Video Surveillance in the Cloud: Dependability Analysis

Aleksandra Karimaa
Turku Centre for Computer Science, Teleste Corp.
Turku, Finland
alkari@utu.fi

Abstract—**Cloud computing with storage virtualization and new service-oriented architecture brings a new perspective to the aspect of dependability of video surveillance solutions and other safety-critical applications. The existing research is focused mainly on security challenges of cloud applications in general. The area of safety-critical systems is relatively unexplored especially beyond aspects of system security. We believe the overview of system dependability shall be done to cover other dependability attributes. It shall bring new arguments for expansion of video surveillance systems towards cloud technology, global resources distribution and virtualization. The article reviews the main drivers towards surveillance in cloud technology. We research the dependability characteristics in context of transition of video surveillance architecture towards cloud solutions. Finally, we propose the areas of focus for system development and design.**

Keywords-surveillance; cloud; dependability

Introduction and motivation

The main motivations driving video surveillance towards cloud computing is the scalability of computing and storage resources which provide; cost effective scalability, flexibility of resource management and improve system performance.

The transition of video surveillance towards cloud solutions can be seen rather as a continuous process than a disruptive innovation. There are multiple factors which indicate that the development towards a cloud solution is a natural evolution for the development of surveillance systems.

The architecture of video surveillance systems develops towards a model that includes dumb clients and a core of servers - it is identical with the architectural principles of cloud computing. Moreover, the systems themselves are becoming more often distributed, creating the structure of multiple local sites connected in mesh-like structures. The connectivity between single locations is based upon IP (Internet Protocol). Additionally, there are ongoing processes of standardization for architectural solutions and external interfaces (refer to ONVIF [1], PSIA [2], and Web Services architecture standardization by W3C [3]). In the case of surveillance systems, the process is driven by the requirement for multi-vendor integration with open and well defined interface environment enabling a cloud-based architectural solution. An open and standardized environment motivates the development of other value-added features (such as quality or security) which can then be offered as a product differentiator driving market maturity. Addressing the current weak points of dependability should have a positive impact on a number of cloud-based safety-critical systems. Finally, typical video surveillance systems have high demands for massive storage requirements (recording of video streams) and high-performance computing (coding the streams and system intelligence) which are major advantages of cloud and virtualization technologies.

However, system transition towards cloud solutions is not without its challenges. In order to benefit from a cloud-based system, there is certain amount of system and software development required. The systems should be able to accommodate automated mechanisms available in the cloud infrastructure, utilize advantages of cloud architecture and also handle cloud architecture limitations. A good example is the video format conversions requirement which accommodates available service models (cost of storage at data centre and the cost of network transmission). Another example includes extension of system failover mechanisms to accommodate virtual machine failover availability.

One of the problems with this transition towards a cloud-based system might be the flexibility of the offering. A cloud service offering may be focused on supporting the scenario where the video transmission happens from the cloud to the user whereas in surveillance system the video is transmitted from the user or camera towards the cloud (for storage purposes).

This article reviews the transition alternatives from a traditional to a cloud-based surveillance system. An overview of dependability objectives for a surveillance system is also described. Next, the objectives of dependability objectives: availability, security, reliability and maintainability are analyzed. The article is closed by a discussion chapter containing a short summary of the topic for the transition process.

Transition alternatives

The process of transition of a surveillance solution towards a cloud-based system is expected to be quite complex, this is due to security concerns of cloud-based systems and the immaturity of the current market offering of cloud services. Therefore, it is expected that the transition will be gradual and some of scenarios will be more attractive than others.

Hardware virtualization provides an interesting alternative for being a first step for the transition to cloud technologies. It changes traditional relationship between software and hardware – software is no longer dependent on hardware location. One application can run in multiple locations and many applications can share the same hardware. Hardware virtualization increases resource utilization and efficiency, as well as lowers capital investment and maintenance cost. Some level of hardware virtualization is well presented even for popular desktop environments. More advanced options can be introduced by Private Clouds and Public Cloud as part of IaaS (Infrastructure as a Service) services.

