Computer Systems Science & Engineering
DOI:10.32604/csse.2021.015437
Article

Tech Science Press

A Data Security Framework for Cloud Computing Services

Luis-Eduardo Bautista-Villalpando[1,*] and Alain Abran[2]

[1]Department of Electronic Systems, Autonomous University of Aguascalientes, Aguascalientes, 20131, Mexico
[2]Department of Software Engineering and Information Technology, ETS, University of Quebec, Montreal, H3C 1K3, Canada
[*]Corresponding Author: Luis-Eduardo Bautista-Villalpando. Email: eduardo.bautista@edu.uaa.mx
Received: 21 November 2020; Accepted: 16 December 2020

Abstract: Cyberattacks are difficult to prevent because the targeted companies and organizations are often relying on new and fundamentally insecure cloud-based technologies, such as the Internet of Things. With increasing industry adoption and migration of traditional computing services to the cloud, one of the main challenges in cybersecurity is to provide mechanisms to secure these technologies. This work proposes a Data Security Framework for cloud computing services (CCS) that evaluates and improves CCS data security from a software engineering perspective by evaluating the levels of security within the cloud computing paradigm using engineering methods and techniques applied to CCS. This framework is developed by means of a methodology based on a heuristic theory that incorporates knowledge generated by existing works as well as the experience of their implementation. The paper presents the design details of the framework, which consists of three stages: identification of data security requirements, management of data security risks and evaluation of data security performance in CCS.

Keywords: Cloud computing; services; computer security; data security; data security requirements; data risk; data security measurement

1 Introduction

A cyberattack is a malicious activity conducted against an organization through its IT infrastructure via the internal or external networks, or the internet. The Accenture Security report [1] forecasts that cybercrime will remain a large-scale concern for years to come and that, between 2019 and 2023, approximately $5.2 trillion in global value will be at risk from cyberattacks—an ongoing challenge for corporations and investors alike. The report also mentions that cyberattacks are difficult to prevent because the targeted companies and organizations are often relying on fundamentally insecure networks and new technologies such as the Internet of Things (IoT), which could reach two billion devices by the end of 2020, not including smartphones, PCs, and tablets.

Other literature, such as the 2017 CISCO Annual Cybersecurity Report [2], provides the following indications:

- Public security breaches in organizations are having a measurable impact on opportunities, revenue, and customers;
- As result of these breaches, one in five organizations lost customers due to an attack, and nearly 30% lost revenues;
- When breaches occur, the functions most likely to be affected are operations and finance (36% and 30%, respectively), followed by brand reputation and customer retention (both at 26%);
- 27% of connected third-party cloud applications introduced by employees into enterprise environments in 2016 posed a high security risk.

In Europe, the European Union Agency for Network and Information Security (ENISA) Threat Landscape Report 2017 [3] mentions that threat researchers discovered that a majority of new vulnerabilities examined were attributable to the use of middleware related to corporate cloud and software-as-a-service (SaaS) platforms after users grant access to cloud services. Technical issues in cloud computing services (CCS) is one of the major findings in cloud security, and its vulnerabilities in middleware are becoming more apparent and raising concerns. Middleware is core in CCS integration and is becoming a frequent threat vector strongly affecting cloud computing (CC) and IoT technologies. More recently, the CISCO 2018 Annual Cybersecurity Report [4] mentions that adversaries are taking malware to unprecedented levels of sophistication and that the evolution of malware was one of the most significant developments in the attack landscape. The advent of network-based ransomware crypto-worms eliminates the need for the human element in launching ransomware campaigns. Moreover, adversaries are becoming more adept at evasion and at weaponizing cloud services and other technologies such as command-and-control (C2) tools, in order to gain more time to operate and inflict damage.

Throughout 2019, several forms of hijacking such as DNS hijacking, formjacking and cryptojacking increased considerably compared to previous years and were the main types of threats according to the Symantec ISTR 2019 report [5] and the CISCO Cybersecurity threat report 2019 [6]. In addition, these reports mention that ransomware, remote access trojans (RATs), office phishing, social media extortion, cloud computing security and IoT security were the types of threats with greater presence.

One of the main challenges in cybersecurity then is to provide mechanisms to secure most of the technologies on which these threats are present, including CCS because of increasing industry adoption and migration of traditional computing services to CCS.

This work proposes a framework to evaluate and improve the data security of CCS from a software engineering perspective which evaluates the levels of security within the CC paradigm by means of engineering methods and techniques applied to CCS.

To effectively manage and control the use of cloud technology within an organization, decision makers must assess the potential impact of CCS on their competitive edge [7]. And for setting up a cloud framework that specifically addresses organization information security, Ramgovind [7] recommended adapting and incorporating current data protection, trust and privacy policies into a comprehensive set of CCS guidelines that includes governance and audit practices.

The methodology for the design of this framework was based on ‘heuristic theory’ that is described in section 3. Such methodology incorporates knowledge generated by existing works related to the study area as well as the experience of their implementation. Therefore, our proposed framework is based on a series of processes carried out through a set of tasks and their respective activities. The framework is designed to integrate a measurement method that allows assignment of quantitative values to the data assurance within the CCS.

