Journal of King Saud University – Computer and Information Sciences 34 (2022) 3111–3120

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A systematic literature Review: Risk analysis in cloud migration

Maniah [a,b], Benfano Soewito [b,*], Ford Lumban Gaol [b], Edi Abdurachman [b]

[a] Informatics Management Department, Politeknik Pos Indonesia, Bandung 40151, Indonesia
[b] Computer Science Department, BINUS Graduate Program, Doctor of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia

ARTICLE INFO

Article history:
Received 7 October 2020
Revised 11 December 2020
Accepted 11 January 2021
Available online 3 February 2021

Keywords:
SLR
Cloud computing
Cloud Migration
Risk type
Risk component

ABSTRACT

The era of the industrial revolution 4.0 was an era marked by the transition of information and communication technology that was able to create new technology-based investments. Internet of things (IoT), Big Data, and Cloud Computing are the foundations that underlie this 4.0 industrial revolution. Cloud Computing is a service that provides network storage space and computer resources using an internet connection as a medium of access. Cloud Service Providers (CSP) offer attractive services, making more and more companies want to migrate to the cloud. Sometimes the migration process to cloud computing faces problems or even failures, and this is certainly a risk for cloud service users. This study will identify the types of risks and risk components in cloud migration using the Systematic Literature Review (SLR) method. The databases used in selecting articles that match the criteria include: Emerald Online, IEEE Xplore, ScienceDirect, SpringerLink, and between 2015 and 2020. The results of this study, there were 74 articles selected according to the criteria and reviewed. 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%.

Contents

* Corresponding author.
E-mail address: bsoewito@binus.edu (B. Soewito).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

1. Introduction

Systematic literature review (SLR) is a method used in research to analyze or review and summarize the results of previous studies

https://doi.org/10.1016/j.jksuci.2021.01.008
1319-1578/

and the results of this SLR can be used as recommendations for researchers to conduct subsequent studies. In this study, researchers used the SLR method to carry out the process of selecting articles according to the criteria selected and reviewed (Al-Ruithe et al., 2019) focusing on the type of risk and risk components that may arise during the cloud migration process.

A large data management system within a company certainly requires a very large data storage area to support the company's business nets. This if done independently (on premise) certainly creates many challenges, one of which is that the application workload will increase due to accessing the data set. Therefore, many companies that have this large data set are looking to migrate to the cloud. The impetus for migrating to the cloud is to reduce business operating costs and want to improve the performance of existing application systems (Leff and Rayfield, 2015).

Cloud computing is a platform that provides communication services and is in the form of Internet-based computing that can share resources, data and applications that run in a cloud environme@@nt (T.K and B, 2016). Based on the type of service, the Cloud is divided into 4 (four), namely: Private Cloud, which is a Cloud service that is aimed at a group or group and limits access only to that group; Public Cloud, which is a Cloud service that can be accessed by any customer with an internet connection; Community Cloud, which is a Cloud service aimed at the community which can consist of two or more organizations that have similar Cloud requirements; and Hybrid Cloud, which is a Cloud service that combines at least two types of Cloud services from Private Cloud, Public Cloud or Community Cloud (Huth and Cebula, 2011). According to The National Institute of Standards and Technology (NIST) - Reference Architecture, there are 5 (five) main actors in the Cloud ecosystem that describe their functions and roles, namely: consumers, providers, brokers, operators, and auditors (Iorga and Karmel, 2012). According to the type of service, there are 3 (three) types or types of services in the cloud, namely: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Höfer and Karagiannis, 2011).

The benefits of using cloud computing technology to the possible risks that arise from this technology are described in detail in section 1. The use of cloud computing technology services provides many advantages in supporting the company's business. The advantages of cloud services include: unlimited storage, provisioning and updating, guaranteed privacy more secure (Ko et al., 2011). In addition, users of cloud services can optimize server utilization, dynamic scalability, and minimize the development of new application life cycles (Al-Ruithe et al., 2019). But behind the benefits obtained by cloud service users, there are also problems or risks that arise, as illustrated when there is a cloud outage by Amazon, because data storage is centralized in the cloud, this can paralyze the company's business that depends on that data (Gupta and Gupta, 2014). Attacks on the cloud computing environment can cause data loss as well as financial losses for cloud service providers as well as cloud servic@@e users (T.K and B, 2016). This is a form of risk that appears in the cloud environment, namely the risk of threats to data security and confidentiality of information (Paquette et al., 2010; Wang, 2011), and also the risk of information vulnerability (Inuwa, 2015; Tchernykh et al., 2019) .

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.

The next section describes the research methodology used in this study, followed by section 3 explain the reasons why migrate to cloud computing. Section 4 explain the results and discussion, which contains analysis of the results of the literature review, which relates to the types of risks and risk components in the cloud migration process, as well as trends in state-of-the-art results. Section 5 describes the future cloud challenges, and finally the conclusion is presented at the end of this paper, namely in Section 6.

2. Research methodology

The methodology used in this research is systematic literacy review (SLR). The stages in this research are divided into 4 (four) main parts, namely: stage 1, stage 2, stage 3, and stage 4 as used by (Buettner and Buettner, 2016). The research question in this study is: "What are the types of risks and risk components in cloud migration?". The solution used to answer this research question is the Systematic Literature Review (SLR) method by conducting a paper selection process that fits the selected criteria (Al-Ruithe et al., 2019). With the SLR method, we can find out the trends of research topics that are of great interest to previous researchers, so that this can be used as a reference for further research. The importance of the SLR method in this research is that researchers can identify and analyze journals systematically according to the recommended stages related to journals about the types and components of risk in cloud migration.

The steps in Fig. 1 start from selecting the database source. The databases used in this systematic literature review include: Emerald Insight, IEEE Xplore, ScienceDirect, SpringerLink, the majority of articles in the form of international journals and the results of international proceedings between 2015 and 2020. The results of the search based on the database are shown in Table 1. Based on the research question, then the keywords used for the search were determined. Search based on compatibility with given keywords, using "Boolean" "OR" and "AND", where the keywords used are: "risk type" or "risk component" or "risk type on public cloud" or "risk component on public cloud" or ["Risk type"] and ["risk component"] and "cloud migration" or ["risk type"] and ["risk component"] and "cloud migration". The literature search strategy is based on a *meta*-database (Fowley et al., 2018), then selected, articles that match the next keyword will be taken (eligible), while those that are not suitable will be ignored (excluded). Articles that match the keywords are articles that are selected (included), then reviewed to get a summary of each article. We collected the paper that published after the year 2015 to 2019 with total 3100 papers (number of papers stage 1) as shown in Table 1. In Fig. 2. can be seen that the number of papers selected was 74 papers distributed from 2015 to 2020. 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 Information security risk which is 25%.

The process of selecting this article was carried out in stages, namely:

1) Stage 1: identify from the source database based on search criteria, at this stage the number of articles that can be identified is 3100 articles.
2) Stage 2: identify the selected articles in the first stage based on the article titles relevant to the research topic, at this stage 1412 articles can be identified.
3) Stage 3: selection of articles based on the suitability of abstract content and keywords, resulting in 230 articles.

