Security in Military Cloud Computing Applications

Miroslav Ďulík[1],
Miroslav Ďulík[2], Junior

[1]Department of Informatics, Armed Force Academy,
Liptovský Mikuláš, Slovakia, miroslav.dulik@aos.sk
[2]Institute of Aurel Stodola, Faculty of Electrical Engineering,
University of Žilina, Slovakia, dulik@lm.uniza.sk

Abstract. Cloud computing presents a significant technology trend not only in public sector but also in military sphere and has become a smart solution for providing a flexible computing environment for military applications. This work describes types of cloud computing models and cloud service model SPI (Software, Infrastructure, and Platform). Consequently we describe the private cloud security model based on the private cloud reference model. This paper shows the security technologies and mechanisms for implementing security in private cloud applications, where the high levels of security is necessary and proper.

Keywords: Military Cloud, Cloud Computing, Private Cloud, Security, Private Cloud Security Model, Security Technologies

1 Introduction

Cloud computing is still an evolving technology paradigm. Its definitions, used cases, underlying technologies, issues, risks, and benefits will be refined in a spirited debate by the public and private sectors. These definitions, attributes, and characteristics will evolve and change over time. The cloud computing industry represents a large system of many models, vendors, and market niches. This definition attempts to encompass all of the various cloud approaches.

Cloud computing is a model for enabling ubiquitous, 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.

2 Essential Characteristics of Cloud Computing

The Cloud can provide the following security benefits:

- Centralized data
- Segmented data/applications
- Better logging/accountability

- Standardized images for asset deployment
- Better resilience to attack & streamlined incident response
- More streamlined audit and compliance
- Better visibility to process
- Faster deployment of applications, services, etc.

In [1] is defined cloud model, which is composed of essential characteristics, service models, and deployment models. For characterization of the basic principle cloud computing are inherent these characteristics:

- *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- *Rapid flexibility.* Capabilities can be flexible provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

The existing computing paradigms e.g. Distributed computing, SOA (Service-Oriented Architecture), networking etc. are building blocks of cloud computing. There are numerous issues associated with theses computing paradigms and some new challenges emerged from cloud computing are required to be addressed properly in order to realize the cloud to its full extent. Current cloud adoption is associated with numerous challenges.

In the next part we offer insight into challenges that organizations has to face with adopting cloud with a focus on what it means to face these challenges and realize business opportunity once these challenges are understood and resolved [2].

- *Cost of Entry*. Implementing a cloud in the organization will require a significant entry cost to satisfy the needs of virtualization and the management layers that compose the fabric to deploy, operate, and monitor the environment. These costs must be realized in each step of the deployment process from prototyping to production. Over time these costs will turn to cost benefits as shared resource usage wins over traditional forms of resource allocation on a per application instance basis.
- *Data Location.* When discussing cloud computing, the challenge of data location within the cloud surfaces as an impediment to adoption. This is likely the prime reason that drives the private cloud deployment model into the discussion, because it alleviates the concern of placing enterprise data in the public cloud. In a private cloud deployment model, enterprise data remains in-house but due to the management characteristic of a private cloud the infrastructure required to satisfy data storage is largely commoditized.
- *Security.* Designing for a secure environment is always a challenge as new threats continue to emerge on a regular basis. In that sense this is not a new concern for cloud computing, but the attack surfaces and vectors are different in cloud computing and must be understood. Private clouds mitigate many of these attack surfaces since the entire operation is in-house, however organizational concerns still exist when meeting compliance requirements.
- *Compliance.* In any IT organization the goals of IT must be met while maintaining conformance to organizational and regulatory compliance requirements. This compliance will drive cloud computing deployment models and the management layers to establish and implement management boundaries for sensitive data storage and transmission throughout the cloud infrastructure.
- *Application Programming Models*. When considering cloud computing adoption within the organization, a challenge will likely surface around the existing application programming model and tools for development and test. This will drive an evaluation of the migration effort to move legacy application to the cloud and ongoing development of new applications for the cloud.