This work is organized as follows. Section 2 presents the background and related work on CCS security, introduces data security in cloud services and describes some of the most relevant security frameworks in

CCS. Section 3 details the design of our Data Security Framework for Cloud Computing Services (DSF^{CCS}) with its life cycle described in three stages: identification of data security requirements, management of data security risks and evaluation of CCS data security performance. Finally, section 4 presents the conclusions and suggests future work.

2 Background and Related Work

2.1 Cloud Computing Services (CCS)

Cloud computing (CC) is defined in ISO/IEC 17788 [8] as a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. This CC paradigm is composed of key characteristics, CC roles and activities, cloud capability types, cloud deployment models and cloud services.

In addition, ISO/IEC 17789 [9] groups CCS into categories where each is a group of services that process a common set of capabilities. The cloud services in these categories can include capabilities from one or more of the cloud capability types such as application capabilities, platform capabilities or infrastructure capabilities. Thus, representative cloud services categories include: Network as a Service (NaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

2.2 Cloud Computing Security

ISO/IEC 17789 [9] also mentions that for efficient provisioning of cloud services, cross-cutting aspects must be taken into account, including both architectural and operational considerations. One of these cross-cutting aspects is cloud security that applies to infrastructure, services, cloud service providers, cloud service customers, cloud service partners, etc. All of the above cross-cutting aspects need to be secured, and how they are secured should be distinct and based on what is being secured. Thus, it is critical to recognize that cloud security is an aspect that spans across all views of the CC reference model from physical security to application security.

2.3 Security Issues in CCS

The related work on cloud computing security (CCSec) is reported next from a historical viewpoint, from early time-sharing systems, availability of internet resources and, more recently, containers providing a way to run isolated systems on single servers.

Subashini and Kavitha [10] showed that the initial security challenges related to the CC paradigm included, but were not limited to, accessibility vulnerabilities, virtualization vulnerabilities and web application vulnerabilities. These authors established that in the physical domain, security challenges were related to physical access issues, privacy and control issues from third parties having physical control of data, issues related to identity and credential management, data verification, tampering, integrity, confidentiality, data loss and theft. They pointed out that each CCS model establishes different levels of security requirements and that there are significant trade-offs for each model in terms of integrated features, complexity vs extensibility and security.

Bashir and Haider [11] looked at the evaluation of practical solutions for CCS security threats. Their study identified the most common vulnerable security threats in cloud computing with a focus on enabling researchers and security professionals to know about users and vendors concerns and to carry on critical analysis of the different security models and tools proposed. Their work also summarized tools and models proposed to address security and privacy concerns in CCS from different research contexts. For example, they identified contexts for secure provenance in CC, trusted CC, data-centric cloud security, security audit in public infrastructure clouds, transparent cloud security, security management of virtual machines, privacy management for CC and data protection models for service provisioning in the

cloud. For each of these identified contexts, these authors proposed a tool or model to improve security, such as: the bilinear pairing method, the trusted CC platform, DS 2 platform, a reachability audit model, a transparent cloud protection system, an image management security framework, a privacy manager tool and a data protection framework.

Zissis and Lekkas [12] proposed a security solution that includes trusting a third party tasked with assuring specific security characteristics within a distributed information system while realizing a trust mesh between involved entities forming federations of clouds. One of the main contributions of this work is the identification of security requirements in the different CC service levels (e.g., IaaS, PaaS, SaaS). The authors stated that understanding and documenting such security requirements is imperative in designing a solution for the assurance of data protection and information security. To achieve this, they claimed that employing trusted third-party services within the cloud leads to the establishment of the necessary trust level and provides ideal solutions to preserve the confidentiality, integrity and authenticity of data and communications. They defined a trusted third party as an impartial organization delivering business confidence, through commercial and technical security features to an electronic transaction, which supplies technically and legally reliable means of carrying out, facilitating, and producing independent evidence about and/or arbitrating on an electronic transaction.

Finally, Mishra et al. [13] focused their work on specific cloud services, including Infrastructure as a Service (IaaS). These authors mentioned that IaaS is largely reliant on virtualization and container technologies, seen as providing all the security and process isolation a customer might want. These technologies allow multiple tenants to coexist in the same physical infrastructure, sharing its resources and, at the same time, creating an isolated environment for each one. According to these authors, from a security perspective, a virtual machine (VM), a container and a physical server do not differ and a compromised VM or container can be used to affect the host servers and other VMs and containers in the same virtual or physical network. In addition, the authors mentioned that in cloud environments, the risk increases. For instance, attackers do not need to compromise a VM or container in order to attack other VMs or the network, they only need to pay for a cloud service and, as consumers, can initiate an attack while avoiding the traditional security network devices. Thus, the absence of a security perimeter and the highly volatile nature of VMs and containers will force organizations to adopt robust security processes which may lead to a high security computing infrastructure.

