Security Risk Assessment on Cloud: A Systematic Mapping Study

Giusy Annunziata
gannunziata@unisa.it
University of Salerno
Salerno, Italy

Alexandra Sheykina
asheykina@unisa.it
University of Salerno
Salerno, Italy

Fabio Palomba
fpalomba@unisa.it
University of Salerno
Salerno, Italy

Andrea De Lucia
adelucia@unisa.it
University of Salerno
Salerno, Italy

Gemma Catolino
gcatolino@unisa.it
University of Salerno
Salerno, Italy

Filomena Ferrucci
fferrucci@unisa.it
University of Salerno
Salerno, Italy

ABSTRACT

Cloud computing has become integral to modern organizational operations, offering efficiency and agility. However, security challenges such as data loss and downtime necessitate tailored compliance solutions. Risk assessment is crucial for identifying and mitigating cloud-related threats, yet a standardized approach remains elusive. Our study aims to fill this gap by conducting a systematic mapping study on the prevailing methodologies. Through a meticulous analysis of 21 scholarly papers, we explore various aspects of security risk assessment for the cloud. The results provide valuable insights into delivery models, standards, and validation practices, contributing to a comprehensive understanding of cloud risk assessment.

CCS CONCEPTS

• **Security and privacy → Software security engineering**; • **Software and its engineering → Cloud computing**.

KEYWORDS

Risk assessment, security testing, cloud computing

ACM Reference Format:
Giusy Annunziata, Alexandra Sheykina, Fabio Palomba, Andrea De Lucia, Gemma Catolino, and Filomena Ferrucci. 2024. Security Risk Assessment on Cloud: A Systematic Mapping Study. In *28th International Conference on Evaluation and Assessment in Software Engineering (EASE 2024), June 18–21, 2024, Salerno, Italy*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3661167.3661287

1 INTRODUCTION

Cloud technologies have permeated various sectors, including business, industry, and medicine, offering numerous benefits. These include cost reduction by eliminating the need for expensive equipment and utility costs, quick data recovery in emergencies, extensive and ubiquitous access to computing resources, and secure data storage with controlled access.

EASE 2024, June 18–21, 2024, Salerno, Italy

ACM ISBN 979-8-4007-1701-7/24/06
https://doi.org/10.1145/3661167.3661287

Cloud computing is one of the fastest-growing areas of information technology. More and more projects are moving computing resources from their data centers to cloud storage, entrusting their data to cloud providers. At the end of 2022, the global market for public cloud services reached $478.32 billion, and the industry's largest segment is SaaS solutions (software as a service). This is stated in a Gartner study, the results of which were presented on November 13, 2023 [12]. The global public cloud market continues to grow. Gartner estimates the global public cloud market at $563.59 billion in 2023. This represents a growth of 17.8% compared to the previous year. Gartner predicts that by 2027, more than 70% of enterprises will use industry cloud platforms to accelerate their business operations.

Advanced security features ensure secure data storage and processing. However, despite the use of the latest security standards and industry certifications, there remains the risk of any cybercrime, including theft of valuable information, which can compromise company's operations and damage its brand and reputation.

Recently, several cloud security issues have been encountered. The Cloud Security Alliance Top Cloud Computing Threats 2019 [6] report identified data breaches due to misconfiguration and inadequate change control as the top 2 threats to cloud security. According to Gartner, through 2025, 99% of all cloud security failures will be due to some level of human error. On the other hand, data protection laws, including the EU General Data Protection Regulation, the Health Insurance Portability and Accessibility Act, and the Payment Card Industry Data Security Standard (PCI DSS), mandate safeguarding customer data and impose significant penalties for breaches. Furthermore, 69% of businesses identify data loss or leakage as their primary worry. Consequently, 42% of organizations view legal and regulatory compliance as a significant challenge, necessitating tailored cloud compliance solutions [9].

With the surge in remote work and the widespread adoption of cloud services, security in the cloud has become paramount. There's a rising demand for Secure Access Service Edge (SASE) products. According to Group [15], the SASE market surpassed $6 billion in 2022, marking a growth of approximately 34% compared to 2021. Similarly, the Security Service Edge (SSE) sector within the global cloud security industry saw a monetary increase of about $1 billion (38%) in 2022 compared to the previous year.

Ensuring the security of cloud technologies is not a trivial task. To correctly evaluate security, it is advisable to always consider it within the framework of an integrated approach: both from the point of view of security tests and from the point of view of risk

assessment. Several studies have proposed new approaches, tools, and methods for risk assessment in cloud environments. Secondary studies have been published that explore various aspects of security risk assessment in the cloud, such as threat modeling [7, 10], adoption issues at different delivery models such as IaaS, PaaS, and SaaS [4, 11], and features of the risk assessment model, to bring order to all published studies, and further research [10, 11, 18].

These previous studies, however, focused on specific aspects of the discipline, and have failed to provide a comprehensive overview of the field. As a result, significant research angles like evaluation and validation approach solutions have been left largely unexplored.

In this paper, we conducted a systematic mapping study on the current status of security risk assessment in cloud environment research to fill this gap. Our study is guided by 5 research questions. This systematic mapping study aims to provide a broad and holistic overview of security risk assessment in the cloud, determine its achievements, and identify current research gaps. To increase the reliability and repeatability of our results, we followed existing guidelines when defining our research protocol [17, 23, 24]. We identified 21 relevant primary studies, published between 2010-2023. In particular, our study aims to identify the most investigated topics in cloud security risk assessment, industry standards applied, deployment models studied, and validation and evaluation approaches considered. Additionally, we report demographic information on research and identify open challenges for future research.

The outcomes of our systematic mapping study offer valuable insights into the progress and evolution of cloud-based risk assessment, focusing on the methodologies and frameworks under examination. Our primary objective is to streamline the transfer of knowledge and establish a central repository of information for both researchers and industry professionals, thereby fostering the advancement and expansion of cloud security technologies. In light of our findings, we pinpoint several potential research directions and explore their implications.

The paper is organized as follows: Section 2 delves into the concepts related to risk assessment for the cloud environment and analyzes the related literature. While Sections 3 and 4 outline the research methodology used for our study and present the results obtained, respectively. These findings and limitations of the study are subsequently discussed in Section 5. Section 6 provides final remarks and future research directions.

2 BACKGROUND AND RELATED WORK

This section provides a comprehensive overview of the context and related research pertinent to our study.