2.1 Cloud computing in military sphere

Cloud computing is based mainly on Internet (protocol TCP/IP) and offers cost reduction, flexibility, reliability, availability and energy-saving, and these gain has became a solution for flexible computing applications.

Cloud technology has great utility for the military. Transitioning to cloud based solutions and services advances the military's long term objective to reduce cost ownership, operation and sustainment of hardware and other commoditized IT. Procuring these as services will allow the military to focus resources more effectively to meet evolving mission needs. Over time it will significantly boost IT operational efficiency, increase network security, improve interoperability with mission partners, and posture the military to adopt innovative technology more quickly at lower cost.

The importance of this trend for military is proved for example in USA DoD (Department of Defense) strategy "Cloud Computer Strategy" [3] issued in July 2012 and Army document "Army Cloud Computing Strategy", issued in March 2015 [4].

According to US Army researchers, this move will provide mobility, scalability, resource sharing, automation, and cost savings which will be available in diverse platforms. Previous command and control systems developed were usually using proprietary protocols thus it was very difficult to share data with the other organizations. Based on tactical cloud computing, new services can be developed using toolkits, software development kit, and a common framework which can be easily distributed and implemented.

This new development, various command and control systems can be interrelated thereby allowing seamless exchange of information via web services. These new systems must still comply with the security and standards guidelines.

Presents command and control systems send rare information to big data centers tens or hundreds of km away. However, real time access is not very possible with limited network connectivity and low bandwidth. Thus, the modern military information systems (for example cloud placed directly on battlefield) is able with limited resources in tactical environments can still be flexible and robust, and similar to that of enterprise capabilities like inter-cloud federation, cloud integration with military communications, security, fault tolerance, load balancing, rapid provisioning, and resource management.

The military will continuously assess and weigh the potential benefits of various cloud deployment models against potential risks, such as:

- Increased technical complexity
- System performance and outages
- Competitive, congested and contested cyber electromagnetic environment
- Data storage and information security
- Changes in vulnerability attack vectors
- Government data storage legal compliance

2.2 Types of cloud computing deployment models

In cloud computing, we define cloud computing into two distinct sets of models:

- *Deployment Models*: This refers to the location and management of the cloud's infrastructure.
- *Service Models*: This consists of the particular types of services that you can access on a cloud computing platform.

There are four primary Deployment Models. A deployment model defines the purpose of the cloud and the nature of how the cloud is located [5]:

- *Private cloud*. The private cloud infrastructure is operated for the exclusive use of an organization. The cloud may be managed by that organization or a third party. Private clouds may be either on- or off-premises.

- *Community cloud*. A community cloud is one where the cloud has been organized to serve a common function or purpose. It may be for one organization or for several organizations, but they share common concerns such as their mission, policies, security, regulatory compliance needs, and so on. A community cloud may be managed by the constituent organization(s) or by a third party.
- *Public cloud.* The public cloud infrastructure is available for public use alternatively for a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud.* A hybrid cloud combines multiple clouds (private, community, or public) where these clouds retain their unique identities, but are bound together as a unit. A hybrid cloud may offer standardized or proprietary access to data and applications, as well as application portability.

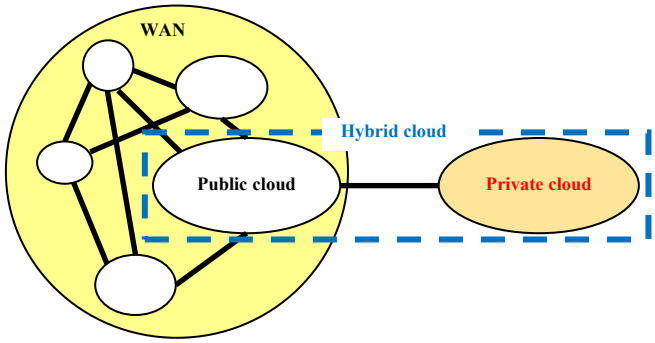

Figure 1 Types of clouds [6]

Individuals typically use public clouds-such as those provided e.g. by Amazon.com, Google, and Apple. Large entities with vast amounts of sensitive data have turned to private, "secure" clouds. The most concerned users, current and future, are government agencies, especially the military, processing high sensitive data [7], [8].

