Information & Security

Published since 1998

R. Iliev & K. Ignatova
vol. 43, no. 1 (2019): 89-97
https://doi.org/10.11610/isij.4308

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Implementation of Cloud Technologies for Building Data Centres in Defence and Security

Rosen Iliev* (✉), *Kristina Ignatova

Bulgarian Defence Institute, Sofia, Bulgaria
https://www.mod.bg/bg/EXT/InstitutOtbrana/index.htm

ABSTRACT:

This article presents an analysis of cloud technologies as key current trend in the development of IT infrastructure, their main characteristics, security levels and the increased requirements they must meet when considered for defence and security applications. It provides an overview of main standards and requirements that modern data centres have to meet to ensure a high level of availability of the provided IT services. Specific requirements have been formulated for building a sustainable system of modern data centres for defence and security needs, and attention has been paid to data protection when using cloud technologies. A solution is proposed for implementing cloud technologies and an approach for building an integrated data centre system for defence and security needs in organizing collaborative work between officials within the organization.

ARTICLE INFO:

RECEIVED: 20 JUN 2019
REVISED: 3 SEP 2019
ONLINE: 17 SEP 20XX

KEYWORDS:

cloud technologies, data centre, virtualization, cloud computing, defence, security

Introduction

Cloud technologies have entered very fast into all spheres of the modern world. By using them, the hardware is reduced and the reliability of the information services is increased, the development of information infrastructures of different organizations is optimized. A major advantage of cloud computing is the ability to

✉ Corresponding Author: E-mail: r.iliev@di.mod.bg

allocate costs and resources between users, as well as access to information services for them regardless of where they are located. The important thing to achieve this is by providing available network connectivity.

Cloud computing is a technology which provide computing services to users, and these services (software and information) are typically in the form of WEB. It also provides access to the hardware and system resources of the data centres that offer these services. In this way of organization and operating computer systems, the provided computer resources (processor time and computer memory) can be optimally distributed and dynamically enhanced through virtualization technologies.

Cloud computing includes collaboration, agility, scaling and availability and provides opportunities for cost savings through optimization and efficient resource management. This is also the solution for outsourced software, platforms and infrastructure. This technology allows ubiquitous access to cloud computing configurable resources, such as networks, servers, storage arrays, applications and data centre services.

According to their visibility clouds are divided into private, public, hybrid and community.[4]

Each of them has different security features and levels, which determine their applicability.

The public cloud is an IT infrastructure, platform, or service that is publicly available on the Internet and maybe free of charge or active against payment. This cloud is deployed in the field of CRM, communications, offices, and so on. In the field of defence and security, it is appropriate to support information systems for work with outside clients and organizations. An example of such type of cloud is a Gmail platform.

The Private Cloud is a cloud infrastructure that combines the IT services of a company or organization and is not accessible to external organizations and individuals. It is managed by a private (internal) data centre organization and thus the company assures the integrity and security of its data. The private cloud has a higher price and security level than the public cloud. It is protected by a firewall and can only be accessed through an internal secure network. Processes, services, and information are managed within the organization itself, so there are no additional safeguards, legal requirements or network constraints in the cloud that exist in public cloud structures. Cloud service providers and customers build optimized and controlled infrastructure with increased security by eliminating network access for external users.

Private cloud is preferred option for building internal information infrastructure in organizations related to defence and security. An example of a private cloud is the IT infrastructure of a bank.

The Hybrid Cloud is a combination between private cloud and public cloud, and aims to reduce the cost of performing different functions within the same organization by increasing the flexibility of the infrastructure, going beyond the corporate physical data centres. An example of a cloud organization is a bank that manages data and IT systems in-house, but uses a public cloud backup to store the backup encrypted copy of the data. It is precisely this type of cloud that would be very suitable for use in the defence and security sphere, as it offers higher security for the data it stores.

The Community cloud is an infrastructure shared by several organizations that form a community that shares close interests such as: security, terms of use, compatibility requirements and more. This cloud type offers a higher degree of privacy, security, and compatibility policy. It is appropriate for building IT platforms for co-operative activities of various military organizations. An example of such a cloud is the Google Gov Cloud project.