2.1 Security testing and Risk assessment for cloud security

With the growing adoption of cloud computing, guaranteeing the security of such systems becomes a paramount task. Security testing plays a vital role in enhancing the overall cybersecurity stance of an organization, fostering the development of a strong and adaptable environment amid the continually evolving threat landscape. Concurrently, risk assessment empowers organizations to take proactive measures in navigating uncertainties and formulating strategic decisions. This proactive approach not only supports long-term success but also serves to mitigate potential adverse consequences. Security risk assessment and security testing contribute to an overall assessment of the security of a system on different levels. Integrating risk assessment and security testing is critical to ensuring the overall security of a system or application. The initial identification of assets such as data, applications, and hardware in need of protection, followed by a risk assessment to identify potential threats, vulnerabilities, and consequences of security incidents, and the definition of security requirements based on the identified risks will be crucial in the selection of security testing methods, such as penetration testing, vulnerability scanning, code reviews, and security architecture reviews. These methods have already been discussed previously in the scientific literature in the field of risk-based security testing of both conventional software[13, 14, 25, 26] and cloud environments[27]. ISO 29119 [2] defines risk-based testing as a general method that uses risk assessment results to guide and improve the testing process. By integrating risk assessment into security testing, organizations can proactively identify and address potential security threats, reducing the likelihood of security incidents and increasing overall system security.

The customer controls different layers of security regardless of the service provider. The American National Standards Institute (NIST) identifies three cloud delivery models (IaaS, SaaS, PaaS) [20–22], each with its data management model. *Infrastructure-as-a-service* (IaaS), when the consumer uses the provider's computing resources (server, network infrastructure, data storage). *Platform-as-a-service* (PaaS), where the provider provides the consumer with access to the software platform. *Software-as-a-service* (SaaS), when the consumer can use the supplier's ready-made application.

Like any security strategy, developing methodologies or frameworks for assessing cloud risks must adhere to established standards. While it is impossible to guarantee the absolute security of information systems, employing an efficient and effective information security risk assessment method can instill confidence. These standards typically incorporate a knowledge foundation on risks, vulnerabilities, and necessary security requirements. The methodological aspects are often rigorous and based on a well-defined process and structure. Commonly, existing risk assessment methods and standards focus on organizing various steps and activities to be carried out [1, 3].

The reference standards in the analyzed articles are both for traditional applications and those specific to the cloud environment. Among the traditional ones, we find ISO/IEC, NIST, and AS/NZS standards. ISO/IEC developed an "Information Security Management System Standards" or "27000 Family of Standards". In particular, as per the **ISO/IEC 27005:2011** standard, risk assessment involves two processes: Risk Analysis and Risk Evaluation. ISO/IEC 27005 standard, titled "Information technology — Security techniques — Information security risk management," specifies a systematic approach to information security risk management and is designed to be adaptable to various organizational contexts. To fully understand ISO/IEC 27005, you can refer to the concepts, models, processes, and terminology described in **ISO/IEC 27001** and **ISO/IEC 27002**. The document regulates information security measures and helps the provider maintain a high level of security of the IT infrastructure—compliance with ISO 27002 standard. The

regulation describes practical rules for information security management. The other standards of the ISO/IEC family referred to in the analyzed literature are ISO/IEC 31000:2009, and ISO/IEC 27017.

Conversely, the **NIST 800-30** guidance introduces a risk assessment methodology comprising nine key steps: system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, recommendations control, and documentation of results.

Recently, NIST developed Federal Information Processing Standards. **FIPS** proposed confidentiality, integrity, availability, authenticity, and accountability as the key information security principles.

The Australian and New Zealand Standards 4360:2004 serve as a guide for risk management applicable to various types of organizations. The risk management process outlined in **AS/NZS 4360** encompasses 3 primary components: risk management workflow, monitoring and review, and communication and consultation.

All of the above standards apply to traditional applications. Specific standards have recently been proposed for conducting risk assessment in the cloud. The **ISO/IEC 27017** standard serves as a comprehensive guide addressing information security concerns specific to cloud computing. It recommends security measures for both stakeholders: the cloud service providers and their customers. Expanding upon the scope of ISO/IEC 27002, this standard customizes its provisions to suit the distinctive requirements of cloud services. ISO/IEC 27017 covers various control measures, including asset ownership, user access management, and duty distribution. Clearly defining roles and responsibilities plays a crucial role in preventing security vulnerabilities and redundancies, rendering it an indispensable tool for effectively managing and mitigating risks associated with cloud computing.

Another standard specific to the cloud environment is **ISO/IEC 17789** (Information Technology - Cloud Computing - Reference Architecture). This standard presents a cloud computing reference architecture, which includes roles in a cloud computing system, activities in a cloud computing system, and functional components of cloud computing and their relationships.

Most widely recognized risk assessment standards presume that an organization independently manages all its assets and enforces all security management processes internally. Some recent works argue that methodologies that only consider asset-specific risk *evaluation approaches* cannot evaluate various risk elements comprehensively. For example, Albakri et al. [A1] presented a security risk assessment framework that allows cloud service providers to assess security risks in a cloud computing environment and cloud customers' contribution to risk assessment. Through cloud clients' evaluation of the security risk factors, the framework can provide a more realistic and accurate risk assessment, reducing the complexity of customer participation in the risk assessment process [1]. Therefore, an adequate risk assessment methodology is needed to determine the specific risks of the *asset* and *stakeholders* so that they can be controlled [A1, A2].

2.2 Related Work

To grasp the full potential of this field and optimize the advantages derived from existing evidence, it is crucial to undertake a thorough synthesis of the most recent research. Several publications have been made regarding security risk assessment in cloud computing.

Latif et al. [18] reviewed numerous studies that examine risk assessment methodologies in the context of the cloud computing domain. They elaborated on the risk factors of cloud users/business organization cloud environment and mapped them as the actual needs of cloud users/business organization.

In 2015, Aich and Sen [4] described different security issues in three types of services such as IaaS, PaaS, and SaaS, of cloud computing and the possible solutions for remediation.

Amini and Jamil [7] argue that developing risk assessments for cloud computing in complex environments requires comprehensive quantitative and qualitative measures. They examined various risk assessment models, analyzing their strengths and weaknesses. After reviewing the characteristics of cloud computing and the main features of the risk assessment model, the authors proposed a risk classification. They obtained a common baseline to develop a new risk assessment model suitable for cloud computing. In their opinion, most risk factors and indicators will depend on the judgment of decision-makers or experts.

Deshpande et al. [10] reported a review in the field of cloud computing with a focus on security risk assessment and service assurance, doing general thoughts on the risk factors in security and service assurance in a cloud environment [10].

Deshpande et al. [11] conducted a study on cloud computing. They addressed different types of attacks, possible threats to this emerging technology, and existing protection methods and solutions for such attacks. Attacks and threats are analyzed using the cloud service provider model (SaaS, PaaS, and IaaS)[11].

» Our contribution

These previous studies, however, focused on specific aspects of the discipline and failed to provide a complete overview of the field, neglecting some aspects that could be relevant for the correct evaluation of the methodology proposed as evaluation and validation. We tried to fill this gap and proposed a comprehensive mapping study. In particular, our work analyzed delivery models, evaluation and validation approaches, and industry standards applied in security risk assessment for cloud environments.