2.4 Data Security in CCS

Some authors have focused on the assurance of CC data instead of its services since, at the end of the day, data is one of the most important assets of users and organizations and, as a consequence, providers of cloud services. While choosing cloud services allows users and organizations to store their local data in remote data storage when security policies are not deployed properly into such cloud services, data operations and transmissions are at high risk. Velumadhava and Selvamani [14] mentioned that when security measures are not properly deployed for data operations and transmission data is very vulnerable. Since CC provides a facility for a group of users to access stored data remotely, there is a high probability of data breaches. Moreover, the authors point out that data loss or data leakage can have severe impact on business, brand and trust of an organization. They report that data leak prevention is considered to be the most important factor (88%) of critical and very important challenges, followed by the impact of data segregation and protection (92%) on security challenges.

Chen and Zhao [15] mentioned that CCS data security and privacy protection content, and its cloud openness and multi-tenant characteristics with its own particularities, is similar to traditional data security and privacy protection. As an example, the authors analyzed the data security and privacy protection issues in the cloud through seven stages of the data life cycle: generation, transfer, use, sharing, storage, archival and destruction. The objective of their work was to design a set of unified identity management

and privacy protection frameworks across applications of CCS which provides a concise but all-round analysis on data security and privacy across all stages of the life cycle in the cloud.

2.5 Security Frameworks in CCS

Since the emergence of the CC paradigm, authors have worked on developing frameworks for establishing security in cloud environments. For example, Takabi et al. [16] propose a comprehensive security framework for CC environments. They identify a set of security challenges in the cloud such as identity management, access control, policy integration, etc., and develop an overall security framework consisting of key components to facilitate collaboration among different cloud service providers (CSP) by composing ideal integrated services. They propose a number of service integrators with components responsible for the establishment and maintenance of trust between the local cloud provider, external cloud providers and cloud users, providing ideal integrated services and generating global policies.

Zhang et al. [17] focused on the management of security risk for CC environments and proposed an information risk management framework in order to understand critical areas of focus for identifying threats and vulnerabilities. They mention that a well-structured risk management methodology, when used effectively, can help identify appropriate controls for providing mission-essential security capabilities. Their proposed framework has seven processes: processes-selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessment and monitoring, and risk management review.

Almorsy et al. [18] also focused their work on management of CCSec from a collaboration-based approach. They proposed a cloud security management framework based on the alignment of their work with the NITS-FISMA standard [19]. Their framework is based on improving collaboration between cloud providers, service providers and service consumers in managing the security of the cloud platform and hosted services. Such collaboration is carried out among key cloud stakeholders to share required information on security requirements, security controls, security metrics, etc., which is built on top of security standards that assist in automating the security management process.

Other authors have oriented their work to the search for the best cloud security frameworks through comparison and surveys. Devi and San [20] present a survey about data security in cloud computing identifying five important cloud characteristics: on-demand self-service, broad-network access, resource pooling, rapid elasticity and measured services. They surveyed existing data security frameworks with encryption mechanisms and data integrity proofs. Moreover, their work deals with protecting data both from the client and the provider side, emphasizing the speed of processing during implementation of such protection as well as the computational requirements playing a major role in deployment of their data security framework in cloud environments. They also propose a hybrid model which is based on hyperElliptic curve cryptography (HECC) and the secure hashing algorithm (SHA) as a way of providing data security, data integrity and user authentication in cloud computing.

Finally, Giulio et al. [21] compare cloud standards in order to determine whether new security frameworks improve cloud computing security. They refer to "standard" as a structured approach to address IT security built on measurable indicators represented by controls, such as a checklist, or a general and unequivocal set of requirements, such as clauses or principles. In their analysis they question the necessity of creating new security frameworks rather than focusing on the improvement of existing ones. They compare the Cloud Computing Compliance Control Catalogue (C5) by BSI-German Information Security Office, the Federal Risk Authorization Management Program (FedRAMP) by Federal Agencies in public cloud, and the ISO/IEC 27001—Information security management systems, in order to shed light on the necessity of a new standard to define specific cloud computing security requirements. In addition, they analyze the most important security-sensitive measures missing in the three standards, organizing them into an attack model and highlight that the absence of a single security control could generate multiple threats, exposing security

gaps in such standards. Using their analytical comparative framework, they also highlight the insufficiency of all three standards to completely guarantee cloud security.

Although some of the previous works provide solutions to traditional security problems adapted to cloud services (e.g., data encryption, technical security approaches or implementation of traditional guidelines and security standards), none provide a simple and comprehensive mechanism for establishing and measuring data security in CCS.

3 Design of a Data Security Framework for Cloud Computing Services

This section presents the design of our Data Security Framework for Cloud Computing Services (DSF^{CCS}) which proposes a mechanism for securing the data in different CCS types by means of a series of tasks and activities that allows the measurement and evaluation of CCS data security.

The methodology used to design the DSF^{CCS} framework is based on the "Heuristical Theorizing" research approach from Gregory and Muntermann [22]. Heuristic theorizing is defined as the process of proactively generating design theory for prescriptive purposes, starting from problem-solving experiences and prior theory and iterating between the searches for satisficing a problem solution and the synthesis of new information that is generated during a heuristic search. The authors define heuristic as a rule of thumb that provides a plausible aid in structuring the problem at hand or in searching for a satisficing artifact design or a problem-solving process.

The methodology of heuristic theorizing involves the heuristic search for a satisficing problem solution alternating between two stages:

a) Structuring the problem at hand, and

b) Generating new design components.

