Document name	Code	Segment	Created by
Ahmad2020-Cloud_Computing_Trends_and_Cloud_Migration_Tuple	RISK and SECURITY > security	And top 5 leading pubic cloud service providers along with their cloud services are Microsoft (SaaS, IaaS, and PaaS), Amazon (IaaS and PaaS), IBM (SaaS, IaaS, and PaaS), Salesforce (SaaS and PaaS), and SAP (SaaS, IaaS, and PaaS) [4], whereas cloud management and security services are the integral offerings of all cloud vendors.	Ivon Miranda Santos
Ahmad2020-Cloud_Computing_Trends_and_Cloud_Migration_Tuple	RISK and SECURITY > security	Secure: Security and privacy have been the most debated and stumbling block for migration to the cloud. Security is important in all the aspects such as migration, services, and data. Security needs careful planning. Security requirements, metrics, and measurements should be well defined. This term is also used in combination with compliance and transparency.	Ivon Miranda Santos
Ahmad2020-Cloud_Computing_Trends_and_Cloud_Migration_Tuple	RISK and SECURITY > Security risk concerns	Secure: Security and privacy have been the most debated and stumbling block for migration to the cloud. Security is important in all the aspects such as migration, services, and data. Security needs careful planning. Security requirements, metrics, and measurements should be well defined. This term is also used in combination with compliance and transparency.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Other identified security risks were associated with the data intrusion and data storage in the cloud computing environment.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Security plays an important role in the wider acceptance of cloud computing services [2]. Existing literature is focused on different security solutions, including technology and security policy implementation. The latter study introduced new attacks on the cloud environment from criminological perspectives	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > security	A study [3] identified several security issues affecting cloud computing attributes. The same research proposes to over-come the identified problems concerning the security of cloud. A security guide, developed in this research, enables the cloud user organizations to be aware of security vulnera-bilities and approaches to invade them.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > security	Security vulnerabilities and challenges arise from the usage of cloud computing services. Currently, cloud comput-ing models are the primary source of these challenges and vulnerabilities.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Multi-Tenancy is referred as resource sharing and associ-ated risks of data confidentiality and integrity. Multi-Tenancy has been called a serious concerning issue for professionals in cloud computing. Professionals' understanding about attack surfaces and attack vectors is most important [16]. In [17], VOLUME 9, 2021 57793B. Alouffi et al.: Systematic Literature Review on Cloud Computing Security an increased number of cloud computing service users resulted in data security and privacy threats	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Data privacy	Multi-Tenancy is referred as resource sharing and associ-ated risks of data confidentiality and integrity. Multi-Tenancy has been called a serious concerning issue for professionals in cloud computing. Professionals' understanding about attack surfaces and attack vectors is most important [16]. In [17], VOLUME 9, 2021 57793B. Alouffi et al.: Systematic Literature Review on Cloud Computing Security an increased number of cloud computing service users resulted in data security and privacy threats	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Before the latter reviewed study, research [29] highlighted that cloud computing has an alarming security risk to cus-tomers' data.	Ivon Miranda Santos

Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	A. SECURITY THREATS AND RISK MITIGATION STRATEGIES (RQ1) Data loss due to its leakage is a severe threat to cloud security. Data compromise and modifications occur without keeping the backup copy by altering or deleting the original information. Also, data storage on cloud media has less reliability because insiders and third parties can access the data. In irre-sponsible media, the companies' offering of cloud service are regarded as fraudulent [37]. Utility based approach can be used to overcome the latter-mentioned challenge by detecting the malicious behavior of users. This utility allows users to recover their data. Unity service is a personal repository service, which is different from other cloud services.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Fig. 5 shows us the seven identified types of cloud com-puting security concerns in research studies. Data tampering and leakage are the deepest valued concerns for both clients and cloud computing service providers. These types of cloud computing security issues encompass cloud computing users who cannot access cloud computing resources. They are either attackers, hackers, or users who attempt to access the cloud computing services for which they are not registered. Although data intrusion threat has a close resemblance with the earlier types of data tampering and leakage, intruders use different means of entering the data clouds. In [41], data con-fidentiality and availability have been called primary secu-rity concerns irrespective of other security lapses between clients and cloud computing services. A secure communica-tion between clients and cloud computing service providers is the second-highest score regarding cloud computing security risks. We have pointed out the IaaS level concerns as a separate type of cloud computing security risks	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Data tampering and leakage is the real concern of users in several domains. A cloud-based healthcare system may have challenges of patients' data leakage [47]. Forensic data collection and edge computing environments have severe security risks, including forensic data removal or log leak-age.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Data storage, data confidentiality, and data availability in cloud services are among the other identified threats to cloud computing security. For example, outsourcing stored data at the cloud requires an additional security layer to strengthen the data confidentiality. Research [51] introduced a ''cloud storage based on ID-based encryption'' (CS-IBE) with the one file access policy and a user's identity proposed to be used as an encryption key. Although this approach simplifies the key management issues, it shows limited performance for data confidentiality.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Outsourcing the consumers' data and addressing the asso-ciated risks is challenging for both users and cloud service providers. These risks include shadow-IT, security, control and transparency, and business continuity [56]. Interoperabil-ity is another challenge because many consumers are locked to a single CSP due to interoperability issues.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > security	Data security, privacy, and up-time were typically called the essential items in [44]. In addition to these advantages, cloud client did not require the initial capital to invest in the infrastructure. Cloud clients shift their risks to cloud computing service providers.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	Data security, privacy, and up-time were typically called the essential items in [44]. In addition to these advantages, cloud client did not require the initial capital to invest in the infrastructure. Cloud clients shift their risks to cloud computing service providers.	Ivon Miranda Santos

Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Data privacy	Data security, privacy, and up-time were typically called the essential items in [44]. In addition to these advantages, cloud client did not require the initial capital to invest in the infrastructure. Cloud clients shift their risks to cloud computing service providers.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > security	The proposed framework has been adopted by the Saudi Government agencies overseas. Among issues faced by the adopting organization, data security and privacy has been considered the leading factor when deciding whether to adopt it. Legal and policies are other issues that may not allow the adoption of CC services due to security and privacy concerns during the implementation.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Data privacy	The proposed framework has been adopted by the Saudi Government agencies overseas. Among issues faced by the adopting organization, data security and privacy has been considered the leading factor when deciding whether to adopt it. Legal and policies are other issues that may not allow the adoption of CC services due to security and privacy concerns during the implementation.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	The experimental result showed that better performance concerning throughput, response time, accuracy, and total change security features has been achieved. Security features in the blockchain-based cloud include authentication, network security, access mech-anism, and privacy method	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Data privacy	Traceability of users due to modification in data has become possible, increasing the reliability and preserving the users' data privacy.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	This systematic literature review covers a large number of studies to answer the designed research questions. We are sure that a systematic literature review covers the cloud secu-rity issues, cloud security models, risk mitigation strategies, security issues to CSPs and users, and the role of blockchain technology, which are published to date.	Ivon Miranda Santos
Alouffi2021-A_systematic_literature_review_on_cloud_computing_s	RISK and SECURITY > Security risk concerns	VI. CONCLUSION AND FUTURE WORKS First, in this SLR, we have reviewed the literature on cloud computing topics, including cloud security threats and their mitigation strategies. We identified several security risks to cloud computing. Data tampering and leakage is one of the identified risks. Consumers' trustworthiness, data out-sourcing, and its associated risks are significant challenges identified in this SLR. This SLR identified commercial cloud services providers and highlighted the security issues they face during cloud services deployment and implementation. The trustworthiness of cloud users is challenging to con-sumers of commercial cloud services providers. Data unavail-ability, insufficient security measures, and vendor lock-in, lack of interoperability and standards are identified additionally to above-mentioned issues.	Ivon Miranda Santos
Asthana2021-Multi-cloud_Solution_Design_for_Migrating_a_Portfol	RISK and SECURITY > security	This is done by preparing a matrix of applications versus different service cloud providers on metrics like cost, QoS, coverage, security etc. as illustrated in Fig.	Ivon Miranda Santos
Asthana2021-Multi-cloud_Solution_Design_for_Migrating_a_Portfol	RISK and SECURITY > security	We eliminated applications which cannot be moved to cloud because of organization policy or security.	Ivon Miranda Santos
Asthana2021-Multi-cloud_Solution_Design_for_Migrating_a_Portfol	RISK and SECURITY > Security risk concerns	Next, we evaluated if application is feasible. For each application, we built the depen-dency graph around different parts of the application. We showed the sample dependency graph in Fig. 3. Our real-world example application XYZ has the following logical constructs that were used to evaluate the dependencies, risks, security and compliance requirements.	Ivon Miranda Santos

Aydin2021-A_Study_of_Cloud_Computing_Adoption_in_Universities_a	RISK and SECURITY > security	Although personalized learning, being economic, elasticity, measurability, accessibility, low carbon emission, and standardization are shown as some benefits of cloud computing in the education field, security, compliance issue, lock-in, reliability, lack of skills, insufficient support of cloud service providers, policies on the cloud, privacy, and the complexity of cloud technologies are shown as some of its challenges (Njenga et al.,	Ivon Miranda Santos
Aydin2021-A_Study_of_Cloud_Computing_Adoption_in_Universities_a	RISK and SECURITY > security	In this structure, universities can use their own private or community cloud technologies in places where security and privacy are more important and precaution must be kept high, and public cloud technologies in areas where security measures can be kept at a lower level.	Ivon Miranda Santos
Aydin2021-A_Study_of_Cloud_Computing_Adoption_in_Universities_a	RISK and SECURITY > security	It is aimed that this board will carry out tasks that will ensure cloud data security and confidential-ity, develop policies on cloud computing, conduct R&D stud-ies on cloud applications, and carry out activities such as raising awareness of cloud computing.	Ivon Miranda Santos
Aydin2021-A_Study_of_Cloud_Computing_Adoption_in_Universities_a	RISK and SECURITY > security	As PUC is a private cloud and offers the most control over security parameters, the services/applications delivered in this struc-ture will be chosen by each university administration.	Ivon Miranda Santos
Bainomugisha2022-Crane_cloud_A_resilient_multicloud_service_abs	RISK and SECURITY > security	This has led countries and regions to enact Data Protection and Privacy laws such as the European Union (EU)'s operational General Data Protection Regulation (GDPR) that impose stringent policy controls on the use of Personally identifiable information (PII). In Africa, over 80% of the countries have data protection laws with varying degrees of enforcement (Daigle, 2021).	Ivon Miranda Santos
Bainomugisha2022-Crane_cloud_A_resilient_multicloud_service_abs	RISK and SECURITY > Data privacy	This has led countries and regions to enact Data Protection and Privacy laws such as the European Union (EU)'s operational General Data Protection Regulation (GDPR) that impose stringent policy controls on the use of Personally identifiable information (PII). In Africa, over 80% of the countries have data protection laws with varying degrees of enforcement (Daigle, 2021).	Ivon Miranda Santos
dePaula2016-A_systematic_literature_review_on_cloud_computing_a	RISK and SECURITY > security	[S28] proposed a framework to support the migration of legacy systems to the cloud based on security and trust concerns.	Ivon Miranda Santos
dePaula2016-A_systematic_literature_review_on_cloud_computing_a	RISK and SECURITY > security	The authors proposed two solutions to improve its security; especially the isolation of data in the IaaS Cloud, and the isolation of networks within the university by adopting the Tree-Rule Firewall approach.	Ivon Miranda Santos
dePaula2016-A_systematic_literature_review_on_cloud_computing_a	RISK and SECURITY > security	S36] proposed the use of a real option model to help companies think and decide when to switch to cloud based on the expected benefits, uncertainties and the value a company puts on money. [S37] investigated different approaches to reduce both cost and task completion time of computations using Amazon EC2's spot instances for resource provisioning. In the case of [S38], the authors focused on the following factors: availability, portability, integration, migration236 A.C.M. de Paula and G.d.F. de Carneiro complexity, data privacy and security	Ivon Miranda Santos
dePaula2016-A_systematic_literature_review_on_cloud_computing_a	RISK and SECURITY > Data privacy	S36] proposed the use of a real option model to help companies think and decide when to switch to cloud based on the expected benefits, uncertainties and the value a company puts on money. [S37] investigated different approaches to reduce both cost and task completion time of computations using Amazon EC2's spot instances for resource provisioning. In the case of [S38], the authors focused on the following factors: availability, portability, integration, migration236 A.C.M. de Paula and G.d.F. de Carneiro complexity, data privacy and security	Ivon Miranda Santos