3 RESEARCH METHOD

The *goal* of our study was to create a comprehensive view of the scientific literature related to risk assessment for cloud computing; our *purpose* is to have a general overview of how, nowadays, risk assessment is applied in the context of cloud computing. The *perspective* is of both researchers and practitioners. The former are interested in having a single source of information that offers a comprehensive view of current research on risk assessment on cloud. They are interested in identifying and correctly evaluating risks in cloud services by applying solutions proposed by researchers.

To satisfy these objectives we want to comprehensively explore the existing literature though a Systematic Mapping Study. It has been conducted following the guidelines in [17, 23, 24]. In

terms of reporting, we followed the *ACM/SIGSOFT Empirical Standards*—documents that seek to express specific expectations for one or more types of research and determine its quality.[1]

3.1 Research Questions

To obtain a comprehensive view of the state of the art of cloud risk assessment and identify possible research gaps, we have defined some research questions:

RQ1 *What Risk Assessment Standards are applied in Cloud?*

Our first research question aims to provide an overview of the most commonly applied frameworks for conducting risk assessment in cloud environments, reflecting the diverse international efforts to ensure the implementation of effective security controls and risk management practices tailored specifically for cloud computing.

RQ2 *Which Cloud service delivery models for risk assessment are considered?*

The second research question analyzes the different cloud service delivery models for risk assessment such as Infrastucture. By gaining insights into this aspect, organizations can make informed decisions regarding selecting and implementing risk assessment processes in cloud environments. Ultimately, this understanding enhances the effectiveness and efficiency of risk management practices, ensuring better alignment with organizational goals and requirements in cloud-based operations.

RQ3 *What types of validation are applied on the Risk Assessment in Cloud?*

The third research question focuses on investigating the types of validation applied to risk assessment in the cloud. By analyzing these types of validation, organizations can improve the effectiveness, reliability, and compliance of their risk management practices, thereby strengthening their ability to mitigate risks and safeguard cloud-based operations.

RQ4 *What types of evaluation approach are applied to conduct Risk Assessment in Cloud?*

The fourth research question aims to investigate the assessment approaches applied to conduct risk assessment in the cloud by identifying which specific types of risks the literature focuses on. By analyzing these approaches, it is possible to obtain information that will then be useful for organizations to improve the relevance, effectiveness, and alignment of their risk management practices with cloud implementation goals and stakeholder expectations.

RQ5 *What are the limitations of the actual application of Risk Assessment in Cloud?*

The final research question aims to identify the limitations of current risk assessment applications in the cloud. Examining the weaknesses of existing processes provides valuable insights for future researchers to explore innovative solutions and advancements in these areas. Additionally, uncovering these limitations is essential for organizations, as they can pinpoint specific aspects requiring attention and understand how to effectively address gaps in their risk assessment practices.

3.2 Search, Inclusion and Exclusion Criteria

We followed the guidelines in [17, 23, 24] to formulate our search string. Our string consists of two parts. The first term includes keywords *"cloud"* that way we are sure not to exclude anything relevant and not limit ourselves only to combinations of cloud system or cloud service, etc. The second group considers processes to ensure cloud security, such as "risk assessment", "security risk evaluation", and related abbreviations and synonymous combined. Keywords in the same group serve as alternatives (using the OR operator), but a pertinent paper must encompass all features from each group. The groups are linked by the boolean AND operator. The search string was modified to conform to the syntax of the relevant search engines [17]. Evaluators searched the articles' metadata, specifically examining the title, abstract, and keyword list.

Search String

("cloud" AND ("security risk assessment" OR "risk assessment of security" OR "security vulnerability evaluation" OR "security threat analysis" OR "security vulnerability assessment" OR "security risk evaluation" OR "security threat assessment")

We selected Scopus[2] as the database to search for articles related to our work because it is a large database of abstracts and citations containing papers published in peer-reviewed venues by multiple publishers (e.g., Elsevier, IEEE, ACM, Springer, Wiley). By using Scopus, we ensure access to a diverse range of scientific literature, which enables us to conduct a thorough and comprehensive search of articles while improving the robustness and completeness of our research findings.

We executed the query on the selected database on *22 February 2024*, applying Scopus filters to search on abstract, title, and keyword. We retrieved a total of 171 papers. Subsequently, we applied a set of predefined inclusion and exclusion criteria, detailed in Table 1, to refine the initial pool of articles and ensure that only relevant studies were included in our analysis.

Table 1: Selection criteria applied in the study selection phase.

Exclusion Criteria	Inclusion Criteria
Article not in English	Published in peer-reviewed journals or conference proceedings
Short Paper	Subject areas are computer science and engineering
Magazine	Articles on cloud risk assessment
Book	
Secondary study on the matter	
Conference Papers which have an extension in journal	
Papers whose full-text read was not available	

[1]The *ACM/SIGSOFT Empirical Standards*: https://github.com/acmsigsoft/EmpiricalStandards

[2]Scopus:https://www.scopus.com

3.3 Quality Assessment

Petersen et al. [24] suggest performing a quality assessment but advise against setting excessively stringent criteria to avoid excluding potentially relevant resources in the context of a systematic mapping study. Therefore, we have devised the following quality assessment strategy, which involves a checklist featuring the following questions:

🔍 ***Q_1*** *Is the motivation of the paper clearly and explicitly reported?*

🔍 ***Q_2*** *Is the cloud risk assessment issue clearly defined?*

🔍 ***Q_3*** *Is the primary result of the paper clearly and explicitly articulated?*

Each question above is assigned a score: 1 if the answer is Yes and explicitly reported, 0.5 if the answer is Yes but not explicitly reported, and 0 if the answer is Not reported. The scores for all three questions are then added together. A primary study that achieves a minimum score of 1.5 is considered acceptable. All the details are reported in the online appendix [8].

3.4 Data Extraction

Starting from the conjectured research questions, we obtained an initial set of information that we intend to collect in the data extraction phase. From an initial reading of the papers, we extracted through an induction approach the information related to the research questions, and then we extracted additional data helpful in understanding the analyzed papers; this information was entered into an Excel form, available in the online appendix [8], and described in Table 2.

Specifically, Table 2 presents data related to each research question, in particular the item extracted (first column), its description (second column), the possible values it can assume (third column), and the research question, if there is a correspondence (fourth column). Some data entries are chosen from a predefined set, while others allow for open-ended responses, and we denote values for closed questions in italics. In addition to gathering fundamental details about risk assessment for cloud delivery models or the employed standards, our focus also encompasses the extraction of data concerning threat or vulnerability modeling and the objectives of the study. This supplementary information enhances our understanding of the characteristics of the scrutinized articles. Moreover, the data extraction form incorporates a "Limitations" field, where we have documented potential constraints of the evaluated methods, aiming to identify challenges and issues.

3.5 Study Selection Process

The entire process unfolded through multiple iterations. The initial iteration served as a pilot, in which we used selection criteria and the definition of the search query to search for articles in the database. Employing a think-aloud protocol, each rater articulated their inclusion and exclusion criteria thought process, following the approach suggested by [5].