Due to the special security needs of military applications cloud computing (e.g. CCC - Combat Cloud Computing [9], COMBAT – mobile-Cloud-based cOmpute/communications infrastructure for BATtlefield applications [10]) desire to create a secure and reliable system is the most proper the private cloud version [11].

The main advantages of Private Cloud Computing [11]:

- Highly available, fault-tolerant architecture
- Military grade datacenter security, hosted on multi-tiered private infrastructure
- More secure that public, community or hybrid cloud offerings

Concise comparison of public and private clouds:

Public cloud

- Low investment hurdle
- Negative loss and control over data
- Higher risk of multi-tenancy data transfer

Private cloud

- High investment hurdle
- IT organization (military) retains control over data
- IT organization (military) control security technologies implementing

3 Private Cloud Computing and Security

In private or hybrid cloud implementations, rather than remove the perimeter network altogether, it is possible place all other networks outside the perimeter into the untrusted zone. Figure 2 provides a conceptual representation of this change.

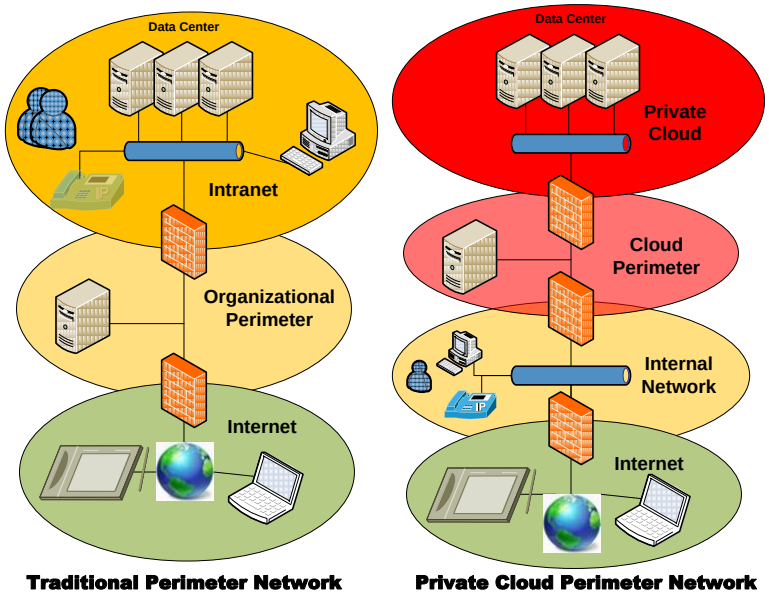

Figure 2 Perimeter network in private cloud environment [12]

3.1 SPI model of cloud computing

The cloud provides options for approach, sourcing, and control. It delivers a well-defined set of services, which are perceived by the customers to have infinite capacity, continuous availability, increased agility, and improved cost efficiency. To achieve these attributes in their customers' minds, IT must shift its traditional server-centric approach to a service-centric approach. This implies that IT must go from deploying applications in silos with minimal leverage across environments to delivering applications on pre-determined standardized platforms with mutually agreed upon service levels. A hybrid strategy that uses several cloud options at the same time will become the norm as organizations choose a mix of various cloud models to meet their specific needs.

Cloud options typically are categorized by the following SPI (Software, Infrastructure, and Platform) service models [13]:

- *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- *Cloud Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storages, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

It is useful to think of cloud computing's service models in terms of a hardware/software stack. One such representation of the cloud reference model is shown in Figure 3 [6]. At the bottom of the stack is the hardware or infrastructure that comprises the network elements. As you move upward in the stack, each service model inherits the capabilities of the service model beneath it. IaaS has the least levels of integrated functionality and the lowest levels of integration, and SaaS has the most.

