

## Data Security Methods in Cloud Computing

Livia Maria BRUMĂ

Economic Informatics Doctoral School

The Bucharest University of Economic Studies, Bucharest, Romania

liviabruma@rocketmail.com, brumalivia@gmail.com

*Digital technology has become an important part of organizations due to the global spread of the internet and the increase in the number of smart devices, offering multiple benefits to users. The need for adapting to current requirements, has led to emergence of a new technology, cloud computing, developed for modern people needs, addicted to information and on the run. Information security is one of the main challenges for cloud developers, data loss causing damage in various fields and this is one of the reasons why some organizations do not adopt cloud migration. This paper analyzes the security of cloud computer technology, as well as the issues to ensure the security of the data in the cloud, according to the current technological methods and the specific architecture. The final part of the paper proposes a customized method for data security according to their importance to a particular organization, using current security methods.*

**Keywords:** Cloud Computing, Data Security, Security Methods, Data Life Cycle, Data Classification

**DOI:** 10.24818/issn14531305/24.1.2020.05

### 1 Introduction

The evolution of digital technologies together with the global spread of the internet connection has led to a rapid change in the way of designing, elaborating and implementing the different tasks and daily activities, both within the organizations with economic profile and in the government institutions or for home users. Changes due to the convergence of multiple technologies, notably the Internet of Things, artificial intelligence, Big Data, 5G and cloud computing, have led to a digital transformation of adaptive organizations, aligning with the requirements of users who prefer online interaction for obtaining certain services. Digitalization of companies through new storage and processing technologies has eliminated the barriers imposed by geographic space and helped the industry to become more competitive with key processes: production, distribution, sales, communication and marketing in the digital environment [1].

A characteristic of organizations that use technology to optimize activities is the generation of large volumes of data and information. Thus, aside with tangible assets and human resources, information has become an important

part of a company, becoming part of intangible assets, because it can be used to provide financial benefits and that is essential for having a competitive advantage in the market [2]. Inside an organization there are many types of important data, like customer contacts, financial transactions, contractual obligations to third parties, but also information belonging to the legal framework in force or regarding the confidentiality of personal data [3].

At the same time, the changing on the way of working in companies, the need for a flexible, reliable and easy to implement infrastructure, the extensible storage space in databases, the centralization of the computing and data processing power, associated with the increase of the number of intelligent devices used by consumers, has led to the need for a new technology that can meet current requirements - cloud computing technology. Most smart devices in the Internet of Things (IoT) field use cloud technology components to store and correlate data obtained through the sensors, perform backups to restore the system or use the cloud infrastructure service to provide technical support. Therefore, cloud computing is a model that should allow ❶ as fast as possible,

in a simple way, through the network connection, a wide range of computing resources, storage space, infrastructure with minimal effort for management and maintenance from users or interaction with service distributors [4].

The advantages that have contributed to increase the users number of cloud technology are represented by the financial factors (by reducing the costs and minimum investments in the acquisition of equipment), the continuous availability of services and data, scalability, flexibility and reliability, rapid implementation and minimal effort for configuration the

desired technologies or services [5]. Although there are many advantages of this type of technology, the usage of equipment configured and managed by a cloud service provider to process, transmit and store data may cause concern about maintaining an adequate level of security, so that important information for users is protected. According to a study carried out by CSA - Cloud Security Alliance, the customers main concern of regarding the migration to a public cloud platform is the security of the data along with the leakage risk and the regulatory compliance (Figure 1) [6].

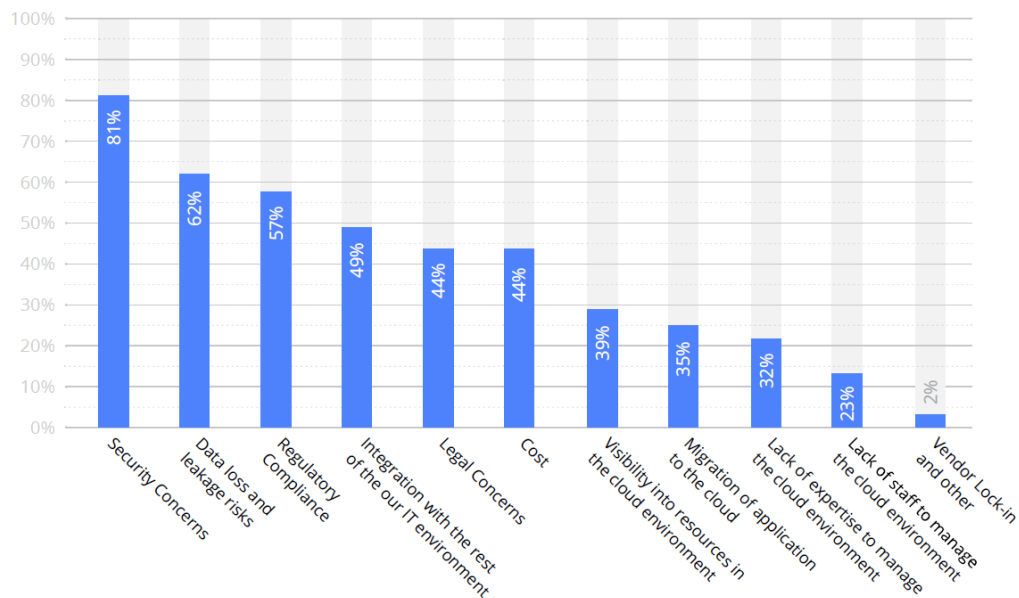


Fig. 1. The main reasons for concern of cloud users [6]

