Using cloud computing technologies in IP-video surveillance systems with the function of 3d-object modelling

Kirill Zhigalov [1,*], *Karen* Avetisyan [2]

[1]V.A. Trapeznikov institute of Control Science of Russian Academy of Sciences, Moscow, Russia
[2]Moscow University of the Ministry of Internal Affairs of the Russian Federation n.a. V. Ya. Kikotya, Moscow, Russia

Abstract. This article is devoted to the integration of cloud technology functions into 3D IP video surveillance systems in order to conduct further video Analytics, incoming real-time data, as well as stored video materials on the server in the «cloud». The main attention is devoted to «cloud technologies» usage optimizing the process of recognition of the desired object by increasing the criteria of flexibility and scalability of the system. Transferring image load from the client to the cloud server, to the virtual part of the system. The development of the issues considered in the article in terms of data analysis, which will significantly improve the effectiveness of the implementation of special tasks facing special units.

1 Introduction

Video surveillance as a service based on cloud storage systems is one of the most important trends of modern security systems. Currently, Video Surveillance as a service in infrastructure is used at both government and commercial facilities.

Software as a service. Access to the application is carried out by means of the network, and most often through an Internet browser. In this case, the main advantage of the VSaaS model for the client is the absence of costs associated with the installation, updating and maintenance of equipment and software running on it. In the model VSaaS there are:

- application is adapted for remote use;
- multiple clients can use the same application;
- payment for the service is charged either as a monthly subscription fee or based on the total volume of transactions;
- application support is included in the payment;
- application upgrades can be performed by service personnel smoothly and transparently for customers.

2 Three types of cloud services

From the point of view of software developers, the SaaS model allows you effectively combat unlicensed use of the software, because the client can't store, copy or install the software.

The software within the SaaS can be seen as a more convenient and cost-efficient alternative to internal information systems.

The development of SaaS logic is the concept of WaaS (Workplace as a service). That is, the client gets at his disposal, fully designed software with everything necessary for work on a virtual workstation. According to recently published Soft Cloud data, the following SaaS applications are in demand: mail; communications (VoIP); anti-spam and antivirus; helpdesk; project management; remote education; Customer Relationship Management; data storage and backup.

All three types of cloud services are interconnected and represent a nested structure. In addition to the various ways of providing services, there are several options for deploying cloud-based systems.

Private cloud is used to provide services within the same organization, which is both the customer and the service provider. This option is implementation of the «cloud concept», when the company creates it to perform its internal tasks. Public cloud is used by cloud providers to provide services to other organizations. Mixed or hybrid cloud is a mixed model of private and public deployment models.

3 Implementation of 3d camera systems

Advanced data storage, intelligent 3D modeling functions, data retrieval using a set of approaches, tools and methods for processing structured and unstructured data of huge amounts of information, all these tasks can be implemented in cloud video surveillance systems using 3D cameras. Development of mobile device access services opens new perspectives in ensuring the security of controlled objects. In recent years 3Dcamera systems in IP video surveillance are integrated in large international corporations such as Google, Apple and others.

Speaking about the advantages of 3D IP-video surveillance systems, we will highlight one of their key criteria that is scalability and flexibility of building a video surveillance system, i.e. the ability to include in the 3D IP-video surveillance system the required number

* Corresponding author: kshakalov@mail.ru

of cameras with a sufficient number of channels, combining 3D video cameras into clusters, using of frame-by-frame or stream video compression standard, the possibility of creating hybrid systems, the flexibility of which allows forming a geographically distributed video surveillance system, expanding it to the size of the city, territorial subject or the whole state.

Cloud data storage. Storage of 3D IP video surveillance data on «Cloud» is becoming increasingly popular [1]. This approach allows you to avoid the cost of purchasing and maintaining equipment for storing large volumes of high-quality video received from security IP-systems [2]. In its turn, it promotes the development of the services like video Surveillance services (VSaaS).

Data protection in the network video surveillance system. IP-video surveillance of security systems imposes high requirements on the security and confidentiality of the resulting video information. The question of unintentional receipt of information relating to personal data is acute. Such a threat takes place in view of the wide range of cyber-attacks, since the components of IP-based surveillance systems are network devices. From the legal point of view,all the requirements of the

Reliable data protection against unauthorized access is provided by the use of encryption mechanisms, and the main criteria that increase the cryptographic stability will be not only the encryption algorithm itself, but also the length of the key (bit), as well as the frequency of its replacement [3].