Figure 1 shows the four main types of clouds according to their visibility, focusing on their most important action in terms of their use in defence and security.

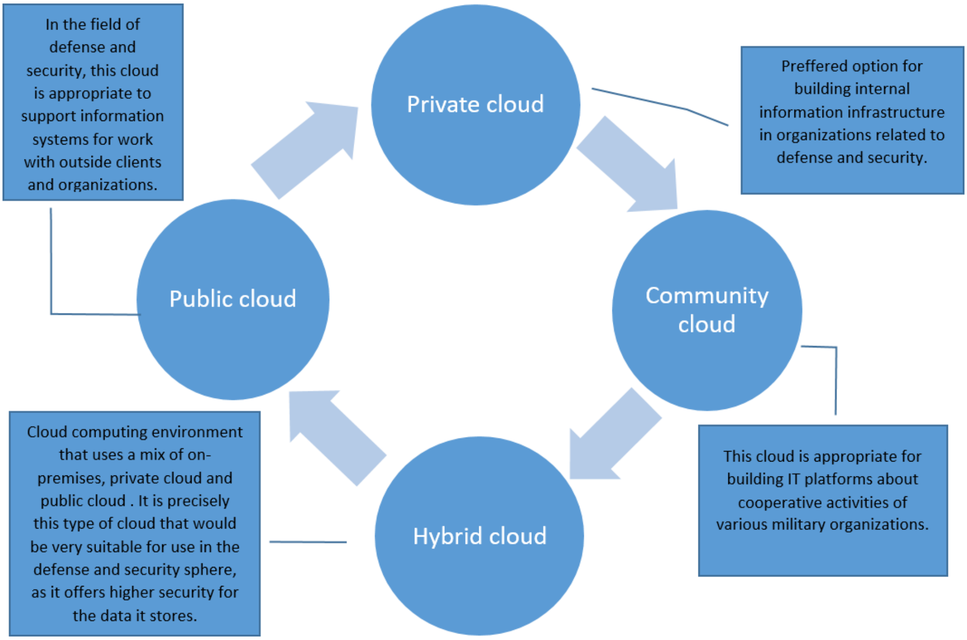
In the field of defense and security, this cloud is appropriate to support information systems for work with outside clients and organizations.
Private cloud
Preffered option for building internal information infrastructure in organizations related to defense and security.
Public cloud
Community cloud
Cloud computing environment that uses a mix of on-premises, private cloud and public cloud . It is precisely this type of cloud that would be very suitable for use in the defense and security sphere, as it offers higher security for the data it stores.
Hybrid cloud
This cloud is appropriate for building IT platforms about cooperative activities of various military organizations.

Figure 1: Cloud types according their feasibility in defence and security.

One of the first and most known cloud provider companies are Amazon (Amazon Web Services), Google (Google AppEngine), VMWare, Microsoft (Microsoft Azure), Apple (Apple iCloud), IBM, Citrix Systems, Oracle in Bulgaria - Cloud.bg and others.[7]

Data Centres Based on Cloud Technologies

Modern data centres are engineering and technical facilities designed to provide information resources with a high level of security and affordability. This places higher demands on the performance and reliability of their systems for processing and storing information, the communications environment, power supply, air conditioning, fire protection, security and other support systems.[3]

With the development of cloud technologies and the need to consolidate services, modern data centres are becoming increasingly important and emerging as cores for processing, storing and providing information. New standards are introduced for their construction, which determine the level of availability (reliability) of the centre, its cabling, the types of spaces (premises), the permissible operating environment conditions, as well as the requirements for disasters and fire. These standards are developed by various institutes, associations and companies, such as Uptime Institute Tier Certifications, TIA 942, EU Code of Conduct in Data Centres, ISO / IEC 24764, BDS EN 50173-5, DCA, ASHRAE Standard, NFPA Standard, and more.