Therefore, the security of the information and data processed in the cloud is the main challenge for the developers of this technology. The data management must be performed in such a way that, for any stage of the data at a certain point of time - in transit, stored, processed - the minimum three properties of information security, the CIA triad (confidentiality, integrity, availability) are ensured. Thus, *confidentiality* can be ensured using encryption, access control and authorization, *integrity* through the use of mechanisms that prevent data alteration and *availability* using different methods to facilitate access at any time to the desired resources - load balancer, redundancy equipment. Other features can be pro-

vided to increase the level of security, including non-repudiation and authenticity. The main issue of security in cloud computing is given by the existence of numerous and diversified technologies, interconnected through the same infrastructure, including networks, databases, operating systems, virtualization, etc. Within the software, firmware and hardware design and implementation processes, security breach errors can occur, which can be later exploited by opponents. Also, the vulnerabilities of on-premise technologies are applicable in the cloud environment, but the impact generated by a cyber-attack is at a higher level. Cyber-attacks have become complex, causing significant financial damage and their impact affects the image

of brands for a long-term period. According to a study released by VMware, in 2018, security incident costs led to losses of \$ 600 billion and 46% of them were caused by insiders [7].

The paper gradually addresses the issue of cloud security starting from the ❶ current security methods used in cloud, taking into account two essential aspects - the virtualization mechanism and the service-oriented architecture, followed by ❷ an analysis of the cloud data security according to the three states of digital data, as well as by its life cycle and ending with ❸ the proposal of a method of data security, differentiated and personalized,

depending on the impact that the loss of confidentiality, integrity and availability of information may have.

## 2. Security Methods Used in Cloud

Depending on the needs of the organizations that want to use the services offered through the cloud technology, there are several implementation models, defined according to the location of the infrastructure and the entity that has control over it. Choosing a cloud deployment model is one of the most important decision, as each model satisfies organizational needs in a different way, involves different associated costs and has different advantages and disadvantages (Table 1).

**Table 1.** Cloud deployment models

Cloud	Characteristics	Advantages	Disadvantages
Public	<ul style="list-style-type: none"> <li>– deployed and managed by a cloud provider</li> <li>– shared resources with other users</li> </ul>	<ul style="list-style-type: none"> <li>– scalable / flexible</li> <li>– involves low costs</li> <li>– easy to use</li> </ul>	<ul style="list-style-type: none"> <li>– shared resources</li> <li>– operated by third parties</li> <li>– low security</li> </ul>
Privat	<ul style="list-style-type: none"> <li>– the infrastructure and services management provided by the organization</li> </ul>	<ul style="list-style-type: none"> <li>– high degree of security and control</li> <li>– independent of the internet</li> </ul>	<ul style="list-style-type: none"> <li>– high costs</li> <li>– limited scalability and flexibility</li> <li>– requires specialized employees for administration</li> </ul>
Hybrid	<ul style="list-style-type: none"> <li>– implemented and managed by a particular cloud provider for an organization</li> </ul>	<ul style="list-style-type: none"> <li>– financially profitable</li> <li>– scalable / flexible</li> <li>– medium level security</li> </ul>	<ul style="list-style-type: none"> <li>– shared resources</li> <li>– operated by third parties</li> <li>– low security</li> </ul>

From a data security point of view, it is recommended to use a private cloud, especially by institutions whose information has a higher classification level. Although the public cloud offers benefits in terms of cost and speed of implementation, there is a high risk of compromising stored and processed data, both as a result of cyber-attacks and human or technical errors. The hybrid cloud can be considered as a compromise, between limiting the costs required for implementation and ensuring an adequate level of security, being suitable for organizations that do not carry sensitive data or sensitive information.

Cloud technology is based on two essential concepts, service-oriented architecture and virtualization mechanism. To ensure a safe environment, the two components must be

properly configured. The main security methods and benefits to security are analyzed below through the two components: service-oriented architecture and virtualization mechanism.

### 2.1. Service oriented architecture

Service-oriented architecture offers various benefits, including agile network services that can be easily orchestrated and adapt to customer needs and requirements. By using this method of service delivery, the security of the processed data within the cloud platforms becomes a shared responsibility, between the users and the providers of cloud services, each having certain tasks to ensure the security. The model of security assurance through task sharing can be summarized as follows: the

cloud provider is responsible for ‘Security of the cloud’ and the customer responsibility is ‘Security in the cloud’, with some shared responsibilities.[8] The responsibilities of the

service provider and the client related to security differ depending on the requested service, IaaS (Infrastructure as a Service), PaaS (Platform as a Service) or SaaS (Software as a Service) (Figure 2) [9].