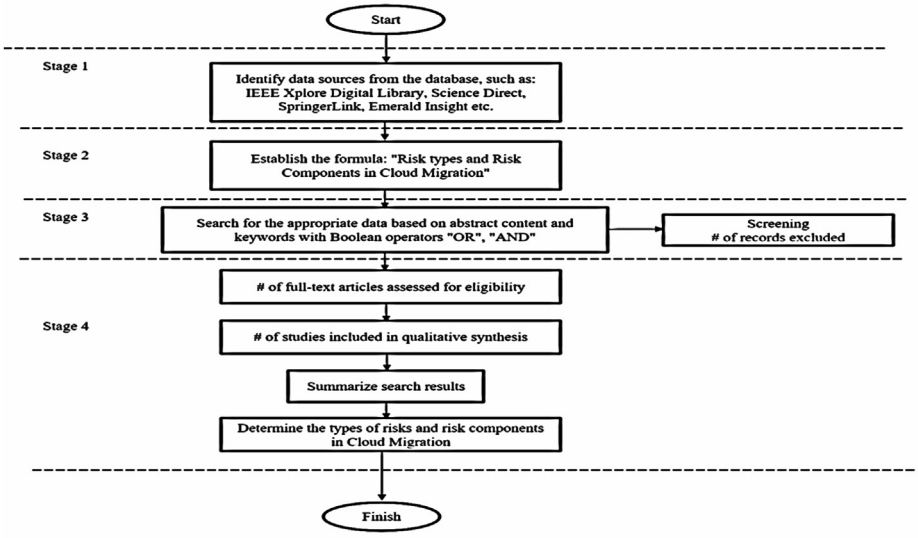

Fig. 1. The steps used in systematic literature review (SLR).

Table 1
Number of publications by database sources.

No.	Source of Database	#of Paper (stage 1)	stage 2 (of titles)	stage 3 (of abstract and keyword)	stage 4 (selected for the final review)
1	IEEE Xplore	1356	945	90	28
2	Emerald Insight	54	20	10	1
3	Science Direct- Elsevier	304	146	55	22
4	SpringerLink	1386	301	75	23
	Total	3100	1412	230	74

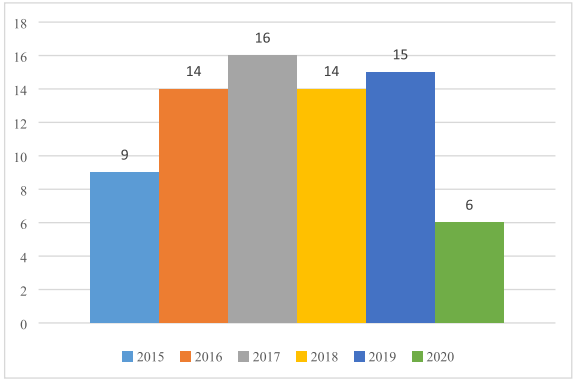

Fig. 2. Number of studies across the years.

4) Stage 4: is the final stage of removing a number of articles that are not eligible based on the search criteria, at this stage 74 articles can be identified. the distribution of the number of articles from 2015 to 2020 can be shown in Table 3.

Based on Table 1 above, the steps taken in this SLR research resulted in 74 articles which were subsequently reviewed by the researcher. The process of screening articles from the IEEE Xplore database source (28 articles), Emerald Insight (1 article), Science Direct-Elsevier (22 articles), and Springer Link (23 articles). The articles reviewed are articles sourced from research results published in international journals and international proceedings. In the final selection stage, the researcher summarizes the solutions and results of the articles being reviewed.

3. Why migrate to the cloud?

Cloud migration can save costs because cloud service providers already provide infrastructure so that it can reduce the provision of their own infrastructure (Ren et al., 2012). Several other reasons for companies migrating to the cloud are: (1) because cloud computing services have scalability, which means that they can meet the needs of information technology resources according to company needs; (2) because the cloud provider has provided settings for both hardware configuration and software updates or server settings and others, so that companies as cloud service users are more focused on developing better innovative products; (3) because the cloud provider has a data center that provides fast and efficient computing services, so this will have an effect on high performance in the cloud compared to the data center owned by the company.

Based on data from cisco.com, it is estimated that in 2020 cloud data centers will process by 93%, while in 2021 the workload of data centers will increase to 94%. The factor driving the migration of workloads from traditional data centers to cloud data centers is a greater degree of virtualization in the cloud space, which enables dynamic deployment of workloads in the cloud to cloud service demands. Cloud data center workload calculations compared to traditional data centers from 2016 to 2021, are shown in Table 2.

From Table 2 shows that the workload of cloud data centers continues to increase, this is because many companies wish to migrate to the cloud. However, by migrating to the cloud, users cannot directly control the system that manages their data and applications, because data users and cloud servers are not in the same domain. Especially for public cloud service users who implement a Shared Multi - tenant Environment. Multitenancy security and privacy are important challenges for cloud users, because multitenancy allows multiple users to run their applications

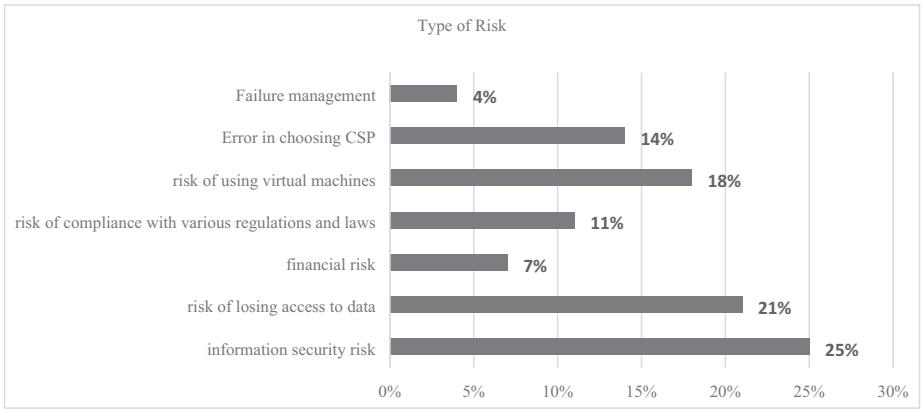

Fig. 3. Trent of risk type.

Table 2
Calculation of Migration Workloads from Traditional Data Centers to Cloud Data Centers *(Cisco.com)*.

Calculation of workload in Millions	2016	2017	2018	2019	2020	2021	CAGR 2016–2021
Traditional Data Centers	41,2	41,4	40,8	39,1	36,2	32,9	5%
Cloud Data Centers	199,4	262,4	331,0	393,3	459,2	533,7	22%
Total workload	241,5	303,8	371,8	432,4	495,4	566,7	19%
cloud data center workloads	83%	86%	89%	91%	93%	**94%**	–
Traditional data center workloads.	17%	14%	11%	9%	7%	6%	–

Table 3
Number of studies by years.