Private Enterprise Clouds are an especially attractive scenario as they offer cost efficiency while maintaining traditional level of security. A Private Cloud is a pool of resources available for sharing within a given private or enterprise entity. In the simplest form, it is dedicated storage or computation hardware with a virtualization layer allowing for the management of multiple virtual units under the same physical unit. Private clouds offer effective resource sharing which provides cost efficient and a scalable alternative for dedicated recording hardware. In a situation where the recoding hardware represents a significant part of surveillance deployment cost, this solution may offer a cost effective solution. Private Clouds offer advantages, such as reliability, performance and without (typical for cloud environments) concerns, such as level of security, management of hosting (especially sharing multiple customer installations on the same physical resources). Additionally, a Private Cloud scenario might be encouraged from a business perspective to provide an adaptation period for familiarization with cloud technology tools and processes. Another argument towards Private cloud computing being first step of the transition to cloud computing is the cost of software adaptation which is relatively low. The basic level of such adaptation should ensure that the system is able to accommodate distributed nature of system storage.

However, the scalability of the Private Cloud might be limited in comparison to Public Cloud..

The choice between Public and Private Cloud computing should be evaluated separately for each part of the surveillance system. Typically, security-critical resources such as user access database, incident video recordings or audio information will not be placed in a Public cloud. However, public camera video recordings or computational resources could be subjects of “full cloud conversion” under public domains.

Dependability analysis for surveillance transition towards cloud

The dependability is one of main properties characterizing the system, next to functionality, performance and cost [4].

There are multiple definitions of dependability. Dependability of a system can be described by the ability to deliver a service that can be trusted and where potential service failures not frequent [4]. ISO definition is focused on availability. IEC definition of dependability combines availability with reliability. In case of safety-critical applications, the safety and security attributes, especially confidentiality and integrity shall be addressed where evaluating system dependability. Additionally, the system maintainability shall be analyzed providing complete overview of dependability of the systems based on a cloud design. Summarizing, the following attributes of dependability shall be analyzed for video surveillance systems: availability, reliability, security (confidentiality, integrity) and maintainability.

A. Availability

Availability of surveillance system is focused on ensuring service continuity by providing access to the system and its resources. Availability and disaster recovery is an essential value of all security-critical systems. Lack of access to system resources and inability to react, investigate and record the incidents are probably the largest risks for surveillance system dependability.

High-end distributed video surveillance systems support high- availability is already implemented providing availability near 99.999 % (five nines availability) of system uptime. The mechanisms to ensure this high level of availability include: keep alive communication, automatic failover for backup devices, software and hardware watchdogs, life cycle management and resource management programs, failover, redundancy and reliability support in the architecture, but also services offering (to provide fast reaction times in case of system problems).

Cloud solutions can offer improvement for availability especially for two types of systems: local small installations and geographically distributed systems. In the case of local, one-box type installations, the offering of cloud services can be used to introduce redundancy mechanisms and disaster recovery tools – before not available for this class of system. It is worth to underline that in case of these local small systems improved availability and virtual accessibility opens new business opportunities, for example outsourcing of business processes which might be a major advantage for small businesses. In case of distributed systems where topology consists of multiple interconnected entities clouds improves availability in a cost efficient way by introducing common redundancy and backup resources and tools. Also, the distributed nature of the cloud itself improves availability – a system hosted in single location is more vulnerable.

A cloud-based offering provides improved system redundancy and a new range of failover mechanisms, for example; the IaaS model disaster recovery service providing a cost competitive alternative to an internal system (both software and hardware) with built-in solutions traditionally relying on watchdog-like applications. The process of migration of a surveillance system is likely to require development to accommodate cloud internal mechanisms for failover and availability and to build-in failover and redundancy mechanisms between hardware and software.