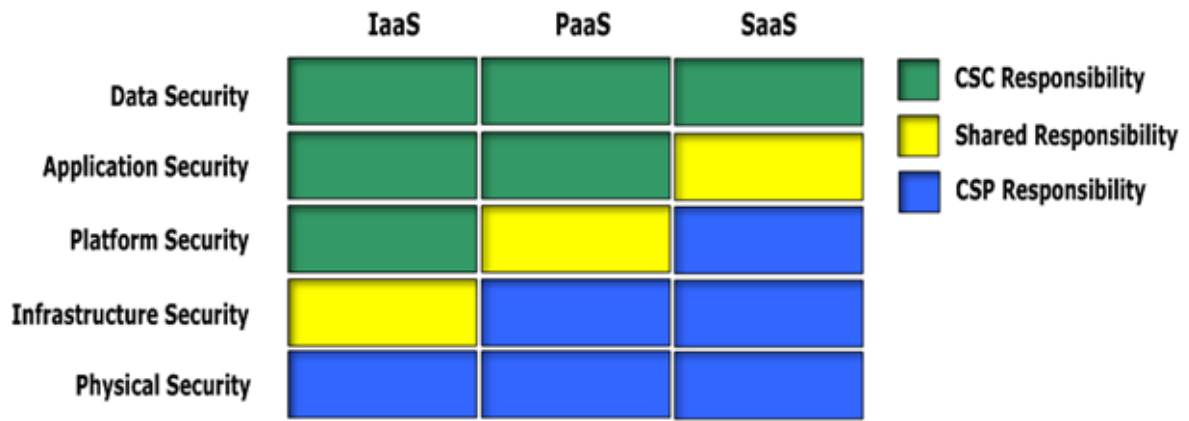


Fig. 2. The matrix of shared responsibilities in Cloud [10]

Depending on the level of responsibility, certain tasks and methods for security assurance

can be identified (Table 2).

Table 2. The main methods used for cloud security

Level of responsibility	Tasks	Methods of ensuring security
Data security	achieving a correct level of data classification and regulatory compliance	<ul style="list-style-type: none"> <li>– level of classification: public, private, confidential</li> <li>– other specific elements (detailed in sections 3 and 4)</li> </ul>
Application security	managing, configuring and reviewing employee access accounts	<ul style="list-style-type: none"> <li>– use of ABS (Attribute Based Signature) algorithms</li> <li>– use single sign on password authentication</li> <li>– use of digital signatures and certificates</li> <li>– use of SAML (Security Assertion Mark-up Language) and OAuth (Open Authorization)</li> <li>– use of multi-factor authentication</li> <li>– setting up accounts based on well-established roles</li> </ul>
Platform security	implement all the security settings for operating systems, applications and platforms	<ul style="list-style-type: none"> <li>– use of antimalware applications</li> <li>– setting up and implementing security policies in accordance with the systems used</li> <li>– keeping the systems updated with the available security patches</li> <li>– creation of accounts in applications with different roles</li> <li>– checking and keeping security logs</li> </ul>
Infrastructure security	the correct configuration of network elements	<ul style="list-style-type: none"> <li>– use of cryptographic algorithms power-no, use of digital certificates and IPSec, SSL, TLS, HTTPS proto-coalitions to secure the transfers</li> <li>– configuration of IDS / IPS type equipment, firewall, DDoS protector</li> <li>– using the VM Introspection technique</li> </ul>
Physical security	protecting the global infrastructure that manages the services offered - hardware, software, network.	<ul style="list-style-type: none"> <li>– access control at the physical level</li> <li>– establishing administrative and security areas</li> <li>– allowing external security audit actions</li> </ul>

- respecting the legal regulations in force

An important fact for users who implement appropriate security measures on their level of responsibility is that security management can also vary depending on the cloud service provider chosen. It is important that before signing a contract for the use of cloud services, to check whether the cloud provider has implemented a strategy for ensuring continuity, prevention and recovery in case of disasters - business continuity. Usually, security responsibilities are set when the contract is signed between the two contracting parties and are stipulated in a document that contains the agreed terms and expectations of each participant regarding the performance of the service contract - SLA - Service Level Agreement.

## 2.2. The virtualization mechanism

Virtualization offers many advantages, like flexibility through the ease of creating and destroying virtual components, increasing the level of resource utilization, thanks to the possibility of sharing them, simplified management for administration and cost reduction. Cloud technology is based on the virtualization mechanism through which an environ-

ment is created and has the physical functionalities of some hardware devices, without having them exist individually (virtual machine - VM). There is also an innovative method of virtualization for running applications, in a simplified software environment (containers), which contains only the elements required for the application: libraries, source code, execution process. The main difference from virtual machines is the virtualization of the operating system, compared to the virtualization of the hardware.

2.2.1 *Virtual machines.* In order to ensure the security of the data processed in the machines created through the virtualization mechanism, certain solutions are needed to monitor the security events so any vulnerabilities or cyberattacks can be detected. A singular event detected by an ordinary security system may not create suspicion of a possible attack vector.

There is a need for a system that correlates data from multiple virtual machines and provides information on possible distributed attacks. Table 3 identifies the minimum characteristics that a system for virtual machine monitoring must meet [11].

**Table 3.** Minimum characteristics of a VMs monitoring system

Characteristics	effectiveness	accuracy	transparency	robustness:	reactivity	accountability:
Details	detection of attacks and breaches of security policies	avoidance false-positive alerts	minimizing detection of the monitoring system	protection in case of infection of a host system	the ability to stop attacks and notify decision makers	the system should not interfere with the applications used in the cloud