Year	2015	2016	2017	2018	2019	2020
Number	9	14	16	14	15	6
Percent	12%	19%	22%	19%	20%	8%

simultaneously on the same infrastructure and opens the door to possible privacy leaks (Rajendran et al., 2015).

4. Result and discussion

This section will explain the results of the article selection process based on the mechanism of systematic literature review (SLR). The final number of articles selected was 74 (seventy-four) which were relevant and related to risk type and component on cloud migration. The search for relevant articles is categorized into main groups, namely: State-of-the-art risk type and State-of-the-art risk component. Based on the a forementioned categories, the results can be briefly described through the distribution years of publication and state-of-the-art analysis for types of risks and risk components in cloud migration.

4.1. Publications year

The results of selecting articles based on the objectives of this systematic literature review, there are 74 (seventy four) articles selected, the distribution of the number of articles related to risk types and risk components from 2015 to 2020 in detail is shown in Table 3 below:

From the data above, we can see the trend in the number of articles in 2015–2020 related to risk types and risk components in cloud migration.

4.2. Analysis state-of-the-art for risk type and risk component on cloud computing

The results of surveys and literature studies on previous studies describe security problems in cloud computing (Efozia et al., 2017), as well as several forms of threats and vulnerabilities to cloud computing (Singh et al., 2016). Security is a big challenge in cloud computing (Amron et al., 2017). The results of a survey conducted by Ghorbel et al. (2017) explained that in addition to technological readiness, human readiness, organizational support, and the environment in implementing cloud computing, things that are important to note are related to security and privacy, where the problems that often arise when migrating to cloud computing are Privacy (Yahuza et al., 2020), also emphasized by Tabrizchi and Rafsanjani (2020) that in cloud computing, security and privacy issues are significant challenges affecting its acceptance, so that it can hinder the adoption of cloud computing (Modi and Acha, 2016). In addition, the challenge in cloud computing is the occurrence of security problems on the virtual layer (Mohamadi et al., 2019), where virtual machines are a challenge for server consolidation in virtualized data centrally (Dong et al., 2019). Survey results from (Abd Al Ghaffar, 2020) Denial of Service (DoS) attacks to distributed DoS (DDoS) attacks are also forms of security threats in cloud computing.

Based on Table 1 described in Section 2, the number of search result articles identified as many as 74 articles relevant to the search topic for risk types and risk components. The results of the analysis based on state-of-the-art in the selected articles

Table 4
Analysis results of each article.

Scope of study	Author	Conclusion
Government cloud computing and national security	(Maeser, 2020)	Data security in cloud computing is in accordance with government regulations.
Analyzing csp trustworthiness and predicting cloud service performance	(Li et al., 2020)	The impact of cloud computing implementation on availability, performance, security, finance.
Lattice-based privacy-preserving and forward-secure cloud storage public auditing scheme	(Gill and Buyya, 2020)	After migrating to a cloud server, it is important to address user data integrity and security issues.
Failure management for reliable cloud computing: a taxonomy, model and future directions	(Han et al., 2019)	In practice, there are still many failure management in cloud computing
A data sharing protocol to minimize security and privacy risks of cloud storage in big data era	(Sun, 2019)	Storage in the cloud is associated with security and data privacy risks.
Privacy protection and data security in cloud computing: a survey, challenges, and solutions	(Weil, 2019)	Privacy and security are the most important issues for the popularity of cloud computing services.
Risk assessment methods for cloud computing platforms	(Wu et al., 2019)	Information Security Risk
Cloud storage security assessment through equilibrium analysis	(Xu et al., 2019)	With an increasing amount of data stored on cloud servers, security and data privacy issues have become increasingly important.
Openness and security in cloud computing services: assessment methods and investment strategies analysis	(Zhao et al., 2019)	Cloud related services and security.
SIV: a structural integrity verification approach of cloud components with enhanced privacy	(Asvija et al., 2019)	Leakage of personal data is a threat to the integrity of components in the cloud.
Security in hardware assisted virtualization for cloud computing—state of the art issues and challenges	(Domingo-Ferrer et al., 2019)	The emergence of cloud technology raises concerns about security, so it needs to be taken seriously.
Privacy-preserving cloud computing on sensitive data: a survey of methods, products and challenges	(Juma and Tjahyanto, 2019)	In the cloud the security concerns of frequent data breaches.
Challenges of cloud computing adoption model for higher education level in zanzibar (the case study of suza and zu)	(Alassafi et al., 2019)	In government systems that adopt cloud technology,data security and risk among technological factors, as a statistically significant challenge.
A validation of security determinants model for cloud adoption in saudi organizations' context	(Patil et al., 2020)	The most significant challenge in the cloud is Security Risk.
Designing in-vm-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing	(Maenhaut et al., 2019)	Use of a virtual machine (VM) is high risk in the cloud.
Resource management in a containerized cloud: status and challenges	(Singh and Mansotra, 2019)	The use of virtual machines in cloud computing has an impact on scalability and operational costs.
Factors affecting cloud computing adoption in the indian school education system	(Abrar et al., 2018)	In adopting cloud computing, the most influential factors are technology, followed by environmental factors, and finally organizational factors.
Risk analysis of cloud sourcing in healthcare and public health industry	(Chang et al., 2018)	The cloud computing environment can pose a security risk threat.
Privacy-aware reversible watermarking in cloud computing environments	(Cheng et al., 2018)	The cloud computing environment affects both information privacy and data privacy.
Accountable privacy-preserving mechanism for cloud computing based on identity-based encryption	(Guo et al., 2018)	The need for a privacy protection mechanism for cloud users.
A privacy-preserving online medical pre diagnosis scheme for cloud environment	(Kozlov and Noga, 2018)	There are still many leaks using online medical information and data, so data privacy is not guaranteed.
Risk management for information security of corporate information systems using cloud technology	(Ficco et al., 2018)	Some of the risks in cloud computing, namely: information security risks. risk of losing access to data, financial risk, and risk of compliance with various regulations and laws.
Hybrid simulation and test of vessel traffic systems on the cloud	(Neware, 2018)	Implement cloud technology for resource virtualization and work environment.
Cloud computing digital forensic challenges	(Siddiqui et al., 2018)	Issues related to digital forensics in the cloud environment, such as data breaches, integrity, data confidentiality etc.
Security analysis of smartphone and cloud computing authentication frameworks and protocols	(Taherkordi et al., 2018)	Defines multiple attacks on cloud computing, especially on multiple security vulnerabilities.
Future cloud systems design: challenges and research directions	(Zhang et al., 2018)	The challenges in cloud computing are related to the design of cloud systems in the future.
Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing	(Subramanian and Jeyaraj, 2018)	Storing Health data in the cloud poses security risks and privacy concerns.
Recent security challenges in cloud computing	(Anjana and Singh, 2018)	The main problems in cloud computing are security and virtualization.
Security concerns and countermeasures in cloud computing a qualitative analysis	(Bryce, 2018)	The use of cloud computing services faces obstacles on the security side.
Invalid source specified. Security governance as a service on the cloud	(Hentschel et al., 2018)	Cloud computing creates various obstacles, such as security attacks, data loss, cyberattacks, attacks, data breaches.
Current cloud challenges in germany: the perspective of cloud service providers	(Alshammari et al., 2017)	Problems in adopting cloud computing are related to security risks and uncertainties for company users.
Security threats and challenges in cloud computing	(Amara and Ali, 2017)	Security attacks in cloud computing also occur in XML Signature Wrapping attacks, Browser Security, and Lock in.
Cloud computing security threats and attacks with their mitigation techniques	(Belbergui, 2017)	Mitigation techniques need to be made in the cloud computing environment as security against threats and attacks**.**
Cloud computing: overview and risk identification based on classification by type	(Ghahramani et al., 2017)	Identifying the security system in the cloud environment, including: confidentiality, availability and integrity**.**
Toward cloud computing qos architecture: analysis of cloud systems and cloud services	(Gonzales et al., 2017)	Quality of service (QoS) is used to ensure the quality of security services in cloud computing.
Cloud-trust – a security assessment model for infrastructure as a service (iaas) clouds	(Sharma et al., 2018)	Cloud-Trust is a security system used to measure the level of confidentiality and integrity offered by CCS or cloud service providers (CSPs).

