# Cloud computing security requirements: A Review



# Cloud computing security requirements: A Review

**G R Tsochev[1], R I Trifonov[1]**

[1] Department of Information Technologies in Industry, Technical University of Sofia, Bulgaria

E-mail: gtsochev@tu-sofia.bg, r_trifonov@tu-sofia.bg

**Abstract.** Cloud computing is a new technology that is undergoing tremendous development today. People who use it are not able to separate the reasonable from the unreasonable arguments that come with the security requirements in the cloud. The claim that cloud computing is hereditarily insecure is as absurd as the claim that cloud computing does not create new security problems. Cloud computing is a way to dynamically increase resources without the need for in-depth knowledge of a brand new infrastructure, without training new workers or designing new software solutions. The article aims to analyse the different cloud security issues and models of cloud architectures. Some of the main problems with security in virtualization, concerns about storing data in the cloud and the assessment of risk tolerance in cloud computing are presented. Legal and regulatory issues for the protection of personal data are addressed.

## 1. Introduction

Cloud Computing is the most important trend in the IT Industry (figure 1). Even the biggest critics seem to agree that – in spite of some over-zealous marketeers – Cloud Computing is one of the most important paradigm shifts of the past decades. But what is it all about? Where did it come from? And what's to be expected? There are probably as many definitions of Cloud Computing as there are self-acclaimed Cloud Specialist.

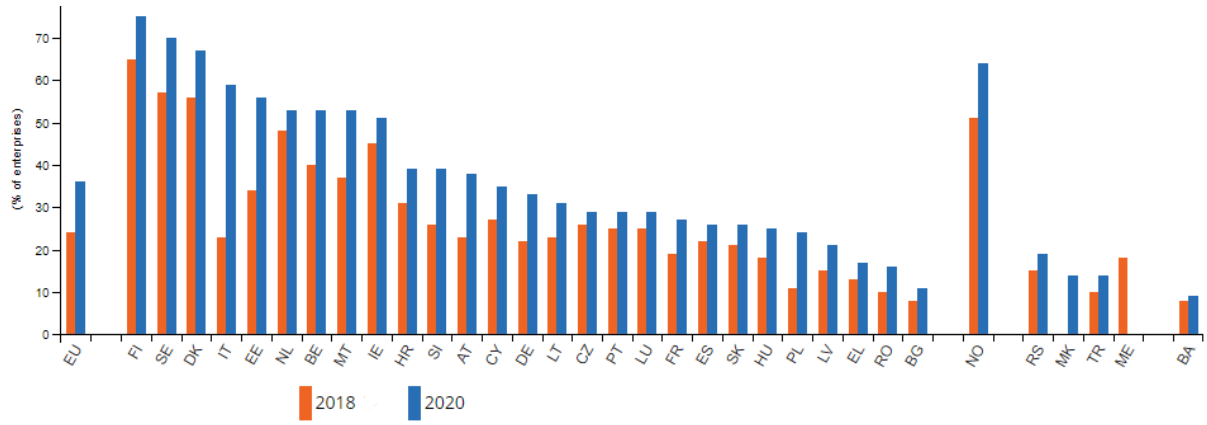


**Figure 1.** Use of cloud computing services in EU [1]

The truth is that the cloud computing concept is really simply, it is has been simple for decades. Have you ever been heard the sayings “Two heads thinks better than one.”, “Nobody knows everything but everybody knows something.” and so on and so on? The technical definition could sound like “Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid.” [2] or “Cloud computing is the utilization of many servers housed in many different locations and interconnected by high speed networks.” [3] although the marketing and sales guys are defining it as a new way of delivering IT services that are cheaper, flexible and really easy to use. As you may already think the truth is somewhere between. The main specifications of the cloud computing are lower cost, flexibility, scalability and “pay-per-view” or usage on demand. Cloud computing is on-demand access to virtualized IT resources that are housed outside of your own data center, shared by others, simple to use, paid for via subscription, and accessed over the Web. While this does reflect a common experience, in reality it is a fairly limiting definition. For example, what about the requirement that everything is provided ‘‘as a service over the Internet?’’ That might seem attractive at first, yet it does not allow for the reality that there are many applications—for sound, unemotional, pragmatic considerations—that will require a private deployment (off the Internet). A team at the National Institute of Standards and Technology (NIST) has been doing some very good work to bring some order to these discussions [4]. Here is their working definition:

“Cloud computing is a model for enabling 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 promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models.” [5]

The most important is to understand that cloud computing is not a technology, it is a concept. It is a concept that could be used in many different ways, cloud computing is Gmail, amazon, Google, SaleForge, torrents, etc. This concept simply means that if you connect two computers and make them work as one they will have more computing power then every one of them separated. Now imagine if you connect thousands (figure 2).

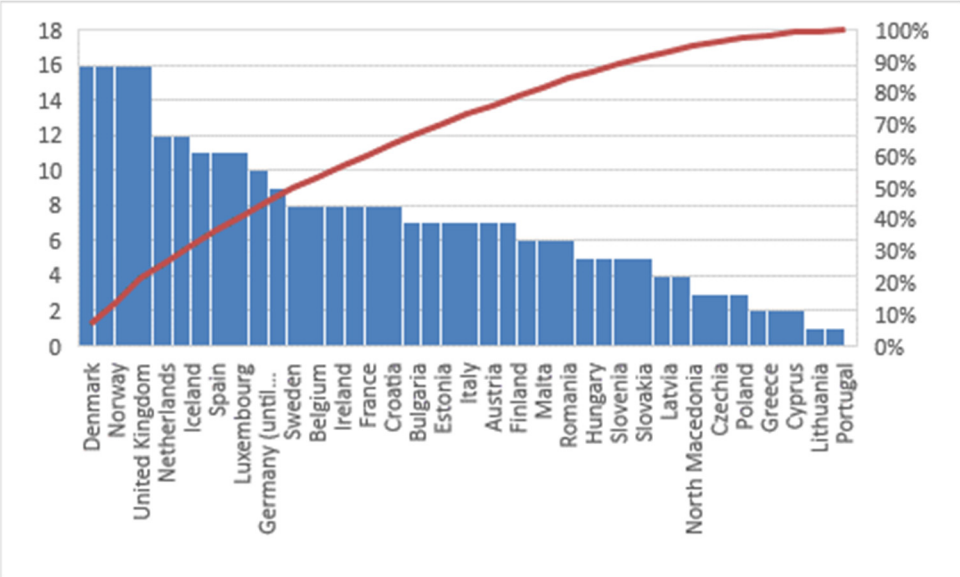


**Figure 2.** Problems experienced when using cloud services [1]

Cloud services have gradually become a key feature of modern computers, smartphones and tablets [6]. Each leading company in the industry offers consumers its own offer in this segment (figure 3),

which significantly intensifies the competition in it. Cloud technologies are a flexible, highly efficient and proven platform for providing IT services over the Internet. However, their increasing use and the provision of cloud services by providers creates a number of risks associated with ensuring the protection of information.