As for the password protection and the establishment of a multi-level system of user rights, for the purpose of increased security a multi-factor approach should be used for authentication, including the analysis of biometric data system, i.e. the retina, fingerprints, voice parameters of the recipient and other characteristics of an object. 3D IP camera before sending a video message over the network may encrypt it, create a cryptogram with the aim of preventing from viewing and alteration of the information. The IP system may be configured to authenticate the connection by means of encrypted certificates perceived by a particular network camera, which prevents an outsider from implementing a man in the middle attack.

In addition, the developers of specialized software systematically upgrade algorithms and means of protection against possible cyber threats. Implementation this integrated approach to face identification of the user significantly increases the security data storage.

Modern video surveillance systems provide wide opportunities for video Analytics. The ability to use data obtained both in real-time mode and to use the accumulated resource in storage systems allows you to set goals such as early detection of an event or an object.

Video Analytics is widely used as an effective tool necessary to systematize the segment of information or data according to certain criteria. In its turn, 3D IP video surveillance, in the future, has the highest potential for video analysis. The software approach allows you to combine a video surveillance system with multiple cameras, ensures easy video search on key criteria and making use of video analytics. Less often, it is an integral part of the platform, providing an integrated approach to solving the company's problems through the effective integration of various components.

Thus, the client receives information at any time and through the mobile device in which the above function takes place.

In order to highlight the additional features provided by the provider of video surveillance, even a special term was created - MVaaS (Managed Video as a Service).

Video Analytics may be implemented through the integration into existing video surveillance systems, where the compatibility of IP cameras, defined by RTSP/ONVIF protocols, as well as with web and analog cameras of standard resolution. Encryption of video streams for the standard SSL and multi-level redundancy. Open APIs and SDKs for integration with third-party applications IFTTT.

Intelligent video Analytics: calculating the number of people who passed through the zone of control – checkpoint (Element, Counter), integration with control systems and control accesses. The placement of cameras on the map for easy navigation.

In addition to software and operator analysis of video and the subsequent formation of analytical reports, the management of some functions of the access control system based on data obtained through video surveillance systems has proved to be quite popular in the market of services.

Subject-subject interaction. The need for the use and management of consolidated data, also in the framework of "smart cities" and other projects of the Internet of Things - IoT, the development of cloud services creates the opportunity of mobile access to video surveillance systems and video analytics functions.

In addition, VSaaS drivers include innovative technologies in the field of video surveillance, reducing the cost of video surveillance equipment and increasing the needs for video Analytics make it possible to argue that the development of the market of 3D IP video surveillance is the main direction in Video-Surveillance-as-a-service. Cloud, on-premises, and hybrid video storage defines a range of topical issues, including:

- about the systematization of the required number of cameras and objects in a single personal account;
- about implementation of flexible management of access rights to cameras and their groups;
- about possibility of remote configuration of the cameras in the personal account;
- about grouping cameras according to the structure of a particular organization;
- about rapid organization of public events.

4 Security problems in ip video systems

A number of positions on security issues in the implementation of the 3D IP video surveillance system remain dispositional [4].

Threats to the security of cloud computing are associated with potential damage to resources, such as

information, processes and systems, and therefore – organizations [5]. They may be of natural or fabricated origin and may be accidental or intentional; may arise inside or outside the organization; divided into casual or intentional, or active or passive. Specific threats detected depend heavily on the specific cloud service you choose. Security risks for CSC are loss and leakage of data, unprotected access to the service, internal threats. Security threats for CSP are unauthorized administrative access, internal threats [5].

Security concerns include those related to the nature and work environment of cloud services. An indirect threat occurs if it creates risks not only in carrying the data of one object, but also for other users. Security challenges for CSC are due to the complexity of the environment, or indirect threats that can cause more immediate threats to the interests of the consumer of cloud services. The uncertainty in respect of liability, loss of trust, loss of control, loss of privacy, lack of services, adherence to one provider of cloud-based services, misappropriation of intellectual property loss of software integrity [6].