(*continued on next page*)

Table 4 (*continued*)

Scope of study	Author	Conclusion
Managing risk in a derivative iaas cloud	(Ramachandra et al., 2017)	On the Infrastructure-as-a-Service (IaaS) cloud platform, it can cause a risk of losing the VM state.
A comprehensive survey on security in cloud computing	(Balco and Law, 2017)	Cloud computing systems can have an impact on threats and security.
Cloud market analysis from customer perspective	(Kumar et al., 2018)	The implementation of cloud computing is very helpful, especially in increasing the accessibility of information in real time, but data security issues become an obstacle.
Exploring data security issues and solutions in cloud computing	(Alsmirat et al., 2017)	Problems that often occur in the cloud computing environment, especially in data security, confidentiality; Integrity; Availability; Authentication and Access Control.
A security framework for cloud-based video surveillance system	(Rizvi et al., 2018)	Data transmission in public networks is often unsafe, especially problems with data security and privacy, and data integrity.
A security evaluation framework for cloud security auditing	(Vijayakumar and Arun, 2019)	Problems for cloud service users are related to file security and data privacy.
Continuous security assessment of cloudbased applications using distributed hashing algorithm in sdlc	(Khan and Ullah, 2016)	Migration to cloud computing poses problems in terms of vulnerability and application security.
A risk assessment framework for cloud computing	(Sharma et al., 2016)	Risk assessment in the cloud computing environment is useful for mitigating threats and minimizing violations.
Challenges in the adoption of hybrid cloud: an exploratory study using systematic literature review	(Kouatli, 2016)	Adoption of the public cloud raises security concerns.
Identity and access management as security-as-a-service from clouds	(Jouini and Ben Arfa Rabai, 2016)	Security-as-a-service is a model for security services in the cloud.
Managing cloud computing environment: gaining customer trust with security and ethical management	(De et al., 2016)	Cloud services provided by CSP need to be reviewed for security, including: data protection and ethics.
Comparative study of information security risk assessment models for cloud computing systems	(Casola et al., 2016)	Security-related risk assessment in a cloud environment.
Goal based threat modeling for peer-to-peer cloud	(Cayirci et al., 2016)	The peer-to-peer networking model can be a security threat and an opportunity for attacks.
Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability	(O'Loughlin and Gillam, 2016)	Opportunities for confidentiality, integrity, and availability risks to cloud computing.
Security-by-design in clouds: a security-sla driven methodology to build secure cloud applications	(Kholidy et al., 2016)	The security model is designed to build security in a cloud computing environment.
A risk assessment model for selecting cloud service providers	(Opara-martins et al., 2016)	The risk profile that often appears in CSP is related to security and privacy.
Sibling virtual machine co-location confirmation and avoidance tactics for public infrastructure clouds	(Masky et al., 2015)	Services in the public cloud are exposed to security threats because of the use of servers together.
A risk mitigation approach for autonomous cloud intrusion response system	(Arabo, 2015)	Security becomes a parameter in risk assessment in the cloud computing environment.
Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective	(Suzic et al., 2015)	The problem that occurs when migrating to cloud computing is vendor lock-in
A novel risk identification framework for cloud computing security	(Kritikos et al., 2015)	To control security in cloud computing, the risk and security factors must first be identified.
Cyber security challenges within the connected home ecosystem futures	(Shaikh and Sasikumar, 2015)	Many security threat problems occur in cyber systems.
Secure data sharing and processing in heterogeneous clouds	(Alqahtany et al., 2016)	The use of multiple cloud services can pose a security threat to its users.
Security enforcement for multi-cloud platforms - the case of paasage	(Molyakov et al., 2015)	The obstacles that occur in multi cloud platforms are data security and virtual machines.
Trust model for measuring security strength of cloud computing service	(Nagaraju and Parthiban, 2015)	The adoption of cloud computing will experience obstacles in terms of data security.
A forensic acquisition and analysis system for iaas	(Singh and Chatterjee, 2016)	The problem in adopting cloud computing is choosing the right CSP.
Model of hidden it security threats in the cloud computing environment	(Lemmens et al., 2006)	Security threats are opportunities for vulnerabilities in cloud computing.
Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway	(Shakeel and Sharma, 2017)	The use of the public cloud raises problems with data security and privacy.

include the authors, the scope and conclusions of the research results are shown in Table 4, and the risk categories based on the risk type and risk component are shown in Table 5.

Table 4 describes the scope of the study, the authors and a summary of the conclusions of each of the articles reviewed. From the results of the review of these articles, it is clear that there is uniformity of research results and this is the key in research with the SLR method. The review results show that currently international organizations are studying national and international regulations related to data security in cloud computing (Maeser, 2020; Zhao et al., 2019; Domingo-Ferrer et al., 2019; Alassafi et al., 2019; Chang et al., 2018), such as the occurrence of data breaches (Juma and Tjahyanto, 2019; Siddiqui et al., 2018; Kumar et al., 2018; Asvija et al., 2019), and Peer-to-peer networking models can threaten security and present an opportunity for attacks (Cayirci et al., 2016). Along with the rapid development of cloud technology, this has an impact on availability, performance, security, and finances (Li et al., 2020; Patil et al., 2020; Ficco et al., 2018; Anjana and Singh, 2018; Bryce, 2018; Amara and Ali, 2017; Masky et al., 2016; Balco and Law, 2017; Arabo, 2015; Efozia et al., 2017; Wu et al., 2019), data confidentiality and integrity (Alsmirat et al., 2017; Rizvi et al., 2018; O'Loughlin and Gillam, 2016; Maniah et al., 2019; Gill and Buyya, 2020). Besides, the use of virtual machines in cloud computing will have an impact on scalability and operational costs (Singh and Mansotra, 2019; Neware, 2018; Mohamadi et al., 2019) and this is a quite high chal-

Table 5
Risk category based on state-of-the-art results.