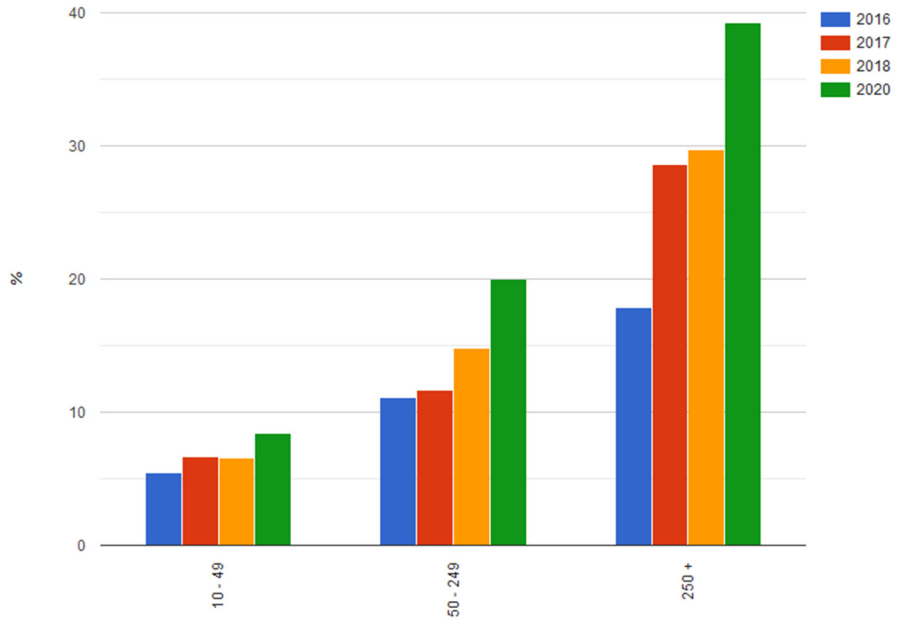


**Figure 3.** Enterprises using paid computer services in the cloud [7]

## 2. Security architecture

In order to avoid ineffective and expensive operation, broken governance, hard to automate controls or procedures and poor security, sound foundations of principles, structure and methodology must be established.

Systems engineering is a methodology for achieving integration by viewing the collective of components as a hole rather than an assembly. Each component should be designed in a way that will interoperate with the rest. Figure 4 shows the scope systems engineering.

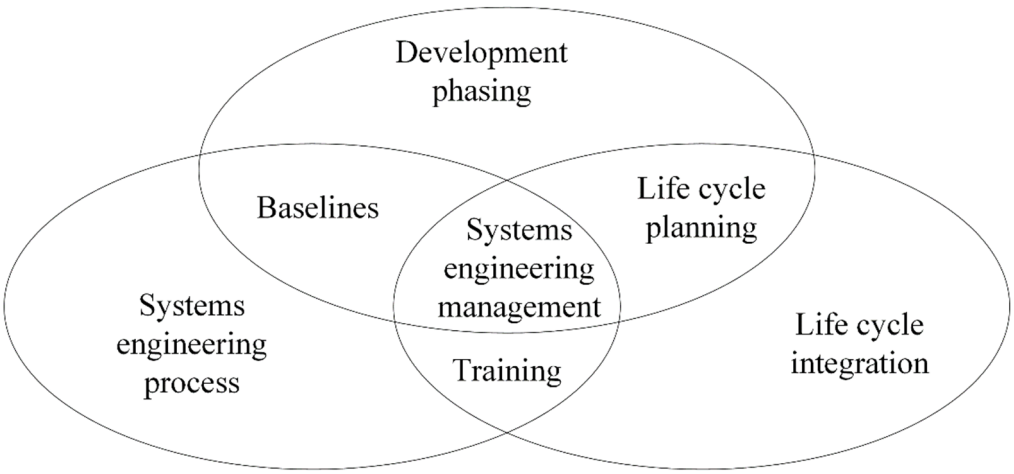


**Figure 4.** Systems engineering management activities [8]

In IT architecture, the focus is on designing the infrastructure of individual components. The primary objective is to achieve an efficient structure that meets the needs or mission of an organization over a long tern in a sustainable manner. It should present stability, room for continual innovation, support business goals and help reduce costs [8].

Security Architecture has been influenced by architectural approaches, engineering and models. The System Security Engineering Capability Maturity Model (SSE-CMM) created in early 2000s emphasizes on the importance of practicing security engineering and many new models are based on it. These type of models can serve as reference models for security engineering, security architecture, security operations as well as cloud computing [8]. Some noteworthy to mention models are:

ISO 27001 - ISO 27006: The International Standards for security. They cover management, best practices, requirements and techniques.

European Network and Information Security Agency (ENISA): The European cyber security agency's recommendations for security issues when adopting cloud computing.