dePaula2016-A_systematic_literature_review_on_cloud_computing_a	RISK and SECURITY > security	The goal was to select a cloud provider based on the suitabil-ity of the service provider to the relevant security and privacy requirements.	Ivon Miranda Santos
dePaula2016-A_systematic_literature_review_on_cloud_computing_a	RISK and SECURITY > security	[S48] highlighted the importance of an informed choice of a Cloud Service Provider (CSP) in minimising one's exposure to the insecurity of a cloud context and proposed a well-defined approach, known as the Complete-Auditable-Reportable (C.A.R	Ivon Miranda Santos
dePaula2016-A_systematic_literature_review_on_cloud_computing_a	RISK and SECURITY > security	A spectrum of techniques and approaches has been identified that cope with vari-ous concerns, i.e., security and trustworthiness, elasticity, portability and inter-operability, and cloud resilience. In addition, many studies look into reference architectures and cloud-based architecture design methods as well.	Ivon Miranda Santos
dePaula2016-A_systematic_literature_review_on_cloud_computing_a	RISK and SECURITY > Security risk concerns	A spectrum of techniques and approaches has been identified that cope with vari-ous concerns, i.e., security and trustworthiness, elasticity, portability and inter-operability, and cloud resilience. In addition, many studies look into reference architectures and cloud-based architecture design methods as well.	Ivon Miranda Santos
Gholami2016-Cloud_migration_process—a_survey__evaluation_framew	RISK and SECURITY > Security risk concerns	The need for a systematic approach is particularly important when organisations are heavily dependent on legacy applications that have been in operation and stored critical data over the years. Moving to the cloud raises many concerns such as security, interoperability, and vendor lock-in.	Ivon Miranda Santos
Gholami2016-Cloud_migration_process—a_survey__evaluation_framew	RISK and SECURITY > security	Moving to the cloud raises many concerns such as security, interoperability, and vendor lock-in.	Ivon Miranda Santos
Gholami2016-Cloud_migration_process—a_survey__evaluation_framew	RISK and SECURITY > security	As this concern can impact migration process, a migration approach, which is used for moving data tier of legacy application to the cloud, has to incorporate security-related activities into its process.	Ivon Miranda Santos
Gholami2016-Cloud_migration_process—a_survey__evaluation_framew	RISK and SECURITY > security	However, the requirement analysis in the context of cloud migration is with a specific focus on elasticity and scalability application requirements [S18], computing requirements [S19], inter-operability requirements for deployment in the cloud [S21], security and regulatory requirements [S23], and storage space requirements in the cloud [S33].	Ivon Miranda Santos
Gholami2016-Cloud_migration_process—a_survey__evaluation_framew	RISK and SECURITY > Data privacy	[S35] numerate several factors are taken into account for component selection such as data privacy, expected workload profile, acceptable network latency and performance variability, availability zone of cloud providers, the affinity of components in the cloud, and the geographical location of cloud servers.	Ivon Miranda Santos
Gholami2016-Cloud_migration_process—a_survey__evaluation_framew	RISK and SECURITY > Security risk concerns	The first aspect is security isolation. Enabling multi-tenant applications, specifically in migration type II, raises security risk as different tenants use the same database and running application instances. It is necessary to assure each tenant can only access to its data and to be protected from unauthorised access by other tenants which are running in the same cloud. As off-the-shelf database management systems might not support multi-tenancy (Jacobs and Aulbach, 2007), securing the data tier of application should be properly addressed. Furthermore, the code blocks of the application reflecting organizational business processes (.e.g. BPEL processes) might need to be secured prior deploying in the cloud to protect from unauthorized access by other tenants. Hence, assuring confidentiality of code execution, for example through encryption mechanisms, in the sense that no other tenants will be able to access, read, or alter the code blocks within the running application instance in the cloud.	Ivon Miranda Santos

Gholami2016-Cloud_migration_process—a_survey__evaluation_framew	RISK and SECURITY > Security risk concerns	Given the above aspects of multi-tenancy, only the approach proposed by Maenhaut et. al. [S29] incorporates explicit activities to add customisability and security isolation to legacy applications are to move to a hybrid or public cloud environments. That is, enabling multi-tenancy requires the following steps: (i) decoupling databases, (ii) adding tenant configuration databases, (iii) providing tenant configuration interface, (iv) dynamic feature selection, (v) managing tenant data, users, and roles, and (vi) mitigating security risks	Ivon Miranda Santos
Gholami2016-Cloud_migration_process—a_survey__evaluation_framew	RISK and SECURITY > security	cloud-specific tests are to perform including security test, interoperability test, and workload test.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > security	Some of the major issues like resource scheduling, security, and interoperability pertaining to cloud are reviewed here, along with possible ways of tackling them.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > Security risk concerns	However, it is not without the security concerns of data monopoly and privacy. In certain cases, distribution of a particular work is not even and it has to be offloaded to a resourceful platform. Migration of the executive unit needs to be done in such a case [8].	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > Data privacy	However, it is not without the security concerns of data monopoly and privacy. In certain cases, distribution of a particular work is not even and it has to be offloaded to a resourceful platform. Migration of the executive unit needs to be done in such a case [8].	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > security	The principal concerns pertaining to public cloud are security threats.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > security	With the expenditure distributed over a less number of users than public cloud, community cloud provides a high level of security and privacy.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > Security risk concerns	• Security—The data being handled by third-party host, privacy of sensitive and important data pose a serious threat.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > Data privacy	• Security—The data being handled by third-party host, privacy of sensitive and important data pose a serious threat.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > Security risk concerns	8.3 Migration Risks Risks associated with migration can be broadly classified into the following: • General risks—In general risks, we look into tuning and monitoring of performance. • Security risks—There are a number of legal consents that migration has to abide by, which includes accessing execution logs and preserving the rights to review trails. The gravity of data leakage in the world of information technology in a cloud environment is recognized.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > Data privacy	10.4.1 Data Privacy Data privacy refers to the act of data abstraction, which means isolating information and display them selectively to the parties concerned. Oblivious RAM or ORAM is used extensively for the protection of data inside a cloud platform. ORAM keeps on shuffling memory continuously while being accessed by the user. It technically behaves as the interface between the physical RAM and the program.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > security	Due to the potential risk of data breach, it is unwise to store information on the cloud without any sort of security.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > security	10.4.5 Cloud Security Alliance	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > security	The CSA is an organization focusing on areas of security guidance in cloud com-puting [62].	Ivon Miranda Santos

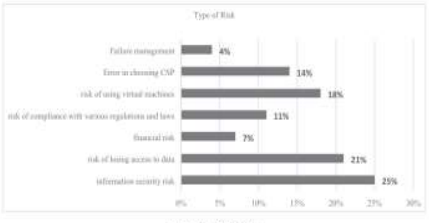
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > Security risk concerns	This paper, as promised, has done an extensive literature review on cloud com-puting. The techniques pertaining to cloud and the different service models serving it are noteworthy. The cloud migration services have been mentioned along with the idea of scheduling algorithms. The potential of Xaas (anything as a service) is remarkable and a prospect of the next generation. The dependence of the IT industry on cloud computing obliges the latter to take a stride forward. Our study concludes that despite the security risks and other factors, cloud computing has immense potential and indispensable for the generations to come.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > security	Our study concludes that despite the security risks and other factors, cloud computing has immense potential and indispensable for the generations to come.	Ivon Miranda Santos
Gourisaria2020-An_Extensive_Review_on_Cloud_Computing	RISK and SECURITY > security	Keeping in mind the security challenges and issues, cloud technology and its use must be developed to provide clients with a safe and dependable working platform.	Ivon Miranda Santos
Hajjat2010-Cloudward_bound_Planning_for_beneficial_migration_of	RISK and SECURITY > security	We articu-late the importance of ensuring assurable reconfiguration of secu-rity policies as enterprise applications are migrated to the cloud.	Ivon Miranda Santos
Hajjat2010-Cloudward_bound_Planning_for_beneficial_migration_of	RISK and SECURITY > security	Cloud Computing, Enterprise Applications, Security Policies, Performance Modeling, Network Configurations	Ivon Miranda Santos
Hajjat2010-Cloudward_bound_Planning_for_beneficial_migration_of	RISK and SECURITY > Data privacy	Further, industry-specific regulations (e.g., in health care industries), and national privacy laws may restrict what data an enterprise may mi-grate to the cloud [11]	Ivon Miranda Santos
Hajjat2010-Cloudward_bound_Planning_for_beneficial_migration_of	RISK and SECURITY > Data privacy	From a data privacy perspective, enterprises may wish to store sensitive databases (e.g., a database that stores credit card information) locally. This may in turn make it desir-able to place other components that extensively interact with such databases local, from the perspective of reducing wide-area com-munication costs and application response times	Ivon Miranda Santos
Hajjat2010-Cloudward_bound_Planning_for_beneficial_migration_of	RISK and SECURITY > security	On mi-grating application servers to the cloud, operators need to reconfig-ure ACLs to ensure that the security policies are still met.	Ivon Miranda Santos
Hajjat2010-Cloudward_bound_Planning_for_beneficial_migration_of	RISK and SECURITY > security	While §3 presented a framework to help decide which servers should be migrated to the cloud, an important challenge that must be ad-dressed is how security policies must be reconfigured.	Ivon Miranda Santos
Hajjat2010-Cloudward_bound_Planning_for_beneficial_migration_of	RISK and SECURITY > security	Our paper takes a step in this direction by devel-oping a framework for deciding what to migrate to the cloud such that enterprises can realize a benefit. Maintaining the security and privacy of data once migrated to the cloud is a challenge [14, 28], and has started receiving attention from the community [19].	Ivon Miranda Santos
Hajjat2010-Cloudward_bound_Planning_for_beneficial_migration_of	RISK and SECURITY > Data privacy	Maintaining the security and privacy of data once migrated to the cloud is a challenge [14, 28], and has started receiving attention from the community [19].	Ivon Miranda Santos
Haugeland2021-Migrating_monoliths_to_microservices-based_custom	RISK and SECURITY > security	First, we focus on introducing multi-tenancy to the applica-tion. To support multi-tenancy, we need a system for Identity Access Management (IAM), and to support customization of the application for the tenants and to configure the storage to isolate tenant data, we need a tenant manager	Ivon Miranda Santos
Haugeland2021-Migrating_monoliths_to_microservices-based_custom	RISK and SECURITY > Data privacy	First, we focus on introducing multi-tenancy to the applica-tion. To support multi-tenancy, we need a system for Identity Access Management (IAM), and to support customization of the application for the tenants and to configure the storage to isolate tenant data, we need a tenant manager	Ivon Miranda Santos
Jamshidi2017-Pattern-based_multicloud_architecture_migration	RISK and SECURITY > security	These help to determine whether the application and/or the organizations security requirements are in accordance with the security mechanisms offered by the cloud provider.	Ivon Miranda Santos