Risk category	Description	References	Weight
Risk type	Information security risk	(Maeser, 2020; Li et al., 2020; Gill and Buyya, 2020; Tabrizchi and Rafsanjani, 2020; Modi and Acha, 2016; Abd Al Ghaffar, 2020; Sun, 2019; Weil, 2019; Wu et al., 2019; Xu et al., 2019; Zhao et al., 2019; Asvija et al., 2019; Domingo-Ferrer et al., 2019; Juma and Tjahyanto, 2019; Alassafi et al., 2019; Patil et al., 2020; Chang et al., 2018; Cheng et al., 2018; Guo et al., 2018; Kozlov and Noga, 2018; Ficco et al., 2018; Subramanian and Jeyaraj, 2018; Anjana and Singh, 2018; Hentschel et al., 2018; Alshammari et al., 2017; Amara and Ali, 2017; Belbergui, 2017; Ghahramani et al., 2017; Singh et al., 2016; Gonzales et al., 2017; Sharma et al., 2018; Masky et al., 2016, 2015; Balco and Law, 2017; Kumar et al., 2018; Alsmirat et al., 2017; Ghorbel et al., 2017; Rizvi et al., 2018; Vijayakumar and Arun, 2019; Khan and Ullah, 2016; Kouatli, 2016; Aslanpour et al., 2020; Jouini and Ben Arfa Rabai, 2016; Casola et al., 2016; Cayirci et al., 2016; Kholidy et al., 2016; Opara-martins et al., 2016; Arabo, 2015; Mohamadi et al., 2019; Kritikos et al., 2015; Shaikh and Sasikumar, 2015; Alqahtany et al., 2016; Molyakov et al., 2015; Efozia et al., 2017; Nagaraju and Parthiban, 2015; Lemmens et al., 2006; Shakeel and Sharma, 2017)	25%
	Risk of losing access to data	(Gill and Buyya, 2020; Tabrizchi and Rafsanjani, 2020; Sun, 2019; Weil, 2019; Xu et al., 2019; Asvija et al., 2019; Juma and Tjahyanto, 2019; Cheng et al., 2018; Ficco et al., 2018; Siddiqui et al., 2018; Subramanian and Jeyaraj, 2018; Hentschel et al., 2018; Ghahramani et al., 2017; Alsmirat et al., 2017; Ghorbel et al., 2017; Rizvi et al., 2018; Yahuza et al., 2020; Vijayakumar and Arun, 2019; O'Loughlin and Gillam, 2016; Molyakov et al., 2015; Nagaraju and Parthiban, 2015; Shakeel and Sharma, 2017)	21%
	Financial risk	(Li et al., 2020; Ficco et al., 2018)	7%
	Risk of compliance with various regulations and laws	(Maeser, 2020; Alassafi et al., 2019; Ficco et al., 2018)	11%
	Risk of using virtual machines	(Maenhaut et al., 2019; Singh and Mansotra, 2019; Dong et al., 2019; Neware, 2018; Anjana and Singh, 2018; Ramachandra et al., 2017; Mohamadi et al., 2019; Molyakov et al., 2015)	18%
	Error in choosing CSP	(De et al., 2016; Opara-martins et al., 2016; Suzic et al., 2015; Singh and Chatterjee, 2016)	14%
	Failure management	(Han et al., 2019)	4%
Risk component	Threat	(Modi and Acha, 2016; Hentschel et al., 2018; Masky et al., 2016, 2015; Balco and Law, 2017; Sharma et al., 2016; Cayirci et al., 2016; Alqahtany et al., 2016; Molyakov et al., 2015)	33%
	Vulnerability	(Modi and Acha, 2016; Khan and Ullah, 2016) 27,73,95	13%
	Impact	(Modi and Acha, 2016; Hentschel et al., 2018; Masky et al., 2016, 2015; Balco and Law, 2017; Sharma et al., 2016; Cayirci et al., 2016; Alqahtany et al., 2016)	27%
	Risk factors	(Abrar et al., 2018; Chang et al., 2018; Cheng et al., 2018; Neware, 2018; Alsmirat et al., 2017; Ghorbel et al., 2017; Kritikos et al., 2015)	20%
	Damage	(Lemmens et al., 2006)	7%

lenge (Maenhaut et al., 2019; Dong et al., 2019). 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).

With increasing amounts of data stored on cloud servers, security 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, including: data protection and ethics (De et al., 2016).

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., 2018; Singh et al., 2016; Khan and Ullah, 2016; Shaikh and Sasikumar, 2015; Lemmens et al., 2006; Abd Al Ghaffar, 2020). 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 security due to shared servers (Masky et al., 2015; Shakeel and Sharma, 2017). The use of diversified cloud services can pose a security threat to its users (Alqahtany et al., 2016; Molyakov et al., 2015).

Efforts made in overcoming security risks in the cloud environment 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 risk mitigation 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).

A study says that the challenges in cloud computing are related to the design of cloud systems in the future (Zhang et al., 2018), while factors that must be considered when adopting cloud computing are technological factors followed by environmental factors, and finally organizational factors (Abrar et al., 2018), besides failure factors. management (failure management) must also be minimized (Han et al., 2019).

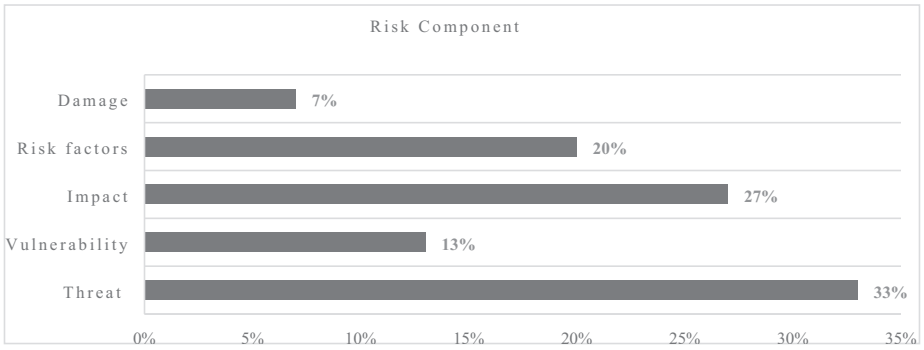

Fig. 4. Trent of risk component.

Table 5 shows the number of articles that review issues of risk types and risk components that often appear in cloud environments. 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 regulations and laws (weight = 3) , risk of using virtual machines (weight = 5), Error in choosing CSP (weight = 4), and Failure management (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 components 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.

Based on Fig. 4, the types of risks that often arise in the cloud migration environment can be explained as follows:

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).
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.
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)
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).
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 understanding the existing regulations or rejection of the regulations that have been established
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).
7) **Failure management** is a risk that occurs in the cloud environment 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 independent failures (Han et al., 2019).