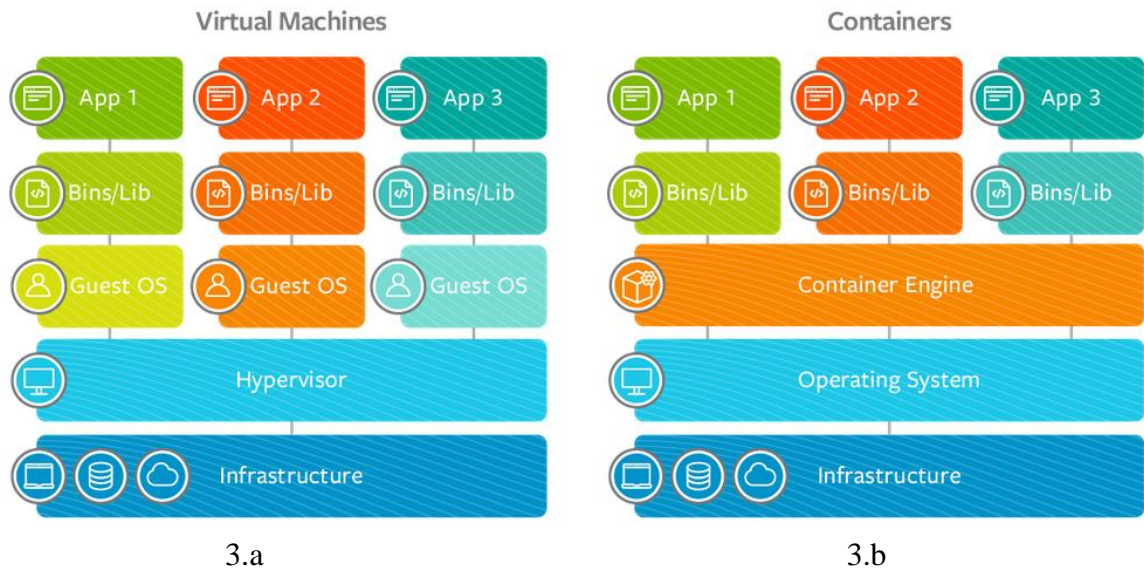
In order that the events generated by the individual security systems to be used effectively, it is proposed that the requirements described above should be added to the possibility of correlating and aggregating events, the rate of attack detection being improved.

2.2.2 *Containers* provide stability to the operating system and ease in orchestration, through the dedicated platforms, such as Kubernetes and Docker. Container security is based on the principle of process isolation at

the top level of the kernel and the correct configuration of the network. Most applications run on the root account, thus creating a vulnerability for running malicious applications and increasing the risk of losing data and processed information. Another vulnerability of the containers is the improperly configured images that can hide different security breaches, such as the existence of unnecessary remote connection services, malicious files

and few restrictions for authenticating and authorizing actions. Figure 3 shows the architecture of virtual machines (3.a) and containers

(3.b).



**Fig. 3.** Architecture of virtual machines and containers [12]

Cloud technology uses both virtualization methods, containers and classic virtualization, presenting financial benefits, flexibility and minimal use of physical resources. The main features of these two types of virtualization

(Table 4) can provide a stable and secure environment, if the requirements of the security strategies are properly respected and configured. Currently, virtual machines offer a higher level of security compared to container virtualization [13].

**Table 4.** Main characteristics of virtual machines and containers

Virtual machines	Containers
<ul style="list-style-type: none"> <li>• provides security tools through the operating system used</li> <li>• lower performance</li> <li>• longer start-up time</li> <li>• fast duplicate, scalar</li> <li>• ideal for production</li> <li>• hardware level virtualization</li> </ul>	<ul style="list-style-type: none"> <li>• reduced management resources</li> <li>• ideal for testing and development</li> <li>• small image size</li> <li>• reduced and simplified security updates</li> <li>• high processing speed</li> <li>• virtualization at the operating system level</li> <li>• efficient use of resources</li> <li>• high scalability and elasticity</li> </ul>

The current strategies for information protection are based on certain principles of implementation of security methods, taking into account the vulnerabilities of the hardware and software components of a computer system: in-depth defense, the principle of minimum privilege, task separation, minimalist design, fail-safe [14].

**3 Ensuring the Data Security in Cloud**

The strategies and methods of securitization offer a high level of security, if they are used according to the procedures and implemented correctly. Cloud data security control can be done by the following methods:

- control of data that is uploaded from the

- cloud;
- data protection and data management in the cloud through masking methods, access control, architecture configuration, security events monitoring;
- information management throughout the data life cycle, ensuring the auditing process, managing the physical location of data centers and implementing strategies to ensure the availability and recovery of data in case of disasters.

Also, to ensure the security of data in the cloud must take into account several aspects, such as: ❶ data state and ❷ data life cycle. The state of the data at a given time (in use, transit or at rest) implies the use of different security methods, as follows:

*a) Data at rest* (stored in certain memory areas). The data in this state is stored in the cloud on different physical media devices (hard disks and tapes) or virtualized, in a structured or unstructured way: databases, file servers, network storage units (NAS) - Network Attached Storage (SAN), e-mail servers, restore images. Depending on the contracted service in the cloud, media storage can be provided adequate to the amount of data for the needs of organizations, with scaling possibilities. There are several masking methods to secure data at rest, like: encryption, tokenization, etc. [15]

*a.1) Data encryption* - this method of data masking offers a very high level of data security if advanced encryption techniques are used (fully homomorphic encryption (FHE), attribute-based encryption (ABE), attribute-based encryption are used Hierarchical (HABE)), strong encryption rates and ensure the proper management of the keys. Data encryption can be done in several ways depending on the file format and the needs of your organization:

- encryption of files and directories - it is based on a security policy that sets *what* data needs to be encrypted and *who* has access to it;
- full encryption of the virtualized disk -

the virtualized disk is fully encrypted ensuring the confidentiality of the data (if the encryption keys are properly managed);

- virtual machine encryption - encryption of the configuration files and disk belonging to the virtual machines (but the problem of encryption key management remains);
- encryption of specific units: databases, e-mail. [16]

*a.2) Data tokenization* - unlike encryption, the tokenization does not use a mathematical algorithm, but replaces the data with random values, and the original data and the token are stored in secure databases for later retrieval. Securing the data through tokenization has the advantage that, if the token is compromised, the real data is secure, only the substituted value is affected. [17]

*b) Data in transit* (in the process of transmission through the communication channel). There are two situations when the data is in motion:

- in transit through the communication channel that connects the client with the data center;
- in transit inside the data center.