Jamshidi2017-Pattern-based_multicloud_architecture_migration	RISK and SECURITY > security	The key risk is that underlying architecture issues are not addressed. A monolithic legacy application in the cloud is still monolithic with limitations such as lack of scalability. Scalability is coarse-grained and can-not easily be achieved if, for example, the architecture does not allow the database to be updated by multiple instances.	Ivon Miranda Santos
Kratzke2017-Understanding_cloud-native_applications_after_10_ye	RISK and SECURITY > security	The descriptive validity might be insufficient for specific aspects. According to Fig. 6 there are less evaluating or validating studies than solution proposals. That might indicate that our search filters omitted evaluating and validating studies. However, we think, this just describes the current state of research. We had a broad view on CNA and searched not intentionally for specific aspects like cloud forensics, security, business applicability and so on. Our study should not be taken to draw any conclusions on these specific aspects.	Ivon Miranda Santos
Kratzke2017-Understanding_cloud-native_applications_after_10_ye	RISK and SECURITY > security	CNA properties PROP.1 Elasticity of stateful CNA components. PROP.2 Synchronizing platform and application elasticity. PROP.3 Security engineering for (multi-cloud) CNA.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Furthermore, some selected services from a single cloud cannot totally satisfy the user requirements, such as security and compliance or business and technical needs.50 This is why services used in the composition process must be combined from several clouds.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Given the emergence of a high number of new service providers (eg, Windows Azure Platform, Amazon S3, and EC2), the offered QoS, the pricing models, and the existing security policies of cloud services vary from one provider to another.61 Therefore, proposing methods that combine several services from multiple locations becomes a necessity.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > Data privacy	Given that the delivery of a high-quality service composition in the crosscloud is not yet guaranteed, Dou et al53 proposed a new method called HireSome-II to ensure the privacy of service composition for processing big data applications.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > Security risk concerns	Because of the importance of data privacy and given that companies that use the composed services are exposed to many security problems, Nacer et al19 presented an approach that reuses the existing fragments from the cloud.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > Data privacy	Because of the importance of data privacy and given that companies that use the composed services are exposed to many security problems, Nacer et al19 presented an approach that reuses the existing fragments from the cloud.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	So to remedy such problem, some authors have chosen to combine services that belong to the same cloud as the composition criteria,49,55,57 same thing for the security issues, as researchers resort to combine services according to their privacy level such as Nacer et al19 and Zemni et al.59,60 in order to protect the user's data.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > Data privacy	So to remedy such problem, some authors have chosen to combine services that belong to the same cloud as the composition criteria,49,55,57 same thing for the security issues, as researchers resort to combine services according to their privacy level such as Nacer et al19 and Zemni et al.59,60 in order to protect the user's data.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	8 SECURITY AND PRIVACY ISSUES IN THE MULTICLOUD	Ivon Miranda Santos

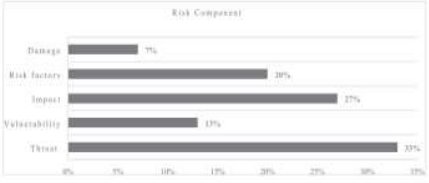
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Given the sensitive nature of the user's information stored in the cloud, guaranteeing their security and privacy should be addressed with a high and urgent priority.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Cloud users are always afraid of losing their data because of the low degree of security and the lack of mechanisms for protecting privacy in the cloud environment.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	To ensure the legal compliance and the privacy of the data stored and manipulated in the cloud environment, a set of security protocols (PasS) is used. The latter offers a full control on the privacy of the cloud consumer's data. Before sending them to the cloud, the consumers are also responsible for adding privacy enforcement structures to the data to protect it from disclosure.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > Data privacy	To ensure the legal compliance and the privacy of the data stored and manipulated in the cloud environment, a set of security protocols (PasS) is used. The latter offers a full control on the privacy of the cloud consumer's data. Before sending them to the cloud, the consumers are also responsible for adding privacy enforcement structures to the data to protect it from disclosure.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	The security is also considered as the biggest barrier, especially in the federated and multicloud environment.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	For example, when dealing with SaaS applications, the major security concern is often about the data protection and location, the security policies of the cloud providers, etc.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Given the cloud environment complexity and dynamicity, the traditional security solutions are no longer effective in dealing with themulticloud security issues.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	From today's security solutions, we could mention the secure cloud storage, which is a cloud service responsible for protecting the data existing in some cloud models or other platforms.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	This solution gives the consumers access to control their sensitive information on the cloud, to always ensure their privacy.77 Another security solution is named the intelligent protection, which is also a cloud security service developed to ensure the security of servers and applications existing in the cloud infrastructures.77 Protecting the private and critical information from loss or theft, facing control and privacy issues, guaranteeing data integrity and confidentiality, etc are some of the challenges involved while dealing with cloud services.78 The issues surrounding security are serious in 1 single cloud as in a multicloud environment.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > Data privacy	Protecting the private and critical information from loss or theft, facing control and privacy issues, guaranteeing data integrity and confidentiality, etc are some of the challenges involved while dealing with cloud services.78 The issues surrounding security are serious in 1 single cloud as in a multicloud environment. But what makes the multicloud much better is that the trust, reliability, and security capabilities are distributed among (and ensured by) several cloud providers.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	But what makes the multicloud much better is that the trust, reliability, and security capabilities are distributed among (and ensured by) several cloud providers.	Ivon Miranda Santos

Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	For example, Nacer et al19 considered that scattering the business activities and deploying them in multiple clouds will enhance their security.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Security: It is among the most important issues in cloud computing in general whatever its aspect: physical, logical, or data security. As reported in Sengupta et al,93 the security issues concern either	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Access: such as authentication, authorization, and access control in each cloud; 3. the differentinfrastructures and platformsin the multicloud environment, including the storage and the security aspects in each data center.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Hence, because services involved in the composition are selected from several clouds, the security issue becomes more serious.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	Multicloud ser-vice composition tools should also define environment constraints and security concerns when dealing with different dimensions and modalities of cloud service composition.	Ivon Miranda Santos
Lahmar2018-Multicloud_service_composition_A_survey_of_current_a	RISK and SECURITY > security	A challenging problem in a distributed, dynamic, and untrusted cloud environment is to consider security constraints in service composition.53 In fact, there are several security issues when composing services with uncertain availability and security constraints.	Ivon Miranda Santos
Lichtenthaler2019-Requirements_for_a_model-driven_cloud-native_	RISK and SECURITY > security	[6] discuss relevant services for their transformed applica-tion, which include reliable message queuing, caching and security-concerned services like virtual cloud networking and managed firewalls.	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > security	Findings – Research synthesis/SLR led to the identification of 31 issues/challenges, which may be termed as most critical based on their occurrence/frequency in past studies included. The topmost ten issues/ challenges amongst 31 identified include top management approach, change management, training and development, effective communication, system integration, business process reengineering, consultants/ vendors selection, project management, project team formation, team empowerment/skilled people and data conversing/migration. However, other issues/challenges identified such as security risks/data security, cloud awareness, functionality limitations, service level agreements and subscription expenses are more related to cloud ERPs	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > Security risk concerns	Findings – Research synthesis/SLR led to the identification of 31 issues/challenges, which may be termed as most critical based on their occurrence/frequency in past studies included. The topmost ten issues/ challenges amongst 31 identified include top management approach, change management, training and development, effective communication, system integration, business process reengineering, consultants/ vendors selection, project management, project team formation, team empowerment/skilled people and data conversing/migration. However, other issues/challenges identified such as security risks/data security, cloud awareness, functionality limitations, service level agreements and subscription expenses are more related to cloud ERPs.	Ivon Miranda Santos

Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > Security risk concerns	however, cloud ERP solutions are also facing other challenges. ERP implementation is a complex and challenging process (McCrea, 2011; Mijacc et al., 2013). It requires to invest all types of resources for effective ERP implementation. This study has identified some issues and challenges (Table VI) such as security risks/data security, regulatory legal requirements (service level agreement (SLA) issues), functionality limitations, cloud awareness, subscription expenses and among others of cloud ERP that supports findings of past studies carried out so far (Salleh et al., 2012; McCrea, 2011).	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > Security risk concerns	5.2.1 Security risks/data security. Data security is about the safety of data against unauthorized access, use and disclosure. As compare to traditional ERP, there are more threats and security risks on cloud ERP because of high ability along with the accessibility of information from distributed databases. Meganathan and Jeyanthi (2014) mentioned data security in the cloud and lack of confidence as challenges related to cloud ERPs. Similarly, Sørheller et al. (2018) also suggested data security as one of the six challenges identified in his review. High availability of cloud services options led to more security risks (Elmonem et al., 2016). Fauscette (2013) identified security concern as more critical among then inhibitors for cloud ERP. Moreover, data security issues such as confidentiality, integrity and availability are identified in past research (Saa et al., 2017). According to Dillon et al. (2010), mentioned different drawbacks in cloud-based ERP relate to data security, performance and availability. Elmonem et al. (2016) say that managing security-related issues in cloud ERP is a complex and challenging process. So, to tackle this problem cloud vendors offer service of private cloud, which is more secure as compare to the public cloud. This study supports the earlier findings in relevant research.	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > security	As compare to traditional ERP, there are more threats and security risks on cloud ERP because of high ability along with the accessibility of information from distributed databases.	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > security	Meganathan and Jeyanthi (2014) mentioned data security in the cloud and lack of confidence as challenges related to cloud ERPs.	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > security	High availability of cloud services options led to more security risks (Elmonem et al.,	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > security	(2010), mentioned different drawbacks in cloud-based ERP relate to data security, performance and availability.	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > security	(2016) say that managing security-related issues in cloud ERP is a complex and challenging process.	Ivon Miranda Santos
Mahmood2020-Erp_issues_and_challenges_a_research_synthesis	RISK and SECURITY > Security risk concerns	awareness, subscription expenses, SLAs, and security risks/data security are mostly related to cloud ERP. Enterprises should focus on these socio-technical issues and challenges before going to implement ERP systems. The findings of this study confirmed that findings of past research relating to ERP issues/challenges are still valid and applicable.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	The output of this study shows that there are 7 types of risk in cloud migration, namely information security risk, risk of losing data access, risk of using virtual machines, errors in choosing CSPs, risk of compliance with various laws and regulations, financial risk, and management failure, the weights of 25%, 21%, 18%, 14%, 11%, 7%, and 4% respectively, as well as 5 risk components, namely threats, impacts, risk factors, vulnerabilities, and damage with a weight of 33%, 27%, 20%, 13%, and 7%.	Ivon Miranda Santos

Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	The output of this study shows that there are 7 types of risk in cloud migration, namely information security risk, risk of losing data access, risk of using virtual machines, errors in choosing CSPs, risk of compliance with various laws and regulations, financial risk, and management failure, the weights of 25%, 21%, 18%, 14%, 11%, 7%, and 4% respectively, as well as 5 risk components, namely threats, impacts, risk factors, vulnerabilities, and damage with a weight of 33%, 27%, 20%, 13%, and 7%.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	Attacks on the cloud computing environment can cause data loss as well as financial losses for cloud service provi-ders as well as cloud servic@@e users (T.K and B, 2016).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	Based on literature review on previous research that discusses risk categories in the cloud (Djemame et al., 2011), elements of risk in the cloud (Djemame et al., 2016), research on the classification of assets that are assessed at risk for big data in cloud computing (Bt Yusof Ali et al., 2018), challenges in adopting cloud computing (Khan and Al-Yasiri, 2016), it is important to do further research in the field of cloud computing. In this study, this study is different from previous studies, where this study focuses more on the grouping of what is included in the types of risk in cloud migration, and wants to know what the risk components are, so that this can be used as a reference as components in assessing risk in cloud migration	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	The results of this study are based on the SLR method, which can determine the types of risks, risk components in Cloud Migration, and the trend of risk type that shown in Fig. 3. In Fig. 3. shown that the highest trend of risk type is Infor-mation security risk which is 25%.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	Multitenancy security and privacy are important challenges for cloud users, because multitenancy allows multiple users to run their applications	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Data privacy	Multitenancy security and privacy are important challenges for cloud users, because multitenancy allows multiple users to run their application	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	The results of surveys and literature studies on previous studies describe security problems in cloud computing (Efozia et al.,	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	Security is a big challenge in cloud com-puting (Amron et al.,	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	(2017) explained that in addition to technological readiness, human readiness, organizational support, and the envi-ronment in implementing cloud computing, things that are impor-tant to note are related to security and privacy, where the problems that often arise when migrating to cloud computing are Privacy (Yahuza et al.,	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	 Fig. 3. Trent of risk type.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	The review results show that currently international orga-nizations are studying national and international regulations related to data security in cloud computing (Maeser, 2020; Zhao et al.,	Ivon Miranda Santos

Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	As with the use of virtual machines in medical data and information management, there are frequent leaks (Kozlov and Noga, 2018), and health data storage in the cloud poses security risks and privacy concerns (Subramanian and Jeyaraj, 2018), as well as frequent vendor lock-in problems (Suzic et al., 2015).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	As with the use of virtual machines in medical data and information management, there are frequent leaks (Kozlov and Noga, 2018), and health data storage in the cloud poses security risks and privacy concerns (Subramanian and Jeyaraj, 2018), as well as frequent vendor lock-in problems (Suzic et al., 2015).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	With increasing amounts of data stored on cloud servers, secu-rity and data privacy issues are becoming increasingly important (Xu et al., 2019; Weil, 2019; Sun, 2019; Tabrizchi and Rafsanjani, 2020; Cheng et al., 2018; Guo et al., 2018; Ghahramani et al., 2017; Ghorbel et al., 2017; Rizvi et al., 2018; Yahuza et al., 2020; Vijayakumar and Arun, 2019; Masky et al., 2016; Opara-martins et al., 2016; Molyakov et al., 2015), so this is of particular concern because it can hinder the cloud adoption process (Modi and Acha, 2016; Khan and Al-Yasiri, 2016; Nagaraju and Parthiban, 2015), besides it can cause distrust for corporate cloud users (Alshammari et al., 2017). For this reason, it is necessary to carry out a risk assessment related to security in the cloud environment (Casola et al., 2016), the hope is that the services provided by cloud service providers (CSPs) need to be reviewed for security, includ-ing: data protection and ethics (De et al., 2016).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	With increasing amounts of data stored on cloud servers, secu-rity and data privacy issues are becoming increasingly important (Xu et al., 2019; Weil, 2019; Sun, 2019; Tabrizchi and Rafsanjani, 2020; Cheng et al., 2018; Guo et al., 2018; Ghahramani et al., 2017; Ghorbel et al., 2017; Rizvi et al., 2018; Yahuza et al., 2020; Vijayakumar and Arun, 2019; Masky et al., 2016; Opara-martins et al., 2016; Molyakov et al., 2015), so this is of particular concern because it can hinder the cloud adoption process (Modi and Acha, 2016; Khan and Al-Yasiri, 2016; Nagaraju and Parthiban, 2015), besides it can cause distrust for corporate cloud users (Alshammari et al., 2017). For this reason, it is necessary to carry out a risk assessment related to security in the cloud environment (Casola et al., 2016), the hope is that the services provided by cloud service providers (CSPs) need to be reviewed for security, includ-ing: data protection and ethics (De et al., 2016).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	Several attacks that occur in the cloud environment have an impact on cloud security vulnerabilities, such as Insider attacks, Impersonation attacks, Reply attacks, Online / Offline password guessing attacks, Parallel processing attacks, Forgery attacks, User / Server anonymity attacks, Man-in-the-Middle attack, Parallel processing attack, Impersonation attack, Denial-of-Service attack, Shoulder surfing attack (Taherkordi et al.,	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	On the Infrastructure-as-a-Service (IaaS) cloud platform, it can pose a risk of losing the VM state (Rashid Dar and Ravindran, 2019), likewise for services on the public cloud the opportunity to threaten secu-rity due to shared servers (Masky et al.,	Ivon Miranda Santos

Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	Efforts made in overcoming security risks in the cloud environ-ment include making mitigation techniques in the cloud computing environment as security against threats and attacks (Belbergui, 2017; Sharma et al., 2016; Yangui, 2016); implementing a Quality of service (QoS) system that can be used to ensure service quality security in cloud computing (Gonzales et al., 2017). Other efforts in risk mitigation in the cloud environment, such as: the Cloud-Trust system, which is a system used for security systems that are used to measure the level of confidentiality and integrity offered by CCS or cloud service providers (CSP) (Sharma et al., 2018), as well as the model security-as-a-service which is a model for security services in the cloud (Jouini and Ben Arfa Rabai, 2016). All of these riskmitiga-tion efforts constitute a security model designed to build security in the cloud computing environment (Kholidy et al., 2016). And of course, for cloud service users, it is also important to choose the right CSP (Singh and Chatterjee, 2016).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	Efforts made in overcoming security risks in the cloud environ-ment include making mitigation techniques in the cloud computing environment as security against threats and attacks (Belbergui, 2017; Sharma et al., 2016; Yangui, 2016); implementing a Quality of service (QoS) system that can be used to ensure service quality security in cloud computing (Gonzales et al., 2017). Other efforts in risk mitigation in the cloud environment, such as: the Cloud-Trust system, which is a system used for security systems that are used to measure the level of confidentiality and integrity offered by CCS or cloud service providers (CSP) (Sharma et al., 2018), as well as the model security-as-a-service which is a model for security services in the cloud (Jouini and Ben Arfa Rabai, 2016). All of these riskmitiga-tion efforts constitute a security model designed to build security in the cloud computing environment (Kholidy et al., 2016). And of course, for cloud service users, it is also important to choose the right CSP (Singh and Chatterjee, 2016).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	Table 5 shows the number of articles that review issues of risk types and risk components that often appear in cloud environ-ments. There are types of risk that most often arise are information security risk (weight = 7), risk of losing access to data (weight = 6), financial risk (weight = 2), risk of compliance with various regula-tions and laws (weight = 3) , risk of using virtual machines (weight = 5), Error in choosing CSP (weight = 4), and Failure man-agement (weight = 1). So that the percentage of the most dominant type of risk is the risk of information security by 25%, followed by the risk of losing access to data by 21%. Meanwhile, the possible risk components that often arise are threat (weight = 5), impact (weight = 4), risk factors (weight = 3), vulnerability (weight = 2), and damage (weight = 1). So that the percentage of risk compo-nents that most often arose was threat of 33%, followed by an impact of 27%. Trends towards risk types and risk components can be seen in Figures 4 and 5 below.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	 Fig. 4. Trent of risk component.	Ivon Miranda Santos

Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	1) Information security risk is a form of risk that results from the spread of company information systems (Ficco et al., 2018), it can also be caused by the use of servers by many cloud service users together (multitenant).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	2) The risk of losing access to data is a risk that is caused by an attack that suddenly appears while cloud services are being provided, so that data users cannot access the data before the attack is lost.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	3) Risk of using virtual machines is a form of risk that arises due to attacks in the cloud environment such as viruses, worms, malware, etc. (Maenhaut et al., 2019)	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	4) Error in choosing CSP is a risk for cloud service users due to errors in choosing the provider. Errors in choosing CSPs can be minimized by first analyzing and paying attention to CSP's background in providing services to other users, such as security, privacy, and service delivery (Opara-martins et al., 2016).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	5) Risk of compliance with various regulations and laws, a risk caused due to violations of the established regulations. This violation occurs because the possibility of not under-standing the existing regulations or rejection of the regula-tions that have been established	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	6) Financial risk, is a risk in a cloud environment caused by damage to service user data which causes service users to have to bear huge losses from the financial side to recover the damaged data, this data damage is for example due to a cloud server outage (Li et al., 2020).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	7) Failure management is a risk that occurs in the cloud envi-ronment due to the mismatch of the function of the cloud computing system against predetermined conditions, this form of management failure can be in the form of service failures, resource failures, correlated failures and indepen-dent failures (Han et al., 2019).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	Comparison of characteristics related to the level of security and possible threats and vulnerabilities between Cloud Computing and Fog Computing is shown in Table 6.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	challenges as well, network infrastructure security problems are still the main key to cloud computing security risks, for example the use of firewalls [1 05], and many researchers still focus on the issue of adoption. to cloud computing due to its security issues (Buettner and Buettner, 2016).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	challenges as well, network infrastructure security problems are still the main key to cloud computing security risks, for example the use of firewalls [1 05], and many researchers still focus on the issue of adoption. to cloud computing due to its security issues (Buettner and Buettner, 2016).	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	The identification of risk types and risk components in cloud migration as well as the opportunities for their emergence, which have been described in the results of this study, are a researcher's contribution to cloud service users. Attractive service offerings by Cloud Service Providers (CSPs), more and more companies want to migrate to the cloud, but companies as users of cloud services are also faced with risks. Information security risk, which is the type of risk that most often occurs in cloud migration.	Ivon Miranda Santos

Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	Information security risk is closely related to data breaches, so the impact of the risks that often arise is a threat to privacy and data integrity. The use of servers together (multitenant) is also a risk factor that exists in cloud computing. There are several risk factors in cloud migration, including technology factors, environ-mental factors and organizational factors. Choosing the right cloud service provider is also an important thing to pay attention to before migrating to the cloud.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > security	To ensure security on cloud migration, it is a shared responsibil-ity for related parties, for example government, private organiza-tions, education sector and researchers.	Ivon Miranda Santos
Maniah2022-A_systematic_literature_review_Risk_analysis_in_clou	RISK and SECURITY > Security risk concerns	To ensure security on cloud migration, it is a shared responsibil-ity for related parties, for example government, private organiza-tions, education sector and researchers. Research in the field of cloud computing still opens up great opportunities for researchers in the future, but the challenges will certainly increase, for this rea-son, it is necessary for similar studies to be developed continuously in the future.	Ivon Miranda Santos
Mateen2021-A_dynamic_decision_support_system_for_selection_of_c	RISK and SECURITY > Security risk concerns	Its main advantage is to reduce software concerns, but its ma-jor drawback is vendor lock-in. Microsoft Azure and Google App Engine are examples of PAAS. In the IAAS cloud computing structure, a repository and other resources are maintained by the service provider. The market for IAAS is network architects. Its main advantage is full control, and its major drawback is less efficiency. The examples for IAAS include Microsoft Azure and Amazon Web Service (AWS) [2]	Ivon Miranda Santos
Mateen2021-A_dynamic_decision_support_system_for_selection_of_c	RISK and SECURITY > security	The research in [6,7] emphasized the main issues related to cloud security.	Ivon Miranda Santos
Mateen2021-A_dynamic_decision_support_system_for_selection_of_c	RISK and SECURITY > Data privacy	The significant issues of concern, and the enterprise prerequisites perceived by analyzing the after-effects of the study, are watched all through the implementation of the model. An organization's higher priority is on data privacy and safety [18].	Ivon Miranda Santos
Mateen2021-A_dynamic_decision_support_system_for_selection_of_c	RISK and SECURITY > security	During evolution of the KBDSS, twelve (16) specialists were involved; IT managers, security authorities, and cloud computing experts were questioned, and their findings were reported.	Ivon Miranda Santos
Mateen2021-A_dynamic_decision_support_system_for_selection_of_c	RISK and SECURITY > Data privacy	The decision to shift data to the cloud environment is not a simple task as it involves multiple contradictory aspects. Some of these complex factors include performance, pri-vacy, data security, legal concerns, scalability, service availability, quality of service, and mainly the cost [24].	Ivon Miranda Santos
Monrat2019-A_Survey_of_Blockchain_From_the_Perspectives_of_Appl	RISK and SECURITY > Security risk concerns	Specifically, for the financial services sector, blockchain needs to overcome ten key hurdles before becoming a reality in the sector. These include matters concerning with its costs and benefits, cost mutualization, incentives alignment, evolving standards, scalability, gov-ernance, legal risks, security, simplification and regulatory interventions. Laws and regulations could impact how far and how fast the technology could develop. Therefore, regulatory approaches would need to be cleverly balanced against its innovative spirits while recognizing the possibility of the technology to unintentionally contribute to systemic risks in the financial system.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Security risk concerns	from the view point of the business to retain the flexibil-ity to change providers according to business concerns or even keep in-house some of the components that are less mission-critical due to security related risks. Inter-operability and portability among cloud providers can avoid the problem of vendor lock-in. It is the way to-ward a more competitive market for cloud providers and customers.	Ivon Miranda Santos

Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Security risk concerns	Giving an-swers to these questions is deceptively easy and straight-forward, but the reality is different. Presently, for many companies, there is a large amount of sensitive data and IT assets in-house which can deter them to migrate to the cloud due to risks of vendor lock-in, security and privacy issues. For these reasons, it becomes not only critical to consider security and privacy concerns but also related issues such as integration, portability, and interoperability between the software on-premise and in the cloud [35], should be taking into account.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Security risk concerns	As a result, data portability and interoperability concerns were the most discussed theme in relation to vendor lock-in. However, participants were less interested to divulge about the security and contract exit strategies, including data own-ership and privacy risks. Subsequent to the pilot inter-views a questionnaire was designed for a survey. The main issues raised at the interviews were incorporated into the questionnaire.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Data privacy	As a result, data portability and interoperability concerns were the most discussed theme in relation to vendor lock-in. However, participants were less interested to divulge about the security and contract exit strategies, including data own-ership and privacy risks. Subsequent to the pilot inter-views a questionnaire was designed for a survey. The main issues raised at the interviews were incorporated into the questionnaire.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Security risk concerns	Adoption of cloud computing by UK businesses The survey affirms that the concept of using cloud com-puting services to address the business IT needs has established a mainstream deployment across organisa-tions of various sizes. To further substantiate this matter, interestingly about 36 % of participants confirmed using a hybrid (public and private) cloud deployment model as opposed to a private cloud. Only 46 % of UK firms par-ticipated in the survey use public cloud services, in spite of the associated security risks (Fig. 4). The rate of adop-tion has been motivated by numerous indicators for effective cloud deployment decision. The most cited rea-sons for adopting cloud computing includes better scal-ability of IT resources (45.9 %), collaboration (40.5 %), cost savings (39.6 %) and increased flexibility (36.9 %). This suggests that organisations are allured to utilising cloud services due to the perceived business benefits of cost savings, IT flexibility and business agility.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Security risk concerns	Respondents identified systems and data security risks, loss of control and over dependence on a single cloud provider (35.1 %) as core existing barriers to future cloud implementation.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > security	Moreover, the find-ings tie in with a recent study published by [41], of which (57 %) participants identified “the biggest chal-lenge in managing data security and privacy is compli-ance”.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Data privacy	Moreover, the find-ings tie in with a recent study published by [41], of which (57 %) participants identified “the biggest chal-lenge in managing data security and privacy is compli-ance”.	Ivon Miranda Santos

Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Security risk concerns	Vendor lock-in concerns and challenges in cloud migration As cloud computing adoption rate soars across the UK market, the risks of vendor lock-in is also prevalent. How lock-in critically affects an organisations' business application and operation in the cloud cannot be over-emphasized or underestimated. For example, Fig. 8 paints a clear admonitory picture of how UK businesses rate the risks of vendor lock-in against the decision to migrate/adopt cloud services. The risks (in Fig. 8) were identified from the initial pilot interviews and also from the literature [9–11, 13]. Moreover, the following risks (i.e. inability to move data and applications in/out of cloud environments, data ownership and cyber breaches) in Fig. 8 were critical themes that emerged from the un-structured interviews with IT practitioners. The results in Fig. 8, highlights that besides the risks of data breach and cyber-attack, or failure to meet agreed service levels, UK businesses are also concerned about having corpor-ate data locked-in to a single cloud provider. These con-cerns affect the wider business functions where an enterprise is using cloud to perform essential business activities to keep operations running.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Security risk concerns	This paper confirms that UK organisations are increas-ingly adopting cloud services, and it also reveals that they have been progressively migrating services per-ceived as non-mission critical (i.e. where lock-in and se-curity risks seem lower) such as general purpose applications suites, email and massaging applications.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Data privacy	On a conclusive note, it is believed that the discussions presented herein, above all, indicate hypothetically that vendor lock-in risks will reduce cloud migration, which in turn affects the widespread adoption of cloud com-puting across organisations (small or large). Thus an emerging research agenda arises as to investigate: 1) ways to come up with multijurisdictional laws to support interoperability and portability of data across cloud pro-viders platform, along with effective data privacy and se-curity policies; and 2) novel ideas of avoiding vendor dependency on the infrastructure layer, platform, and through to the application layer as lock- cannot be com-pletely eliminated, but can be mitigated.	Ivon Miranda Santos
Opara-Martins2016-Critical_analysis_of_vendor_lock-in_and_its_i	RISK and SECURITY > Security risk concerns	Thus, for most organi-sations today, the challenge is clear that they simply do not understand potential effect of lock-in to the busi-ness. While the business benefits of cloud computing are compelling, organisations must realise that achieving these benefits are consistent with ensuring the risks of vendor lock-in and security implication of such risk is clearly understood upfront. When identified, such risks should be mitigated with appropriate business continuity plans or vendor selection, prior to migration to the cloud.	Ivon Miranda Santos
Perrons2013-Cloud_computing_in_the_upstream_oil_and_gas_industr	RISK and SECURITY > Security risk concerns	At the moment, however, the public cloud model sometimes comes with security risks. Private clouds are one alternative for managing and mitigating these kinds of threats. The objective of private clouds is not ‘‘to sell capacity over the Internet through publicly accessible interfaces, but to give local users a flexible and agile private infrastructure to run service workloads within their administrative domains.	Ivon Miranda Santos
Petcu2014-Portability_in_clouds_Approaches_and_research_opportu	RISK and SECURITY > security	CSA cloudsecurityalliance.	Ivon Miranda Santos

Petcu2014-Portability_in_clouds_Approaches_and_research_opportu	RISK and SECURITY > security	NIST' spe-cial publications are referring to Cloud architectures, Cloud security, Cloud deployment in the context of various strategies of USA federal government OASIS www.oasis-open.org/, Three important technical committees are activating:	Ivon Miranda Santos
Petcu2014-Portability_in_clouds_Approaches_and_research_opportu	RISK and SECURITY > security	However there are several gaps in the collections of available standards, like proposals for Cloud metrics and real-time monitoring, interfaces for security(-as-a-)services, accountability associated with transparency and responsibility.	Ivon Miranda Santos
Petcu2014-Portability_in_clouds_Approaches_and_research_opportu	RISK and SECURITY > Data privacy	A unified policy of the contractual terms was not yet established at national or international levels, while several proposals are on the way. One of the most disputed topic is the privacy and data protection compliance, for which no general accepted proposal is currently available.	Ivon Miranda Santos
Rai2015-Exploring_the_factors_influencing_the_cloud_computing_a	RISK and SECURITY > security	The paper has also endeavored to consolidate the research on Security issues, which is prime factor hindering the adoption of cloud through classifying the studies on secure cloud migration.	Ivon Miranda Santos
Rai2015-Exploring_the_factors_influencing_the_cloud_computing_a	RISK and SECURITY > security	RQ1- What cloud security requirements have been addressed in recent publications (2011-2014)?	Ivon Miranda Santos
Rai2015-Exploring_the_factors_influencing_the_cloud_computing_a	RISK and SECURITY > security	The aim is to find out what all aspects of cloud security have been researched and what all are not being researched.	Ivon Miranda Santos
Rai2015-Exploring_the_factors_influencing_the_cloud_computing_a	RISK and SECURITY > security	The goal is to understand the existing gaps in cloud security framework and cloud migration process RQ4- What are the obstacles in the cloud migration process and how it is being researched?	Ivon Miranda Santos
Rai2015-Exploring_the_factors_influencing_the_cloud_computing_a	RISK and SECURITY > security	Introduction & Conclusion - Contains cloud security and migration aspects.	Ivon Miranda Santos
Rai2015-Exploring_the_factors_influencing_the_cloud_computing_a	RISK and SECURITY > security	Firstly, each participant was asked for his opinions on the state of art of cloud computing, existing security concerns and the taxonomy of migration tasks.	Ivon Miranda Santos
Ranchal2020-Disrupting_healthcare_silos_Addressing_data_volume_	RISK and SECURITY > security	There have been efforts towards identifying a generic design and the building block services (ingestion, storage, governance, security, privacy) required to build dedicated healthcare cloud platforms.	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	In order to key benefit with hybrid cloud model, there are different security issues that have been shown to address.	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	Keywords—Hybrid cloud; migration; security issues; security techniques	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	In Section 2, we give an overview on work outcomes with comparative study of different existing solution and target the common problems domains and security threads from cloud, incompatible network policies.	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	Section 3 presents hybrid cloud approach, there are different security issues that have been shown to address.	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	Security in the hybrid cloud is still a major concern for many IT organizations.	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	[15] mainly concern the security risks and solutions in hybrid cloud computing for electronic governance.	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > Security risk concerns	This study summarizes major security issues based on a precise literature review.	Ivon Miranda Santos

Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > Security risk concerns	Patil et al. [16] introduce a secure Hybrid Cloud approach for encrypted deduplication of data using key generation. We propose secure hashing algorithm for avoiding deduplication, which generates a unique key for each file. The generated key is stored in private cloud and Key generation process involves inside the public cloud. For security consideration to encrypt the data before updating data into the cloud becomes necessary. For achieving authorized deduplication along with protect data security, hashing algorithm is used which makes technique very secure, to protect data from unauthorized access.	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	The security issues in hybrid cloud include: Security controls and data protection Identity and access management Secure movement of data and workloads across data centers through transport security and network firewalls Securing data residing and processed in third-party environments through encryption and tokenization Compliance with regulatory and policy requirements Poorly constructed SLAs Reconfiguration issues Shared technology issues	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > Security risk concerns	The security issues in hybrid cloud include: Security controls and data protection Identity and access management Secure movement of data and workloads across data centers through transport security and network firewalls Securing data residing and processed in third-party environments through encryption and tokenization Compliance with regulatory and policy requirements Poorly constructed SLAs Reconfiguration issues Shared technology issues	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	Demonstrating threats in hybrid cloud security to introduce a secure authentication framework for hybrid cloud services is required [24].	Ivon Miranda Santos
Raza2019-A_review_on_security_issues_and_their_impact_on_hybrid	RISK and SECURITY > security	Also, a study of hybrid model a framework of security and requirement of cloud security has been exploited and target with problem considerations. It continuously reduces burden of bulk of cost savings and complexity on users. Organization feels secure about their data against security considerations and fault interruptions. It suggests a robust way of serving user through modernize IT operational agility for service delivery requirements.	Ivon Miranda Santos
Repschlaeger2012-Cloud_requirement_framework_Requirements_and_e	RISK and SECURITY > security	Regarding to our research most of the requirements of the dimensions Costs, Reliability & Trustworthiness, IT Security & Compliance and Service & Cloud Management are independent of the service model.	Ivon Miranda Santos
Repschlaeger2012-Cloud_requirement_framework_Requirements_and_e	RISK and SECURITY > Data privacy	IT compliance is separated into provider requirements for privacy (e.g. encryption of data) and compliance (e.g. location of data center). Even standards, identity management and other data privacy requirements are considered. Communication security refers to the provided infrastructure and focuses on the communication protection via secure cryptographic protocols (e.g. SSL) and dedicated firewall settings.	Ivon Miranda Santos
Sailer2018-Healthcare_application_migration_in_compliant_hybrid	RISK and SECURITY > security	There is a rich body of literature that addresses the migration of legacy or enterprise applications to cloud [9–15] and its security and cloud hybrid aspects [12, 16–20].	Ivon Miranda Santos
Sailer2018-Healthcare_application_migration_in_compliant_hybrid	RISK and SECURITY > security	From the security and compliance perspective, ideally the appli-cation or system migrated to a target cloud environment is desired to be at least as secure and compliant as it was originally in the source environment.	Ivon Miranda Santos