Information Technology Infrastructure Library (ITIL): catered toward business needs it focuses on IT service management and is structured around service life cycles and practices.

Control Objectives for Information and related Technology (COBIT): a set of generally accepted best practices for governance and control [9].

The National Institute for Standards and Technology (NIST) covers standards and guidelines for non-government security engineering and architecture.

Security architecture can help bring together a common set of security requirements from multiple stakeholders and address them as a collective with a better solution than can be presented to them individually.

## 3. Some security problems

Restricting the freedom and creativity of users and creating a strong dependence on the cloud service provider is among the issues discussed in cloud computing. According to Richard Stallman, founder of the Free Software Foundation, "cloud computing threatens personal freedom because users provide their personal data to a third party." His suspicions are related to the imposition of certain systems and platforms by software companies on users. This is why Stallman expressed his view that cloud services will be difficult to enter in areas such as defence, government institutions, e-services, etc., where access to internal corporate networks must be strictly restrictive. However, practice shows that this is contrary to his understanding. Such examples are the US government, which switched to cloud services, the Ministry of Finance of the Republic of Bulgaria, which created a private cloud in 2012.

Another problem arising from the use of IT services in the cloud is related to data security. It means becoming highly dependent on the provider and the options it offers to protect data during transfer and storage. Many questions arise that are relevant to future hosting conditions: the possibility of information leaks to competing companies or malicious individuals, what mechanism to implement a possible change of provider, what will follow in the event of a system failure and others.

A service portfolio describes the services of the Cloud provider in terms of business value. It is a dynamic method used to govern investments in service management across the enterprise, in terms of financial values. With Service Portfolio Management (SPM), managers are able to assess the quality requirements and accompanying costs.

Figure 5 shows threats and their classification in cloud computing. The threats are generally grouped into five groups - network, data, related to virtualization, confidentiality and privacy and other common issues.