For securing the communication channel, the most used mechanisms are VPN (Virtual Private Network) services, the use of hardware encryption, DLP (Data loss prevention), URL (Uniform Resource Locator) filtering, and secured protocol: SFTP (Secure File Transfer Protocol), TLS (Transport Layer Security,) SSH (Secure Shell).








*c) Data in use* (data is present in volatile memory, RAM - Random Access Memory, CPU - registers or cache). The data in use can be protected using total hard disk encryption or by using enclaves [18].

Another important aspect of data security that must be taken into considered is the life cycle of the data. The need for security is valid for every stage of the data life cycle, each with certain risks, and the omission of a

stage can lead to substantial losses for organizations [19].

Depending on the stage at which the data is at a given time, there are specific requirements for security (table 5) [20].

**Table 5. Data life cycle**

Phases	Key elements for data security
 Generate	<ul style="list-style-type: none"> <li>- Who owns the data</li> <li>- Classification level</li> <li>- Data management after cloud migration</li> </ul>
 Use	<ul style="list-style-type: none"> <li>- Data access control</li> <li>- Legislative considerations</li> <li>- Use of data for the purpose for which it was generated</li> </ul>
 Share	<ul style="list-style-type: none"> <li>- What kinds of networks will be used: public/private</li> <li>- Data encryption</li> <li>- Access control for sharing privileges</li> </ul>
 Transform	<ul style="list-style-type: none"> <li>- Maintaining integrity</li> <li>- Data sensibility</li> <li>- Use a right format for data</li> </ul>
 Store	<ul style="list-style-type: none"> <li>- Maintaining CIA properties</li> <li>- Data format: structured/unstructured</li> <li>- Data encryption</li> <li>- Data access control</li> </ul>
 Archive	<ul style="list-style-type: none"> <li>- Ensure the legislative framework for data storage</li> <li>- Usage of robust media devices</li> <li>- Archiving the data for a period corresponding to the SLA</li> </ul>
 Destroy	<ul style="list-style-type: none"> <li>- Complete destruction</li> <li>- Compliance with standards regarding data destruction and process auditing</li> </ul>

The security strategies and methods analyzed and presented, offer a high level of security, if they are used according to the procedures and implemented correctly. Despite the fact that these methods can provide data security, numerous cyber security incidents occur every second, ransomware for financial blackmail, rootkeys for taking control, keylogger for clear information, phishing for ex-filtering of credentials, this being just a few examples of malicious applications. Mainly, cyber-attacks occur because the security devices are not properly configured, the operating systems do not have the security patches up to date, the users use weak authentication passwords, the attackers exploit the 0-day vulnerabilities, and the data encryption is used, on a large scale, just for communication channel encryption. Apart from these external causes, insiders can cause major damage, if the security policies applicable to the systems to which these users

have access are not well established: to respect the principle of need to know, to have access only in certain physical areas, etc. In order to support the increase of the level of data and information security, in the last part of this study, is proposed an alternative method of automatically assigning an appropriate security mechanism, depending on the importance of the respective data for the organization.

**4 Securing Data Using CIA Properties**

The proposed method is based on the principle of choosing a data security method depending on the importance of data for an organization. An algorithm can be developed to detect the real impact of losing properties of the information (confidentiality, integrity and availability), which can be integrated into a complex system of personalized information security. This system can be used to choose the right



methods of securing resources and ensuring the adequate level of protection. The algorithm can use file metadata, employee databases, keywords commonly used in different file types, classification levels present in some cases in the header and footer of documents etc. However, certain information is part of different classification categories, depending on the organization which uses them. In this

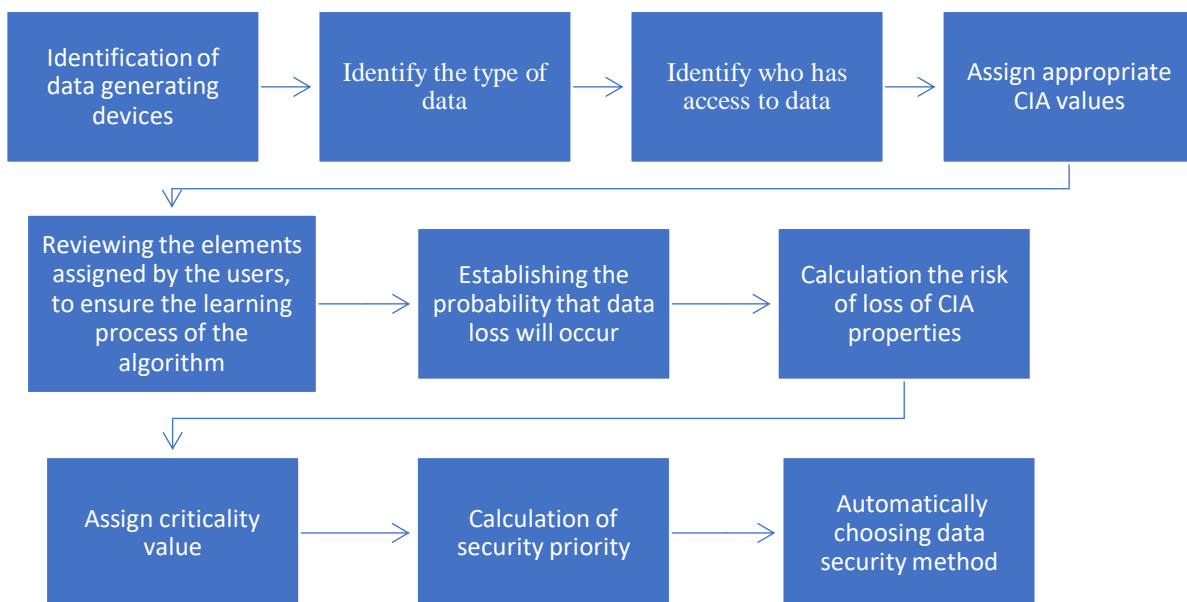
case, an automatic adaptability of the algorithm is needed, which can be acquired over time through the dynamic learning process. In order to test the functionality of this method, values assigned to the mission information from NIST standard 800-60 were used, according to table 6, which shows the potential impact caused by loss of each attribute.