By running a query string on the selected scientific database, we found 171 articles for Scopus. We uploaded all collected articles into a local database. The selection of studies began with a meeting in which the evaluators reviewed the selection criteria [24]. At this point the evaluators continued to apply the advanced inclusion and exclusion criteria defined in 3.2. Specifically, two reviewers (author of the work) screened the articles, applying criteria only to the title, abstract and keywords. After that, we continued to carefully read the remaining studies and again applied the exclusion and inclusion criteria to the body of the article. The final step of the selection phase was to evaluate the quality of the extracted resources to limit the risk of bias and erroneous results [17, 23, 24]. Implementation of this quality assessment protocol resulted in the exclusion of one article. In summary, using the entire procedure resulted in the acceptance of 21 primary studies.

After completing the selection process, we continued the data extraction phase. The evaluators read and analyzed the relevant studies in detail in the data extraction phase. During this phase, the first and second authors acted as evaluators and extracted the data necessary to answer the questions of the selected relevant studies. In this phase we used the data extraction module, defined in section 3.4. We also conducted a post-extraction meeting [24], where ambiguous responses were clarified.

Moreover, to identify more information about the delivery models and evaluation approach (RQ_2 and RQ_4), we conducted an iteration of content analysis session [19]. This methodology consisted of reading into the articles references related to the delivery model used and the evaluation approaches applied, with the goal of assigning a label describing them.

The final goal was to obtain clusters in which to go and categorize the papers read in accordance with the delivery models and evaluation approaches. First, the examiners analyzed an initial set of 21 articles. Each examiner extracted information that allowed to associate a label to each article, through an inductive process. Then, in a meeting, the examiners discussed the labels made up to that point and tried to reach a consensus on the categories assigned.

The result of this phase was a clusterization of the papers according to the labels containing the categories extracted from the papers for delivery models and evaluation approaches. All the information about the used labels are reported in the excel module in the online appendix [8]. The process outlined for conducting the mapping study is visually depicted in the Figure 1.

4 ANALYSIS OF THE RESULTS

The section presents an overview of the distribution of accepted papers and the corresponding insights aligned with our RQs.

4.1 Demographic Analysis

Before presenting the results in our study, we reported some meta-information on the primary studies accepted in our mapping study.

Figure 2 shows the distribution of the number of published articles over the years, which reveals some fluctuations. Specifically, there was a slight increase in publications during 2017 and 2018, indicative of heightened activity and interest in the field. However, this trend experienced a downturn in 2019, followed by a significant peak in 2020, marked by the publication of five papers, suggesting a period of intensive research and exploration within the domain [A8, A12, A16, A18, A20]. Subsequently, there was a

Table 2: Extraction form

Data Item	Description	Values	RQ
Standard	What standards have been applied in developing the framework or methodology?	ISO/IEC, NIST, CSA ecc.	RQ_1
Delivery Model	For which type of cloud delivery model was the risk assessment performed?	*IaaS, SaaS, PaaS*	RQ_2
Validation Analysis	What kind of analysis were used to validate the model (if any)?	*Qualitative, quantitative*	RQ_3
Evaluation Approach	What type of evaluation approach is applied?	*Assets Specific Risk, Stakeholders Specific Risk*	RQ_4
Limitations	What are the limitations of current studies?	Textual description of the addressed problems	RQ_5
Framework/Tool	Is a framework or tool for Risk assessment introduced or used?	Description of the framework or tool used	
Threat/Vulnerability modeling	What kind of vulnerabilities or threats are analyzed?	Description of Vulnerability of Threat or source from which they are extracted	
Case Study	Does the work propose a case study?	*Yes, No*	

Figure 1: Overview of the Research Process

gradual decline in the number of publications. By 2023, the number of publications in the realm of risk assessment for cloud computing dwindled to a solitary paper. This trajectory highlights the dynamic nature of research trends and the evolving focus within the field, underscoring the importance of monitoring and understanding fluctuations in scholarly output over time.

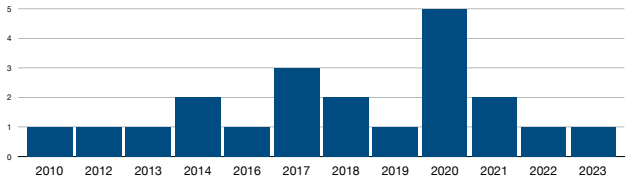

Figure 2: Trend of publications by year.

The Table 3 delineates the distribution of pertinent articles categorized by publisher. A discernible variance among publishers becomes apparent, with each displaying varying levels of engagement with the topic of risk assessment within cloud systems. Notably, the publisher demonstrating the most pronounced interest in addressing this subject matter is the "*Institute of Electrical and Electronics Engineers Inc. (**IEEE**)*". Their substantial contribution underscores a deep-seated engagement with the complexities surrounding risk assessment in cloud environments, with 6 published papers in this field [A14–A16, A20]. Notably, the community demonstrating the most pronounced interest in addressing this subject matter is the "*Institute of Electrical and Electronics Engineers Inc.*" Their substantial contribution underscores a deep-seated engagement with the complexities surrounding risk assessment in cloud environments, with 6 publisher papers in this field [A6, A7, A14–A16, A20].

Subsequently, with a slightly lesser degree of emphasis on the topic there are "*Elsevier Ltd*," "*Springer Verlag*," and "*John Wiley and Sons Ltd*." Nonetheless, their volume of publications underscores a sincere engagement with the nuances and challenges associated with risk assessment within cloud systems.

This nuanced distribution sheds light on the diverse scholarly landscape surrounding risk assessment in cloud computing, illustrating the varying degrees of attention and dedication among different publishing entities toward advancing knowledge and understanding in this critical area.

Table 3: Trend of publications by Publisher.

Publisher	Number of Paper
Budapest Tech Polytechnical Institution	1
Elsevier Ltd	2
Emerald Group Holdings Ltd.	1
Institute of Electrical and Electronics Engineers Inc.	6
John Wiley and Sons Ltd	2
Springer	3
Bentham Science Publishers B.V.	1
World Scientific	1
SciTePress	1

4.2 RQ_1 What Risk Assessment Standard are applied in Cloud?

The results obtained show that most of the items, 43%, use standards developed by NIST [A1, A2, A8, A10, A13, A15–A17, A20], such as FIPS and NIST SP 800-30. 38% apply different standards from the ISO/IEC family [A1, A2, A4, A10, A13, A13, A16], such as ISO/IEC 17789, ISO/IEC 27017, ISO/IEC 27000-27005, and ISO/IEC 31000. Only 2 articles refer to the specific standard for security risk assessment for cloud environments, such as ISO/IEC 17789 and ISO/IEC 27017 [A6]. Other standards applied are IEC-62443 [A8], GB/T 20984-2007[A19], AS/NZS 4360 [A1], and OWASP [A21]. As we can see from Table 4, some studies refer to more than one industry standard. Some work did not reference industry standards [A5, A7, A9, A12, A18]. Certificates do not guarantee security but confirm the functionality of risk management systems related to information security. Therefore, the choice of cloud risk assessment standard should be tailored to the organization's specific objectives,

which meets different needs and emphasizes various aspects of risk management.