Thus, in order to structure our problem, we analyzed solution concepts for the organization of ecosystems from the application areas of security issues, data security and security frameworks in CCS. To address the stage of problem structuring, a problem decomposition structure was applied. According to Gregory and Muntermann [22], decomposing a complex problem into less complex sub-problems involves subdividing the problem into sets of simpler problems and attacking these individually. As result, the main problem of improving data security in CCS was subdivided into three subproblems:

1) Identification of data security requirements in CCS,

2) Management of data risks in CCS, and

3) Evaluation of the performance of the data security in CCS.

The subproblems were defined after reviewing a vast amount of literature and integrating it into our cumulative understanding of the major problem.

The proposed DSF^{CCS} aims to provide a solution to the main problem of improvement of data security in CCS by means of the solution to the three subproblems previously structured. Such a solution for CCS is designed through a set of three activities carried out consecutively during its life cycle: identification of data security requirements, data risk management and performance evaluation of data security in CCS. Fig. 1 presents the major activities in the DSF^{CCS} life cycle, where the output of each activity is the input for the next activity. Each activity is considered completed after their sets of tasks are performed.

Figure 1: Life cycle of the data security framework for cloud computing services - DSF^{CCS}

3.1 Identification of Data Security Requirements in CCS

The first activity developed according to the methodology was the identification of the data security requirements for each of the different CCS. For this, international standards and reports such as the ISO/IEC 27001 on Requirements [23] and the European Union Agency for Network and Information Security (ENISA) [24] were studied to establish a baseline for CCS data security requirements. Close to two hundred security requirements for computer systems were identified and adapted to CCS data security requirements. DSF^{CCS} users can use this inventory of data security requirements to identify those that are relevant to their context or, failing that, help to establish their own specific requirements.

These security requirements have been grouped into twenty-four categories which include the most important aspects of CCS data security—see Tab. 1.

Table 1: Categories of security requirements adapted to the DSF^{CCS}

Security Requirement Category	Description
1. Personnel Security	Requirements that define the procedure for hiring IT staff (identity, nationality, references, etc). and for determining where personnel data is stored.
2 Supply-Chain Assurance	Requirements that apply when the cloud provider subcontracts some operations that are key to the security of the operation third parties.
3. Operational Security	Requirements to ensure that the provider meets appropriate mechanisms to mitigate unauthorized disclosure in addition to commercial agreements with external cloud providers.
4. Software Assurance	Requirements to protect the integrity of the operating systems and applications software.
5. Network Architecture	Requirements to protect the integrity of network technologies.
6. Host Architecture	Requirements for virtual elements located in physical equipment.
7. PAAS—Application Security	Requirements for ensuring a PaaS provider has considered security principles when designing and managing their PaaS platform.
8. SAAS—Application Security	Requirements for ensuring that SaaS providers deliver secure applications while customers are responsible for operational security processes.
9. Resource Provisioning	Requirements for assuring resource availability, e.g., resource overload or failure event.
10. Identity and Access Management	Requirements to ensure that the cloud provider identity and access management system are under their control.
11. Identity Provisioning	Requirements to define that checks are made on the identity of user accounts at registration time.
12. Management of Personal Data	Requirements for ensuring privacy and availability of user data.

(Continued)

Table 1 (continued).

Security Requirement Category	Description
13. Key Management	Requirements for ensuring key management under control of the cloud service provider.
14. Encryption	Requirements for ensuring encryption management under control of the cloud service provider.
15. Authentication	Requirements for ensuring authentication forms used for high assurance.
16. Credential Compromise	Requirements to avoid credential compromise or theft of the same.
17. Identity and Access Management Offered to the Cloud Customer (IAMCC)	Requirements for ensuring identity and access management system offered by the cloud service provider for use and control by the cloud customer.
18. Asset Management	Requirements to ensure the provider maintains a current list of hardware and software assets under the cloud service provider control.
19. Data and Services Portability	Requirements to understand risks related to vendor lock-in.
20. Business Continuity Management	Requirements to assurance continuity in an organization in case of a cloud service disruption.
21. Incident Management and Response	Requirements to contain the impact of unexpected and potentially disruptive events in the cloud service to an acceptable level for the organization.
22. Physical Security	Requirements for minimizing the effects of a physical security breach on multiple cloud service providers which are interrelated.
23. Environmental Controls	Requirements to define the procedures or policies that are in place to ensure that environmental issues do not cause an interruption to service.
24. Legal Requirements	Requirements to define regulatory frameworks to assure that customers and potential customers of cloud service providers comply with their respective national and supranational obligations.

Once security requirements were identified, adapted and categorized, each of these categories were mapped onto the different CCS types, where different CCS types require a different level of data security. It is important to mention that data handled by each type of cloud service has a different level of abstraction and, as a consequence, a different form of security treatment. For example, data stored on a platform as a service (PaaS) are composed mainly of images of virtualization services, while data stored in software as a service (SaaS) come from different sources, mainly applications, databases, raw data, etc. Therefore, the treatment and level of safety for each is different.