Next will be explained related to risk components that often arise in the cloud migration environment as follows:

1) **Threat** are all things that will bring loss to the company's assets stored in the cloud that will pose a risk (Sun, 2020).
2) **Impact** : the amount of the loss against assets based on their value (Chang et al., 2018).
3) **Risk factor** are factors that have the opportunity to influence the process of cloud computing adoption, such as environmental, organizational and technology factors (Abrar et al., 2018).
4) **Vulnerability** is a defect or weakness in system security procedures that is done intentionally or unintentionally, resulting in a system security policy violation (Chang et al., 2018).
5) **Damage** are the values of damage due to the threat (Ficco et al., 2018). The amount of this damage can have an effect on financial risk.

5. Future cloud challenges

The most recent issue related to Cloud Computing is Fog Computing. Fog is a useful tool for handling massive amounts of data and acting as a bridge between the cloud and IoT, whereas Fog Computing is an emerging trend in the Cloud domain that offers a platform for various applications and services running in real-time [102]. With Fog Computing, several application components can be executed in the Platform as-a-Service (PaaS) cloud service and interact with other components hosted and executed in fog, so that their access will be closer to the end user, such as wireless sensors [103]. 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.

The prospect of developing cloud computing technology is very broad, for example the use of the Internet of Things (IoT) which relies on cloud computing technology in sending it to data centers for processing (Li et al., 2020); [104]. Along with the rapid development of cloud computing technology, we must be faced with big

Table 6
Comparison of Cloud Computing and Fog Computing Characteristics [102]

Characteristics	Cloud computing	Fog computing
Security	Undefined	Can Be Defined
Attacks and Vulnerabilities	High probability	Low probability

challenges as well, network infrastructure security problems are still the main key to cloud computing security risks, for example the use of firewalls [105], and many researchers still focus on the issue of adoption. to cloud computing due to its security issues (Buettner and Buettner, 2016).

6. Conclusion

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.

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, environmental factors and organizational factors. Choosing the right cloud service provider is also an important thing to pay attention to before migrating to the cloud.

To ensure security on cloud migration, it is a shared responsibility for related parties, for example government, private organizations, 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 reason, it is necessary for similar studies to be developed continuously in the future.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abd Al Ghaffar, H.-t-A.N., 2020. Government cloud computing and national security. REPS ahead-of-print (ahead-of-print). https://doi.org/10.1108/REPS-09-2019-0125.

Abrar, H., Hussain, S.J., Chaudhry, J., Saleem, K., Orgun, M.A., Al-Muhtadi, J., Valli, C., 2018. Risk analysis of cloud sourcing in healthcare and public health industry. IEEE Access 6, 19140–19150.

M. O. Alassafi, H. F. Atlam, and A. A. Alshdadi, "A validation of security determinants model for cloud adoption in Saudi organisations ' context," Int. J. Inf. Technol., 2019, doi: 10.1007/s41870-019-00360-4.

Alqahtany, S., Clarke, N., Furnell, S., Reich, C., 2016. A forensic acquisition and analysis system for IaaS. Cluster Comput. 19 (1), 439–453.

Al-Ruithe, M., Benkhelifa, E., Hameed, K., 2019. A systematic literature review of data governance and cloud data governance. Pers. Ubiquit. Comput. 23 (5-6), 839–859.

A. Alshammari, S. Alhaidari, A. Alharbi, and M. Zohdy, "Security Threats and Challenges in Cloud Computing," Proc. - 4th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2017 3rd IEEE Int. Conf. Scalable Smart Cloud, SSC 2017, pp. 46–51, 2017, doi: 10.1109/CSCloud.2017.59.

Alsmirat, M.A., Obaidat, I., Jararweh, Y., Al-Saleh, M., 2017. A security framework for cloud-based video surveillance system. Multimed. Tools Appl. 76 (21), 22787–22802.

Amara, N., Ali, A., 2017. "Cloud Computing Security Threats and Attacks with their. Mitigation Techniques". https://doi.org/10.1109/CyberC.2017.37.

Amron, M.T., Ibrahim, R., Chuprat, S., 2017. A review on cloud computing acceptance factors. Procedia Comput. Sci. 124, 639–646.

Anjana and A. Singh, Security concerns and countermeasures in cloud computing : a qualitative analysis Int. J. Inf. Technol. 2018 10.1007/s41870-018-0108-1

Arabo, A., 2015. Cyber security challenges within the connected home ecosystem futures. Procedia Comput. Sci. 61, 227–232.

Aslanpour, M.S., Gill, S.S., Toosi, A.N., 2020. Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. Int. Things 12, 100273. https://doi.org/10.1016/j.iot.2020.100273.

Asvija, B., Eswari, R., Bijoy, M.B., 2019. Security in hardware assisted virtualization for cloud computing – State of the art issues and challenges. Comput. Netw. 151, 68–92.

Balco, P., Law, J., 2017. Cloud market market analysis analysis from customer perspective. Procedia Comput. Sci. 109, 1022–1027. https://doi.org/10.1016/j.procs.2017.05.375.

Belbergui, C., 2017. Cloud computing: Overview and risk identification based on classification by Type. Int. Conf.

C. Bryce, "Security Governance as a Service on the Cloud," pp. 30–35, 2018, doi: 10.1109/UCC-Companion.2018.00030.

H. B. Bt Yusof Ali, L. M. Bt Abdullah, M. Kartiwi, and A. Nordin, Risk assessment for big data in cloud: Security, privacy and trust ACM Int. Conf. Proceeding Ser. 2018 63 67 10.1145/3299819.3299841

Buettner, R., Buettner, K., 2016. A systematic literature review of twitter research from a socio-political revolution perspective. Proc. Annu. Hawaii Int. Conf. Syst. Sci. vol. 2016-March, 2206–2215. https://doi.org/10.1109/HICSS.2016.277.

Casola, V., De Benedictis, A., Rak, M., Rios, E., 2016. Security-by-design in clouds: A Security-SLA driven methodology to build secure cloud applications. Procedia – Procedia Comput. Sci. 97, 53–62. https://doi.org/10.1016/j.procs.2016.08.280.

Cayirci, E., Garaga, A., Santana de Oliveira, A., Roudier, Y., 2016. A risk assessment model for selecting cloud service providers. J Cloud Comp 5 (1). https://doi.org/10.1186/s13677-016-0064-x.

Chang, C.-C., Li, C.-T., Shi, Y.-Q., 2018. Privacy-aware reversible watermarking in cloud computing environments. IEEE Access 6, 70720–70733.

Cheng, H., Rong, C., Qian, M., Wang, W., 2018. Accountable privacy-preserving mechanism for cloud computing based on identity-based encryption. IEEE Access 6 (4), 37869–37882. https://doi.org/10.1109/ACCESS.2018.2851599.

De, S., Barik, M.S., Banerjee, I., 2016. Goal based threat modeling for peer-to-peer cloud. Procedia Comput. Sci. 89, 64–72.

Djemame, K., Armstrong, D.J., Kiran, M., 2011. A risk assessment framework and software toolkit for cloud service ecosystems. Computing no. c, 119–126.

Djemame, K., Armstrong, D., Guitart, J., Macias, M., 2016. A risk assessment framework for cloud computing. IEEE Trans. Cloud Comput. 4 (3), 265–278.

