Identifying a True Cloud Security System

A Technical Guide to Cloud Computing's Essential Characteristics

Introduction

Not all physical security industry cloud offerings are true cloud systems. A true cloud system is specifically engineered for cloud computing. It provides valuable capabilities that premises-based systems can't. They are constrained by cost factors and the fixed computing and storage capacities of on-premises servers. Yet some companies install traditional client-server software on a cloud-hosted server and call it a "cloud-based system". This wrongly implies that the software is designed to utilize cloud computing capabilities. Cloud systems engineering is very different from traditional client-server software engineering.

> True Cloud refers to how well cloud system vendors engineer their applications to take a maximum advantage of cloud computing's key characteristics, and enable system provision under a subscription-based, as-a-service model.

A true cloud system's architecture makes maximum use of modern cloud computing technology, through a "pay only for what you use" subscription model. A true cloud system affordably and securely provides scalable capabilities that can't possibly be achieved in client-shttps://www.ivideon.com/video-surveillance-for-business/erver on-premises systems.

Some end-users, security design consultants, and systems integrators remain cautious about cloud-based security applications. The physical security industry does not have a history of timely and flawless adoption of information technology and IT practices. This led to suspicions (in some cases discoveries) that not all solutions promoted as "cloud-based" are true cloud offerings.

However, true cloud security applications do exist. Given the business world's accelerating adoption of cloud computing (see Figure 1), more organizations are open to deploying cloud-based security applications than many security practitioners and security technology specifiers generally realize. This makes it especially important to be able to identify well-engineered physical security cloud applications.

Figure SEQ Figure * ARABIC 1. Current rates of cloud subscription and adoption

Source: 2017 McAfee Report *Building Trust in a Cloudy Sky*

True Cloud Engineering

Cloud computing is an evolving set of technologies, whose key characteristics have been defined by the U.S. National Institute of Standards and Technology (NIST) in 2011, and the ISO/IEC 17788 international standard for cloud computing in 2014. The nature of a true cloud application is well-documented in the cloud development community, as are the most workable software development practices for the creation of cloud applications.

This paper explains the essential cloud computing characteristics and how they apply to a cloud-based video management system (Cloud VMS). Understanding cloud computing characteristics is a prerequisite for identifying a true cloud system of any type.

Identifying True Cloud Systems

Identifying a true cloud system requires answering these true cloud key questions:

1. How are the essential cloud computing characteristics used? What application features and capabilities relate to which cloud computing characteristics?

2. How is the as-a-service model supported? How will the technology be maintained and automatically kept current with technology advances?

3. What is the system's cyber security profile? What cyber security controls are applied to the cloud system? What are the vendor's cloud security practices? Is the system compliant with any cyber security or data privacy regulatory requirements?

4. What are the cloud system vendor's product development practices? What is the vendor's systems development life cycle (SDLC)? How is continuous delivery supported?

Armed with this information, security system end users, integrators, and design consultants will be able to easily identify and compare true cloud systems.

Define Cloud Computing

The foundation for thinking about cloud computing is The NIST Definition of Cloud Computing, which provides this advice: "Cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and

deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best

use cloud computing." [1] This paper is one such discussion.

The NIST document defines the five essential characteristics of cloud computing and describes three services models by which cloud computing services are provided. NIST describes cloud computing as follows:

"Cloud computing is a model for enabling ubiquitous, [2] convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [3]

The ISO/IEC 17788 standard on cloud computing provides this description:

"Paradigm for enabling network access to a scalable and elastic pool of shareable physical or

virtual resources with self-service provisioning and administration on-demand." [4]

The NIST and ISO/IEC documents describe the characteristics of cloud computing that have enabled the cloud to beneficially transform the way we live and work, and the way organizations of all sizes, including governments, conduct business. It stands to reason that these same enabling characteristics, applied to security applications, could transform the way security works, by providing products that are substantially more security-effective and cost-effective than previous generations of security technology.

That is why it is important to understand what cloud computing is, and what its key characteristics can mean for electronic physical security systems.