Organizations operating in specific industries may be subject to regulations that require the use of certain standards. For example, an organization focused on general information security may consider ISO/IEC 27001 a comprehensive choice, while a financial institution may prioritize standards that ensure the security of financial transactions, such as the PCI DSS. Within this framework, international standards such as ISO/IEC 27001 provide a globally recognized framework, while some countries may have their own standards or regulations that must be followed. In the era of GDPR, the sensitivity of data processed in the cloud is a critical factor. Standards such as ISO/IEC 27001 and PCI DSS provide specific controls for managing different types of sensitive information. Some standards may be more applicable or provide specific guidance for certain service models, such as IaaS, PaaS, or IaaS. Choosing a standard that matches the level of security and risk tolerance desired by the organization. Some standards may require a greater investment of time, expertise or financial resources. Thus, the organization must select a standard it can implement and support.

Ultimately, the goal is to select a risk assessment standard that provides a solid foundation for cloud risk management while meeting your organization's specific needs and priorities.

4.3 RQ_2 Which Cloud service delivery models for risk assessment are considered?

Understanding the service delivery models adopted for Risk Assessment in the cloud is crucial for comprehending the diverse approaches and methodologies utilized in cloud security research. By analyzing a comprehensive set of papers, we aimed to gain insights into prevalent practices and trends regarding the utilization of *Infrastructure-as-a-Service* (IaaS), *Software-as-a-Service* (SaaS), and *Platform-as-a-Service* (PaaS) for conducting Risk Assessment in cloud environments. Our iterative content analysis revealed that a significant majority, 62% of the examined papers, explicitly specify the service delivery model employed for Risk Assessment in the cloud. Among the examined papers, it was found that 17% of them utilize all three service delivery models (IaaS, SaaS, and PaaS) for Risk Assessment in the cloud. Additionally, 8% of the papers exclusively employ a combination of IaaS and SaaS delivery models for their assessments [A2]. Upon examination of the remaining papers, we discovered that 39% of them exclusively utilize the SaaS delivery model for conducting Risk Assessment in the cloud [A1, A3, A14, A15, A21]. Similarly, an equal percentage, 39%, rely solely on the IaaS model [A5, A7, A10, A16, A20]. Notably, none of the analyzed papers utilize the PaaS model independently and unrelated to the other two services. All results are summarized in the Table 4. This finding underscores researchers' diverse preferences and approaches when selecting service delivery models for cloud-based Risk Assessment. While SaaS and IaaS are prominently featured in the literature, the absence of standalone PaaS usage suggests a potential gap in its application for risk assessment purposes. Further exploration of PaaS capabilities and integration with other service models may offer valuable insights into enhancing cloud security practices. Overall, the distribution of service delivery model usage highlights the importance of considering various factors such as scalability, flexibility, and control in selecting the most suitable model for conducting Risk Assessment in cloud environments.

4.4 RQ_3 What types of validation are applied on the Risk Assessment in Cloud?

In the context of $\mathbf{RQ_3}$, we analyzed the validation approach adopted when evaluating security risk assessment techniques in cloud environments. In the analyzed literature there are two approaches to evaluate security risk: qualitative and quantitative. The first uses a relative or descriptive scale to measure the probability of occurrence and impact, while the second uses a numerical scale. The purpose of qualitative risk analysis is to identify the risk that needs detailed analysis and the necessary controls and actions based on the effect of the risk and the impact on objectives. The main goal when using qualitative assessments is to quickly identify risks. This analysis can be used as an initial assessment to recognize risk. Qualitative assessments generally use numerical ratings (1-5) or colors (green, yellow, and red) to classify risks based on their probability of occurrence and impact, and are often represented by a risk matrix. This approach is used in events where it is difficult to express numerical measures of risk. This is, for example, the occurrence without adequate information and numerical data. Instead, a quantitative risk analysis is a high-priority and/or high-impact risk analysis, where a numerical rating is assigned to develop a probabilistic assessment of business-related issues. To conduct quantitative analyses, the Common Vulnerability Scoring System (CVSS) is often referred to, and is a method used to provide a qualitative measure of severity.

Overall, 17 of 21 articles (81%) describe how they validate their approach. The remaining 5 articles either do not apply any analysis or do not specify it explicitly. Half of the articles apply the quantitative analysis [A2, A5, A10, A12, A15, A17], and the other half use the qualitative analysis [A4, A8, A9, A13, A16, A19]. Some articles use two validation techniques [A6, A7, A18, A20, A21], as illustrated in Table 4. The combination of qualitative and quantitative analysis can affect the systematic and hierarchical nature of the evaluation.

4.5 RQ_4 What types of evaluation approach are applied to conduct Risk Assessment in Cloud?

Investigating evaluation approaches is crucial for understanding the focal points of Risk Assessment in cloud projects. Our initial focus was identifying the evaluation approaches applied in the papers under review. Utilizing an iterative content analysis approach, we labeled the analyzed papers in *Assets Specific Risk* or *Stakeholder Specific Risk*. Upon conducting a more comprehensive analysis, we discovered that only 62% of the papers explicitly mentioned evaluation approaches. This finding underscores the need for greater emphasis on delineating evaluation methodologies in cloud risk assessment research, facilitating a more comprehensive understanding and comparison of assessment strategies and outcomes. More specifically, our analysis revealed that 46% of the reviewed papers discuss utilizing Assets and Stakeholders as assessment approaches, with the latter being deemed significant for the risk analysis phase [A1, A2, A4, A17, A20, A21]. However, most papers, comprising 54%, concentrate solely on assets as an assessment approach [A6, A9, A13–A16, A18]. All results are summarized in

the Table 4. This finding suggests a nuanced approach to risk assessment in cloud projects, where consideration of both assets and stakeholders can enhance the comprehensiveness and effectiveness of risk analysis. The prevalence of asset approaches underscores the importance of recognizing and prioritizing asset-related risks in cloud environments. In conclusion, the distribution of assessment approaches underscores the need for a balanced and multifaceted perspective in cloud risk assessment, incorporating asset-based and stakeholder-oriented considerations to mitigate risks effectively.

4.6 RQ_5 What are the limitations of the actual application of Risk Assessment in Cloud?

Upon thoroughly examining the existing literature concerning risk assessment within cloud systems, to assess our RQ_5 our attention has shifted towards identifying the inherent limitations within the proposed methodologies. We aim to gain insight into the prevailing gaps within this domain. The main limitations have been divided into three categories (1) inaccurate estimation, (2) causes of risks, and (3) approaches applied.