Domingo-Ferrer, J., Farràs, O., Ribes-González, J., Sánchez, D., 2019. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Comput. Commun. 140–141 (March), 38–60. https://doi.org/10.1016/j.comcom.2019.04.011.

Dong, S., Abbas, K., Jain, R., 2019. A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. IEEE Access 7, 80813–80828.

N. F. Efozia, E. Ariwa, D. C. Asogwa, O. Awonusi, and S. O. Anigbogu, "A Review of Threats and Vulnerabilities to Cloud Computing Existence," 2017.

Ficco, M., Pietrantuono, R., Russo, S., 2018. Hybrid simulation and test of vessel traffic systems on the cloud. IEEE Access 6, 47273–47287.

Fowley, F., Pahl, C., Jamshidi, P., Fang, D., Liu, X., 2018. A classification and comparison framework for cloud service brokerage architectures. IEEE Trans. Cloud Comput. 6 (2), 358–371.

Ghahramani, M.H., Zhou, M.C., Hon, C.T., 2017. Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services. IEEE/CAA J. Autom. Sinica 4 (1), 6–18.

Ghorbel, A., Ghorbel, M., Jmaiel, M., 2017. Privacy in cloud computing environments: A survey and research challenges. J. Supercomput. https://doi.org/10.1007/s11227-016-1953-y.

Gill, S.S., Buyya, R., 2020. Failure management for reliable cloud computing: A taxonomy, model, and future directions. Comput. Sci. Eng. 22 (3), 52–63.

Gonzales, D., Kaplan, J.M., Saltzman, E., Winkelman, Z., Woods, D., 2017. Cloud-Trust – A Security Assessment Model for Infrastructure as a Service (IaaS) Clouds. IEEE Trans. Cloud Comput. 5 (3), 523–536.

Guo, W., Shao, J., Lu, R., Liu, Y., Ghorbani, A.A., 2018. A privacy-preserving online medical prediagnosis scheme for cloud environment. IEEE Access 6, 48946–48957.

P. Gupta and C. Gupta, "Evaluating the Failures of Data Centers in Cloud Computing," Int. J. Comput. Appl., vol. 108, no. 4, pp. 29–34, 2014.

Han, S., Han, K., Zhang, S., 2019. A data sharing protocol to minimize security and privacy risks of cloud storage in big data Era. IEEE Access 7, 60290–60298.

R. Hentschel, C. Leyh, and A. Petznick, "Current cloud challenges in Germany : the perspective of cloud service providers," 2018.

Höfer, C.N., Karagiannis, G., 2011. Cloud computing services: Taxonomy and comparison. J. Int. Serv. Appl. 2 (2), 81–94.

A. Huth and J. Cebula, "The Basics of Cloud Computing," pp. 1–4, 2011.

U. N. Inuwa, "The Risk and Challenges of f Cloud Computing," J. Eng. Res. Appl. www.ijera.com, vol. 5, no. 4, pp. 2248–962205, 2015, [Online]. Available: http://www.ijera.com/papers/Vol5_issue12/Part - 4/B512040510.pdf.

Iorga, M., Karmel, A., 2012. "Cloud Computing Security Essentials and Architecture".

Jouini, M., Ben Arfa Rabai, L., 2016. Comparative study of information security risk assessment models for cloud computing systems. Procedia Comput. Sci. 83, 1084–1089.

Juma, M.K., Tjahyanto, A., 2019. Challenges of cloud computing adoption model for higher education level in zanzibar (the Case Study of SUZA and ZU). Procedia Comput. Sci. 161, 1046–1054.

Khan, N., Al-Yasiri, A., 2016. Identifying cloud security threats to strengthen cloud computing adoption framework. Procedia Comput. Sci. 94, 485–490.

Khan, S.U., Ullah, N., 2016. Challenges in the adoption of hybrid cloud: an exploratory study using systematic literature review. J. Eng. 2016 (5), 107–118.

Kholidy, H.A., Erradi, A., Abdelwahed, S., Baiardi, F., 2016. A risk mitigation approach for autonomous cloud intrusion response system. Computing 98 (11), 1111–1135.