Client-Server vs. Cloud Software

Client-server software is not designed to take advantage of cloud-computing's scalable resources. It is designed to make optimum use of a server's fixed computing, storage and network capabilities. Client-server software has no ability to change the fixed technology resources on which it runs. This means that the capabilities of a client-server-based system are established by, and constrained by, the fixed resources of the server and network it runs on.Once deployed, scaling up certain system capabilities requires a computer and/or network upgrade.

1 Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing, Special Publication 800-145 (Gaithersburg: National Institute of Standards and Technology, 2011).

2 Ubiquitous: found everywhere.
3 Mell and Grance, The NIST Definition of Cloud Computing.
4 ISO/IEC 17788:2014: Information technology — Cloud computing — Overview and vocabulary.

In contrast, true cloud applications are designed to run on a scalable set of computing and network resources. True cloud applications are able to expand or contract the technology resources allocated to them, according to the work they need to perform.

One technical term for cloud applications is “cloud-native”. A native application is one that has been developed for use on a specific platform or device, and executes more quickly and efficiently because it makes use of the capabilities built into (i.e. native to) the platform or device, without requiring any extra layers of translation or interface. For example, we see the terms “native iOS app” and “native Android app” used to reference mobile apps whose software code is written just for Apple’s iOS or Google’s Android operating system.

Cloud-native is broader in scope as it refers not just to the software code, but to the ability of the application to scale its functionality by utilizing adjustable cloud resources. In November of 2015, the Cloud Native Computing Foundation was established with the specific purpose of creating and driving the adoption of cloud-native design.

Engineering a true cloud system requires developing cloud-native applications, but the concept of true cloud goes beyond that. The concept also refers to how well the cloud computing characteristics are applied to meet two objectives: maximally improving the work of end-user customers, and strongly supporting the effective installation, commissioning, and management of the system under a subscription-based managed services model.

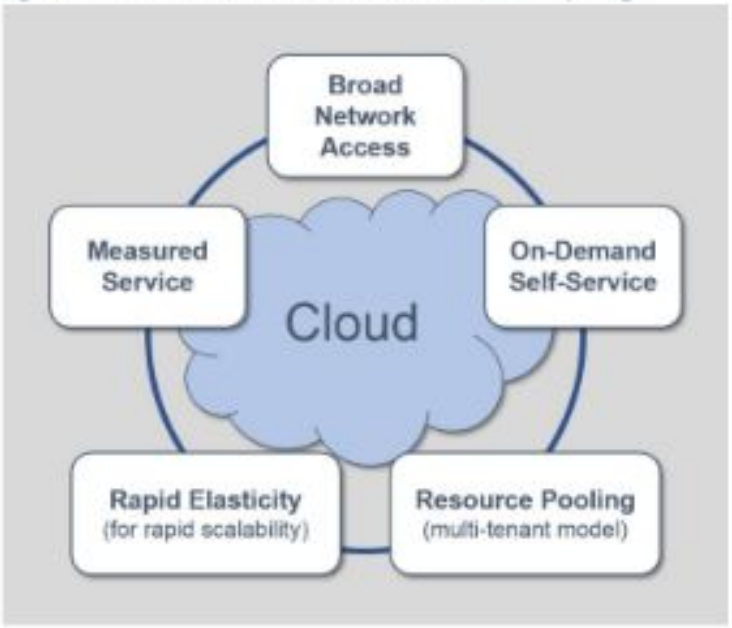
Cloud Computing Characteristics and Service Models

NIST defines five essential characteristics of cloud computing, shown in Figure 2. These characteristics are later described in detail, in the context of the cloud computing service models presented below. NIST defines three commonly known cloud computing service models:

- SaaS - Software as a Service
- PaaS - Platform as a Service
- IaaS - Infrastructure as a Service

These service models form a tiered progression with

Figure . The Essential Characteristics of Cloud Computing



IaaS at the bottom and SaaS at the top. The three tiers are also referred to as the Cloud Computing

Technology Stack. These are depicted in Figure 3.