**Table 6.** Attributes of security of mission information [21]

Information type	Confidentiality	Integrity	Availability
Disaster Management			
Disaster Monitoring and Prediction	LOW	HIGH	HIGH
Disaster Preparedness and Planning	LOW	LOW	LOW
Emergency Response	LOW	HIGH	HIGH
Economic Development			
Business and Industry Development	LOW	LOW	LOW
Financial Sector Oversight	MODERATE	LOW	LOW
General Science and Innovation			
Space Exploration and Innovation	LOW	MODERATE	LOW

The potential impact caused by the loss of confidentiality, integrity or availability can be LOW, MODERATE or HIGH according to

FIPS 199 standard. The steps required for the automatic choice of the mechanism are shown in Figure 4.



**Fig. 4.** The steps of the algorithm for choosing a security method

To test the proposed method, two sets of data were created, each of them with 500 elements. The first data set has assigned CIA properties randomly, using a generator of pseudo-random numbers created in Python, to simulate

data processing in the same way, without taking into account the higher importance of some data. The second set of data was created based on the attributes of the NIST standard 800-60, exemplified in table 6, in which the

data are treated differently. For a mathematical analysis, the three levels of impact (low, moderate, high) received random numeric values per level, from the following intervals: LOW in the range [1,3], MODERATE in the

range [4.7], HIGH in the range [8.10]The two data sets have the number of the element in the first column, followed by the impact of confidentiality, integrity and availability, as presented below.

Dataset1 – Random impact

Data414,4,7,3  
 Data415,10,6,10  
 Data416,1,7,8  
 Data417,5,2,6  
 Data418,2,1,3  
 Data419,4,5,7  
 Data420,6,7,1  
 Data421,4,9,2  
 Data422,6,4,5  
 Data423,9,4,3  
 Data424,2,10,10

Dataset2 - Impact according to NIST 800-60

Data414,5,4,2  
 Data415,5,4,7  
 Data416,10,10,10  
 Data417,10,10,10  
 Data418,9,4,9  
 Data419,10,10,10  
 Data420,3,9,9  
 Data421,2,2,2  
 Data422,2,2,2  
 Data423,3,8,8  
 Data424,8,9,7

The proposed method is based on the calculation of a value, called *Security Priority - Pr*, using two variables: R and Cr.

R - the risk of losing the CIA attributes;  
 For the calculation of the risk, are used the values of the potential impact of loss one of the CIA attribute and the probability to occur:

$$R = \frac{1}{n} \sum_{i=1}^n P_i I_i$$

*P* - the probability that a event to occur

*I* - the potential impact of the event

The probability of event occurrence was randomly generated and used for both datasets. A probability generation method, according to hardware and software equipment used for data protection, can be developed and adapted according to each individual organization. In the proposed method, because the values of the probabilities were used uniformly, we

consider that they did not influence the results in the wrong way.

Cr - criticality of information (the importance of information for the organization that uses it).

Define the values that the variable Cr can take as follows:

*unknown* = 1, *very low* = 2, *low* = 4, *medium* = 6, *high* = 8 and *very high* = 10.

The criticality value for the first data set was randomly assigned, and the value of the second set was assigned based on the potential impact of CIA properties:

- medium, high and very high for data with high CIA impact values: 6, 8 or 10;
- unknown, very low or low for data with low CIA impact values: 1, 2, 4 (see examples below).

Dataset1 – random criticality

Cr414,2  
 Cr415,7  
 Cr410,10  
 Cr417,3  
 Cr418,5  
 Cr419,7  
 Cr420,2  
 Cr421,6  
 Cr422,2  
 Cr423,5  
 Cr424,10

Dataset2 – criticality based on potential impact of CIA properties

Cr414,3  
 Cr415,3  
 Cr410,10  
 Cr417,10  
 Cr418,8  
 Cr419,10  
 Cr420,7  
 Cr421,3  
 Cr422,3  
 Cr423,7  
 Cr424,9