The definition of availability can be extended further to guarantee access to system resources that are provided only for entitled users (unauthorized access is denied). A Cloud provider’s knowledge, awareness and best practices greatly contribute to the level the availability by providing protection of the system infrastructure against low level DoS attacks whilst providing tools and services to protect the resources from being unavailable or corrupted.

Despite the fact that a level of resource availability will be guaranteed by an IaaS cloud service provider (example for Denial of Service attacks) the development related to the improvement of system availability is one of the major tasks for surveillance transition toward cloud computing. There is a significant amount of system development required for the improvement of the authentication, authorization and accounting (AAA) mechanisms as traditionally, these rely partially on high security level of physical access. Special attention shall be paid to improving identity verification which, originally being part of accounting now plays a critical role in security mechanisms applied for communication between the cloud and the rest of the system.

B. Security

Security of a cloud solution is of major concern in the context of a safety-critical system, mainly due to the fact of virtualization; the data no longer resides on dedicated hardware on location that is easy to identify. System security vulnerabilities, such as weak passwords, inefficient virus protection, unauthorized use of access devices or too flexible access rights exist and should be addressed in both traditional and cloud environments.

Security is not defined as single attribute of dependability by Avižienis et al. [4] but it as composite notion of other dependability attributes. Similar approach has been described by Krutz and Vines [6] where security is the concurrent existence of confidentiality, and integrity when availability is ensured.

Confidentiality guarantees the absence of unauthorized disclosure of system resources and other relevant information. Confidentiality is traditionally provided by elements, such as: network security protocols, network authentication services and data encryption protocols. Confidentiality in a cloud system is focused on the confidentiality of transferred data with use of these elements. This means that in the case of a safety-critical system based on cloud architecture there should be a clear security policy in place, defining the exchange of data. It should define entities authorized for access and exchange; the data itself shall be categorized as confidential, sensitive, private, and public to specify the level of protection to be applied. Confidentiality of safety-critical systems based on cloud computing shall be focused on addressing authorization (including identity establishment), access control, rights managements, and encryption requirements (mechanisms and architectural solutions). Identity establishment and management play an important role as being a critical part of process of securing the communication channels between a system and the cloud infrastructure. Cloud-based safety-critical systems shall have at least two factor authentication where type 1 authentication is “something you know” (such as password), type 2 is “something you have” (such as smart card) and type 3 is “something you are“(such as fingerprint). The above suggest the popularity of bio-identification will increase and is being demanded by the safety-critical application market. Additionally, cloud-based surveillance systems shall introduce a public key infrastructure and encryption key management whilst implementing digital certifications and all related issues such as: handling certificate revocations lists, key management, distribution, revocation, recovery, renewal, and destruction. Additional mechanisms can be applied to secure system-to-cloud communication channels, including layered security, segmentation of virtual local area networks and applications, clustering of DNS (Domain Name System) servers for fault tolerance, load balancing and firewalls.

Integrity defines the absence of improper system alterations. The cloud system should ensure the integrity of data during transfer and storage. The system should be able to detect and/or correct data errors and alterations whilst identifying the origin of the data and its accuracy. The integrity of the provided solution shall rely on access control and rights management. It shall be stressed that the integrity of the data shall be secured ‘end-to-end’ including the means of data export. The subject of data integrity is extremely important in the case of video surveillance solutions providing evidence export, reporting and auditing functionalities.

Video surveillance systems, especially the ones with focus on production and delivery of evidence, usually have data integrity mechanisms implemented: they include RAID (Redundant Array of Independent Disks) technologies (to maintain the integrity on the hardware level), file checksums, etc. Data integrity on the physical level can be easily maintained by cloud technology and it is typically part of cloud service offering. Higher level of cloud service offerings, such as PaaS (Platform as a Service) or SaaS (Software as a Service) can also offer file level integrity tools even for exported material. It offers great advantages in terms of flexibility. Different integrity mechanisms can be provided for different surveillance system owners taking into account their different needs and legal considerations, without any internal development required, including: firewall services, communication security management services and intrusion detection services.