Inaccurate Estimation. The primary limitations identified in the reviewed literature are inaccurate risk probability or impact estimation. For instance, in work of Basu et al. [A2], a methodology is proposed to enhance the accuracy of risk calculation by using information such as the provider's cloud security capabilities. However, this methodology lacks testing and validation. In their study, Saripalli and Walters [A17] introduced the QUIRC approach, where the computation of the risk contributed by a particular threat is treated superficially. There is no concrete mechanism for explicitly computing the risk of each threat. Using this approach can result in inaccurate risk quantification. In addition, Nhlabatsi et al. [A15] focused on a weighted approach for risk estimation and mitigation, but defining specific weights proves challenging as they must be calibrated according to client requirements. Finally, we encountered the work of Jelacic et al. [A8], which presented a case study on cloud-based Risk Assessment within systems for smart grid Operational Technology (OT) services. However, the assessment matrix generated in this study lacked measurement metrics such as cost. Furthermore, it failed to account for the dynamic nature of sources and threats contributing to risk estimation, which often evolves. The literature review on risk assessment in cloud computing reveals limitations in calculating risk likelihood or impact estimation, underscoring the need for improved methodologies in this domain.

Causes of Risks. Another much-discussed issue in risk assessment is related to identifying risks and, in particular, their causes. In the analyzed studies, we find the work of Jiang et al. [A9], who points out that with the implementation and promotion of cloud services, many new risk factors may appear and that they should be investigated. Next, Khan et al. [A16] pointed out that it is necessary to conduct a detailed analysis of threats that are difficult to detect using specific events or have a cause-and-effect relationship with other threats. Finally, Albakri et al. [A1] study points out that many approaches consider only specific assets to conduct a risk assessment, neglecting project stakeholders, which may be causes of risks and, therefore, should be considered. In conclusion, it is paramount to prioritize investigating the emergence of novel risk factors in cloud services, conducting thorough analyses of intricate threats, and acknowledging project stakeholders as potential sources of risk. By doing so, we can attain a more comprehensive understanding of risks and enhance our risk management strategies effectively.

Approaches Applied. Among the limitations in some of the literature are the application and approaches used for risk assessment. We see an example from the interviews conducted in Faizi et al. [A4], discussing how Information Security Risk Assessment (ISRA) is applied in organizations. In particular, the practitioners believe there is a need to have one standardized approach, but at the same time, it must be simple to apply, whereas the current approaches used in the cloud context are complex. In addition, Sen and Madria [A18] evidence in the limitations of their work that very often in the requirements phase, many security requirements for cloud systems are identified as high-level; there are no guidelines related to the distribution of resources to address the possible risks that go into impacting those security requirements. Investigating the study of standards for conducting risk assessment in cloud systems is important to promote consistency, reliability, and effectiveness in different areas, ensuring sound risk management practices and informed decision-making.

» Key Results

We have derived results to address our research questions from the analysis of the data extracted from the considered papers. These findings are summarized in **Table 4**. For RQ_5, we categorized the identified limitations into three main categories: *Inaccurate estimation, causes of risks,* and *applied approaches*. This categorization provides a structured framework for understanding the challenges associated with current risk assessment practices in the cloud.

5 DISCUSSION AND LIMITATION

This section addresses the implications and potential threats to the validity of the study.

5.1 Threats to Validity

Descriptive validity pertains to the accuracy and objectivity in depicting observations. To mitigate this threat, a data extraction module was developed and carefully designed that reports data logging during the data extraction phase. We evaluated it in a pilot project with all evaluators and revised it to correct any problems that emerged. We further evaluated the information provided in the form in a post-recovery meeting, as suggested in [24].

Theoretical validity can impact the selection of the scientific database, as the chosen database might overlook pertinent research. We opted for Scopus due to its expansive coverage, including papers from various publishers. The reliability of the conclusions could be compromised by potential biases among researchers engaged in the mapping process. To address this concern, we extensively utilized piloting and consensus meetings.

Interpretive validity to the data elaborates on the researcher's bias, which consequently impacts the validity of the conclusions.

Table 4: Results of Data Extraction for RQ_1, RQ_2, RQ_3 e RQ_4

Paper	Standard (RQ_1)	Delivery Models (RQ_2)	Validation (RQ_3)	Evaluation Approach (RQ_4)
Security risk assessment-based cloud migration methodology for smart grid OT services [A8]	FIPS and IEC-62443		Qualitative	
Application design phase risk assessment framework using cloud security domains [A18]			Qualitative , quantitative	Asset Specific Risks
From rationale to lessons learned in the cloud information security risk assessment: a study of organizations in Sweden [A4]	ISO/IEC 27005, ISO/IEC 31000		Qualitative	Asset and Stakeholder Specific Risks
Security risk assessment within hybrid data centers: A case study of delay sensitive applications [A13]	ISO/IEC 27001, ISO/IEC 27005, NIST		Qualitative	Asset Specific Risks
CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure [A20]	NIST	IaaS	Qualitative , quantitative	Asset and Stakeholder Specific Risks
An assessment model for cloud service security risk based on entropy and support vector machine [A9]		Iaas, SaaS, Paas	Qualitative	Asset Specific Risks
A research for cloud computing security risk assessment [A19]	GB/T 20984-2007		Qualitative	
Data risks in the cloud [A3]		SaaS		
Security risk assessment framework for cloud computing environments [A1]	NIST SP 800-30, ISO/IEC 27000-27005, AS/NZS 4360	SaaS		Asset and Stakeholder Specific Risks
ARA-Assessor: Application-aware runtime risk assessment for cloud-based business continuity [A5]		IaaS	Quantitative	
Design and Implementation of a Threat-Specific Security Risk Assessment Tool [A16]	NIST			
A quantitative methodology for cloud security risk assessment [A2]	ISO/IEC 27005, ISO/IEC 17789	IaaS, SaaS	Quantitative	Asset and Stakeholder Specific Risks
Security Risk Optimization for Multi-cloud Applications [A12]				
SpiralSRA: A threat-specific security risk assessment framework for the cloud [A14]	NIST	SaaS	Quantitative	Asset Specific Risks
A security risk management model for cloud computing systems: Infrastructure as a service [A10]	ISO/IEC 27005, NIST 800-30	IaaS	Quantitative	
Security risks and their management in cloud computing [A16]	ISO 27001	IaaS	Qualitative	Asset Specific Risks
QUIRC: A quantitative impact and risk assessment framework for cloud security [A17]	FIPS		Quantitative	Asset and Stakeholder Specific Risks
A security risk assessment model for business process deployment in the cloud [A6]	ISO 27017	Iaas, SaaS, Paas	Qualitative, quantitative	Asset Specific Risks
Threat-specific security risk evaluation in the cloud [A15]	NIST	SaaS	Quantitative	Asset Specific Risks
Security Evaluation Method of Smart Home Cloud Platform [A21]	OWASP	SaaS	Qualitative, quantitative	Asset and Stakeholder Specific Risks
Security Risk-Aware Resource Provisioning Scheme for Cloud Computing Infrastructures [A7]		IaaS	Qualitative, quantitative	

Experienced researchers were actively engaged in the process to mitigate this potential threat.

