surveillance data as owner’s private data.

12. The visual surveillance system according to claim **Ошибка! Источник ссылки не найден.**1 whenever it realizes end-to-end encryption of surveillance data attributes marked as owner’s private data in such manner that owner’s private data remains encrypted everywhere from the surveillance data gathering device to the user device.

13. The visual surveillance system according to claim **Ошибка! Источник ссылки не найден.**1 whenever it creates an individual pair of keys for end-to-end encryption for every multifunctional surveillance controller.

14. The visual surveillance system according to claim 1 whenever it is capable to transmit control actions to multifunctional surveillance controllers.

15. The visual surveillance system according to claim **Ошибка! Источник ссылки не найден.**4 whenever the multifunctional surveillance controller verifies owner's digital signature in receiving of control action.

16. The visual surveillance system according to claim **Ошибка! Источник ссылки не найден.**4 whenever the multifunctional surveillance controller realizes the procedure of transition into the remote control mode.

17. The visual surveillance system according to claim **Ошибка! Источник ссылки не найден.**6 whenever the multifunctional surveillance controller establishes encrypted connection with the application running in the cloud environment in the remote control mode.

18. The visual surveillance system according to claim **Ошибка! Источник ссылки не найден.**6 whenever the multifunctional surveillance controller realizes the procedure of going out from the remote control mode.

19. The visual surveillance system according to claim 1 whenever it realizes the procedure of registration of the multifunctional surveillance controller in the visual surveillance system.

20. The visual surveillance system according to claim 19 whenever it transmits registration attributes to the multifunctional surveillance controller by means of matrix bar code during the process of registration.

21. The visual surveillance system according to claim 19 whenever the application running in the cloud environment transmits the keys for data encryption and digital signature as part of the registration information by means of matrix bar code.

22. The visual surveillance system according to claim 1 whenever it realizes the procedure of removing of registration of the multifunctional surveillance controller out from the visual surveillance system.

23. The visual surveillance system according to claim **Ошибка! Источник ссылки не найден.**2 whenever it saves surveillance data of previous registration of the multifunctional surveillance controller in the persistent storage and associates a new unique identifier with the controller every time during the process of registration.

24. The visual surveillance system according to claim 1 whenever the application running in the cloud environment and the multifunctional surveillance controller are programmed in such manner that transmission of visual surveillance data from the controller to the application is initiated by the controller.

25. The visual surveillance system according to claim 1, whenever the multifunctional surveillance controller separates the trusted network, which connects the controller with video cameras, from an untrusted public network or the Internet.

26. The visual surveillance system according to claim 1, whenever the multifunctional surveillance controller is programmed to gather visual surveillance data from video cameras in different formats and to convert these data in the unified format before transmission to the application running in the cloud environment.

27. The visual surveillance system according to claim 1, whenever the user device is programmed to transmit all data and control actions to the application running in the cloud environment in encrypted form by means of standard connection oriented protocols including, but not limited, HTTPS, SSL.

28. The visual surveillance system according to claim 1, whenever the user device is programmed to receive all data from the application running in the cloud environment in encrypted form by means of standard connection oriented protocols including, but not limited, HTTPS, SSL.

ABSTRACT:

[000155] Technology to improve protection of private data for using in visual surveillance systems in which the data are transmitted through the Internet or other publicly accessible networks.