3.2 Data Risk Management in CCS

Based on the mapping of the various security requirement categories onto each CCS, the next activity in our methodology is the structuring of the data risk management subproblem. According to the framework a solution to the treatment of data risk is proposed by means of the series of tasks presented next.

The first task is the assessment of risk for specific data security requirements. The analysis of ISO/IEC 27005 on information security risk [25] and NIST—Risk Management Guide for Information Technology Systems [19] allowed us to identify and integrate critical risk management tasks into the DSF^{CCS}. This integration was carried out by adapting the risk management processes in traditional information systems to data risk management in CCS. Such adaptation is required because the aforementioned literature is not developed for cloud computing environments. As a result, the data risk management activity for CCS is decomposed into the set of tasks depicted in Fig. 2.

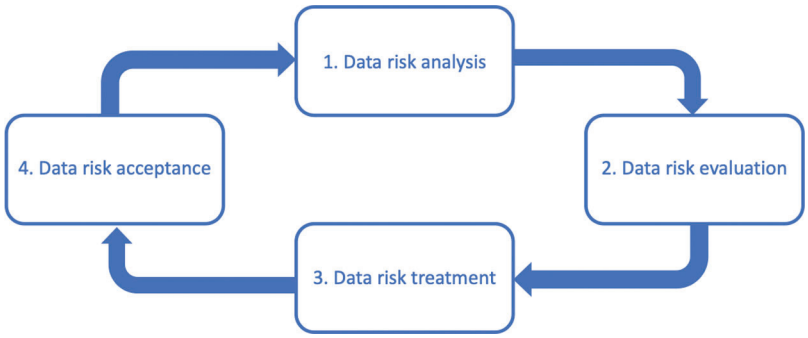

Figure 2: Tasks for data risk management in DSF^{CCS}

These tasks were adapted from [19] and [25] in order to provide a guideline for the management of CCS data security risk. The following subsections describe each of the tasks for addressing the management of data risk in CCS.

3.2.1 Data Risk Analysis

The data risk analysis task is composed of three subtasks—see Fig. 3:

Figure 3: Flow of data risk analysis subtasks

1) Data risk assessment,

2) Data risk identification, and

3) Data risk estimation.

The data risk assessment subtask defines the scope and boundaries of data risk management in the organization for the specific CCS. This task determines the value of data assets and identifies their threats and vulnerabilities.

The second subtask determines what could happen to cause a potential data loss within a specific CCS and how, where and why the loss might happen.

Thirdly, once the critical data risks have been identified, their vulnerabilities and possible incidents known, a data risk estimation methodology may be used to obtain a general indication of the level of data risk in order to reveal the major risk. Such data risk methodology can be qualitative, quantitative or a combination of both. Some data risk estimation methodologies that can be used are: matrix of threats, ranking of threats or likelihood of risks (see [25]).

3.2.2 Data Risk Evaluation

Once the above data risk analysis is carried out, the next task is to perform a data risk evaluation in order to define a criterion for each of the data risks identified. This data risk evaluation task will define the evaluation criteria needed to evaluate the risks identified previously. For this step, using the data risk evaluation criteria defined during establishment of the context, the organization should compare the estimated data risks identified using selected methods or approaches such as the methodologies previously mentioned. The data risk evaluation criteria used should be consistent with defined external and internal data security risk management contexts and take into account the objectives of the organization and stakeholder views. Decisions made in the risk evaluation activity are based mainly on the acceptable level of data risk. However, data risk consequences, likelihood and the degree of confidence in the data risk identification and analysis should be considered as well.

The data risk evaluation task is accomplished using information valuation which covers issues such as:

- Personal information
- Legal and regulatory obligations
- Commercial and economic interests
- Business policy and operations
- Contract or agreement, etc.

3.2.3 Data Risk Treatment

Once the above data risk evaluation is carried out, the next task to be performed according to our methodology is data risk treatment which consists in the development of some strategy to address each of the risks analyzed and evaluated previously. This data risk treatment task establishes a series of actions to reduce, retain, avoid or transfer the data risk according to a defined data risk treatment plan (DRTP). According to [23] a risk treatment plan is an essential part of an organisation implementation process, as it documents the way the organisation responds to identified threats. The data risk treatment options should be selected based on the outcome of the data risk analysis task, the expected cost for implementing these options and the expected benefits. When large reductions in data risk can be obtained at relatively low cost, such options should be implemented. Fig. 4 shows the main options for the data risk treatment task.

Fig. 4 shows three different options for data risk treatment after a data risk evaluation, where such options are not mutually exclusive. Sometimes, organizations can take advantage of a combination of options, such as reducing the likelihood of risk and transferring any residual risk, where a residual risk is the risk remaining associated with an action after natural or inherent risks have been reduced by appropriate actions.

The three data risk options are:

- Data risk reduction. Here, the level of data risk should be reduced by appropriate actions so that any residual risk can be assessed as acceptable.
- Data risk avoidance. For this option, the particular risk should be avoided because it is considered too high, or the cost of implementing other treatment options exceeds the benefits. For example, for a data

risk caused by nature it may be most cost-effective to physically move the data processing facilities to a place where the data risk does not exist or is under control.