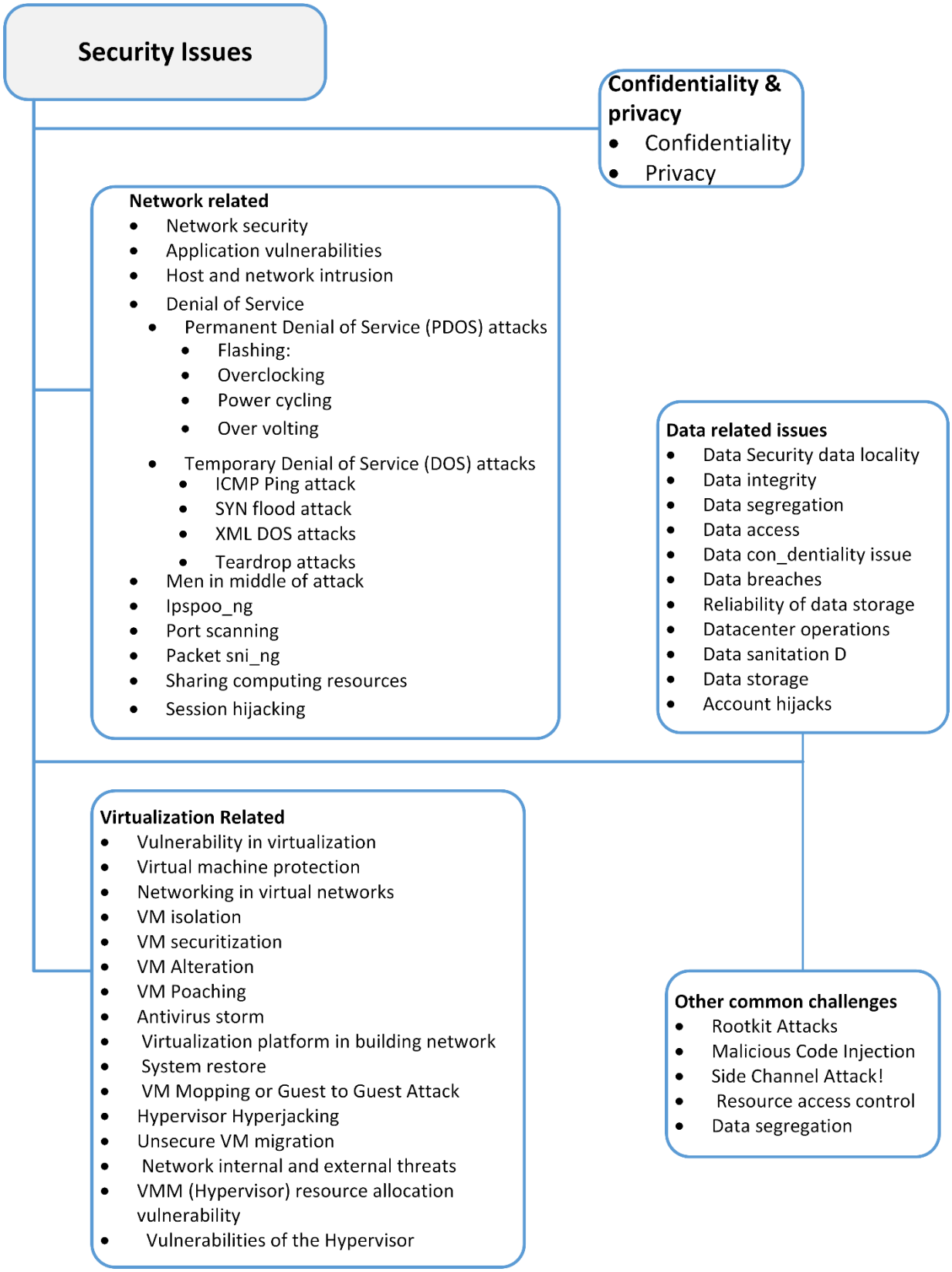


**Figure 5.** Appropriate security

## 4. Legal and regulatory issues for the protection

New laws are proposed all the time which can change the responsibilities of providers and customers and effect different parties under various scenarios. Legal issues can inevitably arise when dealing with data collection, storage or processing and they must be considered in order to be in legal compliance. Failure to do so can lead to potential fines by one or more government or industry regulatory bodies. The Data Protection Agency is the one of the government bodies who can make enterprises accountable for their actions in the European Union.

## 5. Risk Management

It is not always efficient to apply the same architecture and security controls for a low and a high risk environment (for example a banking application is not very likely to co-exist with a social-networking application in a public cloud). Risk can be defined as a function of threats that try to take advantage of vulnerabilities, divided by the countermeasures applied to protect our assets [8].

Risk= (Threats X Vulnerabilities / Countermeasures) X (Asset Value)

Thus a balance between the exposure side and cost side must be made. In order to implement a cost-effective security the risk must be determined according to an appropriate order of magnitude (figure 6).

However it is important to keep in mind that new security threats and vulnerabilities appear daily and more security layers means a better insurance.

Security must be part of the IT plans in the earliest stages in order to become business enabler.