Sailer2018-Healthcare_application_migration_in_compliant_hybrid	RISK and SECURITY > security	An analysis of cloud migration methodologies has been conducted [19], and from the security per-spective the authors conclude that there is little research on the migration of the security and compliance aspects.	Ivon Miranda Santos
Sailer2018-Healthcare_application_migration_in_compliant_hybrid	RISK and SECURITY > security	HIPAA compliance, in particular, introduces technical and security challenges that are an overload to the developers and operators of cloud native solutions.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	On the other hand, multicloud brings several merits such as vendor lock-in avoidance, system fault tolerance, cost reduction, and better quality of service. The biggest challenge is in selecting an optimal web service composition in the ever increasing multi-cloud market in which each provider has its own pricing schemes and delivers variation in the service security level. In this regard, we embed a module in the cloud broker to log service downtime and different attacks to measure the security risk.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Then, the cloud economic problem is transformed into a bioptimization problem, which minimizes cost and security risks simultaneously. To deal with the combinato-rial problem, we extended a genetic algorithm to find a Pareto set of optimal solutions. To reach a concrete result and to illustrate the effectiveness of the deci-sion model, we conducted different scenarios and a small-to-medium business IT development for a 5-year investment as a case study	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	illustrate that the topmost concerns of cloud adopters revolve around security issues such as availability, integrity, and confidentiality.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	It reveals that the development of a decision model with regard to the security risk perspective is crucial, apart from the economic cost viewpoint. The amount of losses owing to cloud disability to meet the security requirement should be taken into consideration because it causes business disruption, service quality degradation, loss in customer sat-isfaction and confidence, and business failure. Since the cloud, as in other new technologies, is beginning to be threatened via known/unknown attacks, this trend needs to quantify cloud security risks.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	The amount of losses owing to cloud disability to meet the security requirement should be taken into consideration because it causes business disruption, service quality degradation, loss in customer sat-isfaction and confidence, and business failure.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Since the cloud, as in other new technologies, is beginning to be threatened via known/unknown attacks, this trend needs to quantify cloud security risks.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	As such, one of the biggest challenges is to select the best procedure and metrics to quantify system security risks that are qualitative in nature. Different works have been done to measure IT security risks, and several economic risk factors such as annual loss expectancy (ALE),21,22 mean time to failure (MTTF),23 and mean failure cost (MFC)24 have been introduced to show the volume of IT unreliabilities.25 For instance, ALE is used for the whole system annual monetary losses, but it does not determine the proportion of the system stakeholders' losses, which is why we adopt the MFC metric and extend it based on our subjective model.2	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Although the speed of data communication between single-cloud modules is higher than that of mul-ticloud options, in case of failure and cybersecurity attacks, deploying multicloud and finding suitable alternatives are effective and reliable tasks due to the automated and quick reconfiguration between clouds without user intervention.27 Moreover, MCE offers low cost, better quality of service (QoS), flexibility, vendor lock-in avoidance, and reliability.27 For instance, DepSky28,29 and multicloud database30 apply data encryption and replication techniques on several datacenters, related to multiple providers in the IaaS level, to create a fault-tolerant system against failure.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Nevertheless, their work focused on network parameters as QoS items without considering security and privacy issues. Hence, it cannot quantify the cloud security risk for mission-critical applications. To obviate the problem, we propose a system framework to embed a module in the cloud broker to log each service downtime and attacks for quantifying the cloud security risk in the future. In our paper, we concentrate specifi-cally on security in MCE while single-cloud computing suffers from failure, unavailability, data exposure, and attacks on data/service integrity and data/service confidentiality from internal/external malice.26	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Hence, it cannot quantify the cloud security risk for mission-critical applications.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	To obviate the problem, we propose a system framework to embed a module in the cloud broker to log each service downtime and attacks for quantifying the cloud security risk in the future.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	In our paper, we concentrate specifi-cally on security in MCE while single-cloud computing suffers from failure, unavailability, data exposure, and attacks on data/service integrity and data/service confidentiality from internal/external malice.26 Mission-critical applications such as transactions on credit bank details, financial information, human healthcare records, etc, can tolerate network delay but not unavailability, data exposure, information disclosure, nefarious data destruction that results in service degrada-tion, disruption in business continuity (BC), unreliability, and business failure.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	In this paper, we classify cloud components and cybersecurity attacks, which are targeted to the components.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Furthermore, it considers threat probability and its effect on BC provided that the threat is materialized; con-sequently, in order to meet the security requirement, it calculates financial losses owing to cloud disability.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	In fact, based on our proposed system framework, every cloud can register and log each cybersecurity attack, downtime, data exposure, etc, in the broker repository.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	3 However, in the related works, there are some drawbacks as well as benefits. For instance, some of the related works focus on just sheer economic or limited factors, which have less influence on security issues.	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Nevertheless, so far, there is yet no decision model to decide between cloud migration versus on-premises IT development with regard to cost and cybersecurity risk perspectives. Moreover, each of which is not agile enough to take into account a variety of service types, a new organization policy, new cloud pricing schemes, and multisourcing cloud for reaching a sustainable decision point. To deal with the aforementioned problem and challenges, we develop an iterative decision model to decide between the development of internal IT and cloud migration for organization. The main contributions of this paper are as follows.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	To adopt the MFC metric as a cybersecurity risk factor24 and extend it to an advanced mean failure cost (AMFC) factor to share losses between stakeholders, specifically for special stakeholders, ie, the cloud adopter such as a company due to cloud security failure.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Indeed, after the development of a business process model by organization management, its policymaker determines the business and security requirement and customizes them in the decision model. The bioptimization problem should be solved with regard to minimization of both cloud service cost and cloud cybersecurity risk to constitute a Pareto set from the ever increasing large search space of multicloud providers along with their bunch of services in the market, which is why we apply a genetic algorithm in a combinatorial algorithm to reach a Pareto frontier	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	The bioptimization problem should be solved with regard to minimization of both cloud service cost and cloud cybersecurity risk to constitute a Pareto set from the ever increasing large search space of multicloud providers along with their bunch of services in the market, which is why we apply a genetic algorithm in a combinatorial algorithm to reach a Pareto frontier.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	In the main phase, our biobjective optimization algorithm explores the search space, enlisted in the primary phase or enlisted off-line, to select appropriate providers for web service composition based on cost and security risks derived from the cloud broker's log file, thus integrating reliable composition.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	In the main phase, our biobjective optimization algorithm explores the search space, enlisted in the primary phase or enlisted off-line, to select appropriate providers for web service composition based on cost and security risks derived from the cloud broker's log file, thus integrating reliable composition. In our evaluation, each cloud with low service cost is not appropriate unless its security risk is also at a low level. For instance, our approach may lead a web service composition with cost = 3000 K, risk = 1000 K, and total cost = 4000 K, whereas an approach that considers only a cost function leads a composition with cost = 2000 K while the risk is 2500 K based on	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	In our evaluation, each cloud with low service cost is not appropriate unless its security risk is also at a low level.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	It indicates that an approach that considers only a cost function and neglects security risk is a misleading procedure. In other words, clouds with low cost and low cybersecurity loss are favorable. Then, the final decision is made by a comparison of an optimal set with internal IT development cost. Since there is no similar work to be compared with our proposed model, we conducted several scenarios to simulate and gain concrete results. The result in the simulation of different scenarios demonstrates that MCE outperforms both single cloud and internal IT development for small- and medium-sized enterprises (SMEs).	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Most importantly, a single cloud has limitations in presenting high availabil-ity, data/service integration, and data confidentiality and fails in several situations.28 Deploying BFs on multicloud can mitigate security risks and increase the degree of reliability. The cloud market encounters new service publishing from both new added providers and current service providers. To address the problem of technology delivery complexity to users, clouds take benefit of brokers; this way, customers can select cost-effective services with better QoS complying with SLA.32,44,48 In this paper, we specifically concentrate on MCE security for mission-critical applications	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	To do so, we present a system framework and add a module in a cloud broker to log matrix information of security SLA (price, availability, integrity, and confidentiality; cf, Section 3.3.2).	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	To do so, we present a system framework and add a module in a cloud broker to log matrix information of security SLA (price, availability, integrity, and confidentiality; cf, Section 3.3.2). By the matrix information in our method, each cloud security risk can be quantifiable. Moreover, adopting SOA techniques provides facilities to deliver services from a multisourcing cloud from a single service to composite web services, which can be provisioned by different providers	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	By the matrix information in our method, each cloud security risk can be quantifiable.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Moreover, using multicloud ser-vices brings several benefits such as lock-in avoidance, a fault-tolerant system, and low security risks in failure, hardware corruption, service disruption, and sanction circumstances.27 Although the advantages of CC are trivial for everyone, each technology such as CC has its new threats and risks as well as related merits especially for the third party with unknown data/service jurisdiction.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Moreover, using multicloud ser-vices brings several benefits such as lock-in avoidance, a fault-tolerant system, and low security risks in failure, hardware corruption, service disruption, and sanction circumstances.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	7 Although the advantages of CC are trivial for everyone, each technology such as CC has its new threats and risks as well as related merits especially for the third party with unknown data/service jurisdiction. Hence, if the threats are materialized, then it may cause lack of control, BF interruption, QoS degradation, loss of customer satisfaction and confidence, disruption in BC, and loss of organization reputation; conse-quently, it causes security risks, potential financial losses, and even business failure.52 CC suffers from several security threats that cannot be disregarded.38	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	As the European Union Agency for Network and Information Security (ENISA)53 and previous research studies14,39,54 stipulate, the security tenets for IS are availability, integrity, and confidentiality. Infor-mation systems availability is achieved when users access and exploit their information or services timely and reliably. Therefore, availability loss disrupts access to user information or services. As such, IS integrity is achieved when improper information modification/destruction is inhibited; it guarantees information custody, nonrepudiation, and authenticity. Therefore, integrity loss makes an unauthorized destruction or modification of information. Similarly, IS confidentiality is achieved when individual information privacy and proprietary is preserved along with keeping authorized restriction access and discloser of information.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Therefore, confidentiality loss makes unauthorized information discloser or raises user access privilege.38-41 If the aforementioned requirements are not met, BC will be jeopardized. There exist several threats that can attack cloud datacenter components to disrupt routine tasks; hence, we classify the datacenter compo-nents, cloud threats, probability of materialization, target of attacks, which lingers to deliver a suitable level of security and its vulnerability in forthcoming sections to quantify multicloud security risks (cf, Section 3.3.2)	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	There exist several threats that can attack cloud datacenter components to disrupt routine tasks; hence, we classify the datacenter compo-nents, cloud threats, probability of materialization, target of attacks, which lingers to deliver a suitable level of security and its vulnerability in forthcoming sections to quantify multicloud security risks (cf, Section 3.3.2).	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	One of the biggest challenges is to quantify the security risk in terms of monetary losses in a multicloud environment; the reason why we extend the AMFC factor is to determine the amount of cloud adopter financial losses due to cloud disability to meet the security objectives.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	One of the biggest challenges is to quantify the security risk in terms of monetary losses in a multicloud environment; the reason why we extend the AMFC factor is to determine the amount of cloud adopter financial losses due to cloud disability to meet the security objectives. Based on our method, a broker can estimate the security risk for a related cloud. Finally, a cloud com-poser selects reliable composition with both low cost and security risk inclination to cover BUs' requirements. A trade-off between service cost and security level is necessary in the case of web service composition especially in the multisourcing option; the optimal solutions will be gained by figuring out the biobjective optimization problem known as a Pareto set.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Based on our method, a broker can estimate the security risk for a related cloud.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Finally, a cloud com-poser selects reliable composition with both low cost and security risk inclination to cover BUs' requirements.	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	In addition, the losses, for the sake of lack of security and IT control, should be taken into consideration. In several scenarios, participant variables should be customized. For instance, in on-premises deployment, we can assume loss omission for the sake of full control over IT, or FC is omitted in the case of full migration to cloud, but loss is constituted with cybersecurity losses owing to cloud disability to cover the security requirement. The final decision is based on cash flows of different deployment options in a determined life cycle along with the security risk measurement. Hence, after calculating the transaction cost, the cash flow is calculated by the net present value (NPV) of an investment.63,64	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	For instance, in on-premises deployment, we can assume loss omission for the sake of full control over IT, or FC is omitted in the case of full migration to cloud, but loss is constituted with cybersecurity losses owing to cloud disability to cover the security requirement.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	In the third phase, security risk is modeled to consider threats classification, probabilities of materializing the threats, and the impact of injury estimation in terms of monetary loss. In the fourth phase, the bioptimization problem is defined to select the optimal deployment in a multicloud scenario, which minimizes service costs and security risks simultaneously. Then, a final decision is made by the problem solution.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	3.1.2 Security requirement As mentioned in Section 2, here, risks are modeled based on the common security objectives availability, integrity, and confidentiality.14,38,66 In a cloud environment, several threats jeopardize BC and its safety and soundness. Hence, the top-most threats will be selected and ranked by Delphi panelists based on the case study context. Consequently, business disruption with related financial losses due to security failure will be calculated in cash flow within the cost analysis phase	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Moreover, the constraints for the least and the most number of sourcing options must be determined. The former is to avoid lock-in and create a fault-tolerant system, and the latter is to avoid redundancy and API complexity. Note that the cost model objective is to find the optimal multisourcing option to minimize the amount of variable CPV, ie, Min CPV = ∑ i∈ICPVi, whereas I is the set of providers, but it may incur high security risks	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	All of the unprecedented events resulting in loss of control or loss of security linger to BC. There-fore, cloud security must be modeled to measure risks and to manage better.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	All of the unprecedented events resulting in loss of control or loss of security linger to BC. There-fore, cloud security must be modeled to measure risks and to manage better. In the forthcoming subsections, several issues are introduced. First, security objectives as security tenets are determined. Then, system assets, threats, target of attacks, and vulnerabilities are identified. Finally, the method to quantify the security risks in economic factors is pro-posed. Furthermore, in a multicloud scenario, multiple providers are offering different virtual devices and computing units with different pricing and security levels in the market, which are taken into account as a bioptimization problem in the decision model.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	3.3.1 Security tenets According to broad research on security issues,14,38-41,69 the triple-vector feature (availability, integrity, and confidentiality) constitutes the security tenets in a cloud environment.	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	As such, data confidentiality is affected once the user's data are inadvertently or maliciously accessed by unauthorized users or even exposed. Overall, violation of each of the security principles leads to the user's business discontinuity, yielding detriment and losses. To measure cybersecurity risks carefully, we classify the level of data criticality such as in the work of Ben et al.26 Data availability can be separately considered for critical data and archival data based on the volume of losses for unavailable data. For instance, minute-by-minute data operation unavailable for a company seems to create great losses because it hampers the delivery of the main services to their customers, whereas archival data unavailable is not time critical, and delay in the access of such data does not incur great detriment.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	When we speak about the likelihood of cloud disability to cover the users' security requirement, we should take the cloud datacenter's components into account as a target of attacks.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	In spite of the provisioned virtual resources, cybersecurity threats do not distinguish between real and virtual components.26 We classify the cloud system components regardless of their type as either physical or virtual.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	However, we adopt MFC from the literature and extend it to AMFC based on our model to measure the system cybersecurity monetary losses.24,26 Hence, the cyberse-curity risk model must be developed, apart from economic cost model development.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	In this section, the AMFC variable is developed to quantify the amount of company losses as the only stakeholder under study, owing to cloud disability to meet the security requirement. It needs some concepts and assumptions such as system stakeholders, security specifications, security requirements, threats, probability of threat materializing, vulnerability, and impacts.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Threat probability matrix (TPMi): The cell TPM (Th , i) is filled by a security team familiar with the threat occur-rence likelihood and its configuration within system operation by sourcing over Cloudi. It indicates the threat occurrence likelihood per unit of operation epoch. The dimension of TPMi is T × 1, as shown in Table 7. Moreover, the amount of matrix values depends on the deployed cloud	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	3.4 Cloud decision model By using multicloud as a multisourcing option to cover business functional and nonfunctional requirements, several bene-fits are brought to users (whether individuals or organizations), such as a fault-tolerant system, lock-in avoidance, low risk, etc. As such, web service composition is selected to meet the needs, which is made possible by multicloud SOA reusabil-ity. Figure 5 shows the web service composition in cloud application. There are several cloud applications with different composition patterns, ie, sequence, parallel, and branch and loop,77-79 which are supported by Business Process Execution Language,80 but for the sake of simplicity, we consider the sequence pattern, as can be seen in Figure 7. Consequently, the cloud decision model intends to find the optimal composition to minimize both service costs and security risks.	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	3.4 Cloud decision model By using multicloud as a multisourcing option to cover business functional and nonfunctional requirements, several bene-fits are brought to users (whether individuals or organizations), such as a fault-tolerant system, lock-in avoidance, low risk, etc. As such, web service composition is selected to meet the needs, which is made possible by multicloud SOA reusabil-ity. Figure 5 shows the web service composition in cloud application. There are several cloud applications with different composition patterns, ie, sequence, parallel, and branch and loop,77-79 which are supported by Business Process Execution Language,80 but for the sake of simplicity, we consider the sequence pattern, as can be seen in Figure 7. Consequently, the cloud decision model intends to find the optimal composition to minimize both service costs and security risks.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	This subsection first introduces a system framework that consists of several modules and then clarifies the problem state-ment, which should minimize 2 equally important objectives, namely, services' costs and security risks, simultaneously.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	A multicloud environment (MCE) is one that contains a set of m clouds, whereas MCE={C1, C2 , … , Cm}, as in previous works.33,81,82 Every cloud includes a set of service files F = {F1, F2 , … , Ff}, whereas every service file contains a set of services S = {S1,S2 , … , Ss}, derived from off-line broker information in the primary phase, which is not the focus of this paper. Moreover, each cloud has its own pricing schemes and security level.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	• The cloud combiner selects a suitable cloud set, which has the most appropriate services to accomplish the user's security requirement along with cost, and produces a cloud combination list based on the set.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	• The service composer receives a cloud combination list from the cloud combiner module and determines the services from which the cloud can best accomplish the user's security requirement.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	• The security violation log registers all of the abnormal manners of each cloud, which is then made accessible to a broker later on; for instance, the number and duration of server unavailability, the number of repudiation information/service, data leakage due to malicious insider/outsider attacks, etc, can be profiled in the form of matrix information to calculate the probability of threat materialization.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Moreover, all web services are bundled with related virtual machine, disk, database, and network specifications and to deploy on a related cloud datacenter. We presumed that business revenue is the same in all deployment options, whether you migrate to cloud or extend your on-premises IT; hence, we take only the pure cost present value, CPV, into account with a minimization trend for the first objective, instead of taking NPV with a maximization trend. The second objective is to minimize cybersecurity risks	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	4.2.3 Cloud risk model As mentioned before, in a multicloud scenario, each cloud is threatened by classes of threats with probability variations. By applying multisourcing, the amount of security risks in terms of monetary loss is calculated by Equation 14. The amount of matrices STM, DM, and TFM do not depend on deployed clouds, whereas matrices ITCMi and TPMi depend on deployed cloud i. The probabilities data distribution were defined in the investigation phase.	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Pareto frontier Pareto optimality is an economical concept with applications in social and engineering sciences.86 It is defined as allo-cating goods among individuals where no individual can improve its situation without worsening another's. Pareto frontier is a set of Pareto efficient options in which connecting members of such set generate a Pareto frontier curve. The Pareto set is used in the field of engineering when the designer should make a compromise among this set instead of considering the full range of each variable. As the ever increasing cloud market provisions a handful of web services by different providers, which has potential conflicts between delivered service cost and its security risk, the solution of bioptimization problems needs to be constituted as a Pareto front in our decision model. The Pareto front is for-mally defined as follows: By considering a design space with n real parameters and m measurement criteria for each design. Let f : Rn→Rm be a function that maps a criteria space point f(x) to each design space point x. If X and Y=f(X) be the set of all possible solutions in Rn and their measured value in Rm, respectively	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	In this case, we separately calculate the security risk of its solution to quantify the goodness of the single-objective approach. The second model is a random biobjective model, which casually selects services from different providers to meet the requested web services. Then, we calculate variables CPV and AMFC as cost function and security risk, respec-tively, for their presented solution based on our formulation.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	As Figure 12 shows, a single-objective model beats a random biobjective model because a single-objective model, at least, strives to minimize the cost function despite neglecting security risks of used clouds.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	As Figure 12 shows, a single-objective model beats a random biobjective model because a single-objective model, at least, strives to minimize the cost function despite neglecting security risks of used clouds. On the other hand, in all scenarios, our model outperforms other models in terms of fitness value because it tries to find an equilibrium between objectives, which are shown in the Pareto set points making a Pareto curve. For instance, Figure 13 illustrates the Pareto set points of Op2 for our real case study, which needs 6 web services in MCE with 40 providers for the first year of investment.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	The genomic individual vector V = (6,6,24,35,24,24) from the Pareto set is one of the optimal solutions, which means that web services numbered 1 and 2 are deployed on Cloud6, web services numbered 3, 5, and 6 are deployed on Cloud24, and web service numbered 4 is deployed on Cloud35, respectively. It also does not violate constraints, ie, 3 providers are engaged along with cohosting web services numbered 5 (healthcare) and 6 (insurance) on the same cloud to decline communication costs. In the aforementioned instance solution, the costs of composited web services are CPV = 94 321, Security Risk = 12 710, and Total Cost = 107 031.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	To see the optimality of our model, in Table 10, we can observe that security risks and total cost generated by our model level off and are better than other models in all scenarios. On the other hand, single scenario beats our biobjective model in the CPV column because it only considers cost function (CPV) to minimize.	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	For instance, in the first scenario, our model leads a composition with Cost = 3.2104 × 105, Security Risk = 1.4732 × 104, and Total Cost = 3.35772 × 105, whereas a single GA leads a composition with Cost = 3.1767 × 105. Meanwhile, the security risk that is neglected by the single-objective GA is calculated by our approach; the amount of security risk in this case is 1.8812 × 104. It implicitly indicates that the total cost is 3.36482 × 105.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Therefore, an approach that considers only a cost function and neglects security risk is a misleading procedure and never yields a sustainable decision because the security risks are the reflection of cloud disability to present availability, data/service integrity, and confidentiality as security SLA.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Therefore, an approach that considers only a cost function and neglects security risk is a misleading procedure and never yields a sustainable decision because the security risks are the reflection of cloud disability to present availability, data/service integrity, and confidentiality as security SLA. Moreover, our model finds the integration of services with the least value of security risks and total cost in most scenarios. Table 10 also indicates that our model can find a better equilibrium between cost and security risk. Consequently, it finds clouds with low cost and good security SLA coverage. To assess our model's scalability and time complexity, we also run several scenarios in the worst case with 30 requested web services from MCE in which the number of providers ranges from 30 to 500, as Figure 14 presents.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Consequently, it finds clouds with low cost and good security SLA coverage.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	With this basis, we extend pure cost calculations for the 5-year investment along with placing the amount of cyberse-curity risk, based on our approach, cost into the total cost of cash flow to reach a sustainable decision about multicloud migration; then, it is compared with on-premises option as Op1.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	With this basis, we extend pure cost calculations for the 5-year investment along with placing the amount of cyberse-curity risk, based on our approach, cost into the total cost of cash flow to reach a sustainable decision about multicloud migration; then, it is compared with on-premises option as Op1. Figure 15 depicts the comparison of options during the whole time of investment. Clearly, in all Figures, inequality Op4 < Op2 < Op3 is rationally valid. Note that since, in Op1, we can have full control on infrastructure, we neglect security risk in this option.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Since the second option is marginally better than the first option, Op1 and its dominance is not noticeable; thus, for the sake of lack of full IT control over cloud infrastructure, increasing the cybersecurity attacks, lack of intact security delivery by cloud, and WAN communication delays, it is better to extend on-premises IT rather than migrating to cloud by a traveling agency company especially for a long-term investment, owing to to economy of scale.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Op5 such as Op2 except for considering security risk. Figure 22 depicts a comparison of the amortized total cost of Op1, Op2, and Op5. Moreover, for the sake of readability and bright discrepancies, all of the total costs are divided by 2.5 × 105 to normalize all values. Although we have taken security risk as monetary losses into account, Op2 is a representative to a risky option in MCE, which is still a promising alternative for our SME under study.	Ivon Miranda Santos

Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Nevertheless, there are several inhibitors such as security, privacy, and reliability concerns that snag a radical shift toward cloud adoption.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	In this paper, we focused on vectors (price, availability, integrity, and confidentiality) as the SLA, where cloud must satisfy an appropriate security level to cover the business process of the nonfunctional requirements apart from low service cost.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	Therefore, we have extended the AMFC variable to quantify each cloud security risk.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	Therefore, we have extended the AMFC variable to quantify each cloud security risk. To do so, we have classified cloud components, internal/external threats, probability of materialization of the aforementioned threats, and target of attacks that disrupt the cloud component, in addition to classifying the security requirement, which may not be met by the victim component; then, we have calculated the cloud security risk based on our method in variable AMFC. Therefore, the problem of web service composition to cover the business process workload was converted into a biobjective optimization problem with service cost and security risk perspectives, which generally belong to an NP-complete problem	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	To do so, we have classified cloud components, internal/external threats, probability of materialization of the aforementioned threats, and target of attacks that disrupt the cloud component, in addition to classifying the security requirement, which may not be met by the victim component; then, we have calculated the cloud security risk based on our method in variable AMFC.	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > Security risk concerns	If we ignore redeployment costs due to to MCE APIs and automation, MCE offers new value-added services with better cost and security SLA in which the situation would be better than the current Op2 status. One important thing to mention is that the application of our proposed model strongly depends on the adopter organization size, the degree of criticality, culture, the environment, and even political issues, which can magnify the cloud security risk regarding	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	One important thing to mention is that the application of our proposed model strongly depends on the adopter organization size, the degree of criticality, culture, the environment, and even political issues, which can magnify the cloud security risk regarding	Ivon Miranda Santos
Shirvani2018-An_iterative_mathematical_decision_model_for_cloud	RISK and SECURITY > security	application importance; hence, the large total cost indirectly shows that cloud security disability creates hesitation from the policymakers to adopt MCE.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	Security and Privacy Preserving Hybrid Clouds	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	Rapid deployment of hybrid clouds for utility, cost, effectiveness and flexibility has made it necessary to assure the security and privacy of hybrid clouds as it transcends different domains.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	In this paper, we present an approach to building a hybrid cloud that preserves the given security and privacy policy by integrating an RWFM security module into a cloud service manager.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	Index Terms—Cloud Computing, Hybrid Cloud, Security and Privacy.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	While cloud computing has shown the promise of meeting the long-held dream of computing as a utility [2], cloud users face security threats both from outside and inside.	Ivon Miranda Santos

Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > Data privacy	There are various stakeholders while negotiating security and privacy of data like the cloud user, the cloud vendor, and third-party vendors that users rely on for security-sensitive software or configurations.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	Thus, it is very important to keep track of the data flow for preserving the security and privacy of data in the cloud. Thus, information-flow security models will be the key to realize the goal [3]. The classic-information flow security models such as DIFC [5], suffer the problem of placing no constraints on the discretionary access by owners of objects/entities.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > Data privacy	Thus, it is very important to keep track of the data flow for preserving the security and privacy of data in the cloud. Thus, information-flow security models will be the key to realize the goal [3]. The classic-information flow security models such as DIFC [5], suffer the problem of placing no constraints on the discretionary access by owners of objects/entities.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	Section IV describes our approach to securing hybrid clouds, and the security guarantees it provides.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	We have developed a dynamic labelling approach for mapreduce computations using RWFM that complements the approach presented in this paper and provides an end-to-end security in a hybrid cloud.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	Threat models and technical challenges in ensuring end-to-end security and privacy of data as it traverses the boundary of edge datacenter and cloud datacenter in an Internet-of-things (IoT) framework have been elucidated in [10].	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > Data privacy	Threat models and technical challenges in ensuring end-to-end security and privacy of data as it traverses the boundary of edge datacenter and cloud datacenter in an Internet-of-things (IoT) framework have been elucidated in [10].	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	In this paper, we have demonstrated that the RWFM model provides a secure architecture for a hybrid cloud assuring full security and privacy compliance in its private cloud and has the capability to keep track of the influences by the public cloud on the data entities.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > Data privacy	In a related work of ours [9] we have shown how the privacy infringements (note that due to the division of data in map-reduce, there is a possibility that the original privacy of the data may be compromised) that are possible in map-reduce frameworks can be overcome through the RWFM model.	Ivon Miranda Santos
Shyamasundar2017-Information_flow_control_for_building_security	RISK and SECURITY > security	Work on integrating both these aspects for realizing an end-to-end security and privacy preserving hybrid cloud is in progress.	Ivon Miranda Santos
SOrheller2018-Implementing_cloud_erp_solutions_A_review_of_soci	RISK and SECURITY > security	Data Security: in cloud-based ERPs, all organizational information, such as financial data and customer details, need to be stored with a third party supplier.	Ivon Miranda Santos
SOrheller2018-Implementing_cloud_erp_solutions_A_review_of_soci	RISK and SECURITY > security	Security is one of the barriers to the adoption of cloud-based solutions [18] and it can be difficult for businesses to decide relying on suppliers for secure storage of such information [2, 14, 19, 20].	Ivon Miranda Santos
SOrheller2018-Implementing_cloud_erp_solutions_A_review_of_soci	RISK and SECURITY > security	Sustainability in the future is pursued by implementing organizational changes, ensuring data security and seeking reliable cloud ERP suppliers.	Ivon Miranda Santos
SOrheller2018-Implementing_cloud_erp_solutions_A_review_of_soci	RISK and SECURITY > security	[12]Gupta S, Misra SC. Moderating Effect of Compliance, Network, and Security on the Critical Success Factors in the Implementation of Cloud ERP.	Ivon Miranda Santos

Stavru2013-Challenges_for_migrating_to_the_service_cloud_paradi	RISK and SECURITY > security	Cloud Computing and its challenges further affect the way agile methods and techniques could be incorporated into the Service Cloud Paradigm. Trust (O1), security and privacy (O3) of data and computation are as much important for the organization as for its customers, so the organization-customer collaboration, central to agile software development, might need to be extended to include the cloud provider (in order to increase transparency, visibility, responsiveness, etc., so needed for the building trust and confidence).	Ivon Miranda Santos
Stavru2013-Challenges_for_migrating_to_the_service_cloud_paradi	RISK and SECURITY > Data privacy	Cloud Computing and its challenges further affect the way agile methods and techniques could be incorporated into the Service Cloud Paradigm. Trust (O1), security and privacy (O3) of data and computation are as much important for the organization as for its customers, so the organization-customer collaboration, central to agile software development, might need to be extended to include the cloud provider (in order to increase transparency, visibility, responsiveness, etc., so needed for the building trust and confidence).	Ivon Miranda Santos
Weerasinghe2022-Taxonomical_classification_and_systematic_revie	RISK and SECURITY > Data privacy	At the implementation level, the developer needs to detect the quality attribute. Services in the microservice architecture are deployed in the distributed environment. This could be different networks, multi-cloud or hybrid clouds. Therefore, data needs to be transferred to each service to complete the business requirement, which ultimately leads to vulnerabilities in the entire software solution. Data security across the microservice is a big concern in the microservice architecture. It is a complicated Sidath Weerasinghe& Indika Perera / IJETT, 70(3), 222-233, 2022 229 assignment to preserve the integrity, confidentiality, and privacy of business data	Ivon Miranda Santos