- Data risk transfer. Finally, in this type of treatment, the data risk should be transferred to another party who can more effectively manage the particular risk after a data risk evaluation. Data risk transfer involves a decision to share some risks with external parties, which can create new risks or modify existing, identified data risks.

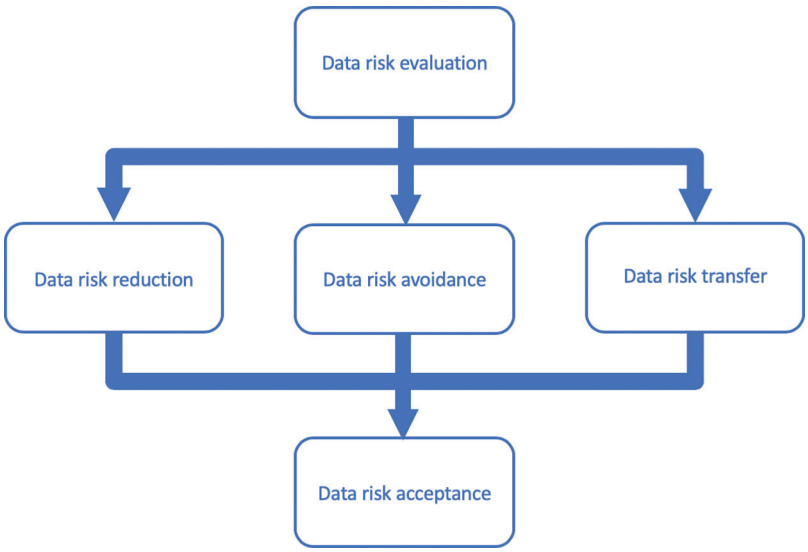

Figure 4: Data risk treatment options after data risk evaluation

3.2.4 Data Risk Acceptance

After data risk treatment is carried out, the next task is data risk acceptance which culminates in a decision to accept the risk and responsibilities for the data risk analysis. As mentioned, data risk management should describe how assessed data risks are treated to meet the data risk acceptance criteria. It is important for managers to review and approve the proposed data risk treatment and resulting data residual risks, and record any conditions associated with such approval in the DRTP. In some cases, the data risk acceptance criteria can be more complex than just determining whether or not a data residual risk may be accepted. For example, it might be argued that it is necessary to accept a data risk because the benefits accompanying the risk are very attractive, or because the cost of the data risk reduction is too high. The output of this task is a list of accepted data risks together with justification for those that do not meet the organization's normal data risk acceptance criteria and must be specified in the DRTP.

It is important to mention that the data risk management task is an iterative process which must be continuously adapted because data risks are not static. Threats, vulnerabilities or likelihood may change abruptly without prior indication and constant monitoring is necessary to detect such changes to give them the corresponding treatment.

3.3 Performance Evaluation of CCS Data Security

Finally, the last activity in our methodology is the structuring of the subproblem of the performance evaluation of data security and the design of a proposed solution. This activity consists in the definition of mechanisms for the measurement, analysis, monitoring and improvement of CCS data security. In this

activity, the subproblem is focused on how to evaluate data security performance and its effectiveness in order to determine:

- What data security requirements, process and controls, need to be measured and monitored.
- The measurement methods for analysis and evaluation in order to ensure valid results.
- When the analysis results and monitoring should be performed, and
- Who should perform the measurement, analysis, monitoring and improvement.

For this, related works such as [23,24,26] were analyzed to establish and adapt different mechanisms for the performance evaluation of CCS data security. It is important to remember these standards and reports were designed to be used in traditional information systems and need to be adapted to the CC paradigm.

It is also important to mention, that when using the DSF^{CCS} the organization should conduct internal security reviews at planned periods of time to provide information conformant to the organization's data security requirements initially specified. This will allow verification that the framework is effectively implemented and maintained. Fig. 5 presents the performance evaluation tasks and their sequence.

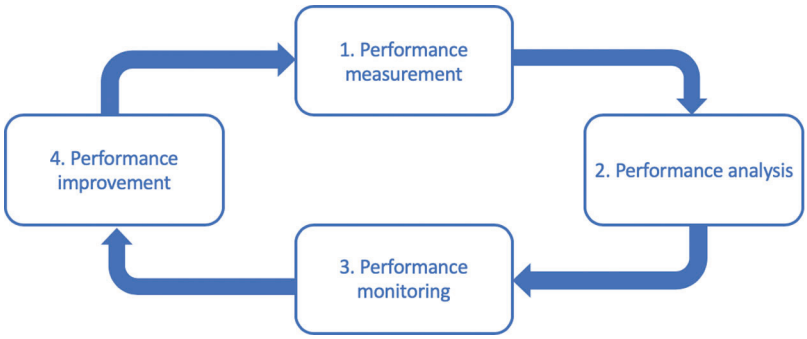

Figure 5: Performance evaluation tasks of CCS data security

Fig. 5 presents each of the performance evaluation tasks of CCS data security. These tasks are carried out sequentially where the output of each task is the input of the following one. It is important to mention that the evaluation of data security is an iterative and continuous improvement process, where in each iteration existing requirements are redefined, or new ones are added, as CCS data security is never a static process. Next each of the performance tasks is presented in detail.