There are several important aspects of the cloud computing service models:

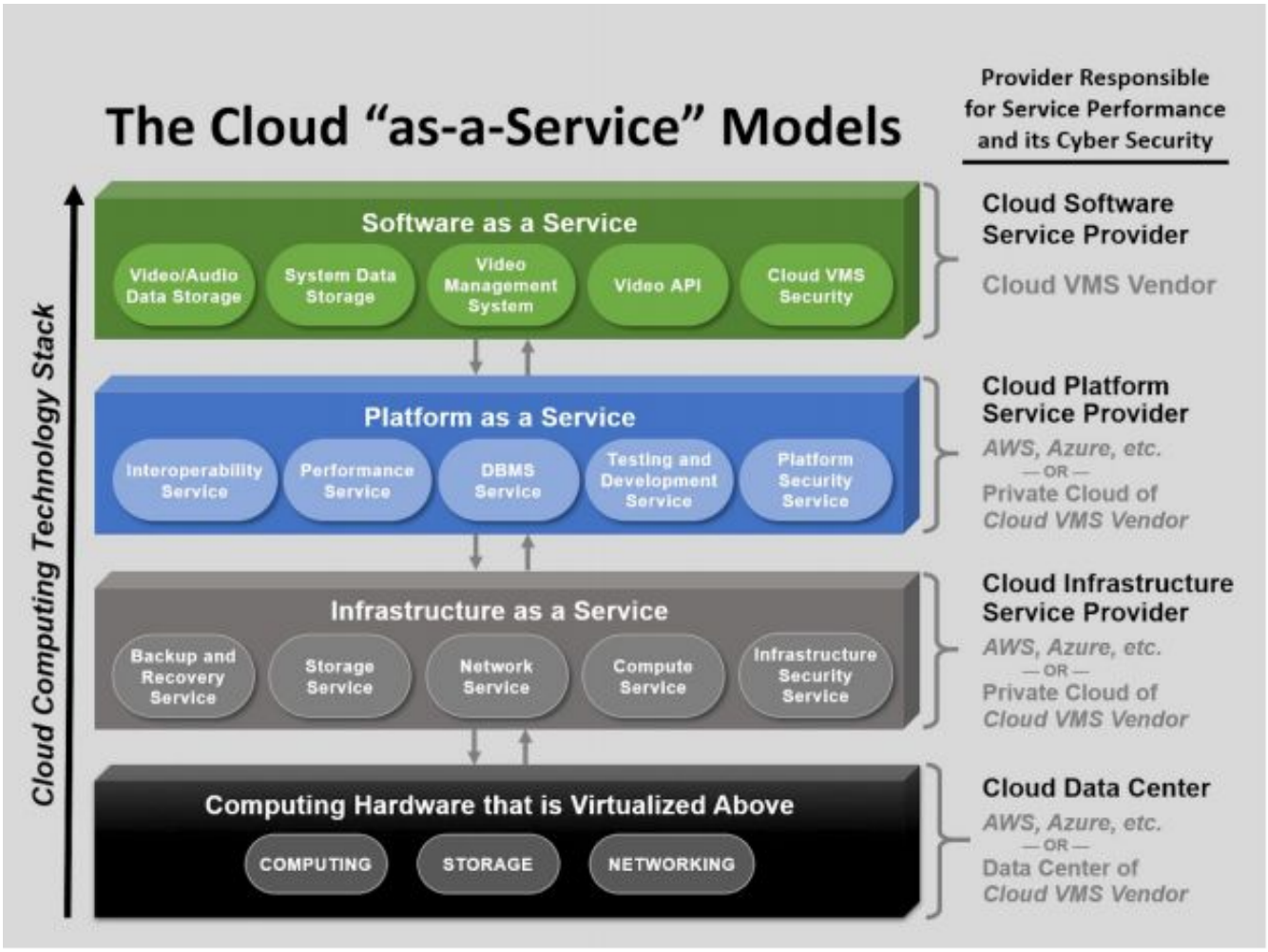
- Each service model provides the resources that make the next service model tier possible. Hence, the technology stack concept.
- The five essential characteristics of cloud computing apply to each tier.
- All cloud engineering technology advancements are in the direction of improving the essential characteristics of cloud computing in one or more of the cloud computing tiers.
- Advancements in the cloud-computing essential characteristics improve:
    - Application development/deployment capabilities
    - Business support for cloud customer service
    - Cost efficiencies
    - Cloud infrastructure performance
    - Cloud technology monitoring and management capabilities
    - Granularity and flexibility of end-user on-demand self-service
    - Micro-billing options for users
    - Portability and interoperability options