R. K. L. Ko et al., "TrustCloud: A framework for accountability and trust in cloud computing," Proc. - 2011 IEEE World Congr. Serv. Serv. 2011, pp. 584–588, 2011, doi: 10.1109/SERVICES.2011.91.
I. Kouatli, "Managing Cloud Computing Environment : Gaining Customer Trust with Security and Ethical Management .," Procedia - Procedia Comput. Sci., vol. 91, no. Itqm, pp. 412–421, 2016, doi: 10.1016/j.procs.2016.07.110.
Kozlov, A.D., Noga, N.L., 2018. Risk management for information security of corporate information systems using cloud technology. Elev. Int. Conf. "Manage. large-scale Syst. Dev. MLSD, 1–5.
Kritikos, K., Kirkham, T., Kryza, B., Massonet, P., 2015. Security enforcement for multi-cloud platforms – The case of paaSage. Procedia Comput. Sci. 68, 103–115.
Kumar, P.R., Raj, P.H., Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing. Procedia Comput. Sci. 125 (2009), 691–697. https://doi.org/10.1016/j.procs.2017.12.089.
Leff, A., Rayfield, J.T., 2015. Integrator : An Architecture for an Integrated Cloud/On-Premise Data-Service. Int. Conf. Web Serv., 98–104 https://doi.org/10.1109/ICWS.2015.23.
Lemmens, J.S., Bushman, B.J., Konijn, E.A., 2006. The appeal of violent video games to lower educated aggressive adolescent boys from two countries. Cyber Psychol. Behav. 9 (5), 638–641.
Li, H., Liu, L., Lan, C., Wang, C., Guo, H., 2020. Lattice-based privacy-preserving and forward-secure cloud storage public auditing scheme. IEEE Access 8, 86797–86809.
P. Maenhaut, B. Volckaert, V. Ongenae, and F. De Turck, Resource Management in a Containerized Cloud : Status and Challenges, no. 0123456789. Springer US, 2019.
Maeser, R., 2020. Analyzing CSP trustworthiness and predicting cloud service performance. IEEE Open J. Comput. Soc. 1, 73–85.
Maniah, Abdurachman, E., Gaol, F.L., Soewito, B., 2019. Survey on threats and risks in the cloud computing environment. Procedia Comput. Sci. 161, 1325–1332.
M. Masky, S. S. Young, and T.-Y. Choe, "A novel Risk Identification Framework for Cloud Computing Security," pp. 0–3, 2015.
Masky, M., Young, S.S., Choe, T.Y., 2016. "A novel risk identification framework for cloud computing security", *2015 IEEE 2nd Int*. Conf. Inform. Sci. Secur. ICISS 2015. https://doi.org/10.1109/ICISSEC.2015.7370967.
Modi, C.N., Acha, K., 2016. Virtualization layer security challenges and intrusion detection / prevention systems in cloud computing: A comprehensive review. J. Supercomput. https://doi.org/10.1007/s11227-016-1805-9.
Mohamadi, R., Abadi, B., Masoud, A., Alizadeh, R.S.H., 2019. Challenges of server consolidation in virtualized data centers and open research issues : a systematic literature review, no. 0123456789. Springer, US.
Molyakov, A.S., Zaborovsky, V.S., Lukashin, A.A., 2015. Model of hidden IT security threats in the cloud computing environment. Aut. Control Comp. Sci. 49 (8), 741–744.
Nagaraju, S., Parthiban, L., 2015. Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. J. Cloud. Comp. 4 (1). https://doi.org/10.1186/s13677-015-0046-4.
R. Neware, "Cloud Computing Digital Forensic challenges," 2018 Second Int. Conf. Electron. Commun. Aerosp. Technol., no. Iceca, pp. 1090–1092, 2018.
O'Loughlin, J., Gillam, L., 2016. Sibling virtual machine co-location confirmation and avoidance tactics for Public Infrastructure Clouds. J. Supercomput. 72 (3), 961–984.
Opara-martins, J., Sahandi, R., Tian, F., 2016. Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. J. Cloud Comput. Adv. Syst. Appl. https://doi.org/10.1186/s13677-016-0054-z.
Paquette, S., Jaeger, P.T., Wilson, S.C., 2010. Identifying the security risks associated with governmental use of cloud computing. Govern. Inform. Quarter. 27 (3), 245–253.
Patil, R., Dudeja, H., Modi, C., 2020. Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. Int. J. Inf. Secur. 19 (2), 147–162.
P. K. Rajendran, B. Muthukumar, and G. Nagarajan, "Hybrid Intrusion Detection System for Private Cloud : A Systematic Approach," Procedia - Procedia Comput. Sci., vol. 48, no. Iccc, pp. 325–329, 2015, doi: 10.1016/j.procs.2015.04.189.
Ramachandra, G., Iftikhar, M., Khan, F.A., 2017. A Comprehensive Survey on Security in Cloud Computing. Procedia Comput. Sci. 110 (2012), 465–472. https://doi.org/10.1016/j.procs.2017.06.124.
A. Rashid Dar and D. Ravindran, "Fog Computing: An Extended Version of Cloud Computing," Int. J. Mod. Electron. Commun. Eng., vol. 7, no. January, pp. 40–45, 2019, [Online]. Available: www.ijmece.org.
Ren, K., Wang, C., Wang, Q., 2012. Security challenges for the public cloud. IEEE Internet Comput. 16 (1), 69–73.
Rizvi, S., Ryoo, J., Kissell, J., Aiken, W., Liu, Y., 2018. A security evaluation framework for cloud security auditing. J Supercomput 74 (11), 5774–5796.
Shaikh, R., Sasikumar, M., 2015. Trust model for measuring security strength of cloud computing service. Procedia Comput. Sci. 45, 380–389.
F. Shakeel and S. Sharma, "Green Cloud Computing : A review on Efficiency of Data Centres and Virtualization of Servers," pp. 1264–1267, 2017.
Sharma, D.H., Dhote, C.A., Potey, M.M., 2016. Identity and access management as security-as-a-Service from clouds. Procedia Comput. Sci. 79, 170–174.
Sharma, P., Lee, S., Guo, T., Irwin, D., Shenoy, P., 2018. Managing Risk in a Derivative IaaS Cloud. IEEE Trans. Parallel Distrib. Syst. 29 (8), 1750–1765.
Siddiqui, Z., Tayan, O., Khurram Khan, M., 2018. Security analysis of smartphone and cloud computing authentication frameworks and protocols. IEEE Access 6, 34527–34542.
Singh, A., Chatterjee, K., 2016. Cloud security issues and challenges: A survey. J. Netw. Comput. Appl. https://doi.org/10.1016/j.jnca.2016.11.027.
Singh, S., Jeong, Y., Hyuk, J., 2016. A survey on cloud computing security: Issues, threats, and solutions. J. Netw. Comput. Appl. https://doi.org/10.1016/j.jnca.2016.09.002.
Singh, J., Mansotra, V., 2019. Factors affecting cloud computing adoption in the Indian school education system. Educ. Inf. Technol. 24 (4), 2453–2475.
Subramanian, N., Jeyaraj, A., 2018. Recent security challenges in cloud computing. Comput. Electr. Eng. 71, 28–42.
Sun, P.J., 2019. Privacy protection and data security in cloud computing: A survey, challenges, and solutions. IEEE Access 7, 147420–147452.
Sun, P.J., 2020. Security and privacy protection in cloud computing: Discussions and challenges. J. Network Comput. Appl. 160, 102642. https://doi.org/10.1016/j.jnca.2020.102642.
Suzic, B., Reiter, A., Reimair, F., Venturi, D., Kubo, B., 2015. Secure data sharing and processing in heterogeneous clouds. Procedia - Procedia Comput. Sci. 68 (316), 116–126. https://doi.org/10.1016/j.procs.2015.09.228.
T.K, S., B, D., 2016. Security attack issues and mitigation techniques in cloud computing environments. IJU 7 (1), 1–11.
Tabrizchi, H., Rafsanjani, M.K., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions, no. 0123456789. Springer, US.
Taherkordi, A., Zahid, F., Verginadis, Y., Horn, G., 2018. Future cloud systems design: challenges and research directions. IEEE Access 6, 74120–74150.
Tchernykh, A., Schwiegelsohn, U., Talbi, E.-G., Babenko, M., 2019. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. J. Comput. Sci. 36, 100581. https://doi.org/10.1016/j.jocs.2016.11.011.
Vijayakumar, K., Arun, C., 2019. Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC. Cluster Comput 22 (S5), 10789–10800.
Wang, X., 2011. Analysis on cloud computing-based logistics information network mode. Seventh Int. Conf. Comput. Intell. Secur. Anal., 1286–1289 https://doi.org/10.1109/CIS.2011.285.
Weil, T., 2019. Risk assessment methods for cloud computing platforms. Comput. Softw. Appl. Conf. https://doi.org/10.1109/COMPSAC.2019.00083.
Wu, Y., Lyu, Y., Shi, Y., 2019. Cloud storage security assessment through equilibrium analysis. Tinshhua Sci. Technol. 24 (6), 738–749.
Xu, J., Liang, C., Jain, H.K., Gu, D., 2019. Openness and security in cloud computing services: Assessment methods and investment strategies analysis. IEEE Access 7, 29038–29050.
Yahuza, M., Idris, M.Y.I.B., Wahab, A.W.B.A., Ho, A.T.S., Khan, S., Musa, S.N.B., Taha, A. Z.B., 2020. Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities. IEEE Access 8, 76541–76567.
Yangui, S. et al., 2016,. "A platform as-a-service for hybrid cloud/fog environments". IEEE Work. Local Metrop. Area Networks 2016. https://doi.org/10.1109/LANMAN.2016.7548853.
Zhang, H., Yu, J., Tian, C., Zhao, P., Xu, G., Lin, J., 2018. Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing. IEEE Access 6, 40713–40722.
Zhao, B., Fan, P., Zhao, P., Ni, M., Liu, J., 2019. SIV: A structural integrity verification approach of cloud components with enhanced privacy. Tinshhua Sci. Technol. 24 (5), 557–574.