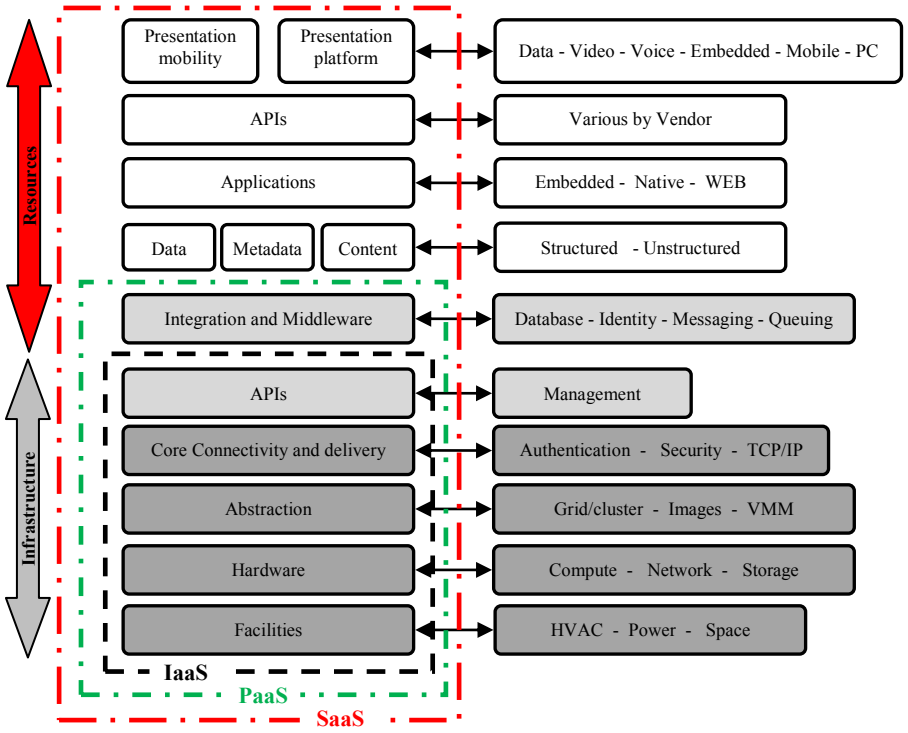

Figure 3 Cloud computing service reference model and underlying cloud infrastructure [6]

3.2 The private cloud reference and security model

The private cloud security model uses the same design as the private cloud reference model but replaces the capabilities with mechanisms for implementing security. Figure 4 shows how these mechanisms tie in to the different layers of the private cloud reference model [14].