Cloud Service Models

Figure 3 below illustrates an example cloud service models structure as described in the NIST Definition of Cloud Computing. There are security responsibilities for each service model, which are defined in Service

Level Agreement terms. (Note: for the sake of readability, not all the service elements are for each model. For example, networking exists in each service model, but is not shown in the platform- or software-as-a-service models.)

Figure 3: The Three NIST Cloud "as-a-service" Models



The cloud computing essential characteristics apply to each service model tier, and must be built into that tier of service by the service provider.

Cloud Computing's Essential Characteristics

The cloud computing essential characteristics, pictured in Figure 2 on the previous page, are explained below, primarily as they apply at the SaaS level of the services structure, because that is the part of the cloud computing technology stack that end users interact with. Some of the general-purpose language of the NIST Definition of Cloud Computing has been updated for this paper with wording that is specific to Cloud VMS deployments. The definition of each essential characteristic is followed by examples of how they can be

applied in a Cloud VMS.

1. **Broad network access**. Cloud VMS capabilities are provided via a network and Accessed through standard mechanisms, such as Internet Service Provider connections and corporate networks that provide Internet access. This enables use by various kinds of client devices (e.g., mobile phones, tablets, laptops, and workstations).

   Implications of Internet Access. Internet network bandwidth is not unlimited, and is not under the control of the Cloud VMS. It depends upon the location and level of Internet service that each end user has available. Therefore, a Cloud VMS must be engineered to detect and respect the available bandwidth, tolerate low-bandwidth conditions, withstand brief network outages, and continue to provide a consistently good user experience.

2. **Resource pooling**. The computing resources of the cloud infrastructure provider (such as Microsoft Azure, Amazon AWS and others) are pooled to serve multiple subscribers using a multi-tenant model, with different physical and virtual resources dynamically assigned and re-assigned according to subscriber demand. Examples of resources include storage, compute processing, memory, network connections and connection bandwidth.

   Multi-Tenant Model. Multi-tenant model is a software architecture in which a single instance of software, or a specific cloud resource, serves multiple subscribers, referred to as tenants. A tenant is a group of users (for a security system, this could be employees and building occupants) who share a common access with specific privileges to the software application and its stored data. Under the multi-tenant model, each subscriber's allocated cloud resources are separate and distinct from those of another subscriber, so that each subscriber can only access its own data and will only use its own allocation of computing resources (necessary for accurate billing).

   Contrast with Client-Server Hosting. This contrasts with how client-server software is hosted in the cloud, with each subscriber being given a separate virtual server, application, and database. In a true cloud application, each cloud system's data center runs only a single instance of its application software and any databases, which is shared by all subscribers using secure isolation of resources allocated to each tenant.

   Affordability. Resource pooling is invisible to the end users of a cloud-based system, but is important because it is a primary cost-efficiency factor that makes cloud computing technology affordable.

3. **On-demand self-service**. An end user can configure the cloud system or select system options, and the system accordingly provisions the required computing capabilities, such as server computing time and storage, as needed automatically without requiring human interaction with cloud service providers.

   Automatic Video Storage on Demand. For example, in a Cloud VMS an end user should be

   able to set the number of days for a camera's video retention period, with the system automatically provisioning or de-provisioning video data storage as needed to achieve compliance with the required retention period. This kind of capability is no small matter, as many video systems are set to record based upon motion in the camera's field of view. If there is a spike in motion activity, as can happen for outdoor cameras in a geography with a rainy season, the volume of recorded video data can increase ten-fold or more. A Cloud VMS should automatically expand the video storage resources as needed to achieve the required video retention. When the rainy period ends and the additional storage provisioned is no longer needed, it will be automatically deprovisioned and returned back to the storage resources pool.