The security priority is calculated as follows:

$$Pr = R * Cr$$

Example:

$$I_{info\_production} = \{10,10,8\}$$

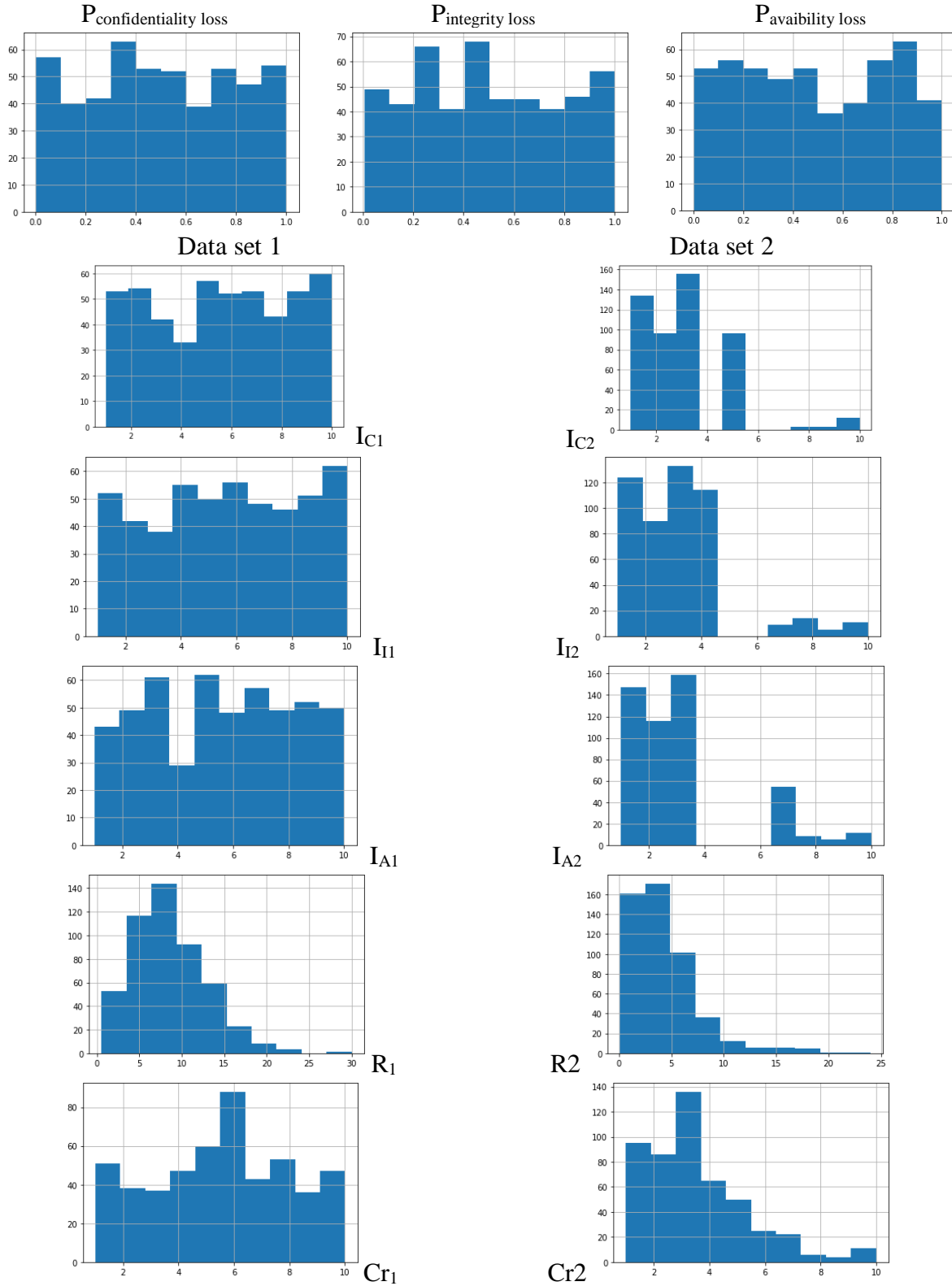
- P = {0.01, 0.02, 0.002}

- Cr=9

$$R = [0.01 * 10 + 0.02 * 10 + 0.002 * 8] = 0.316$$

$$Pr = 0.316 * 9 = 2.844$$

In order to visualize the differences between the data, histograms of the variables, corresponding to the two data sets, were made (Figure 5).



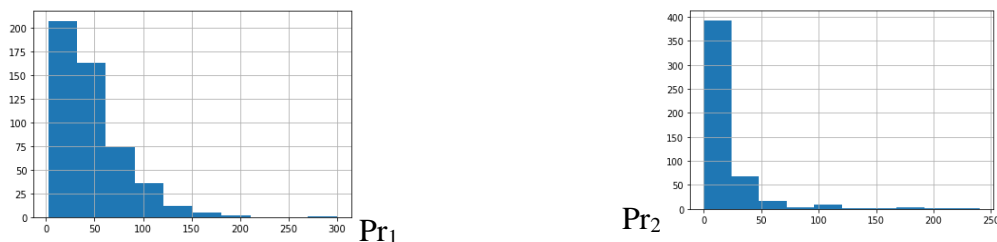


Fig. 5. Histograms of variables associated with the two data sets

Legend:

I<sub>C</sub>, I<sub>I</sub>, I<sub>A</sub>, - impact of loss of CIA attributes  
Cr - values of criticality

R - risk of losing CIA attributes  
Pr - values of security priority

The last step of the algorithm is to choose the appropriate methods for securing information according to previously established parameters (table 7).