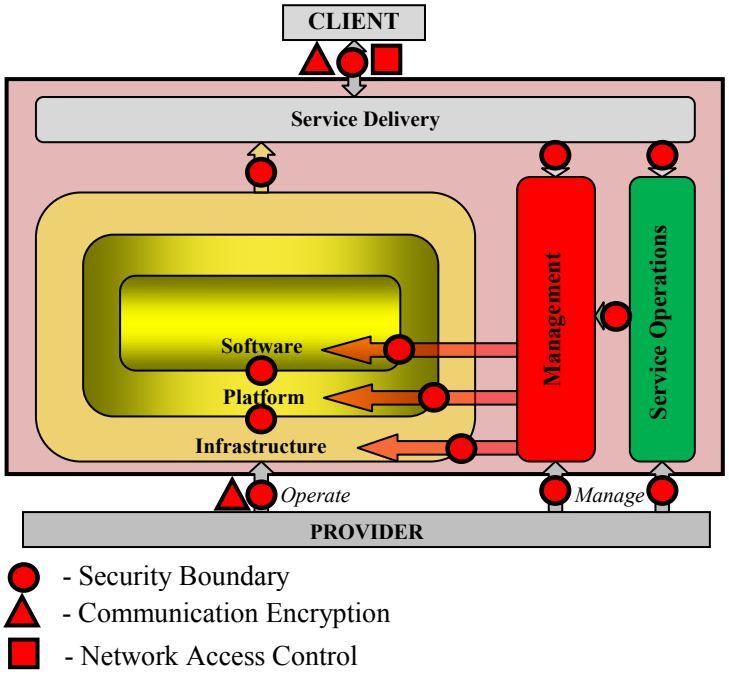

Figure 4 The simplified private cloud security model and security components

The next part of this paper builds up this security model by considering each component of the private cloud reference model and analyzing the factors that apply at each layer and stack and includes the security components [14]:

- Private cloud security wrapper functionality
- Infrastructure security
- Platform security
- Software security
- Service delivery security
- Management security
- Client security
- Legal issues

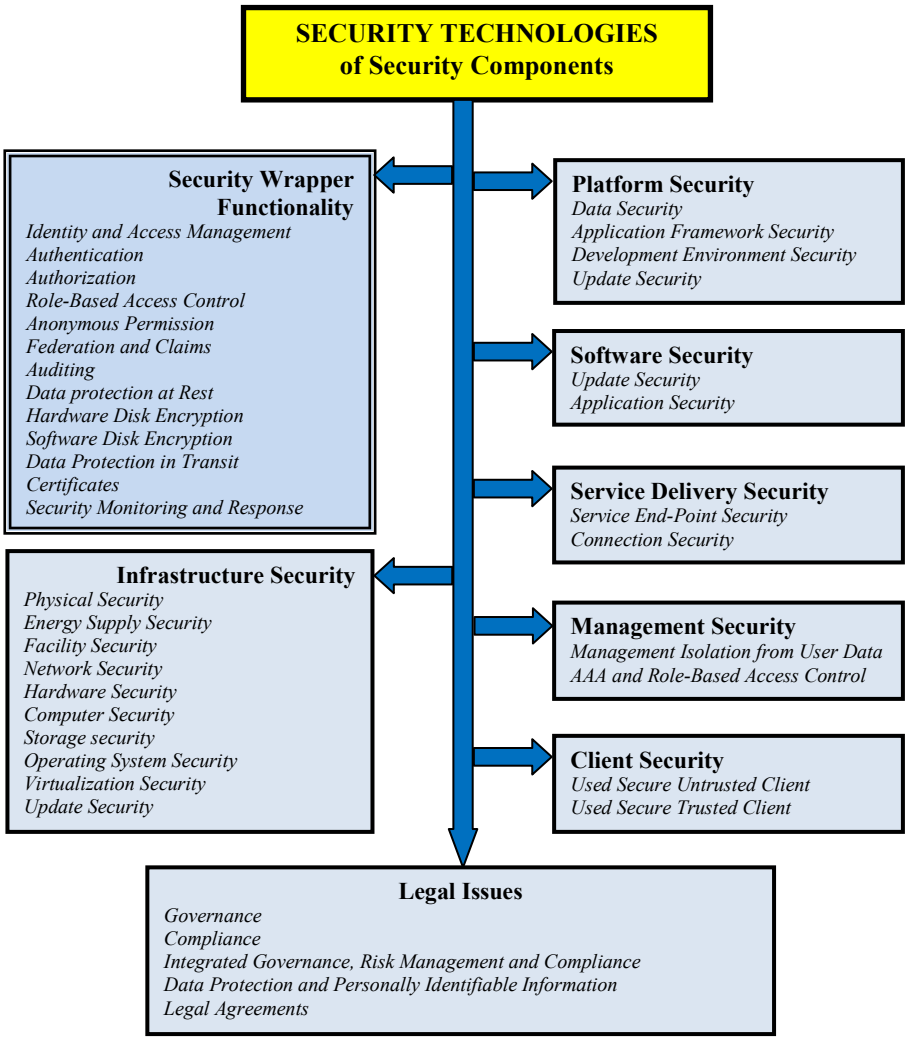

Figure 5 The security technologies of security components in a private cloud security model