   Video Analytics On Demand. A Cloud VMS could provide on-demand use of video analytics functions, a perfect fit for K-12 school districts that want to use activity-recognition analytics to identify prohibited activities that typically occur only during holidays, graduation months, and summer breaks. Analytics usage could be billed in convenient increments, such as a week or a month of usage.

4. **Rapid elasticity**. Capabilities can be elastically provisioned and released, preferably automatically, to scale rapidly up and down commensurate with demand. To the application end user, the capabilities often appear to be unlimited and can be appropriated in any quantity at any time.

   Emergency Mobile User Notification. For example, if a cloud-based emergency notification application needed to send out a message to 5,000 employee mobile users, the network capabilities to establish several thousand mobile device connections at once would be automatically allocated to that subscriber, for the duration needed to accommodate the message broadcast and receipt of the mobile users' return responses.

5. **Measured service**. Cloud systems automatically control and optimize resource use by leveraging a metering capability within the cloud infrastructure, at some level appropriate to

the type of service (e.g., storage, processing, network bandwidth, and active user accounts).

Resource usage can be monitored, controlled, and reported, providing transparency for both the cloud services provider and the subscriber who is utilizing the cloud service.

Measured service enables the implementation of “pay only for what you use” features, which Are found in a well-engineered cloud application.

Cloud computing characteristics can be combined to work together. For example, in the Automatic Video Storage on Demand feature, the combination of resource pooling, On-demand self-service and rapid elasticity work together to optimize the use of storage resources, with measured service also applied, to ensure that the Cloud VMS subscriber pays only for the increments of video storage that are actually used, according to the subscription terms. This is an example of how multiple cloud computing characteristics can be applied to achieve application-specific system capabilities and end-user benefits.

Video Surveillance as a Service (VSaaS)

The security industry has introduced the term Video Surveillance as a Service. There are two architectures for VSaaS. One is a purely SaaS model, where cameras connect directly to the Cloud VMS. The other model combines SaaS with Hardware as a Service (HaaS) for on-site video bridges [5] and local recording. When VSaaS includes a HaaS model for on-site equipment, the hardware may be provided on a subscription-based managed-services model or as a purchase with automatic updates provided by subscription.

Automatic System Updates

Firmware and software updates for on-premises Cloud VMS hardware are automatically provided by the Cloud VMS vendor as part of the VSaaS subscription - no action is needed on the part of the customer or the integrator.

---

5 A bridge device receives audio/video streams from cameras, optionally performs analytic processing and generates related metadata, and encrypts the audio/video streams and analytics metadata. According to system configuration and video processing rules, it sends some of it immediately (i.e. in real time) to the Cloud VMS, and buffers the rest of the data until schedules

or rules call for it to be sent to the Cloud VMS.

Strong Cyber Security Protection

Providing Cloud VMS software and hardware as a service also means that responsibility for system security is no longer a burden on the end-user. It is included as part of the service. A Cloud VMS must include security features like those listed below. “Appliances” refers to the on-premises video equipment provided by the Cloud VMS vendor.

On-Premises Equipment Cyber Security

- No inbound internet connections accepted
- Cameras are isolated from the Internet
- Appliances have no open network ports
- Appliances are protected against pre-installed camera malware
- Appliances use TLS connections to the Cloud VMS
- Encryption applied to buffered and locally recorded video
- Appliance authentication via digital certificates
- Collaboration regarding customer advanced networking requirements