Repeatability is supported by adopting existing guidelines, such as the ones proposed by Kitchenham et al. [17] and Petersen et al. [24]. To ensure result's repeatability, we provide a detailed description of the process, including the actions taken to reduce possible threats to validity. All data collected during our study is publicly available in the replication package accompanying this paper.

5.2 Discussion

The findings of our study have shown several observations that warrant further investigation. They delineate open challenges for researchers engaged or interested in developing methodologies and practices for the adoption of risk assessment in the Cloud.

The results show that the **PaaS** delivery model is never applied alone in the context of risk assessment in the Cloud. This suggests that organizations prefer integrating PaaS with other delivery models, such as *IaaS* and *SaaS*, rather than use only PaaS for risk assessment activities. Different factors can lead to the use of combined delivery models, such as the need for a more comprehensive approach, including both infrastructure and application layers, and the desire for greater flexibility and customization of risk assessment processes. Future research could deepen the reasons for this trend and explore potential implications for improving risk assessment strategies in the Cloud.

One of the primary activities within risk assessment involves identifying and evaluating potential risks. During the data extraction phase of our study, an interesting observation emerged: the sources of identified risks often varied significantly based on the specific application context. Some studies identified risks based on vulnerabilities or threats under analysis, while others relied on established lists or standards in existing literature. Moreover, some works focused on risks associated solely with the migration phase, ignoring other critical risk categories. This fragmented approach to risk identification can result in incomplete or inadequate risk assessments. To address this issue, it is imperative to investigate all potential causes, vulnerabilities, and threats comprehensively. Developing a unified framework encompassing a comprehensive list of possible risks would greatly assist organizations in effectively identifying and managing risks associated with cloud computing. Such a framework would be a valuable tool for organizations, providing them with a structured approach to risk assessment and enhancing their ability to safeguard their cloud environments effectively.

6 CONLUSIONS AND FUTURE WORK

In this systematic mapping study, our objective was to offer a thorough overview of the present state of investigation concerning security risk assessment within a cloud environment. We analyzed 21 studies and extracted essential information to clarify the current state of the literature on risk assessment in the cloud. Our main contributions include (i) a comprehensive synthesis and examination of research endeavors in cloud-based risk assessment, serving as a valuable resource for both researchers and practitioners seeking insights into the evolution and enhancement of risk assessment methodologies for security testing; (ii) identifying gaps in current research, thus emphasizing crucial avenues for future investigations; (iii) providing an online appendix detailing all materials utilized in our systematic mapping study, facilitating further research expansion and the augmentation of our findings.

In the cloud field, further research must be carried out on risk assessment to guarantee the security of these systems, improving the methodologies for calculating the risk probability and estimating the impact; conducting complex threat analyses, considering all project assets and stakeholders as potential sources of risk; ensure sound risk management practices by applying standards to promote consistency, reliability and effectiveness.

In the future, we intend to develop a framework for security risk assessment in cloud environments that complies with industry standards based on the organization's objectives for different cloud delivery and related validation. We also plan to delve into risk-based security testing for cloud environments.

ACKNOWLEDGMENT

This work has been partially supported by the EMELIOT national research project, which has been funded by the MUR under the PRIN 2020 program (2020W3A5FY). This work was partially supported by the SERICS project (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

REFERENCES

[1] ISO/IEC 27017:2015. 2021. *Code of practice for information security controls based on ISO/IEC 27002 for cloud services.* https://www.iso.org/standard/82878.html

[2] ISO/IEC/IEEE 29119. 2021. *Risk-based approach for testing.* https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:29119:-2:ed-2:v1:en
[3] NIST SP 800-144. 2011. *Guidelines on Security and Privacy in Public Cloud Computing.* https://csrc.nist.gov/pubs/sp/800/144/final
[4] Asish Aich and Alo Sen. 2015. Study on cloud security risk and remedy. *Int. J. Grid Distrib. Comput* 8, 2 (2015), 155–166.
[5] Nauman Bin Ali and Kai Petersen. 2014. Evaluating strategies for study selection in systematic literature studies. In *Proceedings of the 8th ACM/IEEE international symposium on empirical software engineering and measurement.* 1–4.
[6] Cloud Security Alliance. 2022. *Cloud Security Alliance's Top Threats to Cloud Computing.* https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning
[7] Ahmad Amini and Norziana Jamil. 2018. A comprehensive review of existing risk assessment models in cloud computing. In *Journal of Physics: Conference Series*, Vol. 1018. IOP Publishing, 012004.
[8] Giusy Annunziata, Alexandra Sheykina, Fabio Palomba, Gemma Catolino, Andrea De Lucia, and Filomena Ferrucci. 2024. Online Appendix — Security Risk Assessment on Cloud: A Systematic Mapping Study. https://figshare.com/s/8c8c3af5213182a94334
[9] CheckPoint. 2022. *Top Trends in Cloud Security.* https://pages.checkpoint.com/2022-cloud-security-report.html
[10] Prachi Deshpande, Subhash Chander Sharma, Sateesh K Peddoju, and Ajith Abraham. 2018. Security and service assurance issues in Cloud environment. *International Journal of System Assurance Engineering and Management* 9 (2018).
[11] Prachi S Deshpande, Subhash C Sharma, and Sateesh K Peddoju. 2019. *Security and Data Storage Aspect in Cloud Computing*. Vol. 52. Springer.
[12] Gartner. 2023. *Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach $679 Billion in 2024.* https://www.collinsdictionary.com/dictionary/english/language
[13] Jürgen Großmann, Martin Schneider, Johannes Viehmann, and Marc-Florian Wendland. 2014. Combining risk analysis and security testing. In *International Symposium On Leveraging Applications of Formal Methods, Verification and Validation*. Springer, 322–336.
[14] Jürgen Großmann and Fredrik Seehusen. 2015. Combining security risk assessment and security testing based on standards. In *Risk Assessment and Risk-Driven Testing: Third International Workshop, RISK 2015, Berlin, Germany, June 15, 2015. Revised Selected Papers 3*. Springer, 18–33.
[15] Dell'Oro Group. 2023. *Enterprises Can't Get Enough SSE as Revenue Rockets 38 Percent in 2022, According to Dell'Oro Group.* https://www.delloro.com/news/enterprises-cant-get-enough-sse-as-revenue-rockets-38-percent-in-2022/#:~:text=âĂŞ%20March%2015%2C%202023%20âĂŞ%20According,representing%2038%20percent%20growth%20as
[16] Afnan Ullah Khan, Manuel Oriol, Mariam Kiran, Ming Jiang, and Karim Djemame. 2012. Security risks and their management in cloud computing. In *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*. Ieee, 121–128.
[17] Barbara Kitchenham, Stuart Charters, et al. 2007. Guidelines for performing systematic literature reviews in software engineering.
[18] Rabia Latif, Haider Abbas, Saïd Assar, and Qasim Ali. 2014. Cloud computing risk assessment: a systematic literature review. *Future Information Technology: FutureTech 2013* (2014), 285–295.
[19] W. Lidwell, K. Holden, and J. Butler. 2010. *Universal principles of design, revised and updated: 125 ways to enhance usability, influence perception, increase appeal, make better design decisions, and teach through design.* Rockport Pub.
[20] NIST. [n. d.]. *General Access Control Guidance for Cloud Systems: NIST Publishes SP 800-210.* https://csrc.nist.rip/News/2020/nist-publishes-sp-800-210-ac-guidance-for-cloud
[21] NIST. 2011. *The NIST Definition of Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
[22] NIST. 2020. *General Access Control Guidance for Cloud Systems.* https://csrc.nist.rip/publications/detail/sp/800-210/final
[23] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. 2008. Systematic mapping studies in software engineering. In *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12*. 1–10.
[24] Kai Petersen, Sairam Vakkalanka, and Ludwik Kuzniarz. 2015. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and software technology* 64 (2015), 1–18.
[25] Fredrik Seehusen. 2015. Using CAPEC for Risk-Based Security Testing. In *Risk Assessment and Risk-Driven Testing: Third International Workshop, RISK 2015, Berlin, Germany, June 15, 2015. Revised Selected Papers 3*. Springer, 77–92.
[26] Johannes Viehmann and Frank Werner. 2015. Risk assessment and security testing of large scale networked systems with RACOMAT. In *Risk Assessment and Risk-Driven Testing: Third International Workshop, RISK 2015, Berlin, Germany, June 15, 2015. Revised Selected Papers 3*. Springer, 3–17.
[27] Philipp Zech. 2011. Risk-based security testing in cloud computing environments. In *2011 Fourth IEEE International Conference on Software Testing, Verification and Validation*. IEEE, 411–414.