Table 7. Assignment of security methods according to Pr

	Security priority	(0 1]	(1 2]	.....	(298 299]	(299 300]
Security methods	Multi-factor authentication				✓	✓
	Use of digital certification	✓	✓		✓	✓
	Full disk encryption				✓	✓
	Encrypted communication channel	✓	✓		✓	✓
	.....					
	Data dispersion				✓	✓

From the comparative analysis, it can be observed that, for the data set number 1 whose impact was assigned randomly, the values of the variable Pr1 are higher than the values of Pr2. Thus, if we did not use a custom security method, for a larger number of data, we should use more complex equipment and methods, without having to, because not all data have the same level of importance for a company. Generating, automatically and correctly, CIA properties for all data processed in the cloud could provide a first step in the different choice of security methods, reducing costs, simplifying current security steps, while obtaining a security level higher than present one.

5 Conclusions

Data and information security is one of the main challenges in all areas of technology reference and the cloud computing environment is no exception to this rule. The variety of technologies used in data centers and cloud architecture and the increasing number of cyberattacks make this requirement difficult to meet. Although there are numerous methods

of data security, cyber security incidents and data loss frequently occur, so innovative and automated methods are needed to minimize the loss and occurrence of security breaches. The proposed security method can be improved and integrated into mechanisms that use machine learning algorithms, in order to develop a customizable mechanism for each organization, through the dynamic learning process, adapting to the type and the real needs of data security.

References

[1] Digitalizarea industriei europene, Valorificarea deplină a pieței unice digitale, available: <https://www.comunicatii.gov.ro/wp-content/uploads/2016/04/Digitalizarea-industriei-europene.pdf>

[2] D. Loshin, *The Practitioner's Guide to Data Quality Improvement*, The Morgan Kaufmann Series on Business Intelligence, 2011

[3] CompTIA Security + Certification (Exam SY0-501), Study Guide 2018

- [4] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, 2011
- [5] A. Squicciarini, D. Oliveira and D. Lin, *Cloud Security Baselines*, in *Cloud Computing Security – Foundations and Challenges*, pp 31-45, edited by John R. Vacca, 2017
- [6] H. Baron, S. Heide, S. Mahmud and John Yeoh - *Cloud Security Complexity: Challenges in Managing Security in Hybrid and Multi-Cloud Environments*, Cloud Security Alliance, <https://blog.cloudsecurityalliance.org/2019/05/21/security-challenges-hybrid-multi-cloud/>, October, 2019
- [7] *The Rising Costs of Cybersecurity Breaches*, <https://www.vmware.com/radius/rising-costs-cybersecurity-breaches/>, October, 2019
- [8] *Shared Responsibility Model*, <https://aws.amazon.com/compliance/shared-responsibility-model/>, October, 2019
- [9] *Oracle and KPMG cloud threat report*, 2018, [https://assets.kpmg/content/dam/kpmg/kz/pdf/Oracle-and-KPMG-Cloud-Threat-Report\\_2018\\_Limited.pdf](https://assets.kpmg/content/dam/kpmg/kz/pdf/Oracle-and-KPMG-Cloud-Threat-Report_2018_Limited.pdf), October, 2019
- [10] *Manufacturing in the cloud: part xvii: cloud responsibility matrix* <http://blog.mesa.org/2018/06/manufacturing-in-cloud-part-xvii-cloud.html>, October, 2019
- [11] R. Di Pietro and F. Lombardi, *Virtualization Technologies and Cloud Security: advantages, issues, and perspectives*, 2018, Available [https://www.researchgate.net/publication/326696873\\_Virtualization\\_Technologies\\_and\\_Cloud\\_Security\\_advantages\\_issues\\_and\\_perspectives](https://www.researchgate.net/publication/326696873_Virtualization_Technologies_and_Cloud_Security_advantages_issues_and_perspectives), October 2019
- [12] *Containers vs Virtual Machines: What's the Difference?* <https://www.bmc.com/blogs/containers-vs-virtual-machines/>
- [13] L. Georgeta GUȘEILĂ, *Integrarea serviciilor de tip cloud computing în centrele de prelucrare a informațiilor*, 2019
- [14] C. Dotson, *Practical Cloud Security A Guide for Secure Design and Deployment*, O'REILLY, 2019
- [15] V. Kumar, S. Chaisiri and R. Ko *Data Security in Cloud Computing*, The Institution of Engineering and Technology, August, 2017
- [16] SANS – *Cloud Security Fundamentals – Security Course*, 2012
- [17] *Tokenization 101: Understanding the Basics*, <https://www.wexinc.com/insights/blog/corporate-payments-edge/credit-card-tokenization-basics/>
- [18] *Security From Chip to Cloud: Data-in-Use Protection Only on IBM Cloud* <https://www.ibm.com/cloud/blog/announcements/security-from-chip-to-cloud-data-in-use-protection-only-on-ibm-cloud>
- [19] Marinela Mircea, *Addressing Data Security in the Cloud*, *World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering* Vol:6, No:6, 2012
- [20] N. Meghanathan, et al. *PRIVACY IN CLOUD COMPUTING: ASURVEY*, 2012
- [21] NIST 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, Available [https://tsapps.nist.gov/publication/get\\_pdf.cfm?pub\\_id=152106](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152106)



**Livia Maria BRUMĂ** has graduated the Faculty of Military Electronic and Information Systems of the Military Technical Academy „Ferdinand I” from Bucharest in 2016. She holds a Master Degree in Electronics applied in robotics for security and defense. At present, she works in cyber security domain and she is involved as a Ph.D. student in the Economic Informatics Doctoral School from the Bucharest University of Economic Studies.