C. Reliability

Reliability is focused on service continuity by defining the mechanisms of fault prevention, tolerance (avoidance) to deliver trusted service and removal (reducing) and fault consequence forecasting to define and meet required system dependability specifications.

A Cloud offering provides improved reliability in the form of services and infrastructure. Reliability oriented cloud services include for example; automatic backup and redundancy services, incident response services and safe failover mechanisms. These services can provide the required reliability level without a large investment in capital and human resources, for example; incident response services typically provide analysis of event notification, response, escalation procedures, post-event follow up and incident response management (including for example risk mitigation planning). This type of service offering is very important for large scale applications; the scalability of the offering also provides cost efficiency for small installations where similar services were not previously available.

Automatic backup and redundancy services are provided by the architecture of cloud infrastructure and its distributed nature. It eliminates the need of expensive backup hardware, software and locations providing resources (such as SAN storage areas or computational resources) on demand. Koslovsi et al. [5] provides an overview of reliability advantages brought by cloud infrastructure virtualization which enables transparent and customized reliability provisioning.

It should be underlined that in order to utilize reliability improvements available in cloud technologies the system should meet specific requirements, which include secure access from remote locations and towards cloud, truly distributed architecture where the available mechanisms are independent from location, discipline in traffic monitoring, management and other security mechanisms and also associate processes to be in place.

D. *Maintainability*

Maintainability is the ability to undergo, modifications, and repairs without the need to disable access to the system. The advantage of the transition of video surveillance systems to the cloud depends in great on the service or infrastructure provider. The providers of the cloud infrastructure shall be carefully evaluated for their ability to maintain the agreed terms through service lifecycle starting from adoption phase. However, the current cloud offering is mature enough to provide full range of services assisting the system customer from early phases of the system planning, through phase of deployment, maintenance and ending on systems disposal services (for example to guarantee correct disposal of system information). It is a considerable improvement compared to traditional systems where quite often the availability of resources to deploy surveillance systems project depends on maintenance demands for the existing installation. Therefore, the transition to cloud opens new opportunities in terms of business models for companies providing such systems.

Conclusions

The transition of video surveillance into a cloud service can offer great advantages on system dependability only if the challenges of the transition are known and addressed. Cloud technologies offer different service models of cloud – IaaS (Infrastructure as a Service), PaaS (Platform as a Service) or SaaS (Software as a Service). The cloud infrastructure of the IaaS-based model seems to be the most suitable for the first step of the transition of video surveillance by providing advantages of hardware virtualization, cost scalability and performance. The transition shall be a continuous process. The plan of gradual transition into cloud computing shall be investigated for each system- external system functionalities such as video content analysis modules could be a good candidate for the first step of such transition.

Acknowledgment

The author gratefully acknowledges the contribution of Pete Ward. It should be stressed that the views in this paper are authors own and do not necessarily represent the views of Teleste.

References

[1] ONVIF, www.onvif.org, visited 14.7.2011

[2] Physical Security Interoperability Alliance PSIA, www.psiaalliance.org, visited 14.7.2011

[3] World Wide Web Consortium W3C, http://www.w3.org, visited 14.7.2011

[4] A. Avižienis, J. C. Laprie, B. Randell, “Dependability and its threats: a taxonomy,” IFIP International Federation for Information Processing, vol. 154/2004, pp. 91–120.

[5] G. Koslovsi, Wai-Leong Yeow, C. Westphal, Tram Truong Huu, J. Montagnat, and P.Vicat-Blanc, “Reliability Support in Virtual Infrastructures,” Proc. IEEE 2nd Internat.Conf. on Cloud Computing Technology and Science (cloudCom) IEEE Press, Dec. 2010, pp. 49-58, doi: 10.1109/CloudCom.2010.23.

[6] R. L. Krutz and R. D. Vines, “Cloud Security: a comprehensive Guide to Secure Cloud Computing,” Wiley Publishing, Inc., Indianapolis, 2010, ISBN: 978-0-470-58987-8.