Military Applications of Cloud Computing

Milena H. Lambeva and Boycho N. Zlatinov

Vasil Levski National Military University, Artillery, Air Defense and CIS Faculty, Department of Computer Systems and Technologies, 1 Karel Shkorpil str., 9713 Shumen, Bulgaria

Abstract. Nowadays cloud computing are being used by many areas of human activities. This paper discusses about application of cloud calculations in defense, with accent on Secure Cloud computing architecture and (DOD) – milcloud that features integrated suite of capabilities designed to drive agility into the development, deployment and maintenance of secure Department of Defense.

Keywords: cloud computing, defense, milcloud.

1. INTRODUCTION

Information superiority determines the outcome in every contemporary armed conflict.

Therefore, modern armies persistently follow the development of information technology. Nowadays, the most popular technology is cloud computing. This technology covers all areas of human activity. It also proved to be appropriate for the sphere of security and defense. Due to the specificity of the subject area related to the confidentiality of information, the research is based on Internet sources and consists of a study of the practice of US military agencies.

2. CLOUD COMPUTING

According to the NIST: "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. This cloud model is composed of five essential characteristics, three service models, and four deployment models." Cloud computing are suitable for use in defense purposes:

- enables networks to be consolidated in order to achieve the goals of efficiency and effectiveness;
- enables more operative information sharing between subdivisions;
- enables the use of different devices (sensors, mobile devices, radars, computers, etc., as Fig. 1 shows).
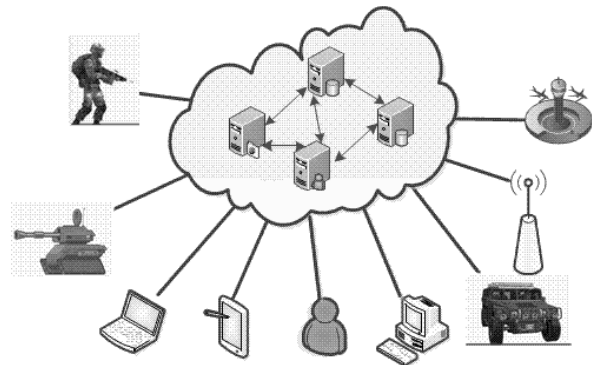

Fig. 1 Diversity of devices in cloud range.

On the other hand, there are a number of challenges:

- Downtime related risk: Because cloud computing services are provided via the internet, there's always a chance that it could be temporarily separated from the data until the connection is back up and running;
- Strong commitment to having an Internet connection. In the event of a conflict, an attack on the Internet connection may be fatal to the afflicted country and resolve the outcome of the conflict in favor of the enemy;

- Confidentiality related risk: The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals;
- Integrity related risk: The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

3. CLOUD COMPUTING IN USA ARMY

3. 1. Secure Cloud Computing Architecture

Defense Information Systems Agency (DISA) is a U.S combat support agency that connects the U.S military and government though IT and communications support.

One of the applications of cloud calculations in defense is Secure Cloud Computing Architecture (SCCA), developed by the Defence Information Systems Agency (DISA). SCCA is a number of services that provides the same level of security that is generally provided to DISA Data Center mission's partners. SCCA comprise four components: Cloud Access Points (CAP), Virtual Data Center Security Stack (VDSS), Virtual Data Center Managed Services (VDMS) and Trusted Cloud Credential Manager (TCCM), as shown on Fig. 2.

- Cloud access points have two major functions: to provide partners on a mission with a special connection with approved commercial providers of cloud services at level 4 and 5 and to protect DISN (Defense Information Systems Network) against any attacks from the external cloud environment;
- VDSS serves as a virtual security enclave to protect applications and data hosted in a commercial environment. It includes two core services: Web Application Firewall (WWF) and Next Generation Firewall (NAF). VDSS's WAF and Next Generation Firewall are designed to detect and prevent threats against web applications and data streams. VDSS mimics the features of the traditional data center security stack;
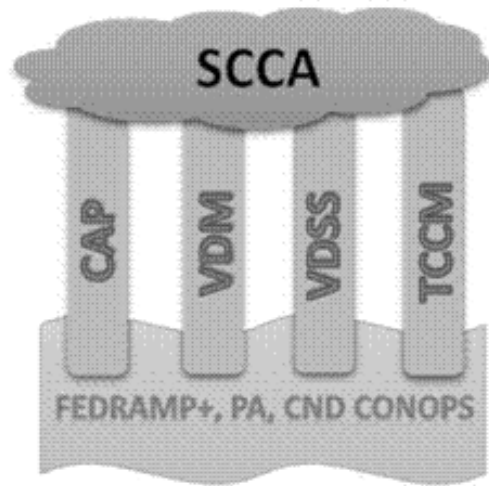

Fig. 1 Diversity of devices in cloud range.