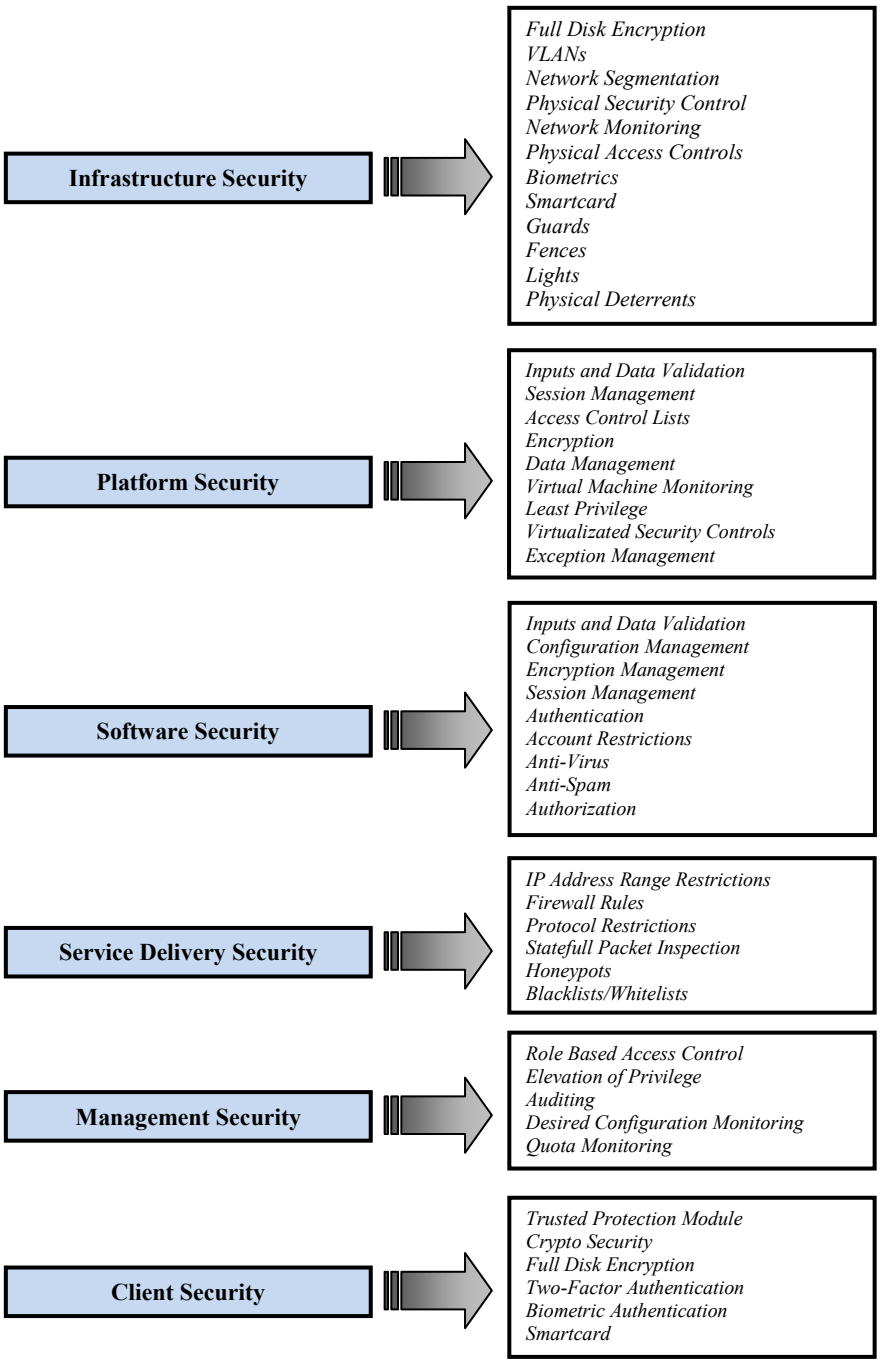

Figure 6 The security mechanisms and services in security components of private cloud security model

This section has presented a spectrum of security issues that organization should consider for information security in private cloud, but it should not be considered exhaustive. More about cloud security threats and countermeasures is at a reference [15].