3.3.1 Performance Measurement of Data Security

The solution designed for the performance evaluation of the CCS data security subproblem includes a measurement method for data security performance. Thus, this performance measurement task proposes a method to assign a numerical value to the data security level in a specific CCS. According to Abran [27], the three steps in a specific measurement context are:

1. Select a measurement method if one already exists, or design one if an existing method does not fit the need.
2. Once a measurement method has been selected or designed, its rules should be applied to obtain a specific measurement result.
3. The measurement result must be exploited in a quantitative or qualitative model, usually in combination with other measurement results of different types.

For the above, different measurement methods for security in the domain of computer security were analyzed within our methodology, including methods based on security controls such as the NIST800-53 [26] or the Cloud Security Alliance controls matrix [28]. These are a good starting point when measuring the presence and effectiveness of data security in a cloud service is needed. Such methods include a list of required or recommended security controls, where a security control is a recommended set of actions for computer security defense that provide specific and actionable ways to stop most of the pervasive and dangerous attacks.

Two aspects in security controls are important: the presence of the control itself and the effectiveness or robustness of the control. This means that the security control needs to be present and effective. Moreover, the user should describe the degree of assurance that is expected from such control or set of controls. For instance, when evaluating the effectiveness of encrypted communication between a specific service and an external user, it is necessary to verify that the implanted security control is properly designed, implemented and verified.

Measuring the effectiveness of data security controls against data security requirements is, at the end of the day, the core of this task and corresponds to the performance measurement of data security. Further research is still required to define a measurement method for CCS data security, which will constitute part of upcoming guidelines for the implementation of this framework.

3.3.2 Performance Analysis of Data Security

The analysis of results corresponding to the measurement of data security performance is important for guiding planning or developing data security and for verifying that required data security controls are properly implemented. Performance analysis also has utility for CCS procurement. For example, a cloud service provider (CSP) may choose to publish the high-level results of a third-party data security evaluation which allows users to compare the data security of two or more cloud services.

On the basis of the data sensitivity or the expected risk of a CCS it is necessary to clearly establish initial data security requirements where appropriate data security controls can be identified and implemented. Thus, having a good understanding of a sound data security approach versus the inherent risks, the assessment of the process leading to identifying the initial data security requirements and their data security controls allows analysis and verification of the effectiveness of such implementations. Therefore, methods for analyzing the performance of data security in CCS must be developed to validate the level of effectiveness of the security mechanisms implemented.

3.3.3 Performance Monitoring of Data Security

As part of the solution to the subproblem of evaluating the performance of CCS data security, performance monitoring of data security should be conducted by the organization in internal reviews at planned intervals to provide DSF^{CCS} related information. That is, the organization must identify new or updated data security requirements as well as the implementation and maintenance of their data security controls. In addition, users of this framework should establish responsibilities and security reports taking into consideration the importance of the process for monitoring results. The above will assure that such results are reported to relevant management and documented information retained as evidence of the data security evaluation and results.

Throughout this activity top management should review the organization's data security analysis to ensure continuing suitability, adequacy and effectiveness. The management review should include the status of actions from previous management reviews, changes in internal and external issues that are relevant to the data security framework and include feedback on the information related to the data security performance, including trends such as:

- Nonconformities and corrective actions

- Measurement results of data security performance
- Result of data risk assessment and status of the data risk treatment plan, and
- Opportunities for continual improvement.

Finally, the output of this activity should include the documentation related to decisions made regarding opportunities for continuous improvement and any need for changes to the DSF^{CCS} as well as evidence of such reviews.

3.3.4 Performance Improvement of Data Security

Finally, once the performance monitoring of data security has been carried out, the organization should continually improve the DSF^{CCS} suitability, adequacy and effectiveness. When a nonconformity occurs, the organization should take action to control and correct it as well as deal with consequences. A nonconformity in data security is a non-fulfillment of a data security requirement: this means that the organization has not fulfilled what is required by its own according to the framework.

In addition, the organization should evaluate the need for action to eliminate the causes of nonconformity to prevent reoccurrences. This includes determining the causes and identification of past similar scenarios. Moreover, during this activity it is necessary to review the effectiveness of any corrective action taken and make changes to the DSF^{CCS} if necessary. Such corrective actions should be appropriate to the effects of the nonconformities encountered and the organization should retain any documented information as evidence of:

a) The nature of the nonconformities and any subsequent action taken, and

b) The results of any corrective action.

4 Summary and Future Works

To improve and evaluate levels of data security in the cloud computing paradigm this work proposed a DSF^{CCS} to evaluate and improve the data security of CCS from a software engineering perspective. The DSF^{CCS} includes a prescribed set of activities for identification of data security requirements, management of data security risks and evaluation of data security performance in CCS. This work described the methodology for the design and development of such activities as part of the framework life cycle. Each of the activities as well as their tasks were adapted from traditional computing security standards to the organization's processes in order to improve its CCS data security levels.

The design of the DSF^{CCS} will need to be adapted and updated on an on-going basis as new threats to data security in CCS emerge. This will include redefinition of security requirements, risk assessment, as well as the review and establishment of new security controls.