LEVEL	Availability requirements
Tier 1	*Ensure 99.671 % availability*
Tier 2	*Ensure 99.741 % availability*
Tier 3	*Ensure 99.982 % availability*
Tier 4	*Ensure 99.995 % availability*

Figure 2: Data centre levels.

The Uptime Institute Tier Certifications[11] defines four levels of accreditation related to the design, construction and stability of the data centre (Figure 2). Service availability levels (centre operation) are determined from the allowable interruption of the data centre for one year. For example, at tier 1, the allowable break is 28 hours per year, and at the highest level (tier 4), only 26 minutes per year.[12] Depending on the requirements and availability needs, it is determined at which level the data centre is built.

The Telecommunications Industries Association (TIA)[16] has developed a data centre standard called TIA 942. It defines the factors leading to the creation of a sustainable data centre in terms of architecture, electricity, mechanics, telecommunication components.

The Bulgarian State Standard (ENS) EN 50173-5 is based on the European standard EN 50173-5 and prescribes general wiring requirements for the provision of IT services as well as the connection of large quantities of equipment within the limited space in the data centres.

The International Organization for Standardization (ISO) also offers a standard for cable systems in data centres. ISO / IEC 24764[17] includes requirements for wiring systems, wires and hardware devices.

The European Code of Conduct in Data Centres[8] addresses the environmental and economic impacts of energy consumption in centres.

A number of authors have identified and outline good practices for building modern data centres.[1, 4, 6, 9] They include the design of data centre and the architecture of the support systems and its overall structure. However, for the needs of defence and security, the integration of the individual centres into a data centre system needs to be done in such a way as to provide the necessary redundancy at the level of "cloud infrastructure." To achieve this, the following approach is proposed:

- Identification of the specific services subject to virtualization in the cloud computing of the defence and security authorities (MoD, Ministry of Interior, etc.) that are used by the respective users and the determination of the single point of failure and their need for redundancy;
- Summarizing data on the average number of concurrent users who use certain services;
- Gather data on the load of hardware resources during work and the amount of information for storing each service;
- Determining the capacity of the hardware resources needed to ensure the performance of a given service in the virtualized cloud computing environment, booking the work of the same.

The size of data centres for defence and security needs depends on the volume, degree of availability and availability of the services offered, and also the number of users of these resources. The data centre should be considered as a small room with built-in infrastructure (guaranteed power supply, air conditioning, fire alarm, fire extinguishing, communication connectivity, etc.), racks for servers, disk arrays, relevant communication equipment and surveillance and management.

When designing and building a new data centre system, the individual centres need to be the same, with a single hardware and software platform to allow for better compatibility, interchangeability, easier training of administrative and operational staff, and etc.

When building up modern data centres, the following three important requirements must be met:

- The continuity of information resources and access to them;
- High consolidation, scalability and flexibility, based on cloud technologies and virtualization;
- Reliable protection and storage of information.

Behind the fulfilment of these conditions, there are many communication-information and support systems that provide the necessary communication, climate, physical and information protection, redundancy and overall – high reliability.

Implementation of Cloud Technologies in Defence and Security

Implementing cloud-based solutions to defence and security will optimize the cost of building high- performance information centres, provide easy access to a wide range of services, enable integrated IT solutions, and make more effective use of information resources. One proposed solution for organizing collaborative work between officials based on the use of cloud technologies in data centres is through:

- Creating highly organized virtual platforms to provide cloud resources of the three types – "Software as a Service" (SaaS), "Infrastructure as a Service" (IaaS), and "Platform as a Service" (PaaS);
- Creating online user applications available through a web browser to meet the computing needs of users while data and software are stored on servers from the centralized infrastructure;
- Reserve critical information in outreach Data Recovery Centres;
- Building IC-environments to integrate multiple services into a single point of access by the user, in accordance with the imposed security policies;
- Establishment of Groupware systems to ensure the high integration of physically remote users involved in collaborative processes and to provide a face-to-face exchange of information between them;
- Providing users with integrated services such as knowledge sharing, group calendars and schedules, document processing in a group environment, organizing workflows, etc.;
- Integrating information and communication resources into a single entity and building unified communications to integrate audio, video and data, as well as user services such as instant messaging, presence information telephony (including IP telephony), video & audio conferencing, data sharing, call control, voice recognition, integrated voice mail, e-mail, SMS and Fax), etc. ;
- Building intelligent management systems based on Soft-Collision and Decision Support Systems by the Managing Authorities. These systems are particularly applicable in the presence of inaccurate and incomplete information on the problems solved, in the necessity to make quick decisions in the absence of sufficiently trained specialists, as they successfully "mimic" the processes of reasoning and decision- making by man;
- Optimizing the energy saving infrastructure (Green Energy);
- Provide enough space for data storage and processor resource in the cloud, as well as the ability to create copies of the documents produced on the local computer;
- Providing "continuity" at the time and place of activity of a user on the web, and this "mobility" of access to documents and services must provide high reliability and security;
- Organizing effective information protection and minimizing the probability of unauthorized access or interference with systems, programs and services.

For defence and security purposes, building data centres by applying cloud technologies is particularly important. The cloud computing will improve the availability and accessibility of services (from anywhere on the network after authorization), making them more reliable and faster (due to large computing capabilities) and providing more redundancy to information resources (low "denial of service"). Cloud computing, distributed over interconnected data centres, will enable self-service (automatic redistribution of resources to achieve optimal use), large capacity (disk space), and flexible administration, monitoring and management of services. It will help ensure faster disaster recovery, as the information is stored in more than one data centre in the cloud.

In recent years, a prototype of a virtualized server platform has been developed at the Defence Institute at the Ministry of Defence to provide cloud computing such as PaaS and SaaS platforms. A platform for deploying multiple virtual servers with built-in specialized software (E-mail server, DV server, WES server, GIS server, servers for Domain Controllers, Groupware, etc.). The information services provided by this cloud infrastructure are organized in a common information WEB environment to work by creating a public information portal for the exchange of information and the ability to use e-mail, document sharing), instant messaging, electronic signature, organization of information and document flow between officials and others. A model for defining the software system state has been developed on the basis of in-depth analysis of virtualization systems in cloud architecture design.[2, 5]

Security of Solutions Based on Cloud Technologies

Cloud technologies are exposed to continuous threats and attacks that may adversely affect organizational data (missions, functions, image or reputation), organizational assets, individuals or other organizations. Their protection is subject to in-depth research to detect and eliminate threats.[18]

Defence and security data centres are also the subject of malicious attacks using both known and unknown vulnerabilities to compromise the privacy, integrity, or availability of the information being processed, stored, or provided.

When building security and defence data centres, attention needs to be paid to the risks associated with project management, investment, legal responsibility, safety, security of information, etc. Risk management must be a cyclical process, consisting of a set of coordinated activities for supervision and control of individual risks. This process is aimed at enhancing strategic and tactical security and involves the implementation of a risk mitigation strategy and the use of control techniques and procedures for continuous lifecycle monitoring of IT systems and data centres as a whole.[15]

Conclusions

Cloud computing and virtualization are the most modern areas at the moment in which many resources and know-how are invested. It has emerged as the main platform for enabling the relative independence of software solutions from hardware, upgrading and multiplying information resources, centralized management and decentralized use of services, integration of various security solutions.

For example, the European Union will fund a € 15.7 million project, called the Vision Cloud (Virtualized Storage Services Foundation for Future Internet), to explore new cloud computing technologies, including data mobility and access control.[10]

Building a system of modern defence and security data centres will improve not only the integration of information resources and services, but will also increase the reliability and reduce the denial of service.

Modern virtualization and cloud infrastructure technologies create an effective storage, accessibility, and computing environment to meet the ever-growing challenges of today's information world. Building a sustainable system of modern data centres is a serious solution not only for the needs of defence and security but also outside them.

References

1. Michael A. Bell, "Use Best Practices to Design Data Center Facilities," *Gartner Research*, April 22 2005, https://www.it.northwestern.edu/bin/docs/DesignBestPractices_127434.pdf, accessed August 15, 2019

2. Maya Bozhilova, "A Model for Defining the Software System State," *Proceedings of Sixth International Scientific Conference "Hemus-2012"* (2012): II-51 - II-56.