4 Conclusion

Based on previous studies and the definition of a private cloud, private clouds will immediately seem to be more secure than public clouds because of how the infrastructure is designed. It gives the organization more control over their policies and security. According to NIST, the internal private cloud is more suitable deployment models that offer an organization greater oversight and authority over security and privacy. Private cloud also better limit the types of tenants that share platform resources, reducing exposure in the event of a failure or configuration error in a control.

Private clouds are built for the exclusive use of one client, providing the highest control over data, security and quality of service. The company owns the infrastructure and has control over applications being provided. Private clouds may be deployed in an enterprise datacenter, and they also may be deployed at a co-location facility.

Acknowledgement

This paper was realized thanks the support of the APVV-0025-12 Project – Mitigation of stochastic effects in high-bitrate all-optical networks.
This work was supported by project ITMS: 26210120021, co-funded from EU sources and European Regional Development Fund.

References

1. Mell, P. – Grance, T.: The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-145. Gaithersburg, Maryland 2011.
2. Private Cloud – A Technical Perspective. https://technet.microsoft.com/en-us/cloud/hh147296.aspx.
3. Cloud Computing Strategy. Department of Defense, Chief Information Officer, DoD, USA, July 2012.
4. Army Cloud Computing Strategy. Office of the Army Chief Information Officer/G-6. Version 1. March 2015.
5. Badger, L. et al.: Cloud Computing Synopsis and Recommendations. NIST Special Publication 800-146. Gaithersburg, Maryland 2012.
6. Sosinsky, B.: Cloud Computing Bible. Wiley Publishing, Inc., Indianapolis, USA, 2011. ISBN: 978-0-470-903356-8.

7. Wilson, J. R.: The challenge of a secure military cloud. November 14, 2013. http://www.militaryaerospace.com/articles/print/volume-24/issue-11/technology-focus/the-challenge-of-a-secure-military-cloud.html
8. Forika, K. T.: Application of cloud computing in the defense industry: An academic and practical viewpoint. AARMS, Vol. 11, No. 2, 2012. National University of Public Service, Budapest, Hungary.
9. Goztepe, K. – Cehreli, I. – Sensoy, S. E.: A Decision Framework for Combat Cloud Computing Strategy. 6th International Information Security & Cryptology Conference. Proceedings. 20-21 September 2013, Ankara, Turkey.
10. Soyata, T. et al.: COMBAT: mobile-Cloud-based cOmpute/communications infrastructure for BATtlefield applications. Proceedings of SPIE, vol. 8403-20, Apr 2012, Baltimore, USA.
11. Simmonds, D. – Wahab, A.: Public Cloud Computing vs. Private Cloud Computing: How Security Matters. Research Paper. Cameron University, Lawton, Oklahoma, 2012.
12. Cloud security Challenges. Microsoft, 2015 http://social.technet.microsoft.com/wiki/contents/articles/6651.cloud-security-challenges.aspx
13. What is Infrastructure as a Service?. Microsoft, 2015 http://social.technet.microsoft.com/wiki/contents/articles/4633.what-is-infrastructure-as-a-service.aspx
14. Private Cloud Security Model. Microsoft, 2015 http://social.technet.microsoft.com/wiki/contents/articles/6653.private-cloud-security-model.aspx
15. Meier, J. D.: Cloud Security Threats and Countermeasures at a Glance. Jul 2010 http://blogs.msdn.cpaperom/b/jmeier/archive/2010/07/08/cloud-security-threats-and-countermeasures-at-a-glance.aspx