Security problems for CSP are uncertainty about responsibility, shared environment, inconsistency and conflict of protection mechanisms, conflict of jurisdictions, associated with changes in the risks of unsuccessful transition and integration (transition to the cloud often involves transferring large amounts of data and major configuration changes). The other may be named as Disruptions in activities, binding to the partner cloud services, the vulnerability of the supply chain, and the interdependence of software.

Security challenges for cloud partners services (CSN) are uncertainty regarding liability, misappropriation of intellectual property loss of software integrity. A common trust model is needed for any system in which multiple suppliers work together to provide a credible service. Due to the extremely distributed nature of cloud computing, accompanied with the presence of several participants, it is necessary that the cloud-computing environment is included into a General trust model. This trust model will enable the creation of Islands and/or federations of trusted entities so that the disparate elements of the system can authenticate the identity and sanctioned rights of other entities and components. Each island of the Federation of trust is based on one or more trusted public key infrastructure (PKI) certificate authorities. Today, there are many trust models available for use in a cloud-based and cloud-based environment.

In a cloud-computing environment, network security enables you to isolate physical and virtual networks and ensure secure communications between all participants. This capability makes it possible to partition the security domain, access controls on the network boundary (such as a firewall), intrusion detection and prevention, and network traffic separation based on security policy. It also protects your network against attacks in physical and virtual network environments. Data isolation, data protection and privacy protection address common data protection issues that often have legal implications. As different cloud computing service means different ways of implementing security controls, the usage of this feature coordinates actions of diverse security mechanisms toprevent conflicts of protection mechanisms.

5 Conclusions

In addition to the above, it should be noted that the IP camera technology itself, and in particular the use of the 3D scanning function, are widely used. In particular, the functions of modular integration of this type of means technically open new opportunities in the field of not only the control and search of persons in public places and on concrete objects, but also their application on unmanned aerial vehicles.

It is a modular function and cloud technology that will allow you to transmit information in real time, whether it is the operational headquarters or the management of a certain level in the performance of any operational, tactical or strategic tasks (Figure 1).

.

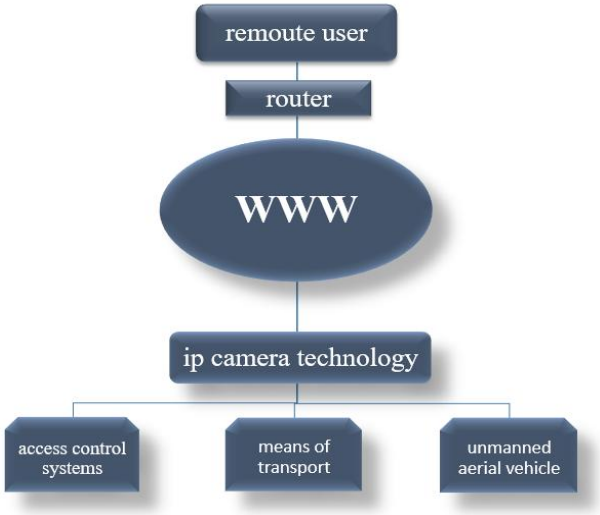

Fig. 1. An example of cloud technology structure

The 3D identification function, including 3D scanning, will allow you to simulate the probed sector in order to make it more responsive for further analytical work and action planning.

Development of cloud technologies, and 3D technologies-identification, given the possible implementation of all kinds of threats come to the fore in effective problem-solving search and identification (including the simulation objects).

References

1. N. Sultan, International Journal of Information Management, **34**, 177 (2014)
2. E. Nikulchev; E. Pluzhnik, D. Biryukov et al., International Journal of Advanced Computer Science and Applications,, **6,** 22 (2015)
3. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance*,

https://cloudsecurityalliance.org/csaguide.pdf (2009)

4. Ch. Hoff, *Security guidance for critical areas of focus in cloud computing*, pp. 12–20. https://cloudsecurityalliance.org/guidnce/csaguide.v3.0.pdf (2011)
5. C. Hewitt, IEEE Internet Computing, **12**, 96 (2008)
6. A.V. Brednik, *Security issues of cloud computing. Analysis of methods of protection of the clouds from cloud security alliance* (Tambov, 2013) [In Rus]