Data Center Physical Security

- Facility alarmed intrusion detection system
- Biometric facility area access control
- 24/7 on-site security personnel
- 24/7 on-site live and recorded video monitoring
- Security desk visitor identity verification and visitor log
- Biometric physical access control
- Local key management is enforced for racks and cabinets
- Extensive screening and background checks for Cloud VMS vendor’s personnel with data center or Cloud VMS access.
- Data center network security
- Network perimeter firewalls
- Network intrusion prevention systems
- Network address translation (NAT)
- Network segmentation to isolate database servers
- Logical and physical separation of data center environments from Cloud VMS vendor’s

corporate network

Redundancy

- Cloud VMS components are redundant (active/active or active/passive)
- Triple-redundant video data storage

Application & Data Security

- Regular server vulnerability scanning
- Regular penetration testing
- API level security
- Multi-tenant data security controls
- Web and mobile application use two-factor authentication
- Use mobile device fingerprint authentication
- Web and mobile application TLS connections to the Cloud VMS
- AES encryption of recorded video
- MD5 checksums provided with each video clip export, stored in the cloud, to enable verification that a downloaded video clip had not been tampered with

Support for As-a-Service Business Model

To properly support the VSaaS model, all the components of a true Cloud VMS, whether located in the cloud data center or on the end user's premises, must be engineered to support the business requirements of the integrator/reseller. This includes providing features like remote system configuration, pre-installation configuration (such as camera configuration setup without requiring the cameras to be installed and online beforehand), customer account management dashboard, system performance metrics for bandwidth and data storage both on-premises and in the cloud (an extension of metered service), automated camera discovery, auto-connection by on-premises equipment to the Cloud VMS, and automatic recovery actions for cameras that are powered up but have gone offline (request video stream, reboot camera, and finally alert users to offline status if not recovered). Another important Cloud VMS capability is a modern well-supported public and secure API, to facilitate the integration of custom applications that are needed in various business sectors.

VSaaS True Cloud Elements

The four true cloud key questions, listed in the section Identifying True Cloud Systems on page, apply to both the SaaS and HaaS portions of a VSaaS system. Although the HaaS hardware elements of a VSaaS deployment are not located in the cloud data center, they must be designed to maximally support the essential cloud computing characteristics, being part of a cloud-based system.

A true cloud system:

- Makes maximum use of the essential cloud computing characteristics
- Supports software and hardware as-a-service delivery
- Has strong cyber security for both on-premises and cloud-based elements
- Is developed through a continuous delivery process

As cloud computing technology advances, and the physical security industry continues to adopt cloud computing, the true cloud key questions will continue to provide the answers needed to identify and compare true cloud systems.

Conclusion

Cloud systems engineering is very different and much more advanced than software engineering for server-based client-server applications. It provides system capabilities previously not possible, which is why cloud-based services continue to transform the way people live and the way organizations operate. Technology in all industries is being transformed by cloud computing capabilities.

In the physical security industry, cloud computing is replacing the product-based 5- to 10-year security system life cycle with service-based continuously-evolving security system capabilities. Product obsolescence is being replaced by continuous delivery. The continuous delivery factor is important, because as organizations continue to change and evolve, so do their physical security risks. Thus, security system deployments must be able to rapidly evolve to address these changes—one reason why true cloud security systems are needed.

About Eagle Eye Networks

Founded in 2012 by owner and CEO Dean Drako, Eagle Eye Networks, Inc., (‘Eagle Eye’) is the leading global provider of cloud-based video surveillance solutions addressing the needs of businesses, alarm companies, security integrators, and individuals. Eagle Eye's 100% cloud-managed solutions provide cloud and on-premise recording, bank level security and encryption, and broad analog and digital camera support – all accessed via the web or mobile applications.

Businesses of all sizes and types utilize Eagle Eye solutions for operational optimization and security. All Eagle Eye products benefit from Eagle Eye’s developer friendly RESTful API platform and Big Data Video FrameworkTM, which allow for indexing, search, retrieval, and analysis of live and archived video. Eagle Eye's open Video API has been widely adopted for integration in alarm monitoring, third party analytics, security dashboards, and point of sale system integrations.

Eagle Eye sells its products through authorized global resellers and installation partners. Headquartered in Austin, Texas, USA, Eagle Eye has offices in Europe and Asia.