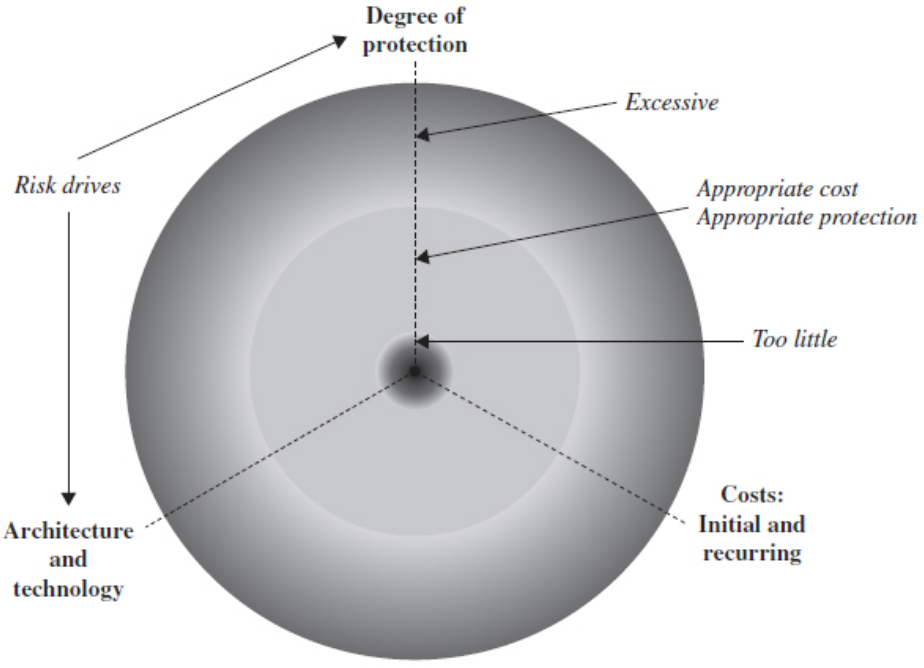


**Figure 6.** Appropriate security [8]

## 6. Conclusion and future work

Businesses and governments will continue to migrate to the cloud environment with the idea of reducing costs, improving efficiency and scalability, and reducing administrative difficulties. The delivery of cloud IT services saves time, money and improves productivity, but despite all the improvements that

are in place, there are many risks to the security of user information that must be considered and addressed in a timely manner.

Security in the cloud is a vast topic that has been and will continue to be discussed many times. What can be concluded is that it provides a field for the development of many new technologies, new methods of protection. This is the theme in which most innovation is born and contributes to the advancement of technology. The advantages of the cloud are indisputable, and therefore more and more large companies are turning to it, which makes it an attractive prey for more and more hackers.

The analysis of cloud security will continue as part of the project "Possibility Investigation of Increasing the Cybersecurity of Systems in Industry 4.0 using Artificial Intelligence". It will be considered what basic methods of artificial intelligence can be applied to increase security or at least to detect anomalies in the context of cloud computing.

## 7. References

[1] Individuals - internet activities https://appsso.eurostat.ec.europa.eu/nui/show.do?Dataset = isoc_ci_ac_i&lang=en

[2] Jain A, Hada Ch and Buksh B 2016 Overview of Cloud Computing With Security Issues, Challenges & Countermeasures, *International Journal of Science, Technology and Management* (IJSTM vol 5 issue 5**)** ISSN: 2394-1537

[3] Talib A M, Atan R, Abdullah R and Azrifah M 2011 Cloud Zone: Towards an integrity layer of cloud data storage based on multi agent system architecture *2011 IEEE Conference on Open Systems* pp 127-132 doi: 10.1109/ICOS.2011.6079311

[4] Gavrilov G and Trajkovik V 2012 *Security and privacy issues and requirements for healthcare cloud computing*

[5] Jansen W A Cloud Hooks 2011 Security and Privacy Issues in Cloud Computing *In Proceedings of the 44th Hawaii International Conference on System Sciences 2011* (2)

[6] Chehlarova N and Miltchev R 2020 Development of Digital Competencies and Skills *The Field of Use of Cloud Services and Electronic Communication 5* pp 41-50

[7] Enterprises Using Paid Cloud Computing Services https://infostat.nsi.bg/infostat/pages/ reports/ result.jsf?x_2=778

[8] Vic Winkler J R 2011 *Securing the Cloud: Cloud Computer Security Techniques and Tactics* (Syngress Publishing)

[9] Mechtr M 2014 Virtual networked infrastructure provisioning in distributed cloud environments. Networking and Internet Architecture *Institut National des Télécommunications* NNT 2014 TELE0028

## Acknowledgments

This research is realized and funded under the scientific-research project № КП-06-ПН47/27 “Possibility Investigation of Increasing the Cybersecurity of the Systems in Industry 4.0 using Artificial Intelligence” by the contract КП-06-Н47/7 with National Science Fund under the Ministry of Education and Science in Bulgaria.