- Five services fall within VDMS, including the Host-Based Security System and Assured Compliance Assessment Solution. They enable mission partners to configure and deliver security policies, push upgrades, and manage roles and security policies;
- TCCM includes the processes and procedures to control and monitor privileged user access for cloud environments. It provides the checks and balances for mission partners to grant them access only to appropriate groups or individuals.

Another product of cloud calculations in defense developed by Defence Information Systems Agency is "milCloud".

3. 2. MilCloud

MilCloud is a set of cloud-services product, govern by the Defense Information Systems Agency. It posses integrated capabilities designed to drive agility into the development, deployment and maintenance of secure Department of Defense (DOD) applications. MilCloud is an Infrastructure as a Service (IaaS) solution that leverages a combination of mature

Commercial off the Shelf (COTS) and government developed technology to deliver cloud services tailored to needs of the DOD. Products used in milCloud portfolio feature the common cloud services characteristics:

- On-Demand, Self-Service: milCloud consumers can place orders on-demand through web-based self-service tools, configure infrastructure resources where appropriate, and manage their mission application's lifecycle running on those resources without manual intervention from DISA support staff;
- Broad Network Access: All milCloud products and services have network connectivity to the DOD Information Networks (DoDINs), and are configured in accordance with relevant DOD security guidelines and approved protocols;
- Resource Pooling: milCloud resources are pooled such that multiple mission partners consume units from pools provisioned by DISA, enabling efficient use of aggregate resources and greater consumption flexibility;
- Rapid Elasticity: The milCloud portfolio has the ability to expand or contract resource use within virtual resource pools.
- MilCloud provides different capabilities. Portfolio includes a comprehensive suite of infrastructure cloud services with a robust self-service ordering and management interface. milCloud products are augmented by, and in some cases directly integrated with, other DISA Enterprise Services:
- Virtual Data Center (VDC) is "virtual floor space." The mission partner has direct access to a web-based self-service control panel to manage the configuration of assets (e.g., processor, storage, network) within the VDC.
- milCloud Orchestrator provides mission partners the opportunity to streamline and automate the management of functions related to the build, test, and migration of

environment configurations in a VDC. In return for an upfront investment in time and engineering resources to create a "recipe, a system operator can expedite creation of instances of that environment. Additionally, milCloud Orchestrator can automate numerous labor intensive and repetitive activities, such as functional regression testing. Mission partner administrators control how recipes are shared and made available to other users in milCloud.

4. THE PROSPECTS OF CLOUD SERVICES IN BULGARIAN ARMED FORCES

According to "Security and defense security and technology strategy", one of the possible ways to increase the capacity and effectiveness of the Bulgarian Army is the use of promising information technologies.

Cloud technologies and virtualization in building the information infrastructure will reduce the surplus and increasing the reliability of services provided to combat units. The research and application of this technology for the needs of security and defense will help to optimize spending on building high – performance information centers, using the wide range of services, creating integrated information - communication solutions and enable more efficient use of information resources.

The application of this technology in defense will ensure higher flexibility in the use of services and easier access (through WEB-browser), higher mobility of users (services can be access via mobile devices), higher availability of services (reservation of the program-technical devices in a separate infrastructure, with independent user support), and higher reliability of storage of data.

The main challenges and future interests and goals are related to the current intentions of the country's investment policy for:

- implementation of information and communication products based on using the

cloud computing and virtualization technology;

- maintaining sufficient research and technology abilities in this technological sub-region;

- researching for opportunities to implement this technology to build high-tech server platforms, due to their high technological and economic significance.

5. CONCLUSIONS

Cloud computing has found application in the civilian sphere and in many foreign armies.

Opportunities for applying cloud technologies for defense purposes have been assessed by the Bulgarian Force Command and have a vision for their implementation.

Their use in the Bulgarian army needs improvement.

REFERENCES

Concept Technology Areas, Subdivisions and Technologies for Implementing the "Strategy for Research and Technology in Security and Defense", Available at:

http://www.micmrc.government.bg/files/conc.pdf, visited on 05.11.2018 (full text in Bulgarian)

National Institute of Standarts And Technology available at https://www.nist.gov/, visited on 01.11.2018

Defense Information Systems Agency, available at: https://www.disa.mil, visited on 01.11.2018