Additional needs have been identified, but were not within the scope of the research work reported in this study, including:

- Integration into the framework of a set of guidelines which include the main data risks in CCS as well mitigation strategies,
- Development of a quantitative performance measurement method to best represent the security levels of CCS data and,
- Methods for analyzing the performance of CCS data security to evaluate the effectiveness of the data security mechanisms implemented.

Finally, one of the main strengths of the framework proposed in this work is that it can be implemented in small or medium organizations that make use of specific cloud computing services in a timely and efficient

fashion from a software engineering perspective that is, based on engineering methods and techniques applied to cloud computing.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Ponemon Institute LLC, "The cost of cybercrime," in *Ninth annual cost of cybercrime study*, Accenture Security, Traverse City, MI, USA, 2019.

[2] Cisco Systems, Inc., "Annual cybersecurity report." San Jose, CA, 2017.

[3] European Union Agency for Cybersecurity, "ENISA Threat landscape report 2017," Heraklion, Greece, January 2018.

[4] Cisco Systems, Inc., "CISCO 2018 Annual cybersecurity report." San Jose, CA, 2018.

[5] Symantec Corp., "Symantec Internet security threat report (ISTR) 2019." Mountain View, CA, USA, February 2019.

[6] Cisco Systems, Inc., "CISCO Cybersecurity threat report 2019." San Jose, CA, USA, December 2019.

[7] S. Ramgovind, M. Eloff and E. Smith, "The management of security in cloud computing," in *2010 Information Security for South Africa*, Sandton, JHB, South Africa, September 30, 2010.

[8] ISO/IEC, "ISO/IEC 17788: Information technology—Cloud Computing—Overview and vocabulary." ISO/IEC, Switzerland, October 15, 2014.

[9] ISO/IEC, "ISO/IEC 17789: Information technology—Cloud computing—Reference architecture." ISO/IEC, GE, Switzerland, October 15, 2014.

[10] S. Subashini and V. Kavitha, "Review: A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[11] S. F. Bashir and S. Haider, "Security threats in cloud computing," in *2011 Int. Conf. for Internet Technology and Secured Transactions*, ABD, United Arab Emirates, pp. 214–219, Dec 2011.

[12] Zissis D. and Lekkas D., "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[13] A. Mishra, R. Mathur, S. Jain and J. S. Rathore, "Cloud computing security," *International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC)*, vol. 1, no. 1, pp. 36–39, 2013.

[14] S. V. Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," in *Int. Conf. on Intelligent Computing, Communication & Convergence*, Bhubaneswar, Odisha, India, 2015.

[15] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 Int. Conf. on Computer Science and Electronics Engineering (ICCSEE)*, Hangzhou, China, March 2012.

[16] H. Takabi, J. B. D. Joshi and G. Ahn, "SecureCloud: Towards a comprehensive security framework for cloud computing environments," in *2010 IEEE 34th Annual Computer Software and Applications Conf. Workshops*, Seoul, South Korea, pp. 393–398, 19-23 July 2010.

[17] X. Zhang, N. Wuwong, H. Li and X. Zhang, "Information security risk management framework for the cloud computing environments," in *2010 10th IEEE Int. Conf. on Computer and Information Technology*. British Airways, UK, pp. 1328–1334, 29 June–1 July 2010.

[18] M. Almorsy, J. Grundy and A. S. Ibrahim, "Collaboration-Based cloud computing security management framework," in *2011 IEEE 4th Int. Conf. on Cloud Computing*, NW Washington, DC, USA, pp. 364–371, 4–9 July 2011.

[19] National Institute of Standards and Technology, "Risk management guide for information technology systems," in *Special Publication (NIST SP)*, NIST, USA, July 1st, 2002.

[20] T. Devi and R. G. San, "Data security frameworks in cloud," in *2014 Int. Conf. on Science Engineering and Management Research (ICSEMR)*. Chennai, India, pp. 1–6, 27–29 November 2014.

[21] C. D. Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell *et al.,* "Cloud standards in comparison: Are new security frameworks improving cloud security?." Honolulu, HI, USA, pp. 50–57, 25-30 June 2017.

[22] R. W. Gregory and J. Muntermann, "Research note: Heuristic theorizing: proactively generating design theories," *Information Systems Research*, vol. 25, no. 3, pp. 639–653, 2014.

[23] ISO/IEC, "ISO/IEC 27001: Information technology—Security techniques—Information security management systems—Requirements. ISO/IEC, GE, Switzerland, October 2013.

[24] European Union Agency for Cybersecurity, "Information assurance framework for cloud computing." ENISA, Heraklion, Greece, November 2016.

[25] ISO/IEC, "ISO/IEC 27005: Information technology—Security techniques—Information security risk management." ISO/IEC, Switzerland, 2008.

[26] National Institute of Standards and Technology, "NIST 800-53 Security and privacy controls for federal information systems and organizations," in Special Publication NIST, Gaithersburg, MD, USA, January 22, 2015.

[27] A. Abran, *Software Metrics and Software Metrology*. Hoboken, NJ, USA: John Wiley & Sons Interscience and IEEE-CS Press, 2010.

[28] Cloud Security Alliance, "Cloud controls matrix 3.0.1," CSA, January, 2019. [Online]. Available: https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/.