APPENDIX

[A1] Sameer Hasan Albakri, Bharanidharan Shanmugam, Ganthan Narayana Samy, Norbik Bashah Idris, and Azuan Ahmed. 2014. Security risk assessment framework for cloud computing environments. *Security and Communication Networks* 7 (2014), 2114–2124.
[A2] Srijita Basu, Anirban Sengupta, and Chandan Mazumdar. 2017. A quantitative methodology for cloud security risk assessment. In *International Conference on Cloud Computing and Services Science*, Vol. 2. SCITEPRESS, 120–131.
[A3] Roger Clarke. 2013. Data risks in the cloud. *Journal of theoretical and applied electronic commerce research* 8, 3 (2013), 59–73.
[A4] Ana Faizi, Ali Padyab, and Andreas Naess. 2022. From rationale to lessons learned in the cloud information security risk assessment: a study of organizations in Sweden. *Information Computer Security* 30 (2022), 190–205.
[A5] Min Fu, Shiping Chen, Jian Yang, Surya Nepal, and Liming Zhu. 2017. ARA-Assessor: Application-Aware Runtime Risk Assessment for Cloud-Based Business Continuity. In *Service-Oriented Computing: 15th International Conference, ICSOC 2017, Malaga, Spain, November 13–16, 2017, Proceedings*. Springer, 511–527.
[A6] Elio Goettelmann, Karim Dahman, Benjamin Gateau, Eric Dubois, and Claude Godart. 2014. A security risk assessment model for business process deployment in the cloud. In *2014 IEEE international conference on services computing*. IEEE.
[A7] Talal Halabi and Martine Bellaiche. 2019. Security risk-aware resource provisioning scheme for cloud computing infrastructures. In *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 1–9.
[A8] Bojan Jelacic, Imre Lendak, Sebastijan Stoja, Marina Stanojevic, and Daniela Rosic. 2020. Security risk assessment-based cloud migration methodology for smart grid OT services. *Acta Polytechnica Hungarica* 17, 5 (2020), 113–134.
[A9] Rong Jiang, Zifei Ma, and Juan Yang. 2021. An assessment model for cloud service security risk based on entropy and support vector machine. *Concurrency and Computation: Practice and Experience* 33, 21 (2021), e6423.
[A10] Mouna Jouini and Latifa Ben Arfa Rabai. 2017. A security risk management model for cloud computing systems: infrastructure as a service. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 10th International Conference, SpaCCS 2017, Guangzhou, China, December 12-15, 2017, Proceedings 10*. Springer, 594–608.
[A16] Afnan Ullah Khan, Manuel Oriol, Mariam Kiran, Ming Jiang, and Karim Djemame. 2012. Security risks and their management in cloud computing. In *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*.
[A12] Rudolf Lovrenčić, Domagoj Jakobović, Dejan Škvorc, and Stjepan Groš. 2020. Security risk optimization for multi-cloud applications. In *Applications of Evolutionary Computation: 23rd European Conference, EvoApplications 2020, Held as Part of EvoStar 2020, Seville, Spain, April 15–17, 2020, Proceedings 23*. Springer.
[A13] Fortune Munodawafa and Ali Ismail Awad. 2018. Security risk assessment within hybrid data centers: A case study of delay sensitive applications. *Journal of information security and applications* 43 (2018), 61–72.
[A14] Armstrong Nhlabatsi, Jin B Hong, Dong Seong Kim, Rachael Fernandez, Noora Fetais, and Khaled M Khan. 2018. Spiralˆ SRA: a threat-specific security risk assessment framework for the cloud. In *2018 IEEE International Conference on Software Quality, Reliability and Security (QRS)*. IEEE, 367–374.
[A15] Armstrong Nhlabatsi, Jin B Hong, Dong Seong Kim, Rachael Fernandez, Alaa Hussein, Noora Fetais, and Khaled M Khan. 2018. Threat-specific security risk evaluation in the cloud. *IEEE Transactions on Cloud Computing* 9, 2 (2018).
[A16] Armstrong Nhlabatsi, Alaa Hussein, Noora Fetais, and Khaled M Khan. 2020. Design and Implementation of a Threat-Specific Security Risk Assessment Tool. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 511–518.
[A17] Prasad Saripalli and Ben Walters. 2010. Quirc: A quantitative impact and risk assessment framework for cloud security. In *2010 IEEE 3rd international conference on cloud computing*. Ieee, 280–288.
[A18] Amartya Sen and Sanjay Madria. 2020. Application design phase risk assessment framework using cloud security domains. *Journal of Information Security and Applications* 55 (2020), 102617.
[A19] Hua Tang, Jiejun Yang, Xiaofang Wang, and Qi Zhou. 2016. A research for cloud computing security risk assessment. *The Open Cybernetics & Systemics Journal* 10, 1 (2016).
[A20] Kennedy A Torkura, Muhammad IH Sukmana, Feng Cheng, and Christoph Meinel. 2020. Cloudstrike: Chaos engineering for security and resiliency in cloud infrastructure. *IEEE Access* 8 (2020), 123044–123060.
[A21] Chensi Wu, Lulin Yang, Maobin Cai, Xiaoying Zhao, and Qifeng Sun. 2023. Security Evaluation Method of Smart Home Cloud Platform. *International Journal of Pattern Recognition and Artificial Intelligence* 37, 06 (2023), 2351012.