3. "Cisco Data Center," www.cisco.com/c/en_uk/solutions/data-center-virtualization/what-is-a-data-center.html, accessed May 09, 2019.

4. "Cloud Technologies," www.icn.bg/bg/blog/novini-ot-icn-bg/oblachni-tehnologichni-modeli-za-predo, accessed on May 09, 2019.

5. Anguel D. Genchev, "Analysis of Virtualization Systems in Cloud Architecture Design," *Proceedings of Conference "Military Technologies and Systems" - MT&S-2013*, Sofia, Defence Institute (2013): II-25 to II-40.

6. Steve Greenberg, Evan Mills, and Bill Tschudi, "Best Practices for Data Centers: Lessons Learned from Benchmarking 22 Data Centers," *ACEEE Summer Study on Energy Efficiency in Buildings*, 2006, https://pdfs.semanticscholar.org/f598/0e93db698188071e70f10858af6bbdb81cda.pdf, accessed August 15, 2019.

7. "Guide to Cloud Computing," *Information Week,* https://www.informationweek.com/cloud/cloud-computing-2019-the-cloud-comes-of-age/d/d-id/1333442, accessed on June 21, 2019.

8. Mark Acton, Paolo Bertoldi, John Booth, Liam Newcombe, Andre Rouyer, and Robert Tozer, "2018 Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency," Version 9.1.0, JRC Technical Reports, European Commission, 2018, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110666/kjna29103enn.pdf, accessed August 30, 2019.

9. “The Best Practices in Data Center Design & Installation” *Colocation America*, May 21 2019, https://www.colocationamerica.com/blog/data-center-design-best-practices, accessed August 15, 2019

10. “Project Description: Internet of Services, Software & virtualization,” *CORDIS EU Research Results*, 2019, https://cordis.europa.eu/project/rcn/95928/factsheet/en, accessed 20 June, 2019.

11. Uptime Institute, https://uptimeinstitute.com/, accessed August 20, 2019.

12. “Datacenter – Part 2: What’s a Tier?” *Network Alliance*, Mar 7, 2018, https://networkalliance.com/datacenter-part-2-whats-a-tier, accessed on August 20, 2019.

13. Michaela Iorga, “Managing Risk in the Cloud,” National Institute of Standards and Technology, 2019, https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=919234, accessed May 09, 2019.

14. “What are the Top Ten Data Center Best Practices?” *TechXact,* 2019, https://www.techxact.com/blog-what-are-top-ten-data-center-best-practices, accessed August 15, 2019.

15. “Standards,” *Telecommunications Industry Association*, 2019, www.tiaonline.org/what-we-do/standards, accessed May 10, 2019.

16. International Organization for Standardization, https://www.iso.org/home.html, accessed May 10, 2019.

17. D. Mahlianov and Nikolai Stoianov, “The Security of the Internet of Things,” *Proceedings of Eighth International Scientific Conference “Hemus-2016”* (2916): III-217 – III-225.

18. Veselin Tselkov and Nikolai Stoianov, “A Formal Model of Cryptographic Systems for Protection of Information in Computer Systems and Networks,” *Proceedings of Bulgarian Cryptography Days – BulCrypt 2012*, Sofia (2012): 15-29.

About the Authors

Rosen **Iliev** is Associate Professor in “Automated Systems for Information Processing and Control” and secretary of the Scientific Council of the Defence Institute “Prof. Tzvetan Lazarov,” in Sofia, Bulgaria. He holds a Masters Degree in Computer Systems and Technologies from the Technical University of Sofia. In his PhD dissertation he explores the application of advanced IT in the process of command and management of engineering troops. His current research interests are in cloud technologies and their application in sensitive domains.

Kristina **Ignatova** is a PhD student in the Defence Institute “Prof. Tzvetan Lazarov,” in Sofia, Bulgaria, working in the field of advanced information and communications technologies and infrastructures.